

# **Dell Secured Component Verification Version 1.5,1.5.1,1.6,1.7,1.8, 1.9, 1.91.0, 1.92.0 und 1.93.0**

Referenzhandbuch für Server und Gehäuse

## 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.

# Inhaltsverzeichnis

<b>Kapitel 1: Übersicht.....</b>	<b>5</b>
Neue Funktionen hinzugefügt.....	5
SCV 1.93.0.....	5
SCV 1.92.0.....	5
SCV 1.91.0.....	5
SCV 1.9.....	5
SCV 1.8.....	6
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.....	8
Unterstützte URLs.....	8
<b>Kapitel 2: Secured Component Verification auf WinPE.....</b>	<b>10</b>
Erstellen eines ISO-Images zum Ausführen von SCV mit WinPE.....	10
Hinzufügen von SCV zu einem benutzerdefinierten ISO-Image.....	11
Ausführen von SCV auf WinPE.....	11
Überprüfen der SCV-Protokolle mit WinPE.....	13
<b>Kapitel 3: Secured Component Verification auf Linux.....</b>	<b>14</b>
Ausführen von SCV auf Linux.....	14
Anzeigen der SCV-Protokolle unter Linux.....	17
<b>Kapitel 4: Secured Component Verification auf Windows Server 2019 und 2022.....</b>	<b>18</b>
Installieren von SCVApp auf Windows Server 2019 und 2022.....	18
Ausführen von SCV auf Windows Server 2019 und 2022.....	21
<b>Kapitel 5: Remoteausführung von Secured Component Verification (SCV).....</b>	<b>25</b>
Remoteausführung von SCV auf Windows Server 2019 und 2022.....	25
Remoteausführung von SCV auf WinPE.....	25
Remoteausführung von SCV auf Linux.....	25
<b>Kapitel 6: SCV-Befehlsdetails.....</b>	<b>27</b>
Abrufen von Informationen zum Ausführen von SCV.....	27
Abrufen von Informationen über den Befehl scv validateSystemInventory.....	27
Remoteverbindung zu einer Managementkonsole und Validierung von Beständen.....	28
Remoteverbindung zu einer Managementkonsole mit einem bestimmten Port und Bestandsvalidierung.....	29
Übereinstimmung des Komponentenspeicherorts gewährleisten und Bestandsvalidierung.....	29
SCV-Version abrufen.....	29
Anzeigen des Zertifikatkennungswerts in der Konsole oder Umleiten an eine Datei.....	30

<b>Kapitel 7: SCVApp MARS-Funktion.....</b>	<b>32</b>
<b>Kapitel 8: SPDM-Funktion.....</b>	<b>34</b>
<b>Kapitel 9: Stamm-CA-Zertifikat für SCV.....</b>	<b>35</b>
<b>Kapitel 10: Rückgabecodes.....</b>	<b>36</b>
<b>Kapitel 11: Wie Sie Hilfe bekommen.....</b>	<b>37</b>
Kontaktaufnahme mit Dell.....	37
Support-Dokumente und -Ressourcen.....	37
Feedback zur Dokumentation.....	37

# 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 URLs

## Neue Funktionen hinzugefügt

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

- SCV 1.93.0
- 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 1.93.0

Die folgenden Funktionen wurden in dieser Version hinzugefügt oder aktualisiert:

- Die neueste Version enthält wichtige Sicherheitskorrekturen in der SCV-Anwendung.

### SCV 1.92.0

Die folgenden Funktionen wurden in dieser Version hinzugefügt oder aktualisiert:

- Support für die Debug-Option für `denscv 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-UI-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/NPAPeP-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.
- Selbst wenn die USB-NIC über iDRAC aktiviert ist, müssen Sie die Netzwerkschnittstelle manuell im Betriebssystem aktivieren. Sie sollte nicht deaktiviert werden, da sie für die bandinterne Kommunikation erforderlich ist.
- 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.
- SCV unterstützt ab Version 1.93.0 keine 1.0-Zertifikate.

## 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, SUSE Linux Enterprise Server 15 SP4, Windows Server 2019 und Windows Server 2022.																
Firmware-Versionen	<ul style="list-style-type: none"> <li>iDRAC 5.10.30.00 und höhere Versionen</li> <li>OME-M 2.00.00 und höhere Versionen</li> <li>PowerEdge BIOS 2.14.2 und höhere Versionen</li> </ul>																
Erforderliche Lizenzen	Secured Component Verification-Lizenz																
Kompatible Versionen	<table border="1"> <thead> <tr> <th>SCV Version</th><th>iDRAC-Version</th></tr> </thead> <tbody> <tr> <td>1.93.0</td><td>7.10.50.00</td></tr> <tr> <td>1.92.0</td><td>7.10.30.00</td></tr> <tr> <td>1.91.0</td><td>7.10.30.00</td></tr> <tr> <td>1.9.0</td><td>7.00.30.00</td></tr> <tr> <td>1.8.0</td><td>6.10.80.00</td></tr> <tr> <td>1.6.0</td><td>6.00.30.00</td></tr> <tr> <td>1.5.0</td><td>5.10.30.00</td></tr> </tbody> </table> <p>SCV 1.91.0 und spätere Versionen sind abwärtskompatibel mit jeder Version von iDRAC. SCV 1.90.0 und frühere Versionen sind jedoch nur mit Version 7.00.30.00 und früheren Versionen von iDRAC kompatibel.</p>	SCV Version	iDRAC-Version	1.93.0	7.10.50.00	1.92.0	7.10.30.00	1.91.0	7.10.30.00	1.9.0	7.00.30.00	1.8.0	6.10.80.00	1.6.0	6.00.30.00	1.5.0	5.10.30.00
SCV Version	iDRAC-Version																
1.93.0	7.10.50.00																
1.92.0	7.10.30.00																
1.91.0	7.10.30.00																
1.9.0	7.00.30.00																
1.8.0	6.10.80.00																
1.6.0	6.00.30.00																
1.5.0	5.10.30.00																

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

# Unterstützte URLs

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](https://developer.dell.com). Im Folgenden sind die Liste der URLs 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"  
}
```

# 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.
  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:** 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**.
5. Starten 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.

