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

Referenzhandbuch für Server und Gehäuse

Mai 2023
Rev. A00

DELL Technologies

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: HINWEIS enthält wichtige Informationen, mit denen Sie Ihr Produkt besser nutzen können.

VORSICHT: ACHTUNG deutet auf mögliche Schäden an der Hardware oder auf den Verlust von Daten hin und zeigt, wie Sie das Problem vermeiden können.

WARNUNG: WARNUNG weist auf ein potenzielles Risiko für Sachschäden, Verletzungen oder den Tod hin.

Inhaltsverzeichnis

Kapitel 1: Übersicht....5
Neue Funktionen hinzugefügt....5
SCV 1.8....5
SCV 1.7....5
SCV 1.6....5
SCV 1.5.1....5
SCV 1.5....6
Secured Component Verification....6
Systemanforderungen....6
Unterstützte Systeme....7
Unterstützte Komponenten....9
Unterstützte URIs....10

Kapitel 2: Secured Component Verification auf WinPE....11
Erstellen eines ISO-Images zum Ausführen von SCV mit WinPE....11
Hinzufügen von SCV zu einem benutzerdefinierten ISO-Image....12
Ausführen von SCV auf WinPE....12
Überprüfen der SCV-Protokolle mit WinPE....14

Kapitel 3: Secured Component Verification auf Linux....15
Ausführen von SCV auf Linux....15
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)....24
Remoteausführung von SCV auf Windows Server 2019 und 2022....24
Remoteausführung von SCV auf WinPE....24
Remoteausführung von SCV auf Linux....25

Kapitel 6: SCV-Befehlsdetails....26
Abrufen von Informationen zum Ausführen von SCV....26
Abrufen von Informationen über den Befehl scv validatesysteminventory....27
Remoteverbindung zu einer Managementkonsole und Validierung von Beständen....27
Remoteverbindung zu einer Managementkonsole mit einem bestimmten Port und Bestandsvalidierung....28
Übereinstimmung des Komponentenspeicherorts gewährleisten und Bestandsvalidierung....28
SCV-Version abrufen....29
Anzeigen des Zertifikatkennungswerts in der Konsole oder Umleiten an eine Datei....29

Kapitel 7: Rückgabecodes....30

Kapitel 8: Wie Sie Hilfe bekommen....31

Kontaktaufnahme mit Dell....31
Support-Dokumente und -Ressourcen....31
Feedback zur Dokumentation....31

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 1,8
- SCV 1.7
- SCV 1.6
- SCV 1.5.1
- SCV 1.5

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:

- 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

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 oder 1.8
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: 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 Systeme

ANMERKUNG: PowerEdge C4140, PowerEdge C6420, PowerEdge C6520 und PowerEdge C6525 werden nur mit SCV 1.5.1 und späteren Versionen unterstützt.

ANMERKUNG: Bevor Sie SCV Version 1.5.1 auf PowerEdge C6420, PowerEdge C6520 oder PowerEdge C6525 ausführen, stellen Sie sicher, dass die iDRAC-Firmware auf Version 5.10.50.00 oder eine neuere Version aktualisiert wird.

- PowerEdge C4140
- PowerEdge C6420
- PowerEdge C6520
- PowerEdge C6525
- PowerEdge C6600
- PowerEdge C6620
- PowerEdge M640
- PowerEdge MX7000-Gehäuse
- PowerEdge MX740c
- PowerEdge MX750c
- PowerEdge MX760c
- PowerEdge MX840c
- PowerEdge R240
- PowerEdge R250
- PowerEdge R340
- PowerEdge R350
- PowerEdge R440
- PowerEdge R450
- PowerEdge R540
- PowerEdge R550
- PowerEdge R640
- PowerEdge R6415
- PowerEdge R650
- PowerEdge R6515
- PowerEdge R6525
- PowerEdge R660
- PowerEdge R660xs
- PowerEdge R6615
- PowerEdge R6625
- PowerEdge R740
- PowerEdge R740xd
- PowerEdge R740xd2
- PowerEdge R7415
- PowerEdge R7425
- PowerEdge R750
- PowerEdge R750xa
- PowerEdge R7515
- PowerEdge R7525
- PowerEdge R760
- PowerEdge R760xa
- PowerEdge R760xd2
- PowerEdge R760xs

- PowerEdge R7615
- PowerEdge R7625
- PowerEdge R860
- PowerEdge R940
- PowerEdge R940xa
- PowerEdge R960
- PowerEdge T140
- PowerEdge T150
- PowerEdge T340
- PowerEdge T350
- PowerEdge T440
- PowerEdge T550
- PowerEdge T560
- PowerEdge T640
- PowerEdge XE2420
- PowerEdge XE8545
- PowerEdge XE8640
- PowerEdge XE9640
- PowerEdge XE9680
- PowerEdge XR11
- PowerEdge XR12
- PowerEdge XR2
- PowerEdge XR4520c
- PowerEdge XR5610
- PowerEdge XR7620
- PowerEdge XR8610t
- PowerEdge XR8620t
- Dell XC Core XC450
- Dell XC Core XC650
- Dell XC Core XC6520
- Dell XC Core XC740xd2
- Dell XC Core XC750
- Dell XC Core XC750xa
- Dell XC Core XC7525
- Dell XC Core XC940 System
- Dell XC Series XC940 Appliance
- Dell XC Core XCXR2
- Dell Precision 7960 Rack
- OEMR R240
- OEMR R340
- OEMR R440
- OEMR R450
- OEMR R540
- OEMR R550
- OEMR XL R640
- OEMR R650
- OEMR R650xs
- OEMR R6515
- OEMR R6525
- OEMR R740xd
- OEMR R740xd2
- OEMR R750
- OEMR R750xa
- OEMR R750xs
- OEMR R7515
- OEMR R7525

- OEMR R840
- OEMR R940xa
- OEMR T140
- OEMR T150
- OEMR T340
- OEMR T350
- OEMR T440
- OEMR T550
- OEMR XL T640
- OEMR XR11
- OEMR XR12
- VxRail E660F
- VxRail S670

Unterstützte Komponenten

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

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.

