

Dell Secured Component Verification **version 1.5, 1.5.1, 1.6, 1.7, 1.8, 1.9, 1.91.0,** **1.92.0, et 1.93.0**

Guide de référence pour les serveurs et les châssis

Remarques, précautions et avertissements

 **REMARQUE** : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

 **PRÉCAUTION : ATTENTION** vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

 **AVERTISSEMENT** : Un AVERTISSEMENT signale un risque d'endommagement du matériel, de blessure corporelle, voire de décès.

Table des matières

Chapitre 1: Présentation.....	5
Nouvelles fonctionnalités ajoutées.....	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
Vérification des composants sécurisés.....	6
Configuration matérielle.....	7
Composants pris en charge.....	8
URI pris en charge.....	8
Chapitre 2: Vérification des composants sécurisés sur WinPE.....	10
Création d'une image ISO pour l'exécution de SCV sous WinPE.....	10
Ajout de SCV à une image ISO personnalisée.....	11
Exécution de SCV sur WinPE.....	11
Comment vérifier les journaux SCV sous WinPE.....	13
Chapitre 3: Vérification des composants sécurisés sur Linux.....	14
Exécution de SCV sur Linux.....	14
Affichage des journaux SCV à l'aide de Linux.....	17
Chapitre 4: Vérification des composants sécurisés sous Windows Server 2019 et 2022.....	18
Installation de SCVApp sous Windows Server 2019 et 2022.....	18
Exécution de SCV sous Windows Server 2019 et 2022.....	21
Chapitre 5: Exécution distante de la vérification des composants sécurisés (SCV).....	25
Exécution distante de SCV sous Windows Server 2019 et 2022.....	25
Exécution distante de SCV sur WinPE.....	25
Exécution de SCV sous Linux.....	25
Chapitre 6: Détails de la commande SCV.....	27
Obtenir des informations sur l'exécution de SCV.....	27
Obtenir des informations sur la commande scv validatesysteminventory.....	27
Connexion distante à une console de gestion et validation de l'inventaire.....	28
Connexion distante à une console de gestion à l'aide d'un port spécifique et validation de l'inventaire.....	29
Vérification de la correspondance de l'emplacement des composants et validation de l'inventaire.....	29
Obtenir la version SCV.....	29
Affichage de la valeur d'un identifiant de certificat sur la console ou redirection de cette valeur vers un fichier.....	30

Chapitre 7: Fonctionnalité SCVApp MARS.....	32
Chapitre 8: Fonctionnalité SPDm.....	34
Chapitre 9: Certificat CA racine SCV.....	35
Chapitre 10: Codes de retour.....	36
Chapitre 11: Obtenir de l'aide.....	37
Contacter Dell.....	37
Documents et ressources de support.....	37
Commentaires sur la documentation.....	37

Présentation

Cette section fournit une présentation de la vérification des composants sécurisés (SCV) et de la configuration matérielle pour l'exécution de l'application sur le système.

Sujets :

- [Nouvelles fonctionnalités ajoutées](#)
- [Vérification des composants sécurisés](#)
- [Configuration matérielle](#)
- [Composants pris en charge](#)
- [URI pris en charge](#)

Nouvelles fonctionnalités ajoutées

Cette section répertorie les nouvelles fonctionnalités ajoutées dans les versions suivantes :

- [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

Les fonctionnalités suivantes ont été ajoutées ou mises à jour dans cette version :

- La dernière version inclut des correctifs de sécurité critiques dans l'application SCV.

SCV 1.92.0

Les fonctionnalités suivantes ont été ajoutées ou mises à jour dans cette version :

- Prise en charge de l'option de débogage pour la commande `scv extractcert`.

SCV 1.91.0

Les fonctionnalités suivantes ont été ajoutées ou mises à jour dans cette version :

- Prise en charge de la fonctionnalité MARS.
- Ajout de la prise en charge SPDM pour la carte NIC Emulex et PERC 12.

 **REMARQUE :** Pour obtenir la liste des systèmes pris en charge pour cette version, consultez les notes de mise à jour.

SCV 1.9

Les fonctionnalités suivantes ont été ajoutées ou mises à jour dans cette version :

- Ajout de la prise en charge de nouveaux serveurs PowerEdge.



