Dell Secured Component Verification Version 1.5,1.5.1,1.6,1.7,1.8, 1.9, 1.91.0 und 1.92.0

Referenzhandbuch für Server und Gehäuse

März 2024
Rev. A07

DELL Technologies

Hinweise, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

WARNUNG: Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

© 2024 Dell Inc. oder deren Tochtergesellschaften. Alle Rechte vorbehalten. Dell Technologies, Dell und andere Marken sind Marken von Dell Inc. oder ihren Tochtergesellschaften. Andere Marken können Marken ihrer jeweiligen Inhaber sein.

Inhaltsverzeichnis

Kapitel 1: Übersicht 5
Neue Funktionen hinzugefügt 5
SCV 1.92.0 5
SCV 1.91.0 5
SCV 1.9 5
SCV 1,8 5
SCV 1.7 6
SCV 1.6 6
SCV 1.5.1 6
SCV 1.5 6
Secured Component Verification 6
Systemanforderungen 7
Unterstützte Komponenten 7
Unterstützte URIs 8

Kapitel 2: Secured Component Verification auf WinPE 9
Erstellen eines ISO-Images zum Ausführen von SCV mit WinPE 9
Hinzufügen von SCV zu einem benutzerdefinierten ISO-Image 10
Ausführen von SCV auf WinPE 10
Überprüfen der SCV-Protokolle mit WinPE 13

Kapitel 3: Secured Component Verification auf Linux 14
Ausführen von SCV auf Linux 14
Überprüfen der SCV-Protokolle mit Linux 17

Kapitel 4: Secured Component Verification auf Windows Server 2019 und 2022 18
Installieren von SCVApp auf Windows Server 2019 und 2022 18
Ausführen von SCV auf Windows Server 2019 und 2022 21

Kapitel 5: Remoteausführung von Secured Component Verification (SCV) 26
Remoteausführung von SCV auf Windows Server 2019 und 2022 26
Remoteausführung von SCV auf WinPE 26
Remoteausführung von SCV auf Linux 27

Kapitel 6: SCV-Befehlsdetails 28
Abrufen von Informationen zum Ausführen von SCV 28
Abrufen von Informationen über den Befehl scv validatesysteminventory 28
Remoteverbindung zu einer Managementkonsole und Validierung von Beständen 29
Remoteverbindung zu einer Managementkonsole mit einem bestimmten Port und Bestandsvalidierung 30
Übereinstimmung des Komponentenspeicherorts gewährleisten und Bestandsvalidierung 30
SCV-Version abrufen 31
Anzeigen des Zertifikatkennungswerts in der Konsole oder Umleiten an eine Datei 31

Kapitel 7: SCVApp MARS-Funktion 33

Kapitel 8: SPDM-Funktion..... 35

Kapitel 9: Stamm-CA-Zertifikat für SCV..... 36

Kapitel 10: Rückgabecodes.....37

Kapitel 11: Wie Sie Hilfe bekommen.....38

Kontaktaufnahme mit Dell.....38

Support-Dokumente und -Ressourcen.....38

Feedback zur Dokumentation.....38

1

Übersicht

Dieser Abschnitt enthält eine Übersicht über Secured Component Verification (SCV) und die Systemanforderungen für die Ausführung der Anwendung auf dem System.

Themen:

- Neue Funktionen hinzugefügt
- Secured Component Verification
- Systemanforderungen
- Unterstützte Komponenten
- Unterstützte URIs

Neue Funktionen hinzugefügt

Dieser Abschnitt enthält eine Liste der neuen Funktionen, die in den folgenden Versionen hinzugefügt wurden:

- SCV 1.92.0
- SCV 1.91.0
- SCV 1.9
- SCV 1,8
- SCV 1.7
- SCV 1.6
- SCV 1.5.1
- SCV 1.5

SCV 1.92.0

Die folgenden Funktionen wurden in dieser Version hinzugefügt oder aktualisiert:

- Support für die Debug-Option für den`scv extractcert`-Befehl.

SCV 1.91.0

Die folgenden Funktionen wurden in dieser Version hinzugefügt oder aktualisiert:

- Unterstützung für MARS-Feature.
- SPDM-Support für NIC-Emulex-Karte und PERC 12 hinzugefügt

ANMERKUNG: Informationen für die Liste der unterstützten Systeme für diese Version finden Sie in den Versionshinweisen.

SCV 1.9

Folgende Funktionen wurden in dieser Version hinzugefügt oder aktualisiert:

- Unterstützung für neue PowerEdge-Server hinzugefügt.

  ANMERKUNG: Informationen für die Liste der unterstützten Systeme für diese Version finden Sie in den Versionshinweisen.

SCV 1,8

Folgende Funktionen wurden in dieser Version hinzugefügt oder aktualisiert:

- Unterstützung für neues Profil für Cloud-Plattformen, die keine Festplatten gemeinsam nutzen.

- Unterstützung für `extractcert` den Befehl.

SCV 1.7

Folgende Funktionen wurden in dieser Version hinzugefügt oder aktualisiert:
- Unterstützung für SLES 15 SP4.
- Unterstützung der PowerEdge-Server der 16. Generation.

SCV 1.6

Folgende Funktionen wurden in dieser Version hinzugefügt oder aktualisiert:
- Unterstützung für Red Hat Enterprise Linux 9.0.

SCV 1.5.1

Folgende Funktionen wurden in dieser Version hinzugefügt oder aktualisiert:
- Unterstützung für PowerEdge-Cloudserver.
- Unterstützung für modulare PowerEdge-Server und -Gehäuse (MX-Serie).

SCV 1.5

Folgende Funktionen wurden in dieser Version hinzugefügt oder aktualisiert:
- Unterstützung für SCVTools.
- Unterstützung für Red Hat Enterprise Linux 8.x.
- Unterstützung für SCVApp für Windows Server 2019 und 2022.

Secured Component Verification

Secured Component Verification (SCV) ist ein Überprüfungsangebot der Lieferkette, mit dem Sie überprüfen können, ob der PowerEdge-Server, den Sie erhalten haben, den Herstellungsspezifikationen im Werk entspricht. Zum Validieren von Komponenten wird während der Werkmontage ein Zertifikat erzeugt, das die eindeutigen Systemkomponenten-IDs enthält. Dieses Zertifikat wird im Dell Werk signiert und im System gespeichert, später wird es von der SCV-Anwendung verwendet. Die SCV-Anwendung validiert den Systembestand anhand des SCV-Zertifikats.

Die Anwendung erzeugt einen Validierungsbericht, in dem der Bestand als mit dem Zertifikat übereinstimmend oder nicht übereinstimmend aufgelistet wird. Außerdem werden das Zertifikat und die Vertrauenskette sowie der Eigentumsnachweis des privaten SCV-Schlüssels verifiziert. Die aktuelle Implementierung unterstützt direkt belieferte Kunden und beinhaltet keine VAR- oder Ersatzteilszenarien.

Die SCV-Anwendung führt die folgenden Funktionen aus:
- Lädt das im System über Dell Technologies APIs gespeicherte SCV-Zertifikat herunter und überprüft das SCV-Zertifikat und den Aussteller
- Überprüft den privaten SCV-Schlüssel, der im SCV-Zertifikat mit dem öffentlichen SCV-Schlüssel gekoppelt ist
- Erfasst den aktuellen Bestand des Systems.

  ANMERKUNG: Eine Liste der unterstützten Systemkomponenten finden Sie im Abschnitt Unterstützte Komponenten.
- Vergleicht den aktuellen Systembestand mit dem Bestand im SCV-Zertifikat.
- Eine Modifikation der im Zertifikat erfassten Komponenten wird als „Nichtübereinstimmung“ erkannt.

Hinweise:

- Die SCV-Anwendung kann direkt über die iDRAC-GUI-Version 7.10.30.00 und höher gestartet werden, es wird jedoch empfohlen, Ihre Komponenten mithilfe der Anwendung zu validieren, um eine optimale Sicherheitsvalidierung zu gewährleisten.
- SCV validiert auch die virtuellen Netzwerkports. Führen Sie bei Systemen mit NPAR/NPAReP-Karten die SCV-Anwendung vor der Aktivierung der Karten aus.
- Stellen Sie sicher, dass TPM aktiviert ist, bevor Sie die SCV-Anwendung ausführen. SCV unterstützt TPM-Version 2.0.
- Stellen Sie sicher, dass Sie die SCV-Anwendung ausführen, bevor Sie Storage-Geräte dem System zuordnen.
- Stellen Sie in modularen Systemen sicher, dass FlexAddress deaktiviert ist, bevor Sie die SCV-Anwendung ausführen.

- Wenn die internen und iDRAC-USB-Ports deaktiviert sind, schlägt die SCV-Validierung fehl.
- Stellen Sie sicher, dass jedes Laufwerk, das aus dem System entfernt wird, in iDRAC oder einer anderen iDRAC-Schnittstelle registriert wird, bevor Sie die SCV-Validierung durchführen. Andernfalls werden falsche Daten in der SCV-Ausgabe angezeigt.
- SCV erfordert USB-NIC-Kommunikation für die In-Band-Validierung. Deaktivieren Sie nicht die USB-NIC während der Ausführung des SCV-Vorgangs.
- In SCV 1.5 mit 1.0-Zertifikat wird einer der Einträge der TPM-Komponente (ECC) als „Übereinstimmung“ mit den erwarteten Details als „Unbekannt“ gemeldet, während die erkannten Details alle Informationen anzeigen. Dies ist ein erwartetes Verhalten, da das Zertifikat 1.0 keine ECC-Informationen enthält.

Systemanforderungen

Tabelle 1. Systemanforderungen für die Ausführung von SCV

Kategorie	Anforderung
Unterstützte Betriebssysteme	WinPE 10.x, Red Hat Enterprise Linux 9.0, Red Hat Enterprise Linux 8.6, Red Hat Enterprise Linux 7.x, SUSE Linux Enterprise Server 15 SP4, Windows Server 2019 und Windows Server 2022.
SCV Tools	SCV 1.5,1.5.1,1.6,1.7,1.8, 1.9,1.91.0 oder 1.92.0
Firmware-Versionen	• iDRAC 5.10.30.00 und höhere Versionen • OME-M 2.00.00 und höhere Versionen • PowerEdge BIOS 2.14.2 und höhere Versionen
Erforderliche Lizenzen	Secured Component Verification-Lizenz

ANMERKUNG: Informationen für die Liste der unterstützen Systeme für eine SCV-Version finden Sie im Abschnitt „Unterstützte Systeme“ in den Versionshinweisen.

ANMERKUNG: Red Hat Enterprise Linux 7.x wird von SCV 1.6 und höheren Versionen nicht unterstützt.

ANMERKUNG: In SCV Version 1.5 wird die TPM-Nichtübereinstimmung angezeigt, während Komponenten auf einem Server mit einer älteren iDRAC- und BIOS-Firmware validiert werden. Stellen Sie vor der Durchführung von SCV sicher, dass die iDRAC-Firmware auf Version 5.10.30.00 und die BIOS-Firmware auf Version 2.14.2 oder eine neuere Version aktualisiert wird.

Unterstützte Komponenten

Tabelle 2. Unterstützte Komponenten für Rack-, Tower- und Cloud-Plattformen

Unterstützte Komponenten für Rack-, Tower- und Cloud-Server
Baseboard
Prozessor
Arbeitsspeicher
Netzteil
Festplatte
Netzwerkkarte
iDRAC
TPM
Systeminformationen
PCIe-Add-on-Karten

Tabelle 3. Unterstützte Komponenten für modulare Gehäuse

Unterstützte Komponenten für modulare Gehäuse
Gehäuse-Controller
Lüfter
Open Manage Enterprise Modular
ChassisRCP
PowerSupply
IOModule
M2Drive

ANMERKUNG: Direkt angeschlossene NVMe-PCIe-SSDs werden nicht im PCIe-Steckplatz angezeigt. Überprüfen Sie die HDD-Liste, um die PCIe-SSD zu erhalten.

ANMERKUNG: Wenn keine Geräte für eine Komponente vorhanden sind, zeigt der SCV-Bestand den Eintrag „Unbekannt“ an.

ANMERKUNG: Der SCV-Bestand zeigt nur Details für die Geräte einer Komponente an, die im System vorhanden sind.