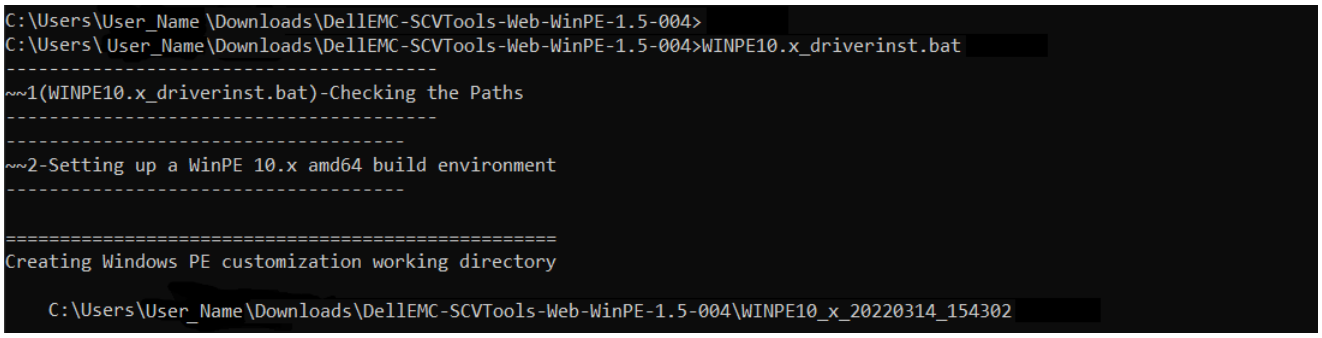

Abbildung 1. Ausführen der Batchdatei über die Eingabeaufforderung

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

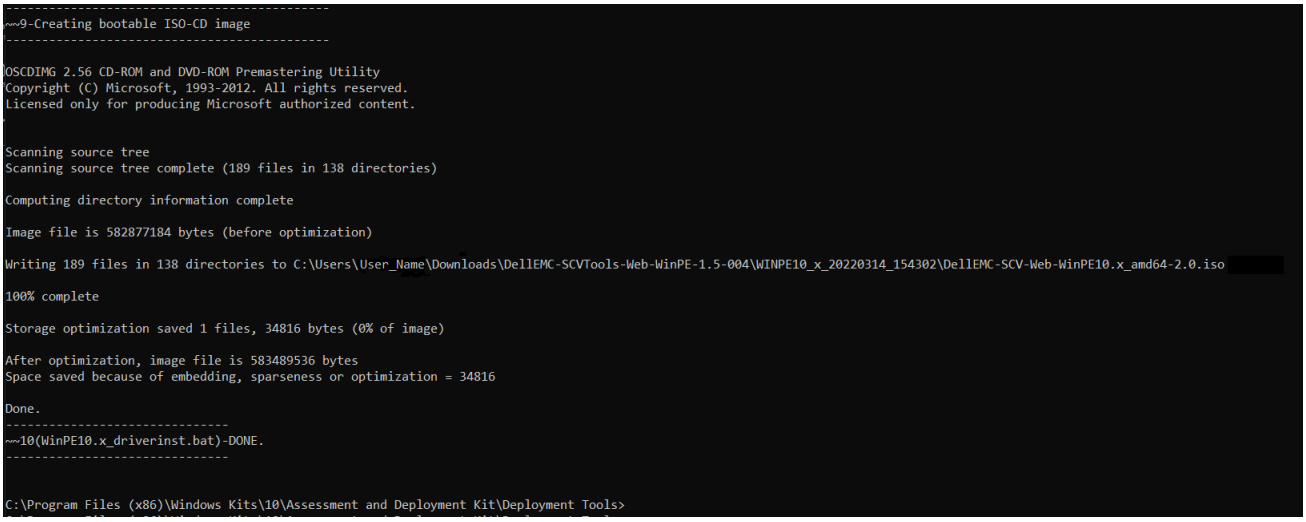

Abbildung 2. Bestätigung für das erfolgreich erstellte ISO-Image

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\OpenSSL** in `X:\Dell\scv`
   c. **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;X:\Dell\scv\openssl;` 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.