REMARQUE : Pour obtenir la liste des systèmes pris en charge pour cette version, consultez les notes de mise à jour.

SCV 1.8

Les fonctionnalités suivantes ont été ajoutées ou mises à jour dans cette version :

- Prise en charge d'un nouveau profil pour les plateformes Cloud qui ne partagent pas les disques durs.
- Prise en charge de la commande `extractcert`.

SCV 1.7

Les fonctionnalités suivantes ont été ajoutées ou mises à jour dans cette version :

- Prise en charge de SLES 15 SP4.
- Prise en charge des serveurs PowerEdge de 16e génération.

SCV 1.6

Les fonctionnalités suivantes ont été ajoutées ou mises à jour dans cette version :

- Prise en charge de Red Hat Enterprise Linux 9.0.

SCV 1.5.1

Les fonctionnalités suivantes ont été ajoutées ou mises à jour dans cette version :

- Prise en charge des serveurs Cloud PowerEdge.
- Prise en charge des serveurs et châssis modulaires PowerEdge (série MX).

SCV 1.5

Les fonctionnalités suivantes ont été ajoutées ou mises à jour dans cette version :

- Prise en charge de SCVTools.
- Prise en charge de Red Hat Enterprise Linux 8.x.
- Prise en charge de SCVApp pour Windows Server 2019 et 2022.

Vérification des composants sécurisés

La vérification des composants sécurisés (SCV) est une offre d'assurance de la chaîne logistique qui vous permet de vérifier que le serveur PowerEdge que vous avez reçu correspond à ce qui a été fabriqué en usine. Afin de valider les composants, un certificat contenant les ID de composants système uniques est généré au cours du processus d'assemblage en usine. Ce certificat est signé dans l'usine Dell et est stocké dans le système. Il est ensuite utilisé par l'application SCV. L'application SCV valide l'inventaire du système par rapport au certificat SCV.

L'application génère un rapport de validation détaillant la correspondance et la non-correspondance de l'inventaire avec le certificat SCV. Elle vérifie également le certificat et la chaîne de confiance, ainsi que la preuve de possession de la clé privée SCV. La mise en œuvre actuelle prend en charge les clients livrés directement et n'inclut pas les scénarios de VAR ou de remplacement de pièce.

L'application SCV exécute les fonctions suivantes :

- Télécharge le certificat SCV stocké dans le système via les API Dell Technology et vérifie le certificat SCV et l'émetteur.
- Valide la clé privée SCV associée à la clé publique SCV dans le certificat SCV.
- Collecte l'inventaire actuel du système.



REMARQUE : Pour obtenir la liste des composants système pris en charge, voir la section [Composants pris en charge](#).

- Compare l'inventaire actuel du système par rapport à l'inventaire dans le certificat SCV.
- Toute modification des composants figurant dans le certificat est identifiée comme une « non correspondance ».

Remarques :

- L'application SCV peut être lancée directement à partir de l'interface utilisateur de l'iDRAC versions 7.10.30.00 et ultérieures, mais il est recommandé de valider vos composants à l'aide de l'application pour une expérience de validation de sécurité optimale.
- SCV valide également les ports du réseau virtuel. Dans les systèmes équipés de cartes NPAR/NPAReP, exécutez l'application SCV avant de les activer.
- Assurez-vous que le module TPM est activé avant d'exécuter l'application SCV. SCV prend en charge le module TPM version 2.0.
- Assurez-vous d'exécuter l'application SCV avant de mapper les appareils de stockage au système.
- Dans les systèmes modulaires, assurez-vous que FlexAddress est désactivé avant d'exécuter l'application SCV.
- Si les ports USB internes et iDRAC sont désactivés, la validation SCV échoue.
- Assurez-vous que tout disque retiré du système s'enregistre dans l'iDRAC ou toute autre interface iDRAC avant d'exécuter la validation SCV. Dans le cas contraire, cette dernière signale des données incorrectes dans le résultat SCV.
- Même lorsque USB-NIC est activé à partir de l'iDRAC, vous devez activer manuellement l'interface réseau dans le système d'exploitation. USB-NIC ne doit pas être désactivé, car il est nécessaire pour la communication intrabande.
- Dans SCV 1.5 avec un certificat 1.0, l'une des entrées du composant TPM (ECC) indique une correspondance avec les détails attendus comme Inconnu, tandis que les détails détectés affichent toutes les informations. Il s'agit d'un comportement attendu, car le certificat 1.0 n'inclut pas les informations ECC.
- SCV ne prend pas en charge les certificats 1.0 à partir de la version 1.93.0.