Unterstützte URIs

SCV unterstützt API (Application Programming Interfaces) für den Zugriff auf Informationen über einen API-Client. Weitere Informationen zur Verwendung von APIs finden Sie im Redfish-API-Handbuch für iDRAC9 unter developer.dell.com. Im Folgenden sind die Liste der URIs und die unterstützten Methoden aufgeführt:

- **SCV-Zertifikate herunterladen**

```
GET: /dtapi/rest/v1/x509-certificates
```

Beispielantwort

```
        {
            "certificate": "<SCV_CERT_CONTENT>",
            "certificate_format": "PEM",
            "id": "scv_factory"
               }
```

- **SCV-Bestand herunterladen**

```
GET : /dtapi/rest/v1/scvs/0
```

Beispielantwort auf iDRAC

```
 {
    "description": "Dell Platform Certificate Profile for PowerEdge Servers",
    "hardware_inventory": [ <ARRAY OF COMPONENT DETAILS> ],
    "profile_version": "<Profile Version Number>",
    "profile_name": "PowerEdge"
 }
```

Beispielantwort auf MX-Systemen

```
 {
    "description": " Dell Platform Certificate Profile for PowerEdge Modular
Infrastructure",
    "hardware_inventory": [ <ARRAY OF COMPONENT DETAILS> ],
    "profile_version": "<Profile Version Number>",
    "profile_name": "PowerEdge MX"
 }
```

2

Secured Component Verification auf WinPE

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:
Themen:

- Erstellen eines ISO-Images zum Ausführen von SCV mit WinPE
- Hinzufügen von SCV zu einem benutzerdefinierten ISO-Image
- Ausführen von SCV auf WinPE
- Überprüfen der SCV-Protokolle mit WinPE

Erstellen eines ISO-Images zum Ausführen von SCV mit WinPE

So erstellen Sie ein ISO-Image, um SCV mit WinPE auszuführen:

1. Laden Sie die SCVTools von der Seite **Treiber und Downloads** unter https://www.dell.com/support herunter.
2. Stellen Sie sicher, dass Windows ADK und das Windows PE-Add-on für ADK im System für WinPE 10.x installiert sind. Um die Dateien herunterzuladen und zu installieren, gehen Sie zu https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install.
3. Führen Sie die selbstextrahierende Datei für die SCVTools aus und klicken Sie auf **Entpacken**, um die Dateien an den Standardspeicherort zu extrahieren.

   ANMERKUNG: Um die Dateien an einen bestimmten Speicherort zu extrahieren, klicken Sie auf **Durchsuchen** und wählen Sie den Ordner aus, in den die Dateien extrahiert werden sollen. Klicken Sie auf **OK** und dann auf **Entpacken**.
4. Starten Sie die Eingabeaufforderung und wechseln Sie in das Verzeichnis, in das die Dateien extrahiert wurden. Führen Sie die Batchdatei (WinPE10.x_driverinst.bat) mithilfe der Eingabeaufforderung aus, um ein startfähiges ISO-Image zu erstellen.

   ANMERKUNG: Bevor Sie die WinPE-Batchdatei ausführen, stellen Sie sicher, dass Sie den Patch von https://support.microsoft.com/en-us/help/5017380 hinzufügen. Um den Patch hinzuzufügen, laden Sie das neueste Servicing Stack Update (SSU) für das Betriebssystem mit dem neuesten kumulativen Update (LCU) unter den in der Batchdatei genannten Pfad herunter und benennen Sie die SSU-Datei in `ssu-19041.1704-x64.msu` und die LCU-Datei in `windows10.0-kb5018410-x64.msu` um.

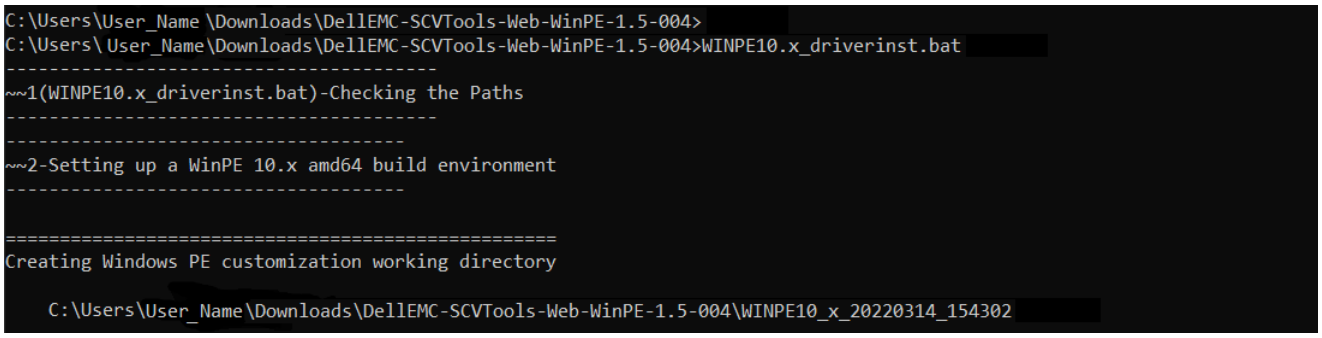


Abbildung 1. Ausführen der Batchdatei über die Eingabeaufforderung

5. Sobald das ISO-Image erfolgreich erstellt wurde, öffnen Sie den Ordner mit dem Namen „WINPE10.x-%timestamp%“, um das ISO-Image zu finden.

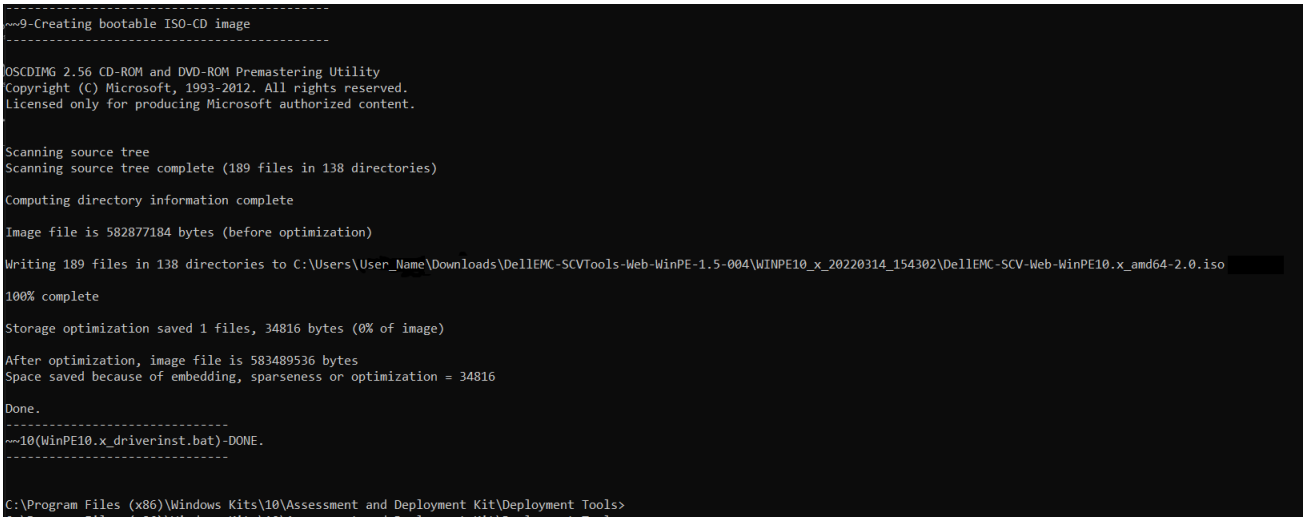


Abbildung 2. Bestätigung für das erfolgreich erstellte ISO-Image

6. Verwenden Sie dieses ISO-Image, um die SCV-Umgebung auf dem Server zu starten.

Hinzufügen von SCV zu einem benutzerdefinierten ISO-Image

So fügen Sie SCV zu einem benutzerdefinierten ISO-Image hinzu:

1. Laden Sie die SCVTools von der Seite **Treiber und Downloads** unter https://www.dell.com/support herunter.
2. Stellen Sie sicher, dass Windows ADK und das Windows PE-Add-on für ADK im System für WinPE 10.x installiert sind. Um die Dateien herunterzuladen und zu installieren, gehen Sie zu https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install.
3. Führen Sie die selbstextrahierende Datei für die SCVTools aus und klicken Sie auf **Entpacken**, um die Dateien an den Standardspeicherort zu extrahieren.

   ANMERKUNG: Um die Dateien an einen bestimmten Speicherort zu extrahieren, klicken Sie auf **Durchsuchen** und wählen Sie den Ordner aus, in den die Dateien extrahiert werden sollen. Klicken Sie auf **OK** und dann auf **Entpacken**.
4. Kopieren Sie die folgenden Ordner in den entsprechenden Ordnerpfad im benutzerdefinierten ISO-Image:
   a. **SCV** in `X:\Dell`
   b. **Toolkit\DLLs** in `X:\windows\system32`
5. Nachdem Sie die Dateien kopiert haben, legen Sie den Pfad für den Ordner mithilfe des Befehls `set PATH=%PATH%;X:\Dell\scv;` fest.
6. SCV kann jetzt zum Ausführen der Validierung verwendet werden.

Ausführen von SCV auf WinPE

1. Melden Sie sich bei iDRAC auf dem System an, auf dem Sie die SCV-Anwendung ausführen möchten.
2. Starten Sie die virtuelle Konsole und klicken Sie auf **Virtuelle Datenträger verbinden**.
3. Klicken Sie auf **Virtuelle Datenträger** und unter **CD/DVD zuordnen** auf **Durchsuchen** und wählen Sie das ISO-Image für SCV aus. Klicken Sie dann auf **Gerät zuordnen** und schließen Sie das Fenster.
4. Klicken Sie im Fenster der virtuellen Konsole auf **Start**, wählen Sie **Virtuelle CD/DVD/ISO** aus und klicken Sie auf **Ja** in der Eingabeaufforderung, um das neue Startgerät zu bestätigen.
5. Klicken Sie auf **Einschalten**, um das System einzuschalten und lassen Sie es über das ISO-Image starten.
6. Nachdem das System über das ISO-Image gestartet wurde, warten Sie, bis das Eingabeaufforderungsfenster im Verzeichnis `X:\Dell>` geladen wurde.
7. Navigieren Sie zu `X:\Dell\scv` und führen Sie den Befehl `scv validateSystemInventory` aus, um den Validierungsvorgang zu starten.

   ANMERKUNG: Stellen Sie beim Ausführen von SCV auf dem Host sicher, dass die USB-NIC-IP-Adresse in iDRAC auf die Standard-IP-Adresse eingestellt ist. Stellen Sie außerdem sicher, dass die ersten drei Oktette der IP-Adresse „169.254.1“ lauten.

ANMERKUNG: Nachdem Sie den Status „bereit“ in der Ausgabe von `racadm getremoteservicesstatus` erhalten haben, achten Sie darauf, etwa 120 Sekunden zu warten, bevor Sie die SCV-Befehle ausführen.

ANMERKUNG: Beim Ausführen des Befehls mit der Option `-d` wird möglicherweise der Fehler „Erfassen des Systembestands: fehlgeschlagen“ beim Ausführen von `scv validatesysteminventory` angezeigt, wenn die Länge des Verzeichnispfads 150 Zeichen überschreitet.