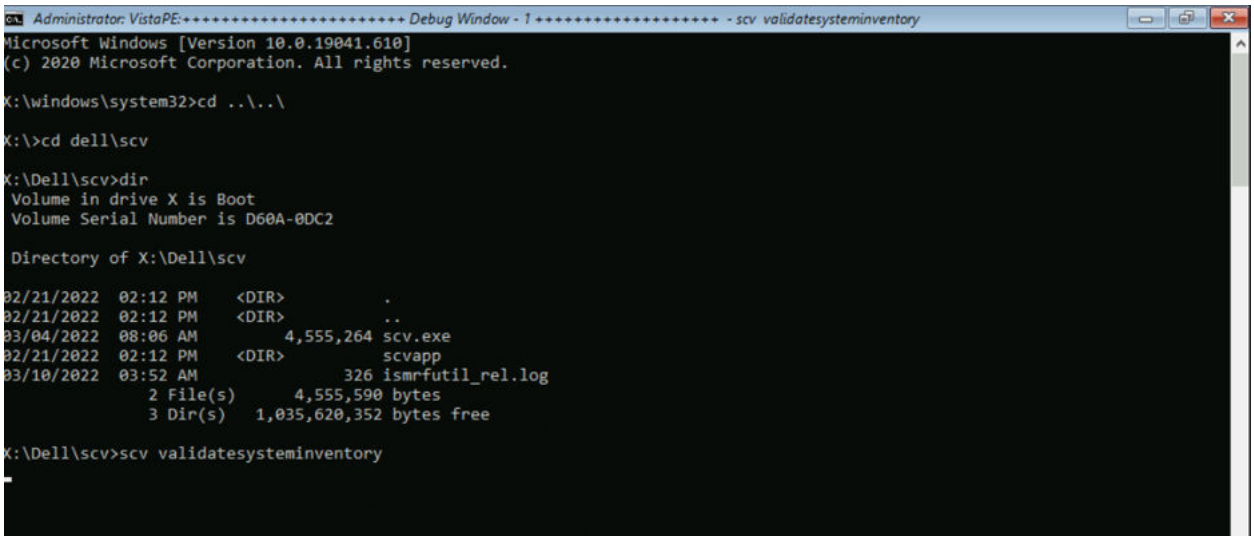

Abbildung 3. Ausführen des Validierungsbefehls

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

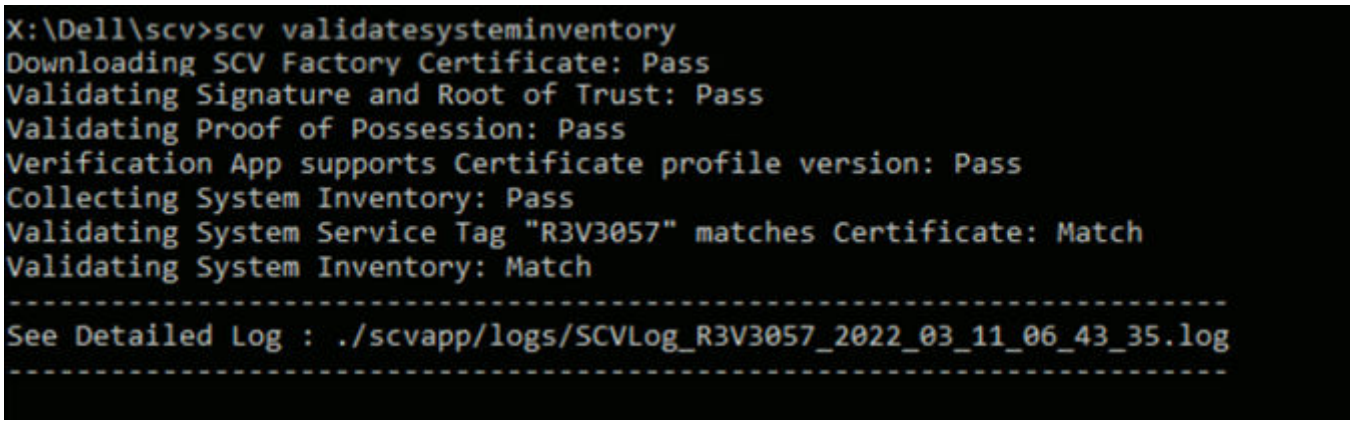

Abbildung 4. Ausführen des Validierungsbefehls mit erfolgreichem Ergebnis

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

```
Mismatch Inventory Summary
--------------------------------------------------------------------------------
Baseboard 1: Mismatch
--------------------------------------------------------------------------------
Checking Component: Baseboard
--------------------------------------------------------------------------------
Baseboard 1: Mismatch
Expected:
{
        "certificate_identifier" : "Unknown",
        "hw_version_number" : "A02",
        "location" : "1",
        "manufacturer" : "Dell Inc.",
        "model" : "0HDV4Y",
        "serial_number" : "CNFCP0015V004L"
}
Detected:
{
        "certificate_identifier" : "Unknown",
        "hw_version_number" : "Unknown",
        "location" : "Unknown",
        "manufacturer" : "Unknown",
        "model" : "Unknown",
        "serial_number" : "Unknown"
}
--------------------------------------------------------------------------------
Overall Baseboard check Status: Mismatch
--------------------------------------------------------------------------------
```

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`.

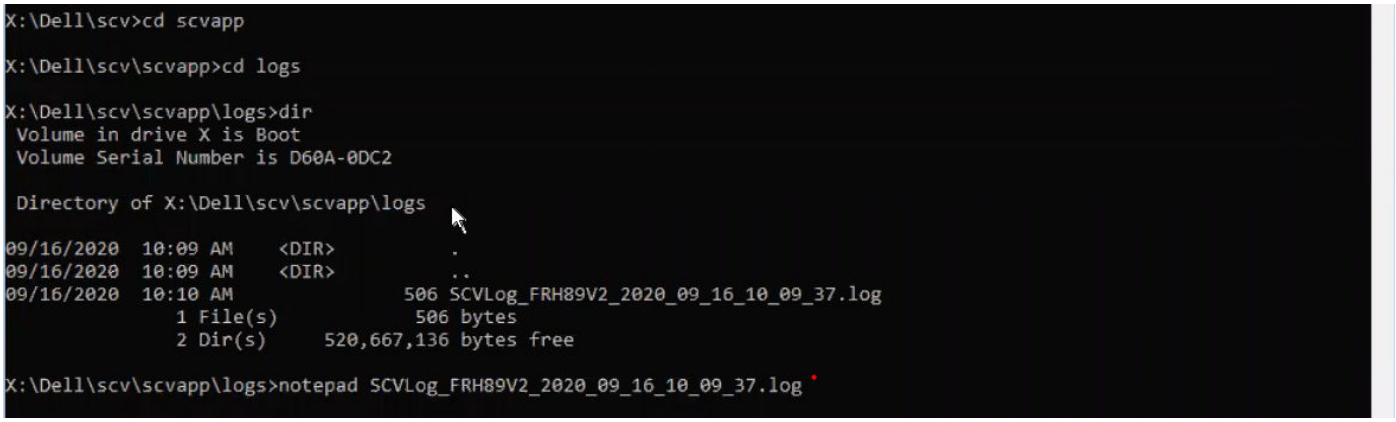

Abbildung 6. Überprüfen der Protokolle mit WinPE

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/supportherunter.
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.

```
[root@localhost SCVTools]# scv validatesysteminventory
Username: root
Password:
Downloading SCV Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "R3V2040" matches Certificate: Match
Validating System Inventory: Match
--------------------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_R3V2040_2022_04_26_18_56_46.log
--------------------------------------------------------------------------------
```