Configuration matérielle

Tableau 1. Configuration matérielle requise pour l'exécution de SCV

Catégorie	Exigence																	
Plateformes d'exploitation prises en charge	WinPE 10.x, Red Hat Enterprise Linux 9.0, Red Hat Enterprise Linux 8.6, SUSE Linux Enterprise Server 15 SP4, Windows Server 2019 et Windows Server 2022.																	
Versions de firmware	• iDRAC 5.10.30.00 et versions supérieures • OME-M 2.00.00 et versions supérieures • BIOS PowerEdge 2.14.2 et versions supérieures																	
Licences requises	Licence de vérification des composants sécurisés																	
Versions compatibles	<table><tr><th>Version SCV</th><th>Version iDRAC</th></tr><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></table>		Version SCV	Version iDRAC	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
	Version SCV	Version iDRAC																
	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 1.91.0 et les versions ultérieures disposent d'une compatibilité descendante avec n'importe quelle version de l'iDRAC. Toutefois, SCV 1.90.0 et les versions antérieures sont uniquement compatibles avec la version 7.00.30.00 et les versions antérieures de l'iDRAC.																	

- 
REMARQUE : Pour obtenir la liste des systèmes pris en charge pour une version SCV, reportez-vous à la section Systèmes pris en charge des notes de mise à jour.
- 
REMARQUE : Red Hat Enterprise Linux 7.x n'est pas pris en charge par SCV 1.6 et les versions supérieures.
- 
REMARQUE : Dans SCV version 1.5, une non-correspondance du module TPM s'affiche lors de la validation des composants sur un serveur doté d'un ancien firmware iDRAC et BIOS. Avant d'exécuter SCV, assurez-vous que le firmware de l'iDRAC est mis à niveau vers la version 5.10.30.00 et que le firmware du BIOS est mis à niveau vers la version 2.14.2 ou toute version supérieure.

Composants pris en charge

Tableau 2. Composants pris en charge pour les plateformes rack, tour et Cloud

Composants pris en charge pour les serveurs rack, tour et Cloud
Carte de base
Processeur
Mémoire
Alimentation
Disque dur
Carte réseau
iDRAC
Module TPM
Informations sur le système
Cartes complémentaires PCIe

Tableau 3. Composants pris en charge pour le châssis modulaire

Composants pris en charge pour le châssis modulaire
Contrôleur de boîtier
Ventilateur
OpenManage Enterprise Modular
ChassisRCP
PowerSupply
IOModule
M2Drive

-  **REMARQUE :** Le disque SSD PCIe NVMe à connexion directe ne s'affiche pas dans le logement PCIe. Vérifiez la liste des disques durs pour obtenir le disque SSD PCIe.
-  **REMARQUE :** L'inventaire SCV affiche des détails uniquement pour les appareils d'un composant présents dans le système.

URI pris en charge

SCV prend en charge les interfaces de programmation d'applications (API) pour accéder aux informations à l'aide d'un client API. Pour plus d'informations sur l'utilisation des API, voir le Guide de l'API Redfish iDRAC9 sur developer.dell.com. Vous trouverez ci-dessous la liste des URI et des méthodes prises en charge :

- **Télécharger les certificats SCV**

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

Exemple de réponse

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

- **Télécharger l'inventaire SCV**

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

Exemple de réponse sur l'iDRAC

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

Exemple de réponse sur les systèmes MX

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

Vérification des composants sécurisés sur WinPE

Cette section apporte des informations concernant les points suivants :

Sujets :

- Création d'une image ISO pour l'exécution de SCV sous WinPE
- Ajout de SCV à une image ISO personnalisée
- Exécution de SCV sur WinPE
- Comment vérifier les journaux SCV sous WinPE

Création d'une image ISO pour l'exécution de SCV sous WinPE

Pour créer une image ISO pour l'exécution de SCV sous WinPE :

1. Téléchargez les outils SCVTools à partir de la page **Pilotes et téléchargements** à l'adresse <https://www.dell.com/support>.
2. Assurez-vous que les modules complémentaires Windows ADK et Windows PE pour ADK sont installés dans le système pour WinPE 10.x. Pour télécharger et installer les fichiers, accédez à <https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install>.
3. Exécutez le fichier de l'auto-extracteur pour les outils SCVTools, puis cliquez sur **Décompresser** pour extraire les fichiers à l'emplacement par défaut.