```
C:\Users\Anirban_Dasgupta\Downloads\SCVTools-Web-WINPE10-1.93.0-360>WINPE10.x_driverinst.bat
-----
~~1(WINPE10.x_driverinst.bat)-Checking the Paths
-----
-----
~~2-Setting up a WinPE 10.x amd64 build environment
-----
=====
Creating Windows PE customization working directory
C:\Users\Anirban_Dasgupta\Downloads\SCVTools-Web-WINPE10-1.93.0-360\WINPE10_x_20246-02_105200
=====
```

**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.

```

----7-Loading HAPI driver
-----
----8-Committing Changes to the Image
-----
Deployment Image Servicing and Management tool
Version: 10.0.19041.1

Image File : C:\Users\Administrator\Downloads\SCVTools-Web-WINPE10-1.93.0-360\WINPE10_x_20240617_155319\media\sources\boot.wim
Image Index : 1
Saving image
[=====100.0%=====]
Unmounting image
[=====100.0%=====]
The operation completed successfully.
    1 file(s) copied.
-----
----9-Creating bootable ISO-CD image
-----
OSCDIMG 2.56 CD-ROM and DVD-ROM Premastering Utility
Copyright (C) Microsoft, 1993-2012. All rights reserved.
Licensed only for producing Microsoft authorized content.

Scanning source tree
Scanning source tree complete (153 files in 104 directories)
Computing directory information complete
Image file is 548438016 bytes (before optimization)
Writing 153 files in 104 directories to C:\Users\Administrator\Downloads\SCVTools-Web-WINPE10-1.93.0-360\WINPE10_x_20240617_155319\SCV-Web-WinPE10.x64-1.93.0.iso
100% complete
Storage optimization saved 11 files, 12775424 bytes (3% of image)
After optimization, image file is 536201216 bytes
Space saved because of embedding, sparseness or optimization = 12775424
Done.
-----
--10(WinPE10_x_driverinst.bat)-DONE.
-----
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools>_

```

**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

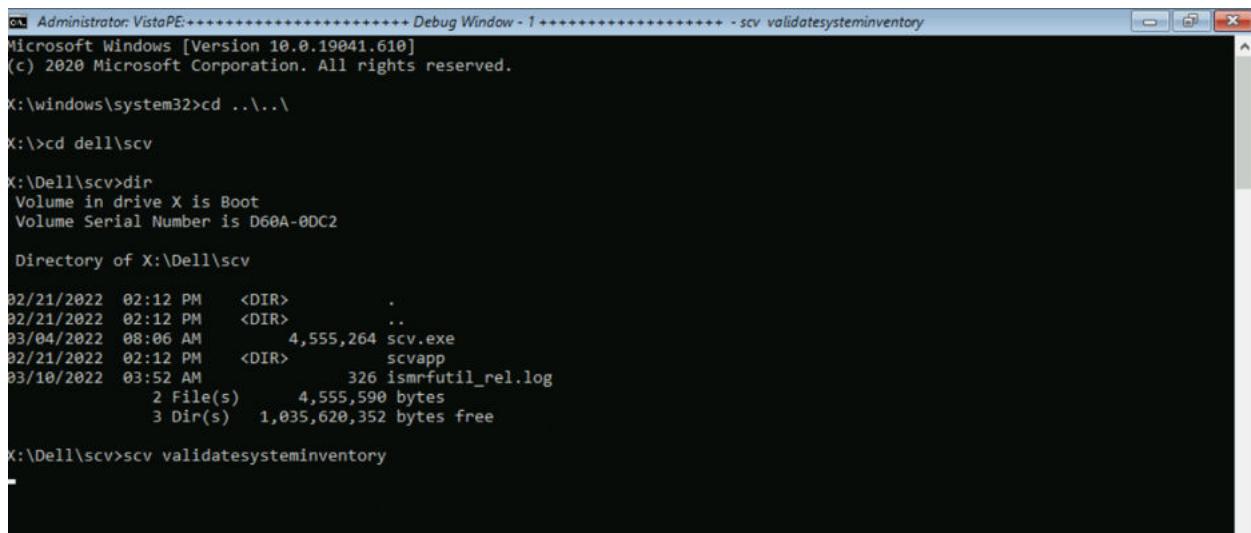
So fügen Sie SCV zu einem benutzerdefinierten ISO-Image hinzu:

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.
4. Kopieren Sie die folgenden Ordner in den entsprechenden Ordnerpfad im benutzerdefinierten ISO-Image:
  - SCV** in X:\Dell
  - 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 255 Zeichen überschreitet.



```

Administrator: VistaPE:+++++ Debug Window - 1 ++++++ - scv validateSystemInventory
Microsoft Windows [Version 10.0.19041.610]
(c) 2020 Microsoft Corporation. All rights reserved.