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.

```
Mismatch Inventory Summary
--------------------------------------------------------------------------------
Baseboard 1: Mismatch
--------------------------------------------------------------------------------
Checking Component: Baseboard
--------------------------------------------------------------------------------
Baseboard 1: Mismatch
Expected:
{
        "certificate_identifier" : "Unknown",
        "hw_version_number" : "A02",
        "location" : "1",
        "manufacturer" : "Dell Inc.",
        "model" : "0HDV4Y",
        "serial_number" : "CNFCP0015V004L"
}
Detected:
{
        "certificate_identifier" : "Unknown",
        "hw_version_number" : "Unknown",
        "location" : "Unknown",
        "manufacturer" : "Unknown",
        "model" : "Unknown",
        "serial_number" : "Unknown"
}
--------------------------------------------------------------------------------
Overall Baseboard check Status: Mismatch
--------------------------------------------------------------------------------
```

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.

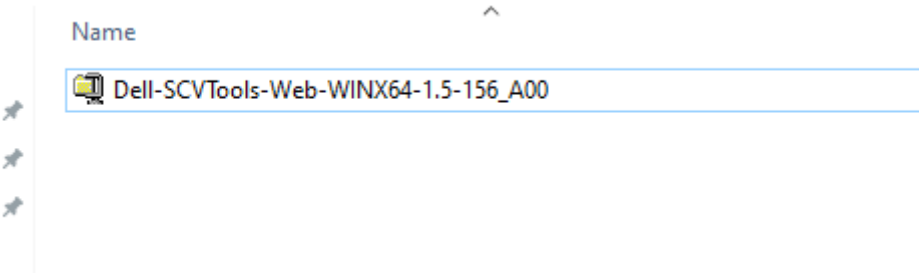

Abbildung 12. ZIP-Datei des SCV-Installationsprogramms

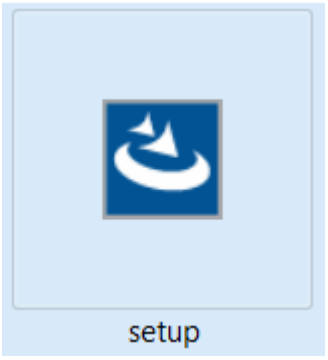

Abbildung 13. SCV-Installationsprogramm

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

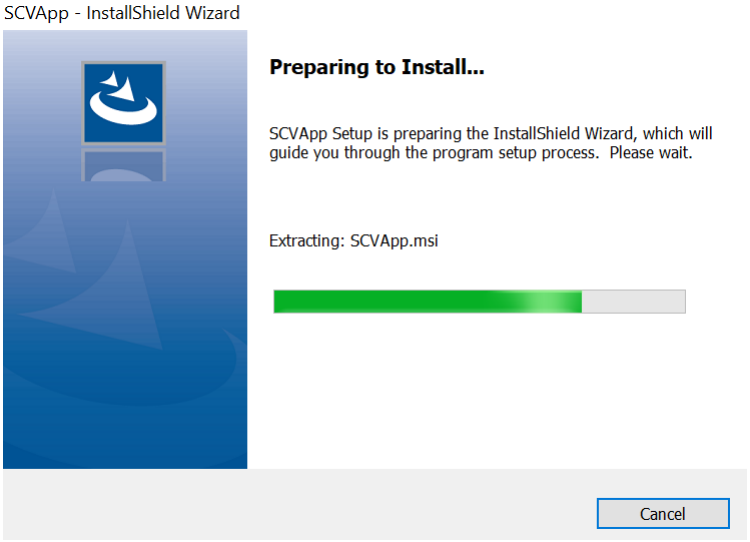

Abbildung 14. Ausführen des SCV-Installationsprogramms

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.