REMARQUE : Pour extraire les fichiers à un emplacement spécifié, cliquez sur **Parcourir** et sélectionnez le dossier dans lequel les fichiers doivent être extraits, puis cliquez sur **OK**, puis sur **Décompresser**.
4. Lancez l'invite de commande et remplacez le répertoire par l'emplacement où les fichiers ont été extraits. Exécutez le fichier de commandes (WinPE10.x_driverinst.bat) à l'aide de l'invite de commande pour créer une image ISO de démarrage.

REMARQUE : Avant d'exécuter le fichier de commandes WinPE, assurez-vous d'ajouter le correctif disponible à l'adresse <https://support.microsoft.com/en-us/help/5017380>. Pour ajouter le correctif, téléchargez la dernière mise à jour de la pile de service (SSU) pour le système d'exploitation avec la dernière mise à jour cumulative (LCU), au chemin mentionné dans le fichier de commandes et renommez le fichier SSU `ssu-19041.1704-x64.msu` et le fichier LCU `windows10.0-kb5018410-x64.msu`.

```
C:\Users\Anirban_Dasgupta\Downloads\Dell-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\Dell-SCVTools-Web-WINPE10-1.93.0-360\WINPE10_x_20246-02_105200
=====
```

Figure 1. Exécution du fichier de commandes via l'invite de commande

5. Une fois que l'image ISO a été créée, ouvrez le dossier créé avec le nom « WINPE10.x-%timestamp% », pour trouver l'image ISO.

```
-----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\Dell-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\Dell-SCVTools-Web-WINPE10-1.93.0-360\WINPE10_x_20240617_155319\Dellemc-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>
```

Figure 2. Confirmation de la création de l'image ISO

- Utilisez cette image ISO pour amorcer l'environnement SCV sur le serveur.

Ajout de SCV à une image ISO personnalisée

Pour ajouter SCV à une image ISO personnalisée :

- Téléchargez les outils SCVTools à partir de la page **Pilotes et téléchargements** à l'adresse <https://www.dell.com/support>.
- Assurez-vous que les modules complémentaires Windows ADK et Windows PE pour ADK sont installés dans le système pour WinPE 10.x. Pour télécharger et installer les fichiers, accédez à <https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install>.
- Exécutez le fichier de l'auto-extracteur pour les outils SCVTools, puis cliquez sur **Décompresser** pour extraire les fichiers à l'emplacement par défaut.
 **REMARQUE :** Pour extraire les fichiers à un emplacement spécifié, cliquez sur **Parcourir** et sélectionnez le dossier dans lequel les fichiers doivent être extraits, puis cliquez sur **OK**, puis sur **Décompresser**.
- Copiez les dossiers suivants dans le chemin du dossier correspondant dans l'image ISO personnalisée :
 - scv** vers X:\Dell
 - Toolkit\DLL** vers X:\windows\system32
- Une fois les fichiers copiés, définissez le chemin du dossier à l'aide de la commande `set PATH=%PATH%;X:\Dell\scv;`
- Le SCV peut désormais être utilisé pour exécuter la validation.

Exécution de SCV sur WinPE

- Connectez-vous à iDRAC dans le système sur lequel vous souhaitez exécuter l'application SCV.
- Lancez la console virtuelle, puis cliquez sur **Connecter un média virtuel**.
- Cliquez sur **Média virtuel**, puis sous **Mapper CD/DVD** cliquez sur **Parcourir** et sélectionnez l'image ISO pour SCV, puis cliquez sur **Mapper l'appareil** et fermez la fenêtre.
- Dans la fenêtre de la console virtuelle, cliquez sur **Amorcer** et sélectionnez **CD/DVD/ISO virtuel**, puis cliquez sur **Oui** sur l'invite pour confirmer le nouvel appareil d'amorçage.
- Cliquez sur **Alimentation** et mettez le système sous tension et laissez-le s'amorcer dans l'image ISO.