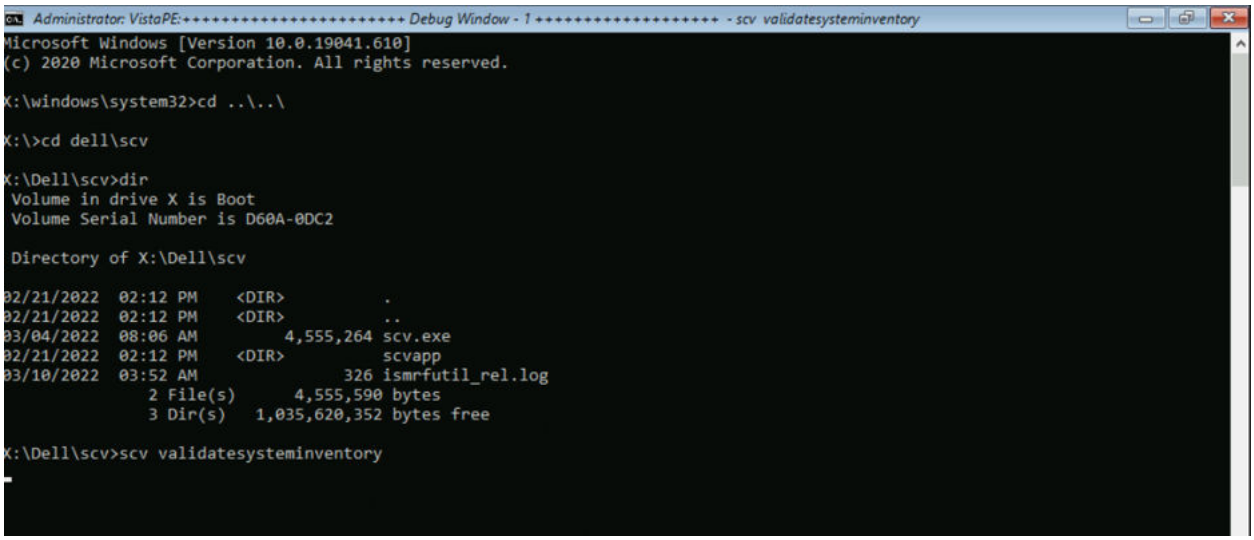


Abbildung 3. Ausführen des Validierungsbefehls

8. Nachdem das System die SCV-Anwendung erfolgreich ausgeführt hat, sollte das Ergebnis `Validating System Inventory: Match` angezeigt werden.

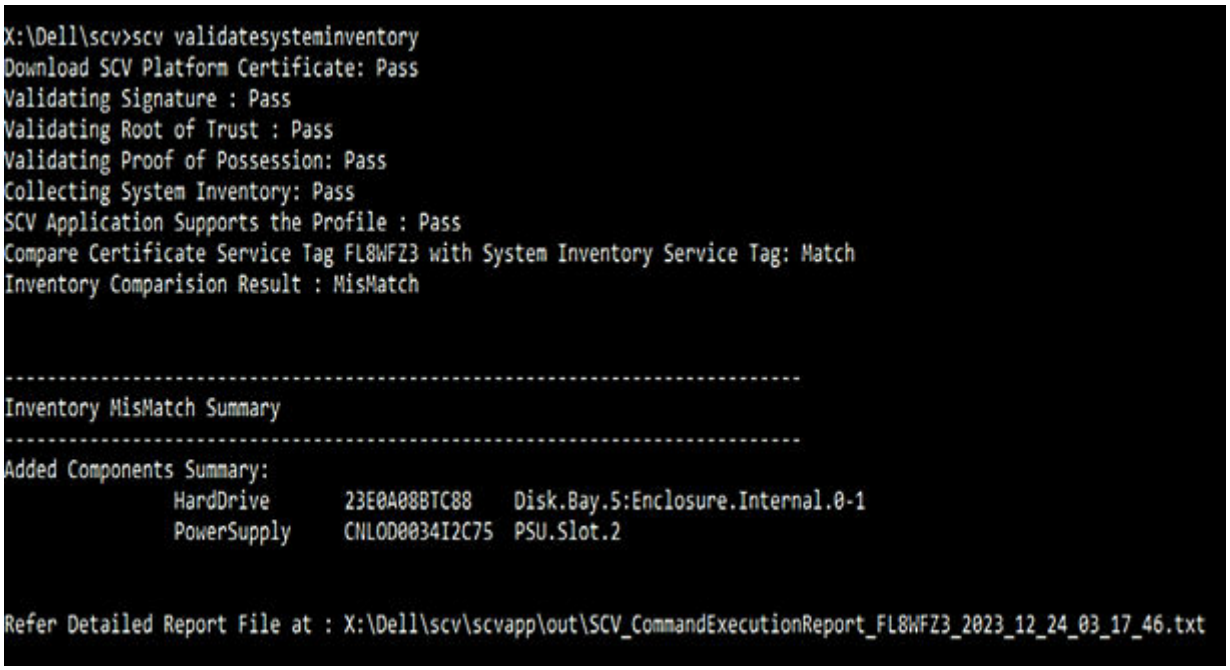


Abbildung 4. Ausführen des Validierungsbefehls mit erfolgreichem Ergebnis

9. Wenn das Ergebnis `Validating System Inventory: Mismatch` lautet, wird unter `Mismatch Inventory Summary` die Komponente angezeigt, die nicht übereinstimmt.

```
--------------------------------------------------------------------------------
System Information
--------------------------------------------------------------------------------
ServiceTag: <Service Tag>
HostIP: <IP address>
PlatformModel: PowerEdge R660
Manufacturer: Dell Inc.

--------------------------------------------------------------------------------
Command Information
--------------------------------------------------------------------------------
Command : ValidateSystemInventory
Execution Mode : Remote
Enforce Order : Not Enforced

--------------------------------------------------------------------------------
Command Execution Status
--------------------------------------------------------------------------------
Download SCV Platform Certificate : Success
Validate SCV Platform Certificate Signature : Success
Validate SCV Platform Certificate Root Of Trust : Success
Validate SCV Platform Certificate Proof Of Possion : Success
Collect System Inventory : Success
Validate System Inventory : Success
SCV Application Support For System Inventory Profile : Supported
Validate Profile Data between SCV Platform Certificate and System Inventory : Success
Compare SCV Platform Certificate Against System Inventory : Success

--------------------------------------------------------------------------------
Component Inventory Comparison Results
--------------------------------------------------------------------------------
Service Tag Comparison Result : Match
Subject Alternate Name Comparison Result : Match
Inventory Comparison Result : MisMatch
OverAll Comparison Result : MisMatch

--------------------------------------------------------------------------------
Inventory MisMatch Summary
--------------------------------------------------------------------------------
Added Components Summary:
                HardDrive       23E0A08BTC88    Disk.Bay.5:Enclosure.Internal.0-1
                PowerSupply     CNLOD0034I2C75  PSU.Slot.2


--------------------------------------------------------------------------------
Added Components
--------------------------------------------------------------------------------
{
    "HardDrive": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.5:Enclosure.Internal.0-1",
            "Manufacturer": "KIOXIA Corporation",
            "Model": "Unknown",
            "SerialNumber": "23E0A08BTC88"
        }
    ],
    "PowerSupply": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x000A0002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "A02",
            "Location": "PSU.Slot.2",
            "Manufacturer": "DELL",
            "Model": "PWR SPLY,1100W,RDNT,LTON",
            "SerialNumber": "CNLOD0034I2C75"
        }
    ]
}
--------------------------------------------------------------------------------
Matched Components
--------------------------------------------------------------------------------
{
    "Baseboard": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00030003",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "A01",
            "Location": "1",
            "Manufacturer": "Dell Inc.",
            "Model": "0NPR40",
            "SerialNumber": "CNIVC0036M0426"
        }
    ],
    "HardDrive": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.7:Enclosure.Internal.0-1",
            "Manufacturer": "KIOXIA Corporation ",
            "Model": "Unknown",
            "SerialNumber": "23E0A086TC88"
        },
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.3:Enclosure.Internal.0-1",
            "Manufacturer": "KIOXIA Corporation ",
            "Model": "Unknown",
            "SerialNumber": "23E0A08ETC88"
        },
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.5:Enclosure.Internal.0-1",
            "Manufacturer": "KIOXIA Corporation ",
            "Model": "Unknown",
            "SerialNumber": "23E0A08BTC88"
        },
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.2:Enclosure.Internal.0-1",
            "Manufacturer":
        }
```

Abbildung 5. Erwartete und erkannte Details für nicht übereinstimmende Komponente

Überprüfen der SCV-Protokolle mit WinPE

1. Nach der Ausführung von SCV in WinPE werden die erstellten Protokolle unter `X:\Dell\scv\scvapp\logs` gespeichert.
2. Um die Protokolle zu überprüfen, navigieren Sie zum Protokollordner und verwenden Sie den Befehl `notepad SCVLog_%service-tag%_%timestamp%.log`.

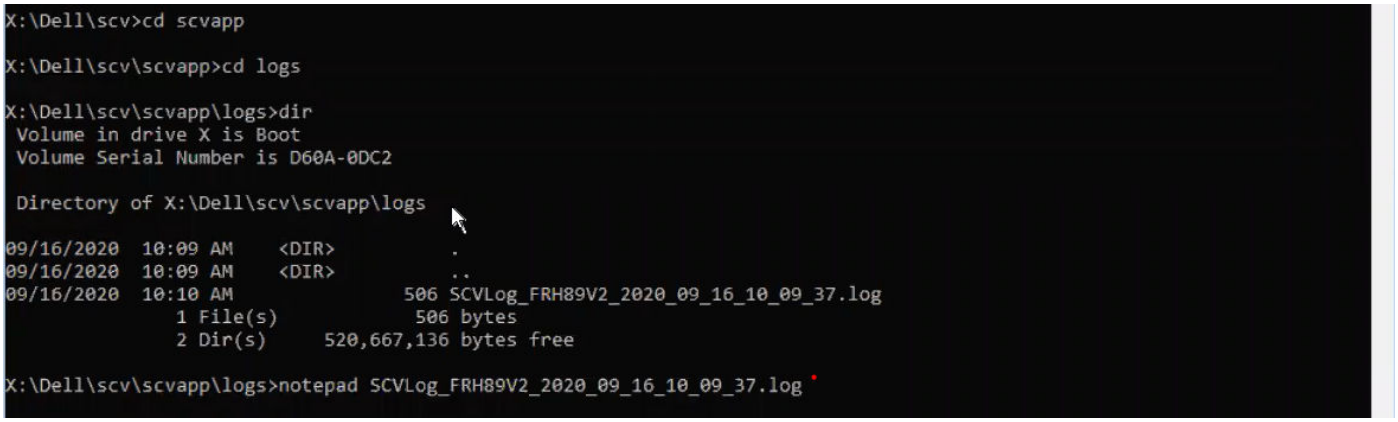


Abbildung 6. Überprüfen der Protokolle mit WinPE

3

Secured Component Verification auf Linux

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

Themen:

- Ausführen von SCV auf Linux
- Überprüfen der SCV-Protokolle mit Linux

Ausführen von SCV auf Linux

1. Laden Sie die SCVTools von der Seite Treiber und Downloads unter https://www.dell.com/support herunter.
2. Navigieren Sie im Terminal zu dem Verzeichnis, in das das SCV-Paket heruntergeladen wurde, und entpacken Sie die Datei mit dem Befehl `tar-zxvf DellEMC-SCV-Web-LX-X.X.X-XXXX_XXX.tar.gz`.

```
[root@auvcetillem1m1 Downloads]# tar -xvf DellEMC-SCV-Web-LX-2000-75.tar.gz
COPYRIGHT.txt
license.txt
SCVTools/
SCVTools/RPMS/
SCVTools/RPMS/supportRPMS/
SCVTools/RPMS/supportRPMS/srvadmin/
SCVTools/RPMS/supportRPMS/srvadmin/RHEL7/
SCVTools/RPMS/supportRPMS/srvadmin/RHEL7/x86_64/
SCVTools/RPMS/supportRPMS/srvadmin/RHEL7/x86_64/scv-2.0.0-136.el7.x86_64.rpm
SCVTools/RPMS/supportRPMS/srvadmin/RHEL8/
SCVTools/RPMS/supportRPMS/srvadmin/RHEL8/x86_64/
SCVTools/RPMS/supportRPMS/srvadmin/RHEL8/x86_64/scv-2.0.0-136.el8.x86_64.rpm
SCVTools/install_scv.sh
SCVTools/uninstall_scv.sh
SCVTools/readme.txt
```

Abbildung 7. Extrahieren der SCV-Tools unter Linux

3. Navigieren Sie zu dem Verzeichnis `SCVTools`, nachdem die Dateien extrahiert wurden, und führen Sie das Skript **install_scv. sh** mithilfe des Befehls `sh install_scv.sh` aus.

   ANMERKUNG: Zur Deinstallation von SCV können Sie den Befehl `sh uninstall_scv.sh` verwenden, um das Skript **uninstall_scv. sh** auszuführen.

```
[root@auvcetillem1m1 Downloads]# ls
COPYRIGHT.txt  DellEMC-SCV-Web-LX-2000-75.tar.gz  ismrfutil-el8-v0  license.txt  SCVTools
[root@auvcetillem1m1 Downloads]# cd SCVTools/
[root@auvcetillem1m1 SCVTools]# ls
install_scv.sh  readme.txt  RPMS  uninstall_scv.sh
[root@auvcetillem1m1 SCVTools]# sh uninstall_scv.sh
[root@auvcetillem1m1 SCVTools]# sh install_scv.sh
warning: scv-2.0.0-136.el8.x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID 34d8786f: NOKEY
Verifying...                          ################################# [100%]
Preparing...                          ################################# [100%]
Updating / installing...
   1:scv-2.0.0-136.el8                ################################# [100%]
[root@auvcetillem1m1 SCVTools]#
```

Abbildung 8. Ausführen des SCV-Installationsskripts

4. Führen Sie nach der Installation von SCV den Befehl `scv validateSystemInventory` aus, um den Validierungsvorgang zu starten.