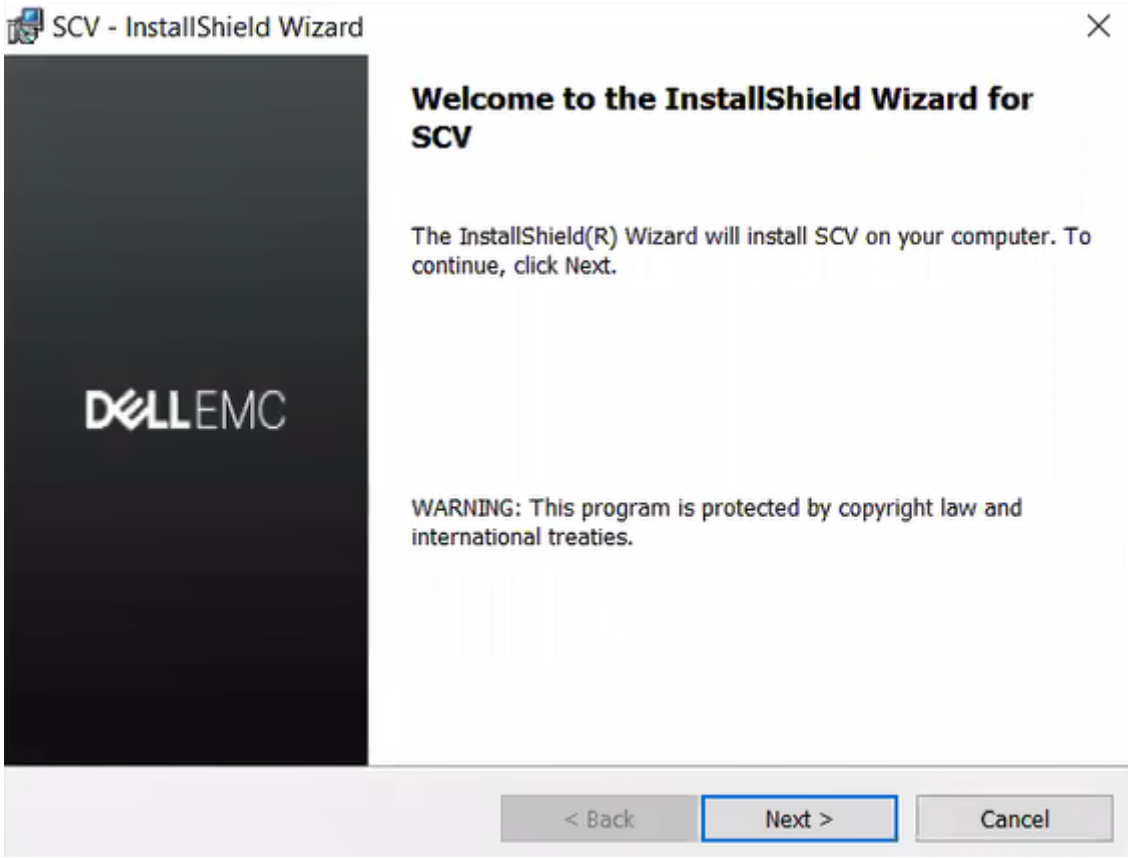

Abbildung 15. InstallShield-Assistent für SCVApp

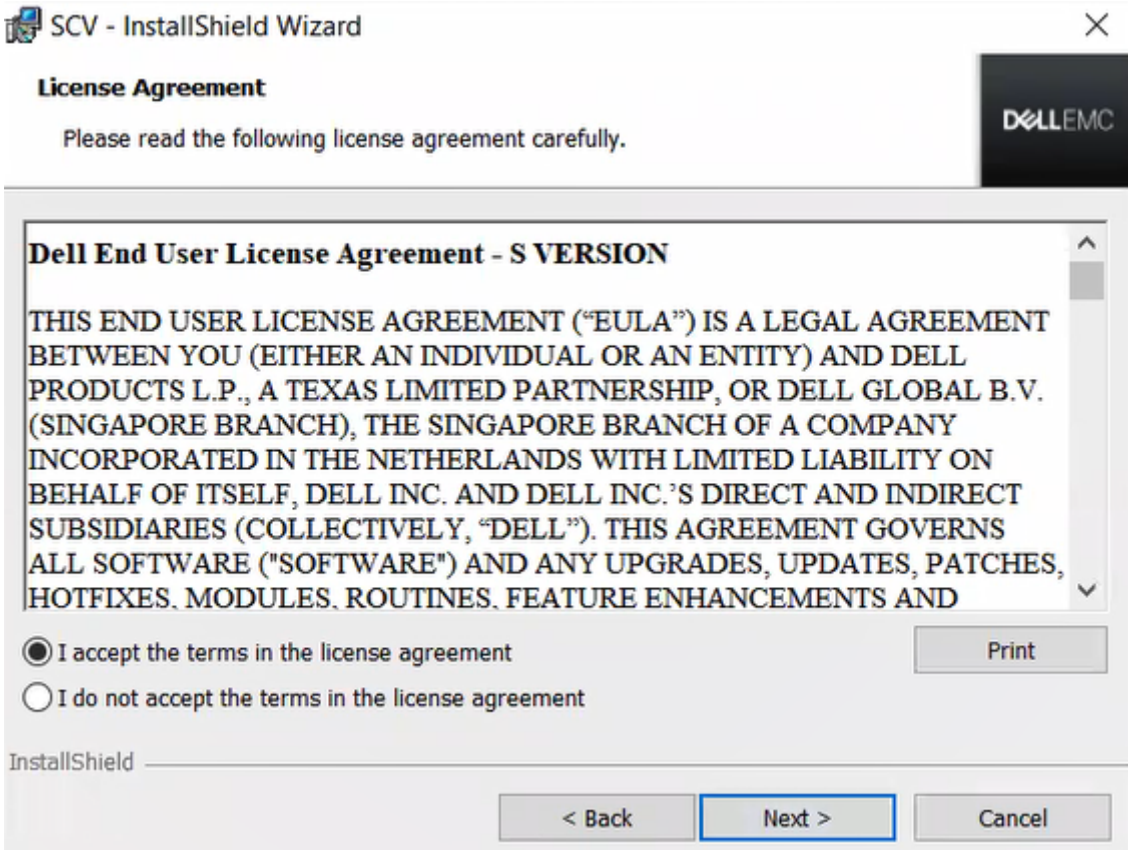

Abbildung 16. Lizenzvereinbarung für SCVApp

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

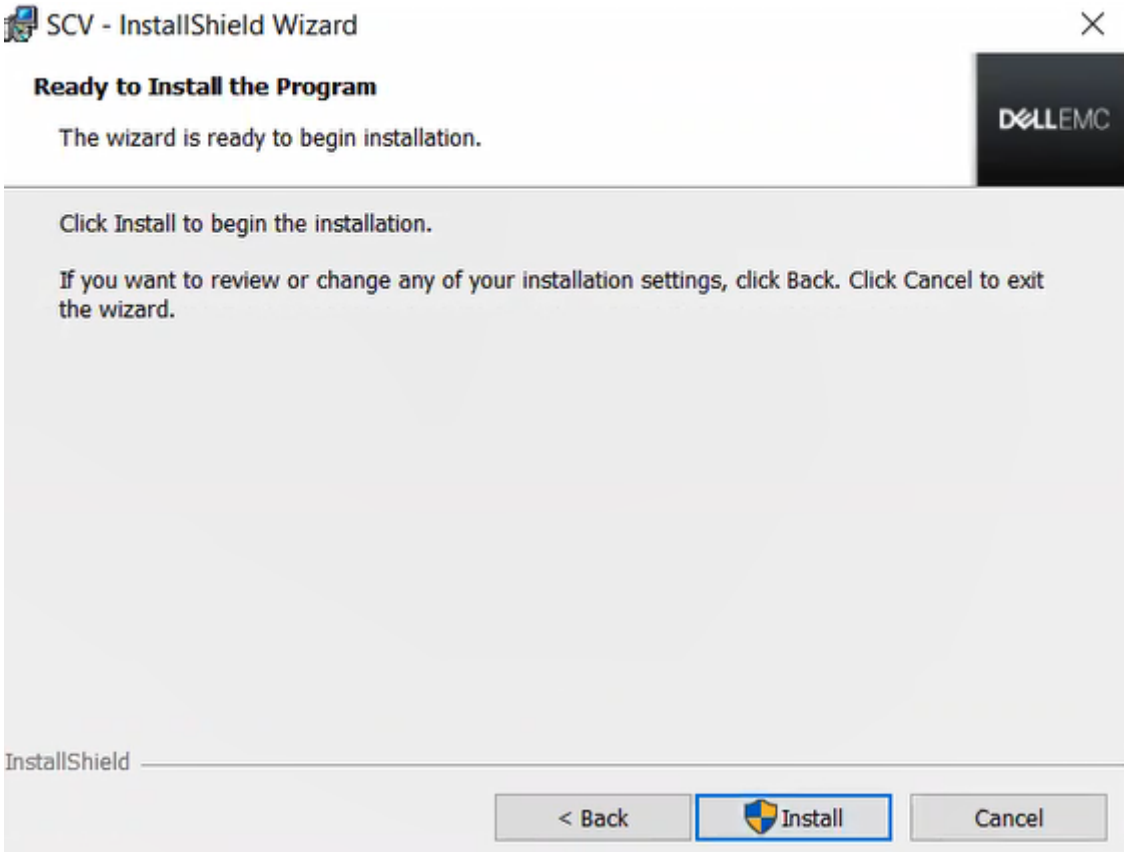

Abbildung 17. Bereit zur Installation von SCVApp

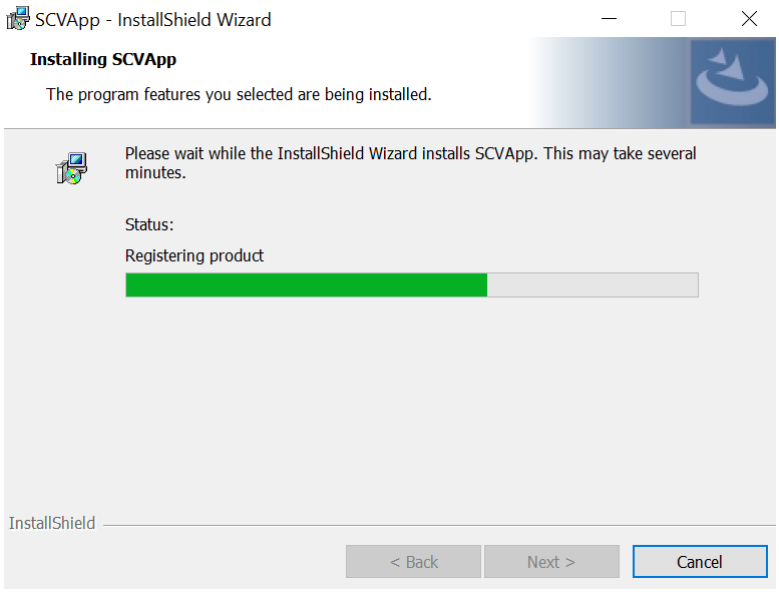

Abbildung 18. SCVApp installieren

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

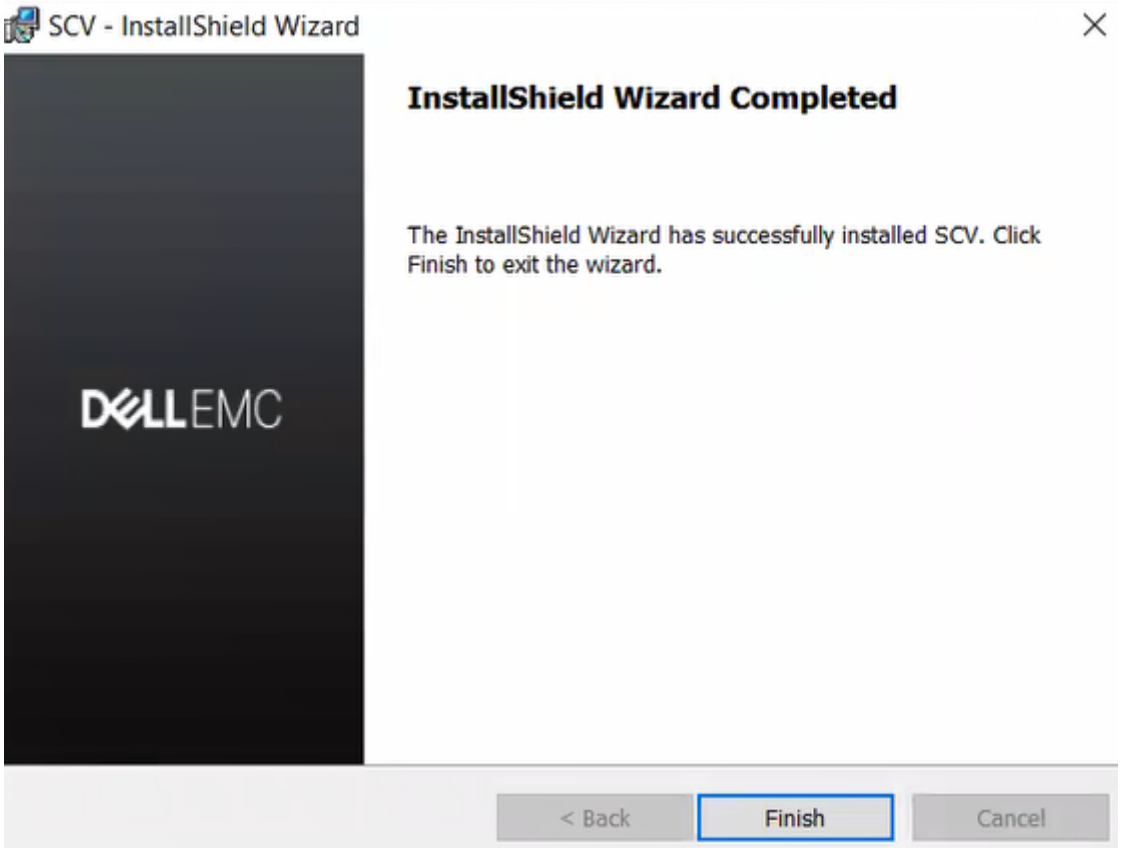

Abbildung 19. SCVApp-Installation abgeschlossen

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 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.

```
X:\Windows\System32>scv validatesysteminventory
Downloading SCV Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "R3V2040" matches Certificate: Match
Validating System Inventory: Match
--------------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_R3V2040_2022_04_26_13_14_37.log
--------------------------------------------------------------------------
```

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.

```
C:\Program Files\DELL\SCVTools>scv validatesysteminventory

Downloading SCV Factory Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "S3S5509" matches Certificate: Match
Validating System Inventory: Mismatch
--------------------------------------------------------------------------
Mismatch Inventory Summary
--------------------------------------------------------------------------
Network 12: Mismatch