6. Une fois que le système est amorcé dans l'image ISO, attendez que la fenêtre de l'invite de commande se charge dans le répertoire X:\Dell>
7. Accédez à X:\Dell\scv, puis exécutez la commande `scv validatesysteminventory` pour démarrer le processus de validation.
 - REMARQUE :** Lors de l'exécution de SCV sur l'hôte, assurez-vous que l'adresse IP de la carte NIC USB de l'iDRAC est définie sur l'adresse IP par défaut. En outre, assurez-vous que les trois premiers octets de l'adresse IP sont « 169.254.1 ».
 - REMARQUE :** Après avoir obtenu l'état « Prêt » dans la sortie `racadm getremoteservicesstatus`, attendez environ 120 secondes avant d'exécuter les commandes `scv`.
 - REMARQUE :** une erreur selon laquelle la collecte de l'inventaire du système a échoué peut s'afficher lors de l'exécution de la commande `scv validatesysteminventory` avec l'option `-d`, si la longueur du chemin d'accès au répertoire dépasse 255 caractères.

```

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  ismrfutil_rel.log
               2 File(s)          4,555,590 bytes
               3 Dir(s)      1,035,620,352 bytes free

X:\Dell\scv>scv validatesysteminventory

```

Figure 3. Exécution de la commande de validation

8. Une fois que le système exécute l'application SCV, le résultat de la commande `SCV validatesysteminventory` doit être `Match`.

```

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>

```

Figure 4. Réussite de l'exécution de la commande de validation et du résultat

9. Si le résultat de la commande `SCV validatesysteminventory` est `Mismatch`, il indique le composant qui ne correspond pas sous `Mismatch Inventory Summary`.

```

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

```

Figure 5. Détails relatifs aux composants attendus et détectés

Comment vérifier les journaux SCV sous WinPE

1. Après l'exécution de la commande SCV dans WinPE, les journaux créés sont stockés sous X:\Dell\scv\scvapp\logs
2. Pour vérifier les journaux, accédez au dossier des journaux et utilisez la commande notepad SCVLog_%service-tag%_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

```

Figure 6. Vérification des journaux sous WinPE

Vérification des composants sécurisés sur Linux

Cette section apporte des informations concernant les points suivants :

Sujets :

- Exécution de SCV sur Linux
- Affichage des journaux SCV à l'aide de Linux

Exécution de SCV sur Linux

1. Téléchargez les outils SCVTools à partir de la page Pilotes et téléchargements à l'adresse <https://www.dell.com/support>.
2. Dans le terminal, accédez au répertoire dans lequel le package SCV est téléchargé, puis décompressez le fichier à l'aide de la commande `tar -zxvf DellEMC-SCV-Web-LX-X.X.X-XXXX_XXX.tar.gz`

```
[root@auvctillem1m1 Downloads]# tar -zxvf 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
```

Figure 7. Extraction des outils SCVTools sous Linux

3. Accédez au répertoire SCVTools après l'extraction des fichiers et exécutez le script `install_scv.sh` à l'aide de la commande `sh install_scv.sh`.

REMARQUE : Pour désinstaller le SCV, vous pouvez utiliser la commande `sh uninstall_scv.sh` pour exécuter le script `uninstall_scv.sh`.