X:\windows\system32>cd ..\..\

X:\>cd dell\scv

X:\Dell\scv>dir
Volume in drive X is Boot
Volume Serial Number is D60A-0DC2

  Directory of X:\Dell\scv

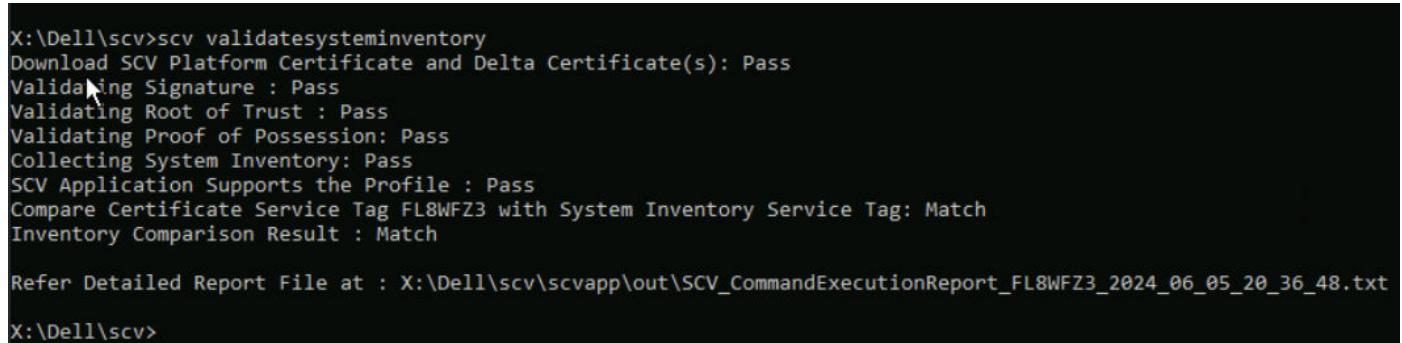
02/21/2022  02:12 PM    <DIR>      .
02/21/2022  02:12 PM    <DIR>      ..
03/04/2022  08:06 AM    4,555,264 scv.exe
02/21/2022  02:12 PM    <DIR>      scvapp
03/10/2022  03:52 AM            326 ismroutil_rel.log
                2 File(s)      4,555,590 bytes
                3 Dir(s)   1,035,620,352 bytes free

X:\Dell\scv>scv validateSystemInventory

```

**Abbildung 3. Ausführen des Validierungsbefehls**

8. Nachdem das System die SCV-Anwendung erfolgreich ausgeführt hat, sollte das Ergebnis des „scv validateSystemInventory“-Befehls Match angezeigt werden.



```

X:\Dell\scv>scv validateSystemInventory
Download SCV Platform Certificate and Delta Certificate(s): 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 Comparison Result : Match

Refer Detailed Report File at : X:\Dell\scv\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2024_06_05_20_36_48.txt

X:\Dell\scv>

```

**Abbildung 4. Ausführen des Validierungsbefehls mit erfolgreichem Ergebnis**

9. Wenn das Ergebnis von „scv validateSystemInventory“ Mismatch lautet, wird unter Mismatch Inventory Summary die Komponente angezeigt, die nicht übereinstimmt.

```
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    CNL0D0034I2C75  PSU.Slot.2
```

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

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\_%servicetag%\_%timestamp%.log.

```
X:\Dell\scv>cd scvapp
X:\Dell\scv\scvapp>cd logs
X:\Dell\scv\scvapp\logs>dir
 Volume in drive X is Boot
 Volume Serial Number is D60A-0DC2

 Directory of X:\Dell\scv\scvapp\logs
09/16/2020  10:09 AM    <DIR>    .
09/16/2020  10:09 AM    <DIR>    ..
09/16/2020  10:10 AM           506 SCVLog_FRH89V2_2020_09_16_10_09_37.log
               1 File(s)      506 bytes
               2 Dir(s)   520,667,136 bytes free

X:\Dell\scv\scvapp\logs>notepad SCVLog_FRH89V2_2020_09_16_10_09_37.log
```

Abbildung 6. Überprüfen der Protokolle mit WinPE

# Secured Component Verification auf Linux

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

## Themen:

- Ausführen von SCV auf Linux
- Anzeigen der SCV-Protokolle unter Linux

## Ausführen von SCV auf Linux

1. Laden Sie die SCVTools von der Seite [Treiber und Downloads](https://www.dell.com/support) 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 -zxf DellEMC-SCV-Web-LX-X.X.X-XXXX_XXX.tar.gz`.

```
[root@auvcetillem1m1 Downloads]# tar -zxf 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 ismroutil-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... #####
Preparing... #####
Updating / installing...
  1:scv-2.0.0-136.el8 #####
[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.

- Nachdem das System die SCV-Anwendung erfolgreich ausgeführt hat, sollte das Ergebnis `scv validateSystemInventory: Match` angezeigt werden.

```
[root@localhost ~]# scv ValidateSystemInventory -r 192.168.1.10 -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): 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 Comparison Result : Match

Refer Detailed Report File at : /root/scvapp/out/SCV_CommandExecutionReport_FL8WFZ3_2024_06_17_20_07_36.txt
```

#### Abbildung 9. Ausführen des Validierungsbefehls mit erfolgreichem Ergebnis

- 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 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 : Mismatch  

Overall Comparison Result : Mismatch  

-----  

Inventory Mismatch Summary  

-----  

Added Components Summary:  

  HardDrive 23E0A08BTC88 Disk.Bay.5:Enclosure.Internal.0-1  

  PowerSupply CNL0D003412C75 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,LT0N",  

      "SerialNumber": "CNL0D003412C75"  

    }  

  ]  

}  

-----  

Matched Components  

-----  

{  

  "Baseboard": [  

    {  

      "ComponentRegistryOID": "2.23.133.18.3.1",  

      "ComponentClass": "0x00030003",  

      "CertificateIdentifier": "Unknown",  

      "HardwareVersionNumber": "A01",  

      "Location": "1",  

      "Manufacturer": "Dell Inc.",  

      "Model": "0HPR40",  

      "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

## Anzeigen der SCV-Protokolle unter Linux

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

```
[root@localhost scv] # vi ./scvapp/logs/SCVLog_RtSTC21_2020_09_15_05_55_28.log
```