--------------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_S3S5509_2022_03_11_21_09_49.log
--------------------------------------------------------------------------
```

Abbildung 21. Validierung mit nicht erfolgreichem Ergebnis

```
Network 12: Mismatch
Expected:
{
        "certificate_identifier" : "NIC.Embedded.2-1-1",
        "hw_version_number" : "Unknown"
        "location" : "F4:02:70:BF:8F:F5",
        "manufacturer" : "Broadcom Corp",
        "model" : "Broadcom Gigabit Ethernet BCM5720",
        "serial_number" : "Unknown",
}
Detected:
{
        "certificate_identifier" : "Unknown",
        "hw_version_number" : "Unknown"
        "location" : "Unknown",
        "manufacturer" : "Unknown",
        "model" : "Unknown",
        "serial_number" : "Unknown",
}
--------------------------------------------------------------------------------
Overall Network check Status: Mismatch
--------------------------------------------------------------------------------
```

Abbildung 22. 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> -u <iDRAC username> -p <iDRAC password>` aus, um den Validierungsprozess zu starten.

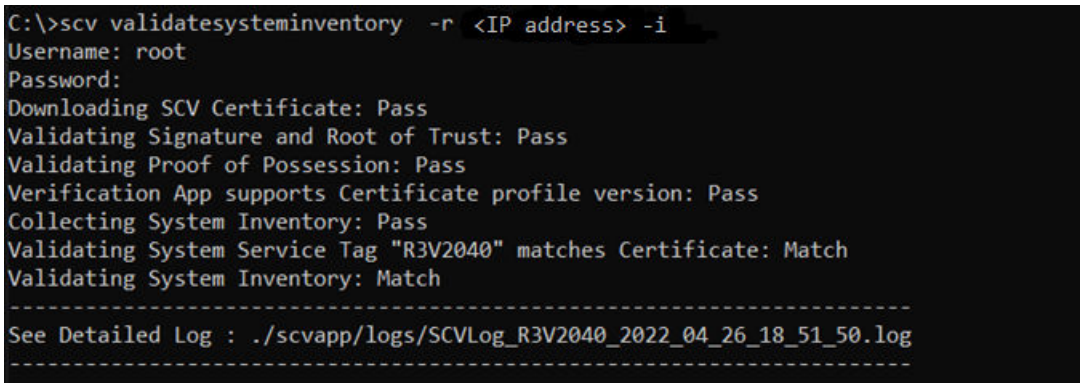

Abbildung 23. Remoteausführung des Validierungsbefehls unter Windows mit erfolgreichem Ergebnis

ANMERKUNG: Das obige Beispiel ist für die Ausführung des Validierungsbefehls im interaktiven Modus. Die Parameter `-p` und `-u` sind nicht erforderlich.