   ANMERKUNG: Stellen Sie beim Ausführen von SCV auf dem Host sicher, dass die USB-NIC-IP-Adresse in iDRAC auf die Standard-IP-Adresse eingestellt ist. Stellen Sie außerdem sicher, dass die ersten drei Oktette der IP-Adresse „169.254.1“ lauten.

   ANMERKUNG: Verwenden Sie den Befehl `scv help`, um weitere Informationen über SCV und die Ausführung zu erhalten.

ANMERKUNG: Nachdem Sie den Status „bereit“ in der Ausgabe von `racadm getremoteservicesstatus` erhalten haben, achten Sie darauf, etwa 120 Sekunden zu warten, bevor Sie die SCV-Befehle ausführen.

5. Nachdem das System die SCV-Anwendung erfolgreich ausgeführt hat, sollte das Ergebnis `Validating System Inventory: Match` angezeigt werden.

```
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag CL04506 with System Inventory Service Tag: Match
Inventory Comparision Result : Match

Refer Detailed Report File at : ./scvapp/out/SCV_CommandExecutionReport_CL04506_2023_11_28_10_30_58.txt
```

Abbildung 9. Ausführen des Validierungsbefehls mit erfolgreichem Ergebnis

6. Wenn das Ergebnis `Validating System Inventory: Mismatch` lautet, wird unter `Mismatch Inventory Summary` die Komponente angezeigt, die nicht übereinstimmt.

```
--------------------------------------------------------------------------------
System Information
--------------------------------------------------------------------------------
ServiceTag: <Service Tag>
HostIP: <IP address>
PlatformModel: PowerEdge R660
Manufacturer: Dell Inc.

--------------------------------------------------------------------------------
Command Information
--------------------------------------------------------------------------------
Command : ValidateSystemInventory
Execution Mode : Remote
Enforce Order : Not Enforced

--------------------------------------------------------------------------------
Command Execution Status
--------------------------------------------------------------------------------
Download SCV Platform Certificate : Success
Validate SCV Platform Certificate Signature : Success
Validate SCV Platform Certificate Root Of Trust : Success
Validate SCV Platform Certificate Proof Of Possion : Success
Collect System Inventory : Success
Validate System Inventory : Success
SCV Application Support For System Inventory Profile : Supported
Validate Profile Data between SCV Platform Certificate and System Inventory : Success
Compare SCV Platform Certificate Against System Inventory : Success

--------------------------------------------------------------------------------
Component Inventory Comparison Results
--------------------------------------------------------------------------------
Service Tag Comparison Result : Match
Subject Alternate Name Comparison Result : Match
Inventory Comparison Result : MisMatch
OverAll Comparison Result : MisMatch

--------------------------------------------------------------------------------
Inventory MisMatch Summary
--------------------------------------------------------------------------------
Added Components Summary:
                HardDrive       23E0A08BTC88    Disk.Bay.5:Enclosure.Internal.0-1
                PowerSupply     CNLOD0034I2C75  PSU.Slot.2


--------------------------------------------------------------------------------
Added Components
--------------------------------------------------------------------------------
{
    "HardDrive": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.5:Enclosure.Internal.0-1",
            "Manufacturer": "KIOXIA Corporation",
            "Model": "Unknown",
            "SerialNumber": "23E0A08BTC88"
        }
    ],
    "PowerSupply": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x000A0002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "A02",
            "Location": "PSU.Slot.2",
            "Manufacturer": "DELL",
            "Model": "PWR SPLY,1100W,RDNT,LTON",
            "SerialNumber": "CNLOD0034I2C75"
        }
    ]
}
--------------------------------------------------------------------------------
Matched Components
--------------------------------------------------------------------------------
{
    "Baseboard": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00030003",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "A01",
            "Location": "1",
            "Manufacturer": "Dell Inc.",
            "Model": "0NPR40",
            "SerialNumber": "CNIVC0036M0426"
        }
    ],
    "HardDrive": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.7:Enclosure.Internal.0-1",
            "Manufacturer": "KIOXIA Corporation ",
            "Model": "Unknown",
            "SerialNumber": "23E0A086TC88"
        },
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.3:Enclosure.Internal.0-1",
            "Manufacturer": "KIOXIA Corporation ",
            "Model": "Unknown",
            "SerialNumber": "23E0A08ETC88"
        },
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.5:Enclosure.Internal.0-1",
            "Manufacturer": "KIOXIA Corporation ",
            "Model": "Unknown",
            "SerialNumber": "23E0A08BTC88"
        },
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.2:Enclosure.Internal.0-1",
            "Manufacturer": "KIOXIA
        }
```

Abbildung 10. Erwartete und erkannte Details für nicht übereinstimmende Komponente

Überprüfen der SCV-Protokolle mit Linux

1. Nach der Ausführung von SCV in Linux werden die erstellten Protokolle unter `scvapp\logs` gespeichert.
2. Um die Protokolle zu überprüfen, navigieren Sie zum Protokollordner und verwenden Sie den Befehl `vi SCVLog_%service-tag%_%timestamp%.log`.

```
[root@localhost scv]# vi ./scvapp/logs/SCVLog_RTSTC21_2020_09_15_05_55_28.log
```

Abbildung 11. Überprüfen der Protokolle in Linux

4

Secured Component Verification auf Windows Server 2019 und 2022

Dieser Abschnitt enthält Informationen zum Installieren und Ausführen von SCVApp:
Themen:

- Installieren von SCVApp auf Windows Server 2019 und 2022
- Ausführen von SCV auf Windows Server 2019 und 2022

Installieren von SCVApp auf Windows Server 2019 und 2022

So installieren Sie SCVApp auf Windows Server 2019 und 2022:

1. Laden Sie das SCV-Installationsprogramm von der Seite **Treiber und Downloads** unter https://www.dell.com/support herunter.
2. Extrahieren Sie das SCV-Installationsprogramm.

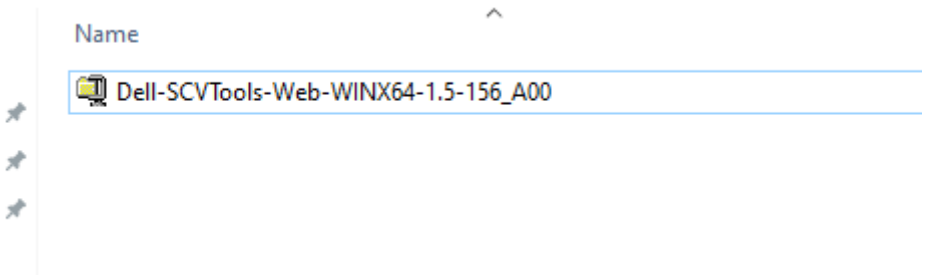


Abbildung 12. ZIP-Datei des SCV-Installationsprogramms

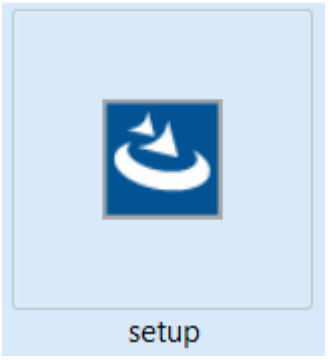


Abbildung 13. SCV-Installationsprogramm

3. Führen Sie die Anwendung aus, um den InstallShield-Assistenten zu starten.

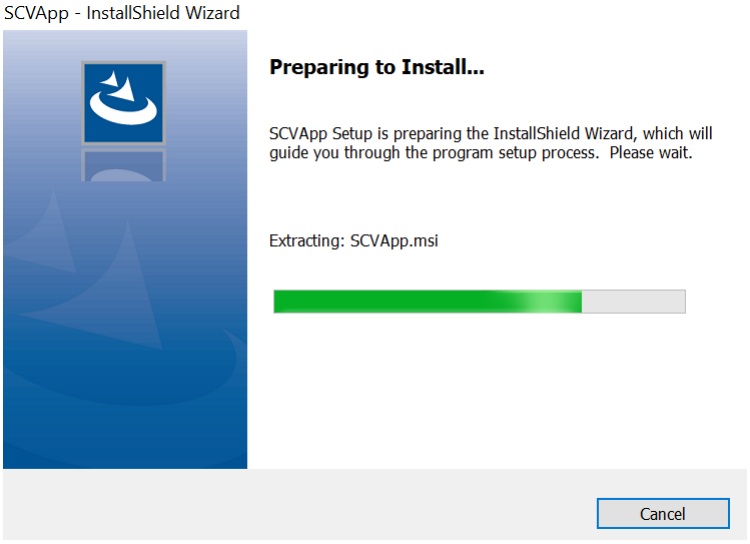


Abbildung 14. Ausführen des SCV-Installationsprogramms

4. Klicken Sie auf **Weiter**, um die Lizenzvereinbarung zu akzeptieren.

ANMERKUNG: Stellen Sie bei der Installation der SCV-Anwendung sicher, dass Sie den Speicherort der Installationsdatei im Installationsassistenten in „C:\ProgramFiles\Dell\SCVTools“ ändern.