# 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.

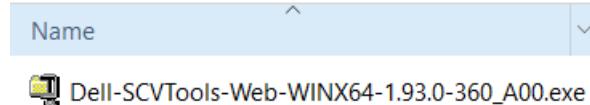


Abbildung 11. ZIP-Datei des SCV-Installationsprogramms

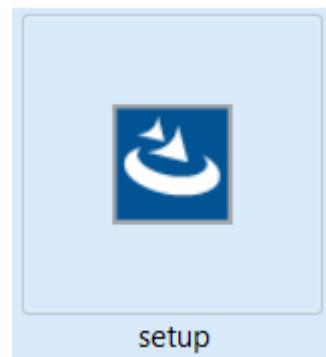
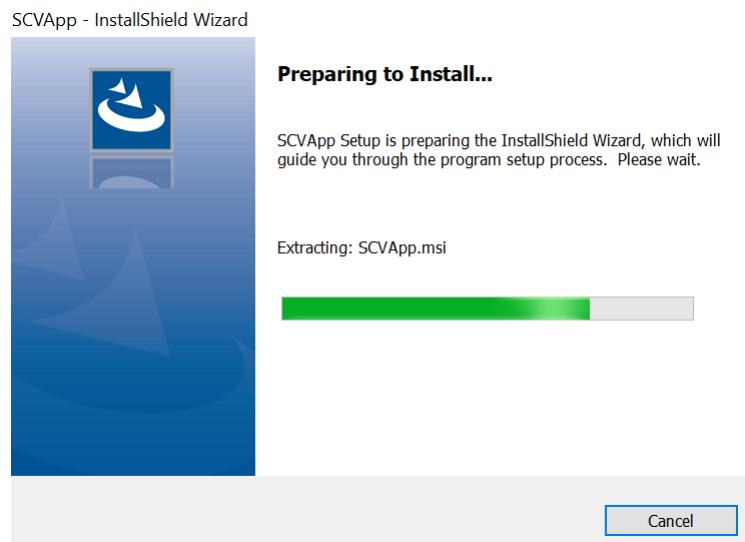


Abbildung 12. SCV-Installationsprogramm

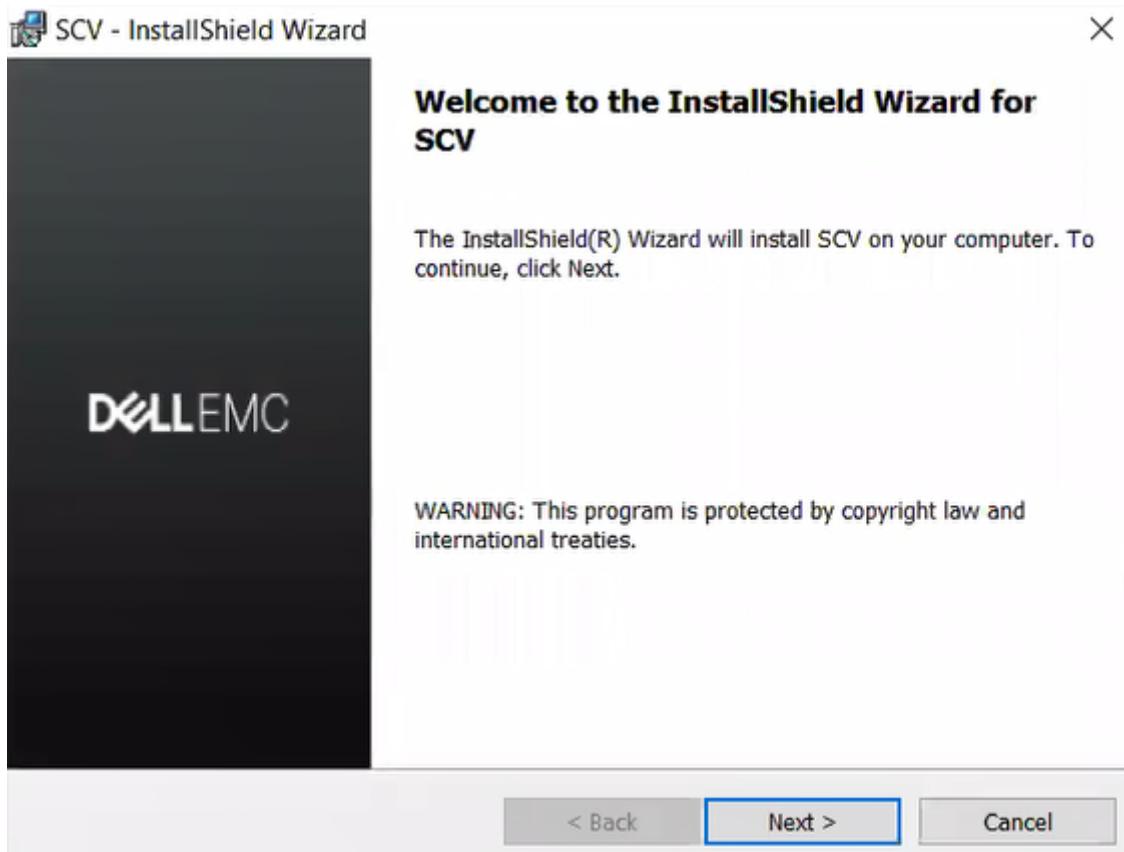
3. Führen Sie die Anwendung aus, um den InstallShield-Assistenten zu starten.