```
[root@auvctillem1m1 Downloads]# ls
COPYRIGHT.txt  DellEMC-SCV-Web-LX-2000-75.tar.gz  ismrfutil-el8-v0  license.txt  SCVTools
[root@auvctillem1m1 Downloads]# cd SCVTools/
[root@auvctillem1m1 SCVTools]# ls
install_scv.sh  readme.txt  RPMS  uninstall_scv.sh
[root@auvctillem1m1 SCVTools]# sh uninstall_scv.sh
[root@auvctillem1m1 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@auvctillem1m1 SCVTools]#
```

Figure 8. Exécution du script d'installation SCV

4. Une fois le SCV installé, exécutez la commande `scv validateSystemInventory` pour démarrer le processus de validation.
- REMARQUE :** Lors de l'exécution de SCV sur l'hôte, assurez-vous que l'adresse IP de la carte NIC USB de l'iDRAC est définie sur l'adresse IP par défaut. En outre, assurez-vous que les trois premiers octets de l'adresse IP sont « 169.254.1 ».

REMARQUE : Utilisez la commande `scv help` pour obtenir plus d'informations sur SCV et savoir comment l'exécuter.

REMARQUE : Après avoir obtenu l'état « Prêt » dans la sortie `racadm getremoteservicesstatus`, attendez environ 120 secondes avant d'exécuter les commandes `scv`.

5. Une fois que le système exécute l'application SCV, le résultat doit être `scv validatesysteminventory: Match`

```
[root@localhost ~]# scv ValidateSystemInventory -r 1000.000.0.00 -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
```

Figure 9. Correspondance de l'exécution de la commande de validation et du résultat

6. Si le résultat est `Validating System Inventory: Mismatch`, il indique le composant qui ne correspond pas sous `Mismatch Inventory Summary`.

```

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

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

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

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

-----
Inventory Mismatch Summary
-----
Added Components Summary:
      HardDrive      23E0A08BTC88      Disk.Bay.5:Enclosure.Internal.0-1
      PowerSupply    CNL0D0034I2C75      PSU.Slot.2

-----
Added Components
-----
{
  "HardDrive": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.5:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation",
      "Model": "Unknown",
      "SerialNumber": "23E0A08BTC88"
    }
  ],
  "PowerSupply": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x000A0002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "A02",
      "Location": "PSU.Slot.2",
      "Manufacturer": "DELL",
      "Model": "PWR SPLY,1100W,RDNT,LTON",
      "SerialNumber": "CNL0D0034I2C75"
    }
  ]
}