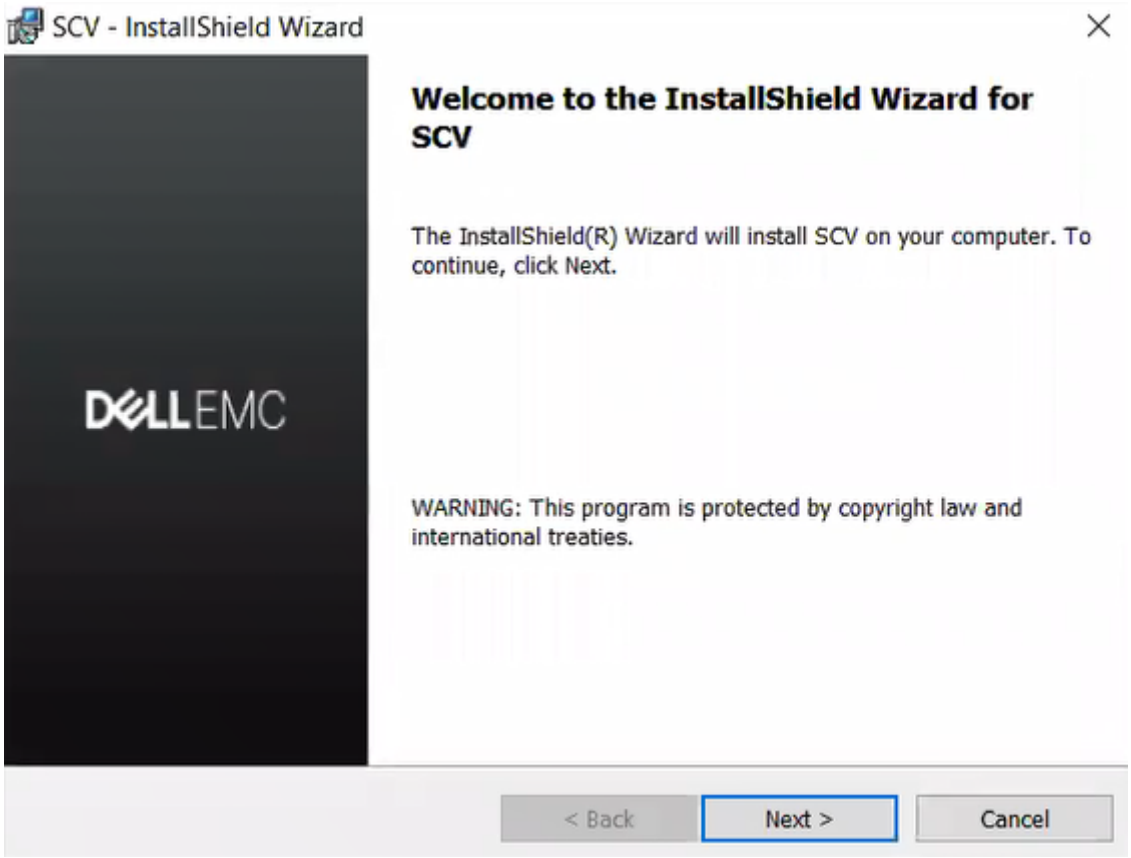


Abbildung 15. InstallShield-Assistent für SCVApp

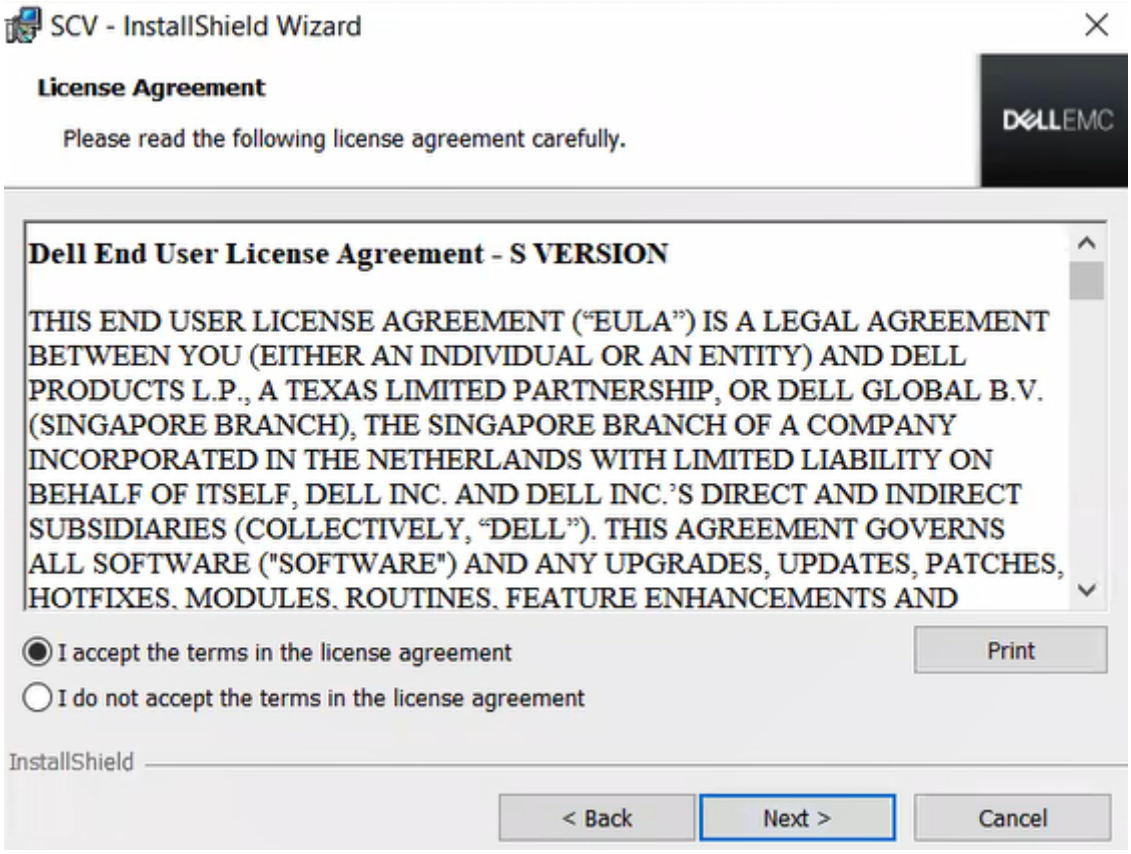


Abbildung 16. Lizenzvereinbarung für SCVApp

5. Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

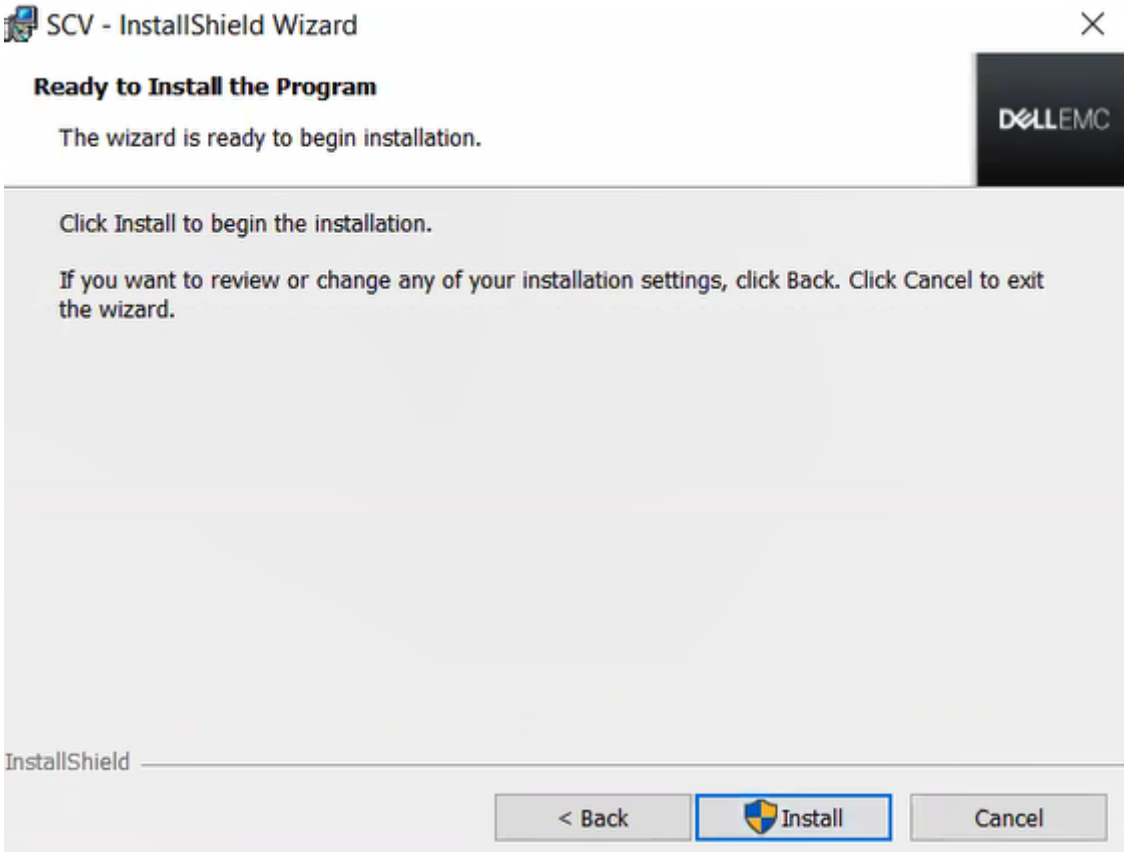


Abbildung 17. Bereit zur Installation von SCVApp

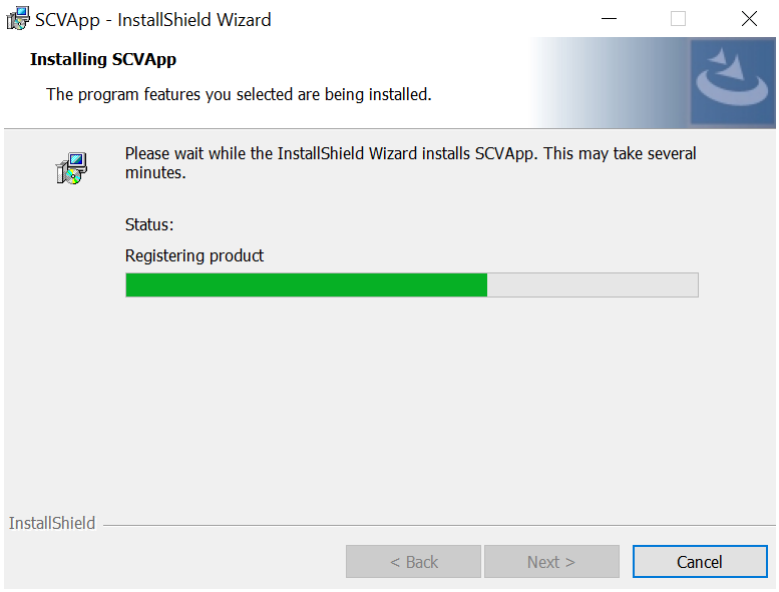


Abbildung 18. SCVApp installieren

6. Klicken Sie nach Abschluss der Installation auf **Fertig stellen**, um den InstallShield-Assistenten zu beenden.

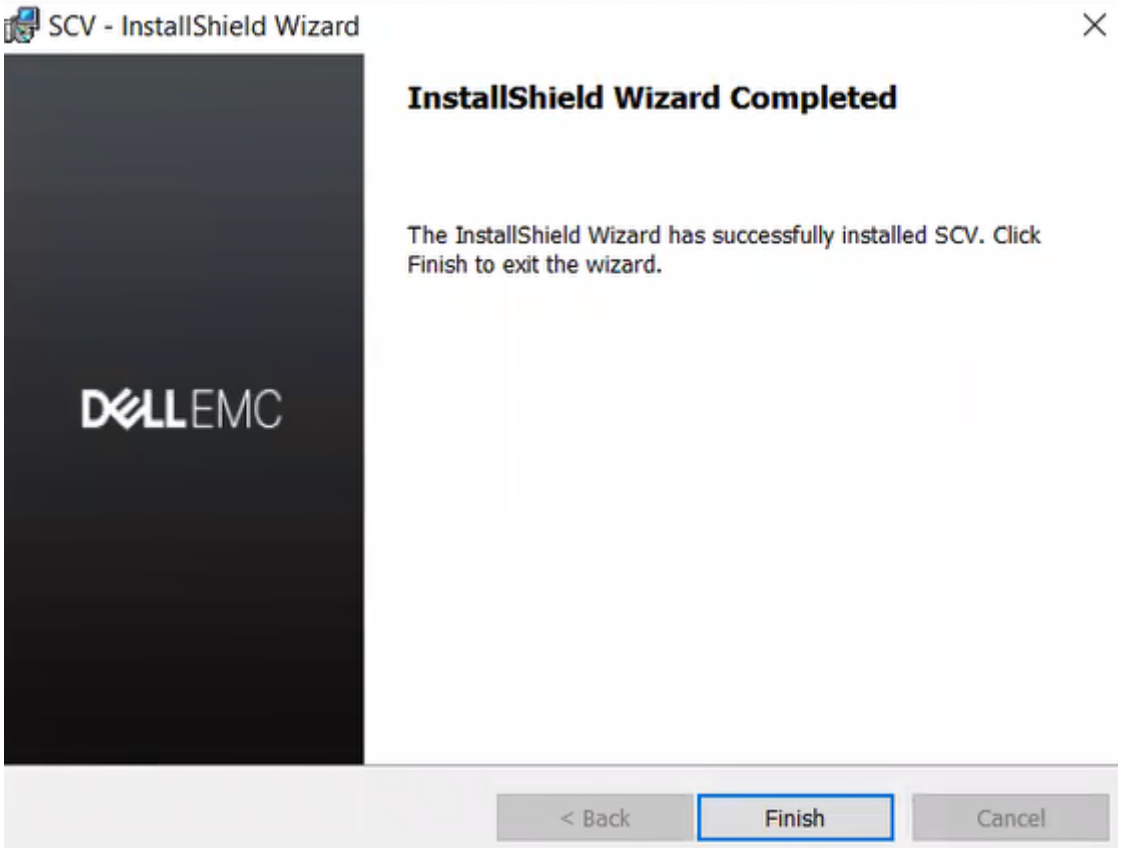


Abbildung 19. SCVApp-Installation abgeschlossen

Ausführen von SCV auf Windows Server 2019 und 2022

1. Öffnen Sie die Eingabeaufforderung und navigieren Sie zum Verzeichnis `SCVTools`.
2. Führen Sie den Befehl `scv validatesysteminventory` aus, um den Validierungsprozess zu starten.

ANMERKUNG: Stellen Sie beim Ausführen von SCV auf dem Host sicher, dass die USB-NIC-IP-Adresse in iDRAC auf die Standard-IP-Adresse eingestellt ist. Stellen Sie außerdem sicher, dass die ersten drei Oktette der IP-Adresse „169.254.1“ lauten.

ANMERKUNG: Der Fehler „Das Verzeichnis scvapp konnte nicht erstellt werden: Fehlgeschlagen“ wird angezeigt, wenn der Befehl `scv validatesysteminventory` in einem anderen Verzeichnis als jenem ausgeführt wird, in dem die Anwendung liegt.