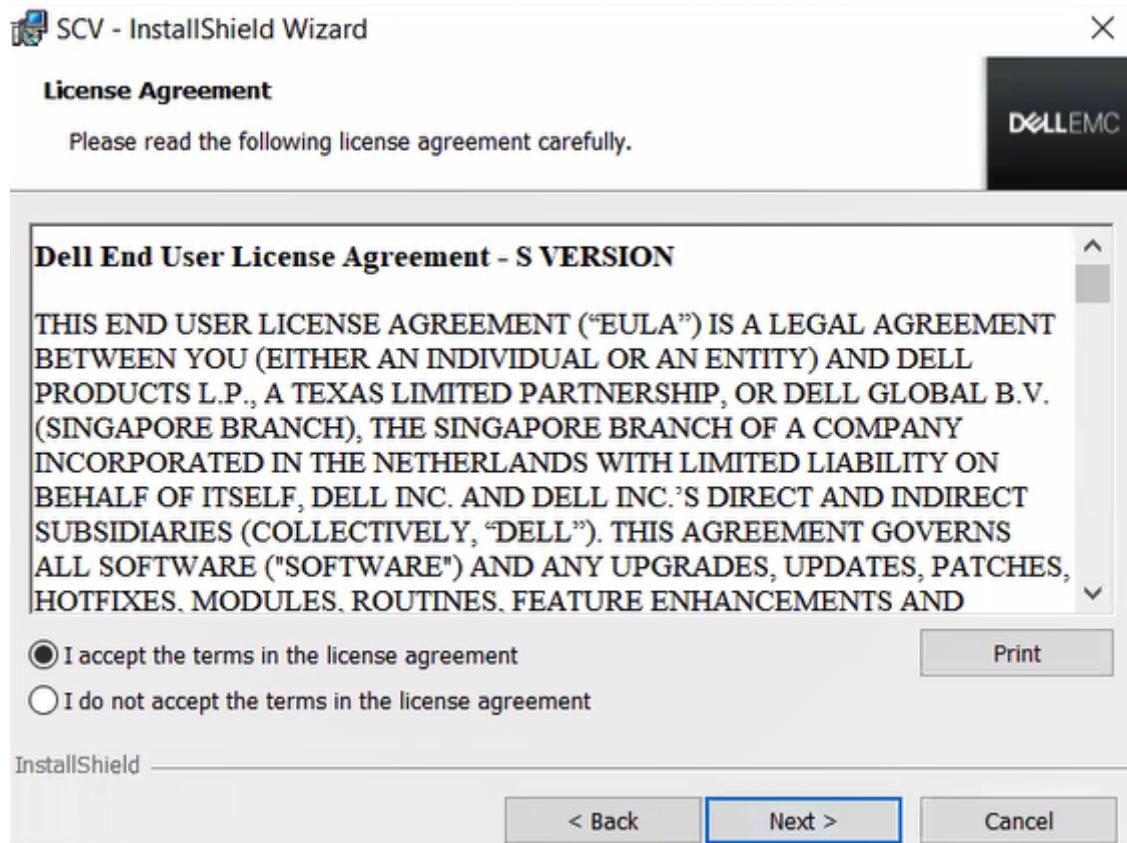
**Abbildung 13. Ausführen des SCV-Installationsprogramms**

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.