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> -u <iDRAC username> -p <iDRAC password>` aus, um den Validierungsprozess zu starten.

```
X:\Dell\scv>scv validatesysteminventory -r <IP address> -i
Username: root
Password:
Downloading SCV Factory Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "S3S5526" matches Certificate: Match
Validating System Inventory: Match
--------------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_S3S5526_2022_03_11_21_28_06.log
```

Abbildung 24. Remoteausführung des Validierungsbefehls unter WinPE mit erfolgreichem Ergebnis

ANMERKUNG: Das obige Beispiel ist für die Ausführung des Validierungsbefehls im interaktiven Modus. Die Parameter `-p` und `-u` sind nicht erforderlich.

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> -u <iDRAC username> -p <iDRAC password>` aus, um den Validierungsprozess zu starten.

```
[root@localhost SCVTools]# scv validatesysteminventory -r <IP address> -i
Username: root
Password:
Downloading SCV Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "R3V2040" matches Certificate: Match
Validating System Inventory: Match
--------------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_R3V2040_2022_04_26_18_56_46.log
--------------------------------------------------------------------------
```

Abbildung 25. Remoteausführung des Validierungsbefehls unter Linux mit erfolgreichem Ergebnis

ANMERKUNG: Das obige Beispiel ist für die Ausführung des Validierungsbefehls im interaktiven Modus. Die Parameter `-p` und `-u` sind nicht erforderlich.