ANMERKUNG: Der Fehler „Herunterladen des SCV-Werkszertifikats: Fehlgeschlagen“ wird angezeigt, wenn der Befehl `scv validatesysteminventory` ausgeführt wird, während die Host-Firewall aktiviert ist. Um den Befehl erfolgreich auszuführen, stellen Sie sicher, dass Sie eine ausgehende Regel für IP-Adresse 169.254.1.1 erstellen.

ANMERKUNG: Nachdem Sie den Gesamtstatus „bereit“ in der Ausgabe von `racadm getremoteservicesstatus` erhalten haben, achten Sie darauf, etwa 120 Sekunden zu warten, bevor Sie die SCV-Befehle ausführen.

ANMERKUNG: Beim Ausführen des Befehls mit der Option `-d` wird möglicherweise der Fehler „Erfassen des Systembestands: fehlgeschlagen“ beim Ausführen von `scv validatesysteminventory` angezeigt, wenn die Länge des Verzeichnispfads 150 Zeichen überschreitet.

```
X:\Dell\scv>scv validatesysteminventory
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag FL8WFZ3 with System Inventory Service Tag: Match
Inventory Comparision Result : MisMatch


---------------------------------------------------------------------
Inventory MisMatch Summary
---------------------------------------------------------------------
Added Components Summary:
               HardDrive       23E0A08BTC88    Disk.Bay.5:Enclosure.Internal.0-1
               PowerSupply     CNLOD0034I2C75  PSU.Slot.2


Refer Detailed Report File at : X:\Dell\scv\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2023_12_24_03_17_46.txt
```

Abbildung 20. Ausführen des Validierungsbefehls mit erfolgreichem Ergebnis

3. Wenn das Ergebnis `Validating System Inventory: Mismatch` lautet, wird unter `Mismatch Inventory Summary` die Komponente angezeigt, die nicht übereinstimmt.

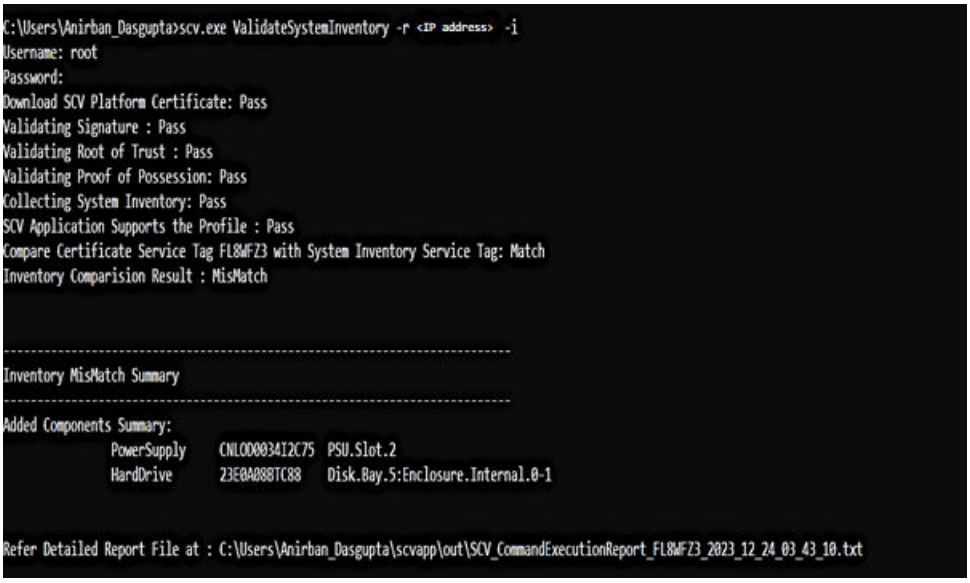


Abbildung 21. Validierung mit nicht erfolgreichem Ergebnis

```
System Information
--------------------------------------------------------------------------------
ServiceTag: <Service Tag>
HostIP: <IP address>
PlatformModel: PowerEdge R660
Manufacturer: Dell Inc.

--------------------------------------------------------------------------------
Command Information
--------------------------------------------------------------------------------
Command : ValidateSystemInventory
Execution Mode : Remote
Enforce Order : Enforced

--------------------------------------------------------------------------------
Command Execution Status
--------------------------------------------------------------------------------
Download SCV Platform Certificate : Success
Validate SCV Platform Certificate Signature : Success
Validate SCV Platform Certificate Root Of Trust : Success
Validate SCV Platform Certificate Proof Of Possession : Success
Collect System Inventory : Success
Validate System Inventory : Success
SCV Application Support For System Inventory Profile : Supported
Validate Profile Data between SCV Platform Certificate and System Inventory : Success
Compare SCV Platform Certificate Against System Inventory : Success

--------------------------------------------------------------------------------
Component Inventory Comparison Results
--------------------------------------------------------------------------------
Service Tag Comparison Result : Match
Subject Alternate Name Comparison Result : Match
Inventory Comparison Result : Match
OverAll Comparison Result : Match

--------------------------------------------------------------------------------
Matched Components
--------------------------------------------------------------------------------
{
    "Baseboard": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00030003",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "X31",
            "Location": "1",
            "Manufacturer": "Dell Inc.",
            "Model": "0M1CC5",
            "SerialNumber": "CNIVC0026T0065"
        }
    ],
    "HardDrive": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.0:Enclosure.Internal.0-1",
            "Manufacturer": "Samsung Electronics Co Ltd",
            "Model": "Unknown",
            "SerialNumber": "S6CSNA0RA02805"
        }
    ],
    "Memory": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00060001",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "A1",
            "Manufacturer": "Micron Technology",
            "Model": "DDR5 DIMM",
            "SerialNumber": "3169944A"
        }
    ],
    "Network": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00090002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "NIC.Embedded.2-1-1",
            "Manufacturer": "Broadcom",
            "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:17",
            "SerialNumber": "Unknown",
            "MacAddress": "EC:2A:72:33:06:17"
        },
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00090002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "NIC.Embedded.1-1-1",
            "Manufacturer": "Broadcom",
            "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:16",
            "SerialNumber": "Unknown",
            "MacAddress": "EC:2A:72:33:06:16"
        }
    ],
    "PowerSupply": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x000a0002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "A04",
            "Location": "PSU.Slot.1",
            "Manufacturer": "DELL",
            "Model": "PWR SPLY,800W,RDNT,LTON",
            "SerialNumber": "CNLOD0024635D4"
        }
    ],
------------------------------
------------------------------
 "Processor": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00010002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Intel(R) Xeon(R) Platinum 8452Y",
            "Location": "CPU1",
            "Manufacturer": "Intel",
            "Model": "b3",
            "SerialNumber": "1BFCF11FD1C1E363"
        }
    ],
    "iDRAC": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00060003",
            "CertificateIdentifier": "MIICVTCCAfugAwIBAgIIAwAAAAAxE+QwCgYIKoZIzj0EAwIwdTEL
             MAkGA1UEBhMCQ04xETAPBgNVBAgMCFNoYW5naGFpMREw
        }
```

Abbildung 22. Erwartete und erkannte Details für nicht übereinstimmende Komponente

```
--------------------------------------------------------------------------------
System Information
--------------------------------------------------------------------------------
ServiceTag: <Service Tag>
HostIP: <IP address>
PlatformModel: PowerEdge R660
Manufacturer: Dell Inc.

--------------------------------------------------------------------------------
Command Information
--------------------------------------------------------------------------------
Command : ValidateSystemInventory
Execution Mode : Remote
Enforce Order : Enforced

--------------------------------------------------------------------------------
Command Execution Status
--------------------------------------------------------------------------------
Download SCV Platform Certificate : Success
Validate SCV Platform Certificate Signature : Success
Validate SCV Platform Certificate Root Of Trust : Success
Validate SCV Platform Certificate Proof Of Possession : Success
Collect System Inventory : Success
Validate System Inventory : Success
SCV Application Support For System Inventory Profile : Supported
Validate Profile Data between SCV Platform Certificate and System Inventory : Success
Compare SCV Platform Certificate Against System Inventory : Success

--------------------------------------------------------------------------------
Component Inventory Comparison Results
--------------------------------------------------------------------------------
Service Tag Comparison Result : Match
Subject Alternate Name Comparison Result : Match
Inventory Comparison Result : Match
OverAll Comparison Result : Match

--------------------------------------------------------------------------------
Matched Components
--------------------------------------------------------------------------------
{
    "Baseboard": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00030003",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "X31",
            "Location": "1",
            "Manufacturer": "Dell Inc.",
            "Model": "0M1CC5",
            "SerialNumber": "CNIVC0026T0065"
        }
    ],
    "HardDrive": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00070002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "Disk.Bay.0:Enclosure.Internal.0-1",
            "Manufacturer": "Samsung Electronics Co Ltd",
            "Model": "Unknown",
            "SerialNumber": "S6CSNA0RA02805"
        }
    ],
    "Memory": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00060001",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "A1",
            "Manufacturer": "Micron Technology",
            "Model": "DDR5 DIMM",
            "SerialNumber": "3169944A"
        }
    ],
    "Network": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00090002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "NIC.Embedded.2-1-1",
            "Manufacturer": "Broadcom",
            "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:17",
            "SerialNumber": "Unknown",
            "MacAddress": "EC:2A:72:33:06:17"
        },
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00090002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Unknown",
            "Location": "NIC.Embedded.1-1-1",
            "Manufacturer": "Broadcom",
            "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:16",
            "SerialNumber": "Unknown",
            "MacAddress": "EC:2A:72:33:06:16"
        }
    ],
    "PowerSupply": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x000a0002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "A04",
            "Location": "PSU.Slot.1",
            "Manufacturer": "DELL",
            "Model": "PWR SPLY,800W,RDNT,LTON",
            "SerialNumber": "CNLOD0024635D4"
        }
    ],
    "Processor": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00010002",
            "CertificateIdentifier": "Unknown",
            "HardwareVersionNumber": "Intel(R) Xeon(R) Platinum 8452Y",
            "Location": "CPU1",
            "Manufacturer": "Intel",
            "Model": "b3",
            "SerialNumber": "1BFCF11FD1C1E363"
        }
    ],
    "iDRAC": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00060003",
            "CertificateIdentifier": "MIICVTCCAfugAwIBAgIIAwAAAAAxE+QwCgYIKoZIzj0EAwIwdTELMAkGA
             1UEBhMCQ04xETAPBgNVBAgMCFNoYW5naGFpMREwDwYDVQQHDAhTa
        }
```

Abbildung 23. Erwartete und erkannte Details für nicht übereinstimmende Komponente

5

Remoteausführung von Secured Component Verification (SCV)

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:
Themen:

- Remoteausführung von SCV auf Windows Server 2019 und 2022
- Remoteausführung von SCV auf WinPE
- Remoteausführung von SCV auf Linux

Remoteausführung von SCV auf Windows Server 2019 und 2022

1. Öffnen Sie die Eingabeaufforderung und navigieren Sie zum Verzeichnis `SCVTools`.
2. Führen Sie den Befehl `scv validatesysteminventory -r <iDRAC IPv4/IPv6[] address> -i` aus, um den Validierungsprozess zu starten.