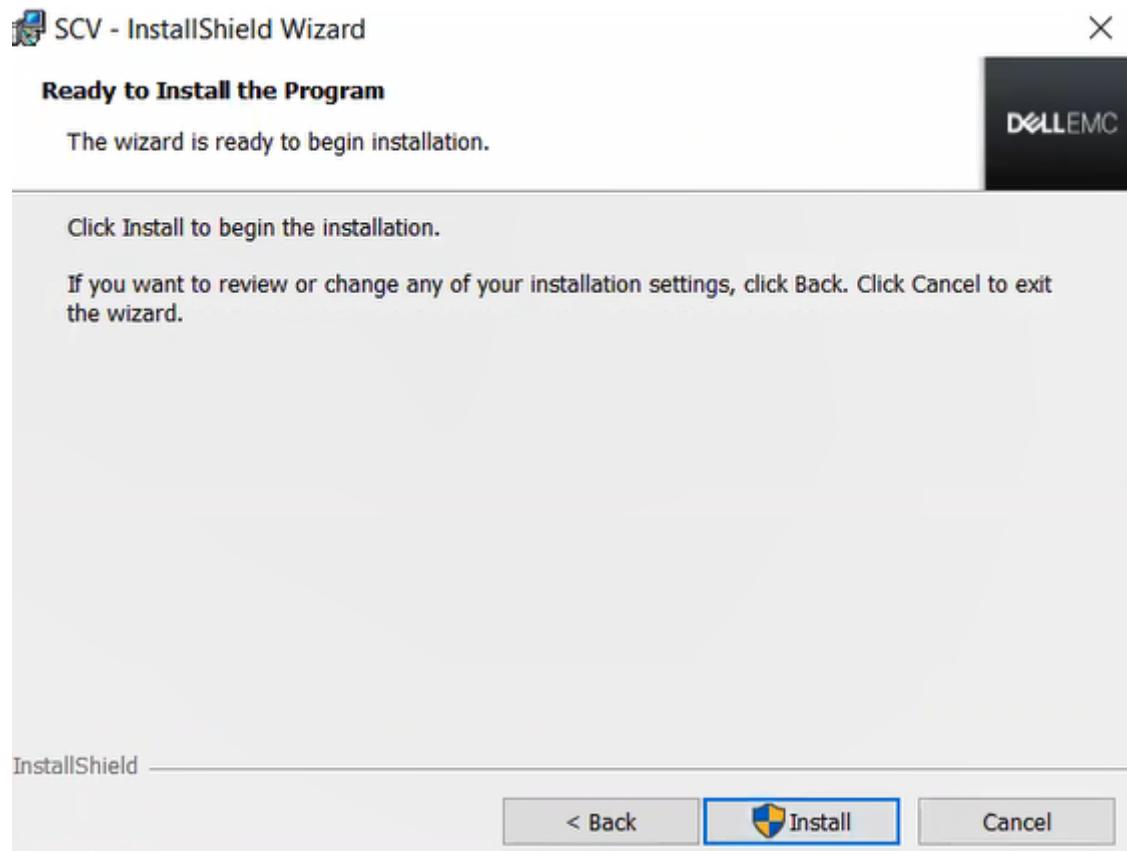


**Abbildung 14. InstallShield-Assistent für SCVApp**

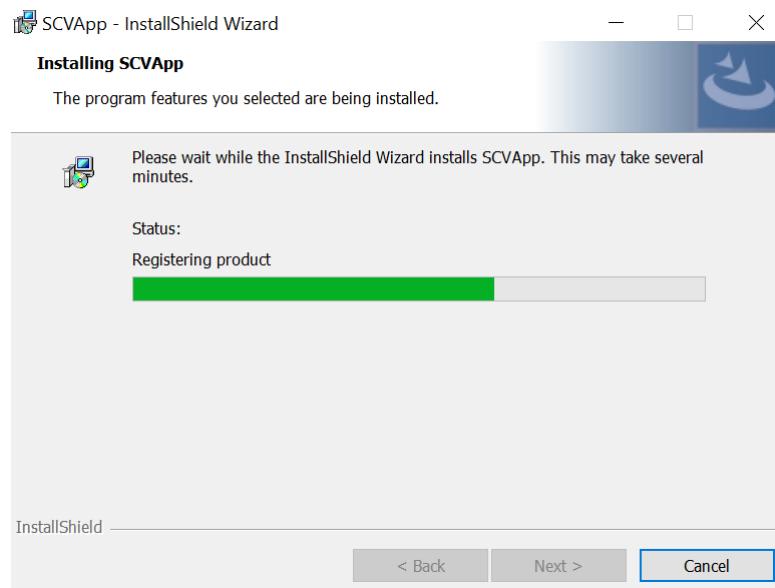


**Abbildung 15. Lizenzvereinbarung für SCVApp**

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

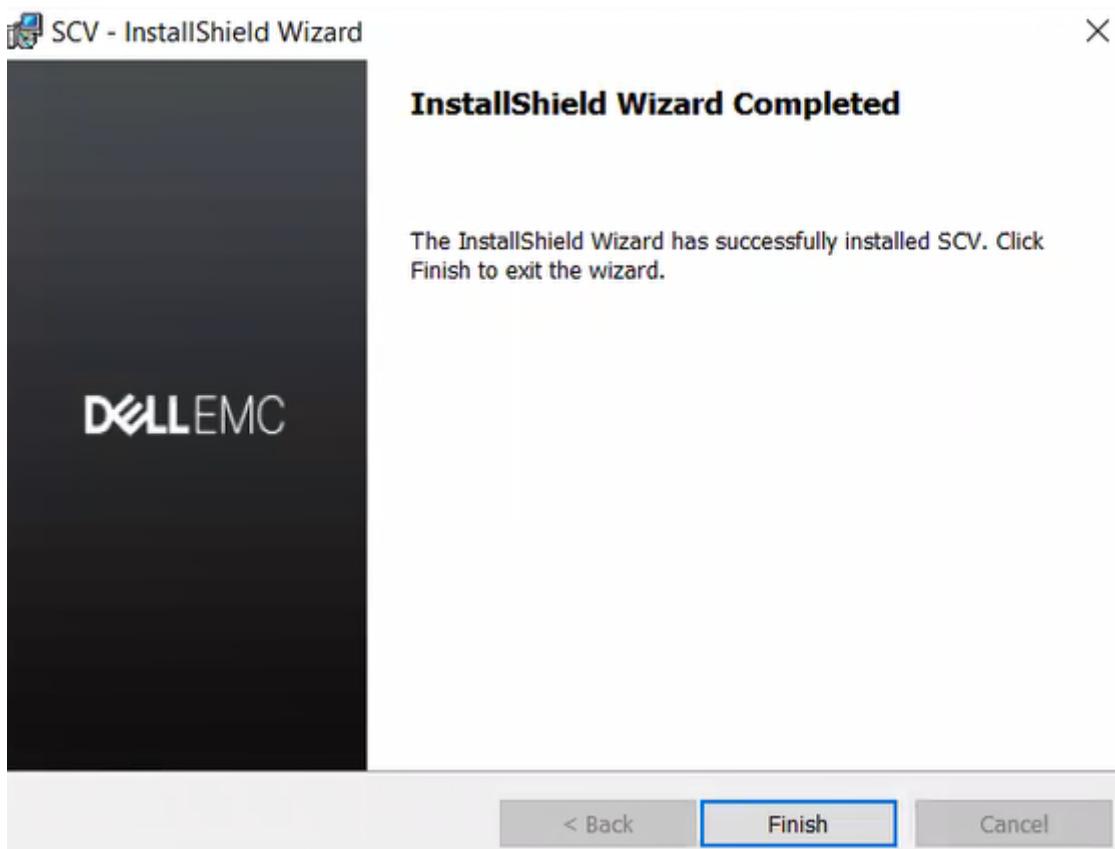


**Abbildung 16. Bereit zur Installation von SCVApp**



**Abbildung 17. SCVApp installieren**

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



**Abbildung 18. 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.

- ① **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.
- ① **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.
- ① **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.
- ① **ANMERKUNG:** Beim Ausführen des Befehls mit der Option `-d <path of the directory>` wird möglicherweise der Fehler „Erfassen des Systembestands: fehlgeschlagen“ beim Ausführen von `scv validatesysteminventory` angezeigt, wenn die Länge des Verzeichnispfads 255 Zeichen überschreitet.

```
C:\Users\Administrator>scv validatesysteminventory
Download SCV Platform Certificate and Delta Certificate(s): 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 CLDBZR3 with System Inventory Service Tag: Match
Inventory Comparison Result : Match

Refer Detailed Report File at : C:\Users\Administrator\scvapp\out\SCV_CommandExecutionReport_CLDBZR3_2024_06_17_16_44_42.txt
```

**Abbildung 19. 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.

```
C:\Users\Administrator>scv validatesysteminventory
Download SCV Platform Certificate and Delta Certificate(s): 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 CLDBZR3 with System Inventory Service Tag: Match
Inventory Comparison Result : MisMatch

-----
Inventory MisMatch Summary
-----
Added Components Summary:
  HardDrive      SJB5N7040I2405V33      Disk.Bay.4:Enclosure.Internal.0-1
  HardDrive      SJB5N7040I2405V2Z      Disk.Bay.5:Enclosure.Internal.0-1
  HardDrive      PHLN1142018X1P6AGN     Disk.Bay.3:Enclosure.Internal.0-1
  HardDrive      PHLN1142015J1P6AGN     Disk.Bay.2:Enclosure.Internal.0-1
  HardDrive      PHLN1142018Z1P6AGN     Disk.Bay.1:Enclosure.Internal.0-1
  HardDrive      PHLN114201751P6AGN     Disk.Bay.0:Enclosure.Internal.0-1
```