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 1. Abrufen von weiteren Informationen über SCV

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

Ausgang

```
C:\Users\Administrator>scv help

SCV -- Secured Component Verification

Syntax:
scv <subcommand> <options> [-d <directory>]
scv <subcommand> <options> [-r <target IP> -u <username> -p <password>] [-d <directory>]
scv <subcommand> <options> [-r <target IP> -i]

NOTE:
- "-r", "-u" and "-p" options are not required when scv is running on Host OS.
- Use the "-d" option to specify the output directory name. If not specified,
  by default the working directory is set as the output directory.
- The "-i" option allows you to interactively enter the username and password.

The detailed logs collected are available in: directory->scvapp->logs folder.
The list of available SCV subcommands:
- version
- ValidateSystemInventory

To display more information about a specific subcommand:
- scv help <subcommand>


C:\Users\Administrator>
```

Abrufen von Informationen über den Befehl scv validatesysteminventory

Tabelle 2. Weitere Informationen zum Befehl scv validatesysteminventory

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

Ausgang

```
C:\Users\Administrator>scv help validatesysteminventory

SCV -- Secured Component Verification

Syntax:
scv ValidateSystemInventory [-r <target IP> -u <username> -p <password>] [-d <directory>] [--enforceorder]
scv ValidateSystemInventory [-d <directory>] [--enforceorder] [-r <target IP> -i]

NOTE:
- "-r", "-u" and "-p" options are not required when scv is running on Host OS.
- Use the "-d" option to specify the output directory name. If not specified,
  by default the working directory is set as the output directory.
- "--enforceorder" option indicates to additionally compare the component slot location along with the serial number.
- The "-i" option allows you to interactively enter the username and password.

The detailed logs collected are available in: directory->scvapp->logs folder.
Description:
Downloads SCV factory certificate,
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 3. Remotevalidierung eines bestimmten Bestands

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> -u <UserName> -p <Password>`
Eingabe	• `-r` – IPv4-/IPv6-Adresse • `-u` – Nutzername • `-p` – Kennwort

Ausgabe

```
C:\Users\Administrator>scv validatesysteminventory -r <IP address> -u root -p calvin
Downloading SCV Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "GD3M8F3" matches Certificate: Match
Validating System Inventory: Match
---------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_GD3M8F3_2022_06_17_09_21_10.log
---------------------------------------------------------------------
```

Remoteverbindung zu einer Managementkonsole mit einem bestimmten Port und Bestandsvalidierung

Tabelle 4. Bestandsvalidierung über einen bestimmten Port

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> -u <UserName> -p <Password>`
Eingang	• `-r` – IPv4-/IPv6-Adresse • `-u` – Nutzername • `-p` – Kennwort

Übereinstimmung des Komponentenspeicherorts gewährleisten und Bestandsvalidierung

Tabelle 5. Übereinstimmung des Komponentenspeicherorts gewährleisten

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`

Ausgang

```
C:\Users\Administrator>scv validatesysteminventory -r <IP address> -u root -p calvin --enforceorder
Downloading SCV Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "GD3M8F3" matches Certificate: Match
Validating System Inventory: Match
---------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_GD3M8F3_2022_06_17_09_18_03.log
---------------------------------------------------------------------
```

SCV-Version abrufen

Tabelle 6. Version von SCV abrufen

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

Ausgang

```
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 7. Anzeigen oder Umleiten des Zertifikatkennungswerts

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> -u <UserName> -p <Password> -component <Component Name> -l <Location> -f <File Name>`
Eingabe	• `-r` – IPv4-/IPv6-Adresse • `-u` – Nutzername • `-p` – Kennwort • `component` – Komponentenname • `-l` – Speicherort • `-f` – Dateiname

Ausgabe

```
C:\Program Files\DELL\SCVTools>scv extractcert -r <IP address> -u root -p calvin -component iDRAC -location 1
Downloading SCV Certificate: Pass
Extracting Certificate Identifier: Pass
MIICVTCCAfugAwIBAgIIAwAAAAAxQPMwCgYIKoZIzj0EAwIwdTELMAkGA1UEBhMCQ04xETAPBgNVBAgMCFNoYW5naGFpMREwDwYDVQQHDAhTaGFuZ2hhaTERMA8GA1UECgwISW52ZW50ZWMxDTALBgNVBAsMBFBST0QxHjAcBgNV
BAMMFTBJVkMwMC1DRTBDLTEwNUUtNjgyNjAeFw0yMjA3MDUxMzU2NDJaFw00MTA5MDMxMzU2NDJaMHExCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEGA1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMx
DjAMBgNVBAsMBUlEUkFDMRowGAYDVQQDDBF1YzoyYTo3MjozNjoxMjpkODBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABElv0GZsBbrNCmRwwHVbWXBhp13lmqPtiUOqIB0OVr/9rTN66pSZpuNeoeQH3INnuy/x95MML7rM5HOG
UBuG2xmjeTB3MAkGA1UdEwQCMAAwCwYDVR0PBAQDAgXgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAdBgNVHQ4EFgQUYVqWFIGsWmAmri7T2UAx9QcnAu8wHwYDVR0jBBgwFoAU00ES2C0yiFfSPYXvc8lVHMrWGDEw
CgYIKoZIzj0EAwIDSAAwRQIgfcoqKl5UwmmPM5akHJXzz4UvQZye7wOS8+f49eD02TACIQDTyvuShyr4lI1YAWf9qqg88xmkJvuQ0C/yN5u7JinYFw==
```

Abbildung 26. Anzeigen des Zertifikatkennungswerts in der Konsole

```
C:\Program Files\DELL\SCVTools>scv extractcert -r <IP address> -u root -p calvin -component iDRAC -location 1 -f abc.crt
Downloading SCV Certificate: Pass
Extracting Certificate Identifier: Pass
```

Abbildung 27. Schreiben des Zertifikatkennungswerts in eine Datei

7

Rückgabecodes

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

Tabelle 8. 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.

8

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.