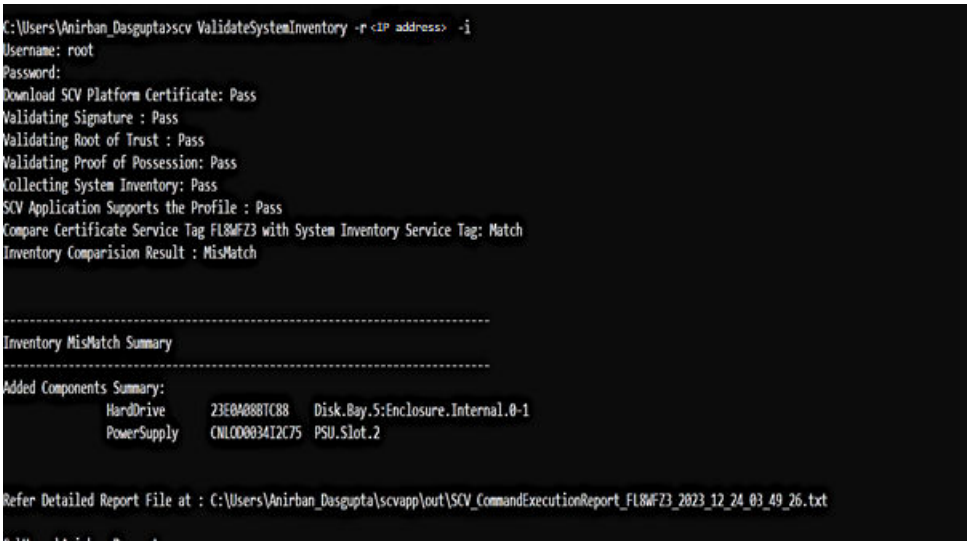


Abbildung 24. Remoteausführung des Validierungsbefehls unter Windows mit erfolgreichem Ergebnis

Remoteausführung von SCV auf WinPE

1. Öffnen Sie die Eingabeaufforderung und navigieren Sie zum Verzeichnis `SCVTools`.
2. Führen Sie den Befehl `scv validatesysteminventory -r <iDRAC IPv4/IPv6[] address> -i` aus, um den Validierungsprozess zu starten.

```
X:\Dell\scv>scv validatesysteminventory -r <IP address> -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag DL8WFZ3 with System Inventory Service Tag: Match
Inventory Comparison Result : Match

Refer Detailed Report File at : X:\Dell\scv\scvapp\out\SCV_CommandExecutionReport_DL8WFZ3_2024_01_24_22_33_43.txt
```

Abbildung 25. Remoteausführung des Validierungsbefehls unter WinPE mit erfolgreichem Ergebnis

Remoteausführung von SCV auf Linux

1. Öffnen Sie die Eingabeaufforderung und navigieren Sie zum Verzeichnis `SCVTools`.
2. Führen Sie den Befehl `scv validatesysteminventory -r <iDRAC IPv4/IPv6[] address> -i` aus, um den Validierungsprozess zu starten.

```
[root@localhost SCVTools]# scv validateSystemInventory -r <IP address> -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag DL8WFZ3 with System Inventory Service Tag: Match
Inventory Comparison Result : MisMatch


--------------------------------------------------------------------------------
Inventory MisMatch Summary
--------------------------------------------------------------------------------
Removed Components Summary:
               TPM     0096797170CFE773D5DA59  RSA
               TPM     00EAC1C8340E7E80FD0F77  ECC


Refer Detailed Report File at : /root/1.93/SCVTools/scvapp/out/SCV_CommandExecutionReport_DL8WFZ3_2024_01_24_09_06_27.txt
```

Abbildung 26. Remoteausführung des Validierungsbefehls unter Linux mit erfolgreichem Ergebnis

6

SCV-Befehlsdetails

Dieser Abschnitt enthält Informationen zu einigen zusätzlichen SCV-Befehlen.

Themen:

- Abrufen von Informationen zum Ausführen von SCV
- Abrufen von Informationen über den Befehl scv validatesysteminventory
- Remoteverbindung zu einer Managementkonsole und Validierung von Beständen
- Remoteverbindung zu einer Managementkonsole mit einem bestimmten Port und Bestandsvalidierung
- Übereinstimmung des Komponentenspeicherorts gewährleisten und Bestandsvalidierung
- SCV-Version abrufen
- Anzeigen des Zertifikatkennungswerts in der Konsole oder Umleiten an eine Datei

Abrufen von Informationen zum Ausführen von SCV

Tabelle 4. Abrufen von weiteren Informationen über SCV

SCV-Hilfe	
Beschreibung	Verwenden Sie den folgenden Befehl, um weitere Informationen über SCV und die Ausführung zu erhalten.
Zusammenfassung	`scv help`

Ausgabe

```
C:\>scv help

SCV -- Secured Component Verification

Usage: scv.exe help <subcommand> [options]...

List of supported subcommands:
        - validatesysteminventory
        - extractcert
        - getcertinfo
        - version
        - mars


Note:
        This is the SCV Help Command
```

Abrufen von Informationen über den Befehl scv validatesysteminventory

Tabelle 5. Weitere Informationen zum Befehl scv validatesysteminventory

scv help validatesysteminventory	
Beschreibung	Verwenden Sie den folgenden Befehl, um weitere Informationen zum Befehl `validatesysteminventory` und dessen Ausführung zu erhalten.

Tabelle 5. Weitere Informationen zum Befehl scv validatesysteminventory (fortgesetzt)

scv help validatesysteminventory	
Zusammenfassung	`scv help validatesysteminventory`

Ausgabe

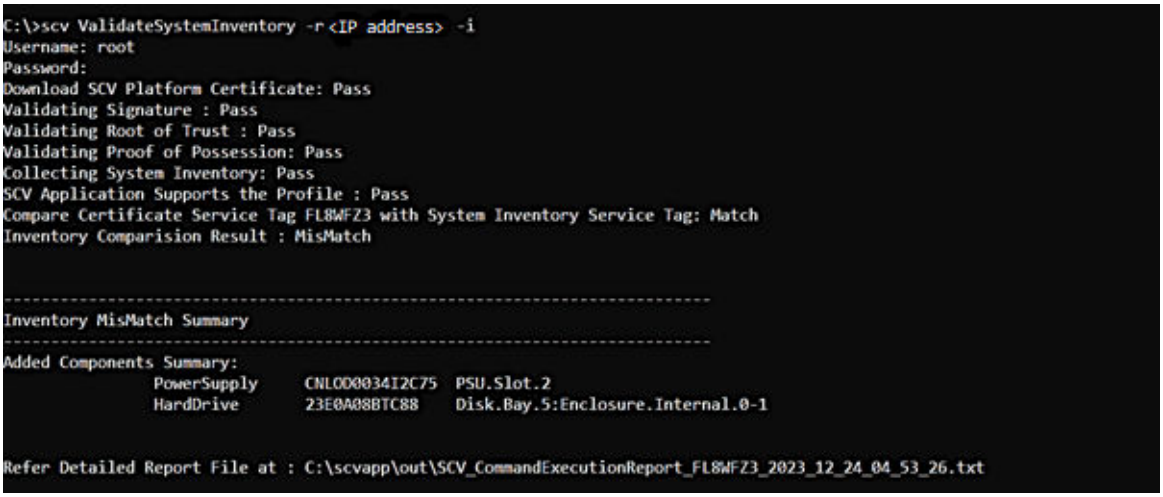
```
PS C:\> scv help validatesysteminventory

SCV -- Secured Component Verification

Usage: scv.exe validatesysteminventory [options]...

List of supported options:
       -r, --remoteip=<Remote Target IP>      Target System IP. Not required when SCV is running on Host OS.
       -u, --username=<UserName>              Username for Authenticating to target system. Not required when SCV is running on Host OS.
       -p, --password=<Password>              Password for Authenticating to target system. Not required when SCV is running on Host OS.
       -i, --interactive                      Enable interactive command execution Mode. UserName and Password will be accepted interactively from the use
r
       -d, --directory=<Directory Path>       Output directory path (MAX 247 Characters). If not specified, Current Working directory will be the output d
irectory.
       -e, --enforceorder                     force component slot location comparision along with the serial number comparision.
       -D, --debug                            Enable Debug log level


List of Example Commands:
       scv.exe validatesysteminventory [ -r|--remoteip -u|--username -p|--password ] [ -e|--enforceorder ] [ -d|--directory ] [ -D|--debug ]
       scv.exe validatesysteminventory [ -r|--remoteip -i|--interactive ] [ -e|--enforceorder ] [ -d|--directory ] [ -D|--debug ]


Note:
       The detailed logs collected are available in: directory->scvapp->logs folder.
       Steps Performed:
              Downloads SCV factory certificate and Delta certificate(s)
              Validates Signature and Root of Trust
              Validates Proof of Possession
              Verifies application supported certificate profile version
              Validates System service Tag
              Collects and validates system inventory.
```

Remoteverbindung zu einer Managementkonsole und Validierung von Beständen

Tabelle 6. Remotevalidierung eines bestimmten Bestands

scv validatesysteminventory -r <IPv4/IPv6 address> -i	
Beschreibung	Verwenden Sie den folgenden Befehl, um eine Remoteverbindung zu einer bestimmten Managementkonsolen-IP herzustellen und den Bestand zu validieren.
Zusammenfassung	`scv validatesysteminventory -r <IPv4/IPv6 address> -i`
Eingabe	• `-r` – IPv4-/IPv6-Adresse

Ausgabe



Remoteverbindung zu einer Managementkonsole mit einem bestimmten Port und Bestandsvalidierung

Tabelle 7. Bestandsvalidierung über einen bestimmten Port

scv validatesysteminventory -r <IPv4/IPv6 address:Port> -i	
Beschreibung	Verwenden Sie den folgenden Befehl, um eine Verbindung mit einer Managementkonsolen-IP über einen bestimmten Port herzustellen und den Bestand zu validieren.
Zusammenfassung	`scv validatesysteminventory -r <IPv4/IPv6 address:Port> -i`
Eingabe	• `-r` – IPv4-/IPv6-Adresse

Übereinstimmung des Komponentenspeicherorts gewährleisten und Bestandsvalidierung

Tabelle 8. Übereinstimmung des Komponentenspeicherorts gewährleisten

scv validatesysteminventory --enforceorder	
Beschreibung	Verwenden Sie den folgenden Befehl, um sicherzustellen, dass der Komponentenspeicherort bei der Bestandsvalidierung übereinstimmt. **ANMERKUNG:** Jeder Komponentenaustausch wird bei Verwendung des Befehls `--enforceorder` als „Nicht übereinstimmend“ identifiziert.
Zusammenfassung	`scv validatesysteminventory --enforceorder`

Ausgabe

```
PS C:\> scv.exe ValidateSystemInventory -r <IP address> -i --enforceorder
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag FL8WFZ3 with System Inventory Service Tag: Match
Inventory Comparision Result : MisMatch


--------------------------------------------------------------------------------
Inventory MisMatch Summary
--------------------------------------------------------------------------------
Added Components Summary:
               HardDrive       23E0A08BTC88    Disk.Bay.5:Enclosure.Internal.0-1
               PowerSupply     CNLOD0034I2C75  PSU.Slot.2

Moved Components Summary:
               HardDrive       23E0A08BTC88    PCIeSSD.SL.3-2


Refer Detailed Report File at : C:\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2023_12_24_04_35_37.txt
```

SCV-Version abrufen

Tabelle 9. Version von SCV abrufen

SCV-Version	
Beschreibung	Verwenden Sie den folgenden Befehl, um die aktuelle Version der SCV-Anwendung anzuzeigen.
Zusammenfassung	`scv version`

Ausgabe

```
C:\Users\Administrator>scv version
SCV version 1.5 (Build 156)
Copyright(c) 2020 - 2022 Dell, Inc.
All Rights Reserved

C:\Users\Administrator>
C:\Users\Administrator>
```

Anzeigen des Zertifikatkennungswerts in der Konsole oder Umleiten an eine Datei

Tabelle 10. Anzeigen oder Umleiten des Zertifikatkennungswerts

scv extractcert	
Beschreibung	Verwenden Sie den folgenden Befehl, um den Wert für die Zertifikatkennung in der Konsole anzuzeigen oder sie an eine Datei umzuleiten.
Zusammenfassung	`scv extractcert -r <IPv4/IPv6 address> -i -component <Component Name> -l <Location> -f <File Name>  -D <Debug>`
Eingabe	• `-r` – IPv4-/IPv6-Adresse • `-component` – Komponentenname

Tabelle 10. Anzeigen oder Umleiten des Zertifikatkennungswerts (fortgesetzt)

scv extractcert	
	• – `l` – Speicherort • – `f` – Dateiname • – `D` – Debug-Protokollebene aktivieren