**Abbildung 20. Ausführen des Validierungsbefehls mit 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": "0M1CCS",
      "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": "56CSNA0RA02805"
    }
  ],
  "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_LT0N",
      "SerialNumber": "CNL0D002463504"
    }
  ],
  -----
  "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": "M1ICVTCACfugAwIBAgIIAwAAAAAxE+QwCgYIKoZIZj0EAwIwDTEL
      MAkGAIUEBhMCQ04xEtAPBglVBAgMCFNoyW5na6FpMREw
    }
  ]
}

```

Abbildung 21. 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 Alternative 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": "0NIC5",
      "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": "DDR3 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_LT0N",
      "SerialNumber": "CNL0D0024635D4"
    }
  ],
  "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": "MIIICVTCAfugAwIBAgIIAwAAAAAx+EQwCgYIKoZIZj9EAwIwDTELMAkGA1UEBhMCQ04xETAPBgNVBAgMCEfNoYh5nafpMREwDwYDVQQHDahTa
    }
  ]
}

```

Abbildung 22. Erwartete und erkannte Details für nicht übereinstimmende Komponente

# 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.

```
C:\Users\Administrator>scv validatesysteminventory -r <iDRAC IPv4/IPv6[] address> -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): 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 7Z67YX3 with System Inventory Service Tag: Match
Inventory Comparison Result : Match

Refer Detailed Report File at : C:\Users\Administrator\scvapp\out\SCV_CommandExecutionReport_7Z67YX3_2024_06_04_18_44_42.txt
```

Abbildung 23. 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 <iDRAC IPv4/IPv6[] address> -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): 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 Comparison Result : Match

Refer Detailed Report File at : X:\Dell\scv\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2024_06_17_16_38_26.txt
```

Abbildung 24. 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 ~]# scv ValidateSystemInventory -r 192.168.1.10 -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): 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 Comparison Result : Match

Refer Detailed Report File at : /root/scvapp/out/SCV_CommandExecutionReport_FL8WFZ3_2024_06_17_20_07_36.txt
```

**Abbildung 25. Remoteausführung des Validierungsbefehls unter Linux mit erfolgreichem Ergebnis**

# 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	
<b>Beschreibung</b>	Verwenden Sie den folgenden Befehl, um weitere Informationen über SCV und die Ausführung zu erhalten.
<b>Zusammenfassung</b>	<code>scv help</code>

### Ausgabe

```
C:\Users\Administrator>scv help
SCV -- Secured Component Verification

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

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

## Abrufen von Informationen über den Befehl `scv validatesysteminventory`

**Tabelle 5. Weitere Informationen zum Befehl `scv validatesysteminventory`**

scv help validatesysteminventory	
<b>Beschreibung</b>	Verwenden Sie den folgenden Befehl, um weitere Informationen zum Befehl <code>validatesysteminventory</code> und dessen Ausführung zu erhalten.

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

<b>scv help validatesysteminventory</b>	
<b>Zusammenfassung</b>	<code>scv help validatesysteminventory</code>

#### Ausgabe

```
localhost:~/SCVTools # scv help validatesysteminventory
SCV -- Secured Component Verification

Usage: scv 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 user
  -d, --directory=<Directory Path>            Output directory path (MAX 247 Characters). If not specified, Current Working directory will be the output directory.
  -e, --enforceorder                         force component slot location comparison along with the serial number comparison.
  -D, --debug                                Enable Debug log level

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

<b>scv validatesysteminventory -r &lt;IPv4/IPv6 address&gt; -i</b>	
<b>Beschreibung</b>	Verwenden Sie den folgenden Befehl, um eine Remoteverbindung zu einer bestimmten Managementkonsolen-IP herzustellen und den Bestand zu validieren.
<b>Zusammenfassung</b>	<code>scv validatesysteminventory -r &lt;IPv4/IPv6 address&gt; -i</code>
<b>Eingabe</b>	<ul style="list-style-type: none"> <li>• <code>-r &lt;IPV4/IPV6 address&gt;</code></li> </ul>

#### Ausgabe

```
C:\Users\Administrator>scv validatesysteminventory -r 192.168.1.73 -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): 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 Comparison Result : Match
```

# 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	
<b>Beschreibung</b>	Verwenden Sie den folgenden Befehl, um eine Verbindung mit einer Managementkonsolen-IP über einen bestimmten Port herzustellen und den Bestand zu validieren.
<b>Zusammenfassung</b>	scv validatesysteminventory -r <IPv4/IPv6 address:Port> -i
<b>Eingabe</b>	• -r <IPV4/IPv6 address>

# Übereinstimmung des Komponentenspeicherorts gewährleisten und Bestandsvalidierung

Tabelle 8. Übereinstimmung des Komponentenspeicherorts gewährleisten

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

## Ausgabe

```
C:\Users\Administrator>scv validatesysteminventory -r 192.168.1.10 -i --enforceorder
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): 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 Comparison Result : Match
Refer Detailed Report File at : C:\Users\Administrator\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2024_06_17_17_27_40.txt
```

# SCV-Version abrufen

Tabelle 9. Version von SCV abrufen

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

## Ausgabe

```
C:\Users\Administrator>scv version
SCV version 1.93.0
Copyright(c) 2020 - 2024 Dell Inc.
All Rights Reserved.
```

## Anzeigen des Zertifikatkennungswerts in der Konsole oder Umleiten an eine Datei

Tabelle 10. Anzeigen oder Umleiten des Zertifikatkennungswerts

scv extractcert	
<b>Beschreibung</b>	Verwenden Sie den folgenden Befehl, um den Wert für die Zertifikatkennung in der Konsole anzuzeigen oder sie an eine Datei umzuleiten.
<b>Zusammenfassung</b>	scv extractcert -r <IPv4/IPv6 address> -i -c <Component Name> -l <Location> -f <File Name> -d <Directory Name>
<b>Eingabe</b>	<ul style="list-style-type: none"> <li>• --remoteip &lt;IPV4/IPV6 address&gt;</li> <li>• --component &lt;Component_name&gt;</li> <li>• --location &lt;Location_name&gt;</li> <li>• --file &lt;File_name&gt;</li> <li>• --directory &lt;Directory_name&gt;</li> </ul>