Ausgabe

```
PS C:\> scv.exe extractcert -r <IP address> --component iDRAC --location 1 -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
-----BEGIN CERTIFICATE-----MIICZDCCAgmgAwIBAgIIAmAAAAA3LbowCgYIKoZIzj0EAwIwdTELMAkGA1UEBhMCQ04xETAPBgNVBAgMCFNoYW5naGFpMREwDwYDVQQHDAhTaGFuZ2hhaTERMA8GA1UEC
gwISW52ZW50ZWMxDTALBgNVBAsMBFBST0QxHjAcBgNVBAMMFTBJVkMwMC1DRTBDLTEwNUUtNjgyNjAeFw0yMzA2MjYyMjM0MDJaFw00MjA4MjUyMjM0MDJaMH8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZ
XhhczETMBEGA1UEBwwKUm91bmQgUm9jazEfMB0GA1UECgwWRGVsbCBUZWNobm9sb2dpZXMgSW5jLjEOMAwGA1UECwwFSURSQUMxGjAYBgNVBAMMEWM0OmNiOmUxOmFhOjQzOjEyMFkwEwYHKoZIzj0CAQYIK
oZIzj0DAQcDQgAEICw0gZp7SJwS9GXAHXxWaSPANvtjjIPMFFvmFbf0F5Bv+GCAMkdmIvOWygNVa7Wqw0pvfN3ziy5OebRpSiQgiKN5M+cwCQYDVR0TBAIwADALBgNVHQ8EBAMCBeAwHQYDVR0lBBYwFAYIK
wYBBQUHAwEGCCsGAQUFBwMCMB0GA1UdDgQWBBRFE1ZnZgc+nDAUmmiehz/9AVoUODAfBgNVHSMEGDAWgBTTQRLYLTKIV9I9he9zyVUcytYYMTAKBggqhkjOPQQDAgNJADBGAiEA/pe5i/eUULQkbkYTrOZG
EGTtjuaZWN3RTRtGV4ALN8CIQDS5RBt2JYvvLEu5U24tb/mZjDRBkkNBAwMa/WZVs/YAA==-----END CERTIFICATE-----
```

Abbildung 27. Anzeigen des Zertifikatkennungswerts in der Konsole

```
PS C:\> scv.exe extractcert -r <IP address> --component iDRAC --location 1 -f abc.crt -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
```

Abbildung 28. Schreiben des Zertifikatkennungswerts in eine Datei

```
PS C:\Users\Raj_Bhawan\scvGo2.0Workspace\SCV\scv_go> ./scv extractcert -r <IP address> -C idrac -l 1 -D -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
-----BEGIN CERTIFICATE-----MIICZDCCAgmgAwIBAgIIAwAAAA3La8wCgYIKoZIzj0EAwIwdTELMAkGA1UEBhMCQ04xETAPBgNVBAgMCFNoYW5naGFpMREwDwYDVQQHDAhTaGFuZ2hhaTERMA8GA1UECgwISW52ZW50ZWMxDTALBgNVBAsMBFBST0QxHjA
cBgNVBAMMFTBJVkMwMC1DRTBDLTEwNUUtNjgyNjAeFw0yMzA2MjYyMjE5MzhaFw00MjA4MjUyMjE5MzhaMH8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEGA1UEBwwKUm91bmQgUm9jazEfMB0GA1UECgwWRGVsbCBUZWNobm9sb2dpZXMgSW5jL
jEOMAwGA1UECwwFSURSQUMxGjAYBgNVBAMMEWM0OmNiOmUxOmFhOjQyOjFjMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEdJN8FTYofXlT5YZb39Wu8rXOc8tALFw823ePqm2XYXyC+IEp5jyLfGoiqXb59SIFgN9wRCyOv1SC9d1P2IqDSaN5MHcwCQYDVR0
TBAIwADALBgNVHQ8EBAMCBeAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB0GA1UdDgQWBBQT3piu45upd2xo2J+QT8F+/zAidjAfBgNVHSMEGDAWgBTTQRLYLTKIV9I9he9zyVUcytYYMTAKBggqhkjOPQQDAgNJADBGAiEA+w8RS3qvx/t4Lp2ww
iZU4t+DNSXqUEtIUL/sdR7UvrMCIQDkhWPNpNXf4ULcbBZ9m7tDI7zWbrY5+dGhzBg1RfoISQ==-----END CERTIFICATE-----
```

Abbildung 29. Anzeigen des Zertifikatkennungswerts in der Konsole mithilfe der Debug-Option

7

SCVApp MARS-Funktion

MAC Address Reporting Service (MARS) ist ein neues Angebot, das MAC-Adressen für den iDRAC und LOM-Port 0 sowie das entsprechende Server-Service-Tag bereitstellt.

SCVApp extrahiert die MAC-Adresse aus dem Zertifikatbestand für das Netzwerk und die iDRAC-Komponente.

Im Folgenden sind nützliche SCVApp-Befehle aufgeführt:

Tabelle 11. Informationen über mars erhalten

scv help mars	
Zusammenfassung	scv help mars
Ausgabe	scv help mars SCV -- Secured Component Verification Usage: scv.exe mars [options]... List of supported options: -d, --directory=<Directory Path> Output directory path (MAX 247 Charactors). If not specified, Current Working directory will be the output directory. -f, --file=<File Path> Input or Output File Path. -D, --debug Enable Debug log level List of Example Commands: scv.exe mars -f|--file [-d|--directory] [-D|--debug]

Tabelle 12. Ausführen des Befehls mars zum Extrahieren der mars-Details und Erstellen der marsreport.csv-Datei

scv mars	
Zusammenfassung	scv mars ./SCVTest.zip ./scvapp/out/marsreport.csv
Ausgabe	scv mars ./SCVTest.zip ./scvapp/out/marsreport.csv : ServiceTags,Components,MacAddresses FYRLCW3,NIC.Embedded.1-1-1,C8:4B:D6:98:93:52 FYRLCW3,NIC.Embedded.2-1-1,C8:4B:D6:98:93:53 FYRLCW3,iDRAC,c8:4b:d6:98:93:4c FYRLCW3,NIC.Embedded.1-1-1,C8:4B:D6:98:93:52 FYRLCW3,NIC.Embedded.2-1-1,C8:4B:D6:98:93:53

Tabelle 12. Ausführen des Befehls mars zum Extrahieren der mars-Details und Erstellen der marsreport.csv-Datei (fortgesetzt)

scv mars	
	FYRLCW3,iDRAC,c8:4b:d6:98:93:4c

8

SPDM-Funktion

Security Protocol and Data Model (SPDM) ist ein Protokoll, das für die Einrichtung von Sicherheitsfunktionen und Authentizität zwischen Hardwarekomponenten verwendet wird. SPDM ermöglicht den Nachrichtenaustausch zwischen iDRAC und Endgeräten wie Storage-Controllern und NIC-Controllern. Dies umfasst Hardwareidentitätszertifikate.

Die SCV-Anwendung unterstützt die Erkennung der Hardwareidentitätszertifikate für SPDM-fähige Endgeräte. Die SCV-Anwendung exportiert die Hardwareidentität der SPDM-fähigen Geräte in das SCV-Zertifikat.

9

Stamm-CA-Zertifikat für SCV

ANMERKUNG: Dieser Abschnitt enthält Details zum Stamm-CA-Zertifikat für SCV.

Dateiformat: Extrahiert Dateien direkt auf die lokale Festplatte

Dateiname: Certificate A00.zip

Dateigröße: 929 Byte

Formatbeschreibung: Dieses Dateiformat besteht aus einem Archiv von Dateien, die in ein Verzeichnis auf der Festplatte dekomprimiert werden können. Die Installation kann dann von diesem Verzeichnis aus durchgeführt werden.

Download-Link: https://dl.dell.com/FOLDER06748569M/1/Certificate A00.zip

Um die Downloadintegrität zu gewährleisten, überprüfen Sie den Prüfsummenwert.

MD5: edb649dbf130e43aeaf5358f1186d312

SHA1: a92d23c8e9e61fd5c4e568cb23be3024df3f886f

SHA-256: c947162dc67f5d441ff22b063d7566c52db23cc0c51746455e492c60943f8165

10

Rückgabecodes

Im Folgenden wird die Liste der Rückgabecodes für SCV-Vorgänge aufgeführt:

Tabelle 13. SCV-Rückgabecodes

Code	Beschreibung
0	Alle Vorgänge waren erfolgreich und der Bestand stimmte überein.
1	Allgemeine Fehlermeldung.
2	Eine andere Instanz des SCV-Vorgangs wird ausgeführt.
3	Die Berechtigung ist für den Nutzer nicht geeignet.
4	SCV-Vorgang konnte nicht gestartet werden, Abhängigkeiten wurden nicht erfüllt.
5	Zertifikatdownload von iDRAC fehlgeschlagen.
6	Validierung der Signatur und des Vertrauensankers fehlgeschlagen.
7	Die Validierung des Eigentumsnachweises ist fehlgeschlagen.
8	Profil wird für die im Zertifikat angegebenen Versionsdetails nicht unterstützt.
9	Profil, Unterschema/Dienstprogramme sind manipuliert, Profilsignatur stimmt nicht überein.
10	Daten können aufgrund eines Dienstprogrammfehlers nicht erfasst werden.
11	Nicht übereinstimmende Bestandsinformationen.
12	Der angegebene Wert liegt außerhalb des zulässigen Bereichs. Das Argument ist länger oder kürzer als zulässig.
13	Ungültigen oder falschen SCV-Befehl eingegeben. Eingegebene Befehle oder Optionen werden auf der aktuellen Schnittstelle/Plattform nicht unterstützt.
14	Die Syntax des Befehls ist falsch.
15	Befehl, der im Werkmodus (SSM) ausgeführt werden soll.
16	Für SCV ist keine erforderliche Lizenz installiert.
17	iDRAC verfügt nicht über genügend Ressourcen (z. B. Arbeitsspeicher)
18	Service nicht verfügbar/ausgelastet.
19	Dateiübertragungsproblem (Inband).
20	Der Sperrmodus ist aktiviert oder abhängige Attribute sind ungültig/nicht konfiguriert.
21	Verbindung kann nicht hergestellt werden (Out-of-Band)
22	Abhängigkeit für eine Spezifikation nicht erfüllt
23	Probleme im Zusammenhang mit der Sitzung.
24	Fehler aufgrund von ungültigen Schlüsseln, Zertifikaten und Signierungsfehlern.
25	Hochladen des Zertifikats fehlgeschlagen.

11

Wie Sie Hilfe bekommen

Themen:

- Kontaktaufnahme mit Dell
- Support-Dokumente und -Ressourcen
- Feedback zur Dokumentation

Kontaktaufnahme mit Dell

Dell stellt verschiedene online-basierte und telefonische Support- und Serviceoptionen bereit. Wenn Sie nicht mit dem Internet verbunden sind, finden Sie weitere Informationen auf Ihrer Bestellung, auf dem Lieferschein, auf der Rechnung oder im Dell Produktkatalog. Die Verfügbarkeit ist abhängig von Land und Produkt und einige Dienste sind in Ihrem Gebiet möglicherweise nicht verfügbar. So erreichen Sie den Verkauf, den technischen Support und den Kundendienst von Dell:

Schritte

1. Rufen Sie www.dell.com/support/home auf.
2. Wählen Sie Ihr Land im Dropdown-Menü in der unteren rechten Ecke auf der Seite aus.
3. Für individuellen Support:
   a. Geben Sie die Service-Tag-Nummer Ihres Systems im Feld **Service-Tag eingeben** ein.
   b. Klicken Sie auf **Senden**.
   Die Support-Seite, auf der die verschiedenen Supportkategorien aufgelistet sind, wird angezeigt.
4. Für allgemeinen Support:
   a. Wählen Sie Ihre Produktkategorie aus.
   b. Wählen Sie Ihr Produktsegment aus.
   c. Wählen Sie Ihr Produkt aus.
   Die Support-Seite, auf der die verschiedenen Supportkategorien aufgelistet sind, wird angezeigt.
5. So erhalten Sie die Kontaktdaten für den weltweiten technischen Support von Dell:
   a. Klicken Sie auf Kontaktaufnahme mit dem technischen Support.
   b. Geben Sie das Service-Tag Ihres Systems im Feld **Service-Tag eingeben** auf der Website für Kontakt ein.

Support-Dokumente und -Ressourcen

- Auf der iDRAC-Support-Startseite finden Sie Produktdokumentation, technische Whitepaper, Anleitungsvideos und mehr:
  - www.dell.com/support/idrac
- iDRAC-Benutzerhandbuch und weitere Handbücher:
  - www.dell.com/idracmanuals
- Weitere Informationen zu PowerEdge-Servern finden Sie in der Dokumentation unter:
  - www.dell.com/poweredgemanuals
- Technischer Support von Dell
  - www.dell.com/support

Feedback zur Dokumentation

Sie können auf all unseren Dell Dokumentationsseiten die Dokumentation bewerten oder Ihr Feedback dazu abgeben und uns diese Informationen zukommen lassen, indem Sie auf **Feedback senden** klicken.