### Ausgabe

```
X:\Dell\scv>scv extractcert -r 192.168.0.100 -c iDRAC -l 1 -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
-----BEGIN CERTIFICATE-----MIICXzCAgagAwIBAgIIBAAAAAAaghswCgYIKoZIzj0EAwIwcjELMAkGA1UEBhMCQ04xEADOBgNVBAgMB1RpYW5qaW4xEADOBgNV
BACMB1RpYW5qaW4xEADOBgNVBAoMB0ZveGNvbmr4xDTALBgNV8AsMBFBST0qxHjAcBgNVBAMFTBGQ1AwMC05NzQxLTC00kITmjmNzAeFw0yMzA0MTIwMDI0MzJaF
w00Mja2MTEwMDI0MzJaMH8xCzAjbGVBYTA1VTM04wDAYDVQIDAVUZXhhczETMBEGA1UEBwVKUm91bmQgUm9jaZfMB0GA1UEGwURGVsbCBUZNobm9sb2dpZXM
gs5SwjLjE0MAwGA1UECwwFSURSQUmxGjAYBgNVBAMMEWVjojhoJcyOmVkojIzOmE4MFkwEwYHkoZIzj0CAQYIKoZIzj0DAQcDQgAEX+xzOMoLfbL7Ar1FFimSXKR4/m
cSL+7pZz1hML5MDKU2eqFHcNg05KxxBrCGky0wVvxrhUATSSdbUrAEYyN5+6NSMhCwCQYDVR0TBAIwADALBgNVHQ8EBAMCBeAwHQYDVR01BBYwFAYIKwYBQUHawE
GCCsGAQUFBwMCMB0GA1UdDgQWBQ/g68GLh21ReExQMNbYupAEk631TAfbgNVHSMEGDAwgBryuNpU7GgY0Vw1MaBv81f/Pxx/eTAKBggqhkjOPQQDAgNHADBEAiAyP
0FDJ2+nuJicZ2/w49RpQuhBcxFVp6hAwhK7hLntwIgNkWr48x501Pmk47N0951Mw5UHF50FQE7JihTSVtu6ow-----END CERTIFICATE-----
X:\Dell\scv>
```

Abbildung 26. Anzeigen des Zertifikatkennungswerts in der Konsole

```
C:\Users\Administrator>scv extractcert -r 192.168.0.100 -c iDRAC -l 1 -f abc.crt -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
```

Abbildung 27. Schreiben des Zertifikatkennungswerts in eine Datei

```
C:\Users\Administrator>scv extractcert -r 000 000.7.7 -c idrac -l 1 -i --debug
Username: root
Password:
Extracting SCV Platform Certificate and Delta Certificate(s): Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Collecting certificate inventory: Pass
SCV Application Support for the certfile : Pass
-----BEGIN CERTIFICATE-----MIICZDCCAmpAuIBAgITAwAAAAA3LbouCgYIKoZTzj0EAwIwdTELMAkGA1UEBhMCQ0IxETAPBgNVBAGNCFNoYw5naGpMREs0wVDVQ0hDAhTaGfuZ3hhuTERMA8GA1UECgwISM522w50ZlMxDTALBgNVBAgMBFBST0QxdHjAcBgNVBAMFTB1VjdW
KC1DRTBDLTERwDUHJigNjAeFwYhMzA2NjYyMjM0MDIaIw0MjAAjMjUyMjM0MDIaIwBxcxAjBglVBAYTA1TMQhxDAYDwQQIDAuV2XhcETMBEGAUUEBwKl9w91bmQglm9jazEFMBGAE1UECgwibGVcbcBUZhllob9s1b2dpZXlgSw5jLjEOMwAgA1UECwF-SURSQUMsGjAYBglVBAw
YEM9a0mNl0mJx0mH0jQ2jg5MfkwEwYHKCZzj0CAYIKoZIzj0M0QcDQgAEIwbgZ75JwS9GXhXk4wASPAwNtjj1PmFFmfbf0F5Bv+GCAMkdm1v0klyNvA7Kqdp4pvnH3ziy5OeRp51og1KNSM4hcwQYDVR0TBA1aDALBgNvH38EBAMCBeAuH0YDwR0LBBywFAYIkwYBQJHAw
YGCxgAQQFBwWCM8BwGAGwDgQMBBFElZnZg+nDAmmeihz/9AVu0DAfBgVHSMEZDAbgFTTQLYLTK1V919h9zyVUcYMMTAkBgghkjhOPQOAgIJgADBGAE1EA/pes51/eULQqbkYTr0ZEGctjuaZkN3RTRGV4ALNBTQDSR8E2JYvvlEu5U24tb/#2j0BkKmBaMa/KZv
/VAA-----END CERTIFICATE-----
```

Abbildung 28. Anzeigen des Zertifikatkennungswerts in der Konsole mithilfe der Debug- oder D-Option

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

**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	<pre>scv mars ./SCVTest.zip ./scvapp/out/marsreport.csv :  ServiceTags,Components,MacAddresses &lt;ServiceTag&gt;,NIC.Embedded.1-1-1,C8:4B:D6:98:93:52 &lt;ServiceTag&gt;,NIC.Embedded.2-1-1,C8:4B:D6:98:93:53 &lt;ServiceTag&gt;,iDRAC,c8:4b:d6:98:93:4c &lt;ServiceTag&gt;,NIC.Embedded.1-1-1,C8:4B:D6:98:93:52</pre>

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

scv mars	
	<ServiceTag>,NIC.Embedded.2-1-1,C8:4B:D6:98: 93:53 <ServiceTag>,iDRAC,c8:4b:d6:98:93:4c

## 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.

SCV 1.93.0 unterstützt PERC 12.2.

## 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

# 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 oder Plattform nicht unterstützt.
14	Die Syntax des Befehls ist falsch.
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 oder 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.

## 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 [Dell Support](#)seite 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](http://www.dell.com/support/idrac)
- iDRAC-Benutzerhandbuch und weitere Handbücher:
  - [www.dell.com/idracmanuals](http://www.dell.com/idracmanuals)
- Weitere Informationen zu PowerEdge-Servern finden Sie in der Dokumentation unter:
  - [www.dell.com/poweredgemanuals](http://www.dell.com/poweredgemanuals)
- Technischer Support von Dell
  - [www.dell.com/support](http://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.