-----
Matched Components
-----
{
  "Baseboard": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00030003",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "A01",
      "Location": "1",
      "Manufacturer": "Dell Inc.",
      "Model": "0NPR40",
      "SerialNumber": "CNIVC0036M0426"
    }
  ],
  "HardDrive": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.7:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation ",
      "Model": "Unknown",
      "SerialNumber": "23E0A086TC88"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.3:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation ",
      "Model": "Unknown",
      "SerialNumber": "23E0A08ETC88"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.5:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation ",
      "Model": "Unknown",
      "SerialNumber": "23E0A08BTC88"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.2:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA

```

Figure 10. Détails relatifs aux composants attendus et détectés

Affichage des journaux SCV à l'aide de Linux

1. Lors de l'exécution de SCV dans Linux, les journaux créés sont stockés sous `scvapp\logs`
2. Pour afficher les journaux SCV, accédez au dossier des journaux et utilisez la commande `vi SCVLog_%service-tag%_timestamp%.log` comme ci-dessous :

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

Vérification des composants sécurisés sous Windows Server 2019 et 2022

Cette section fournit des informations sur l'installation et l'exécution de SCVApp :

Sujets :

- [Installation de SCVApp sous Windows Server 2019 et 2022](#)
- [Exécution de SCV sous Windows Server 2019 et 2022](#)

Installation de SCVApp sous Windows Server 2019 et 2022

Pour installer SCVApp sous Windows Server 2019 et 2022 :

1. Téléchargez le programme d'installation de SCV à partir de la page **Pilotes et téléchargements** à l'adresse <https://www.dell.com/support>.
2. Extrayez le programme d'installation de SCV.

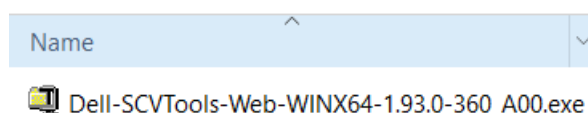


Figure 11. Fichier zip du programme d'installation de SCV

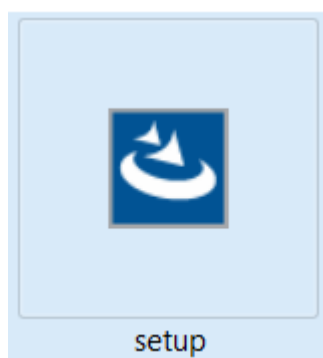


Figure 12. Programme d'installation de SCV

3. Exécutez l'application pour démarrer l'Assistant InstallShield.

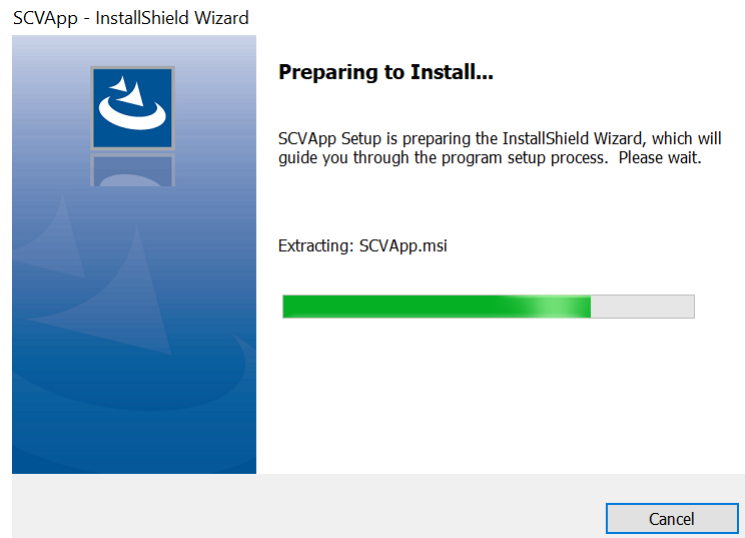


Figure 13. Exécution du programme d'installation de SCV

4. Cliquez sur **Suivant** et acceptez le contrat de licence.

REMARQUE : Lors de l'installation de l'application SCV, assurez-vous de modifier l'emplacement du chemin d'installation sur C:\ProgramFiles\Dell\SCVTools dans l'Assistant d'installation.

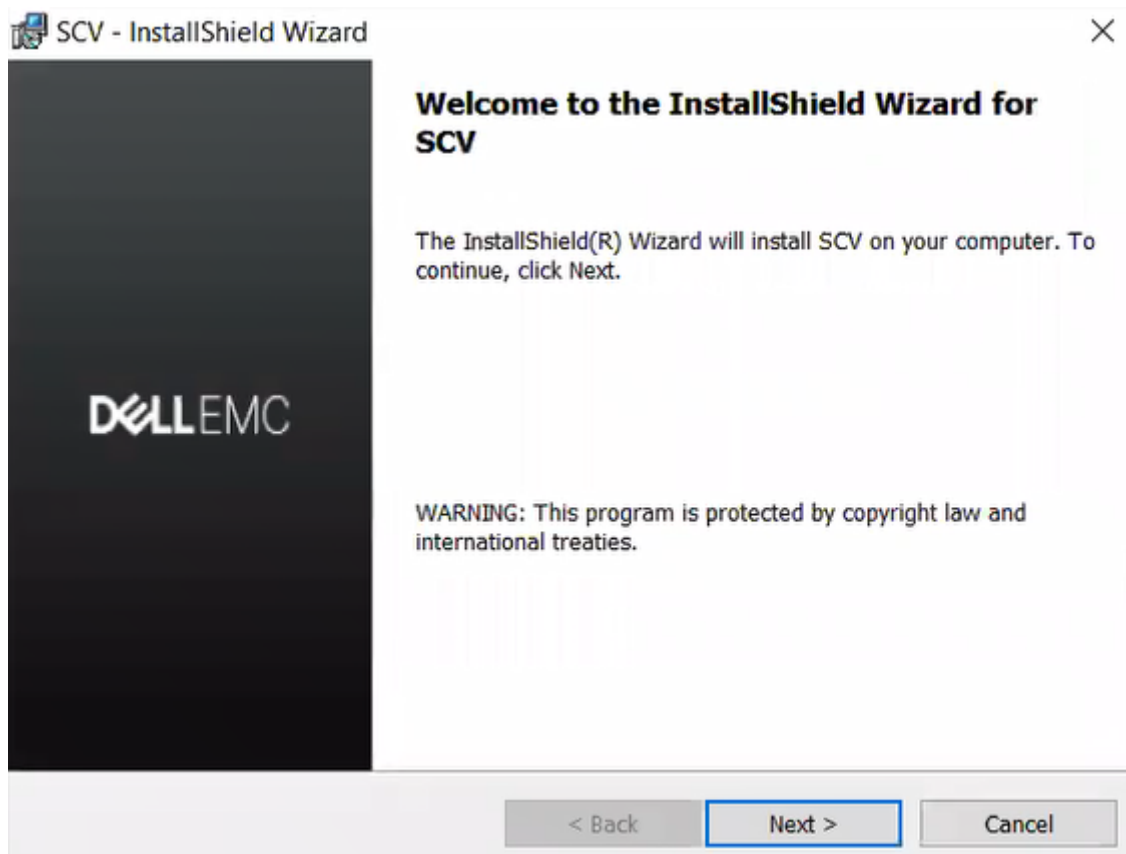


Figure 14. Assistant InstallShield pour SCVApp

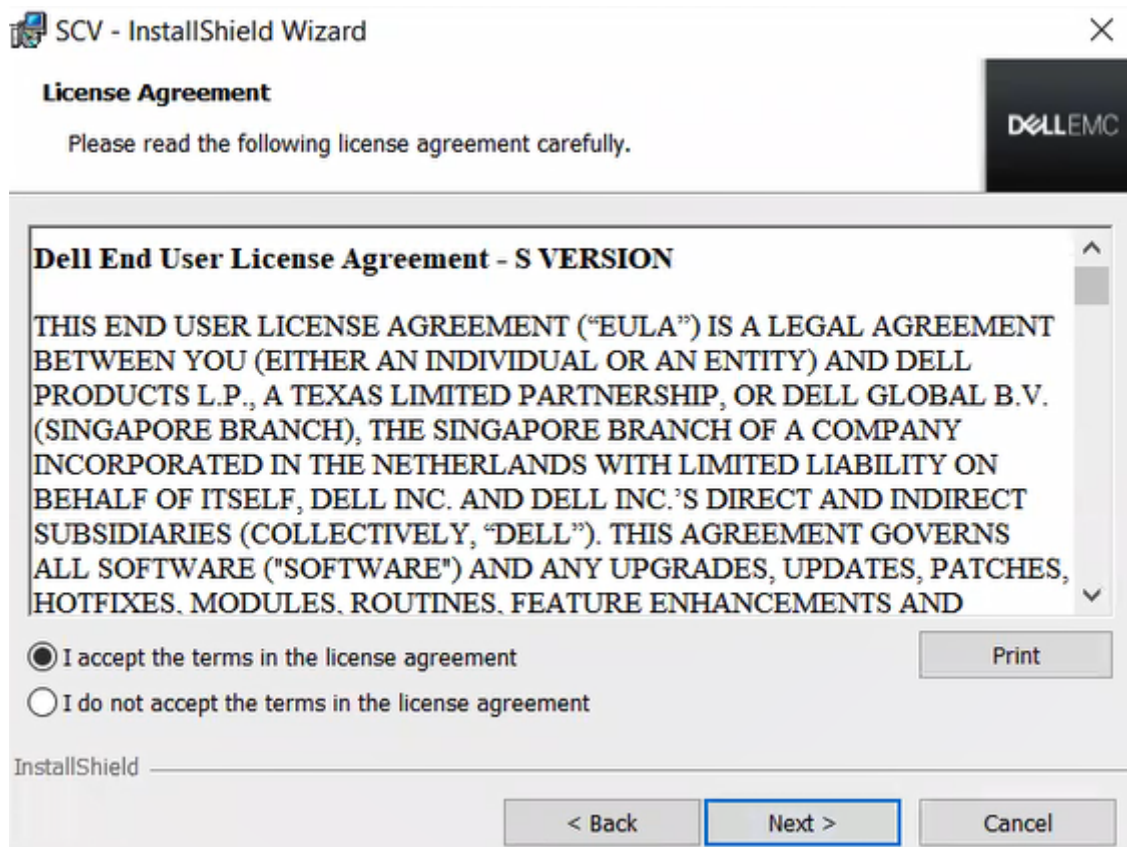


Figure 15. Contrat de licence pour SCVApp

5. Cliquez sur **Installer** pour commencer l'installation.

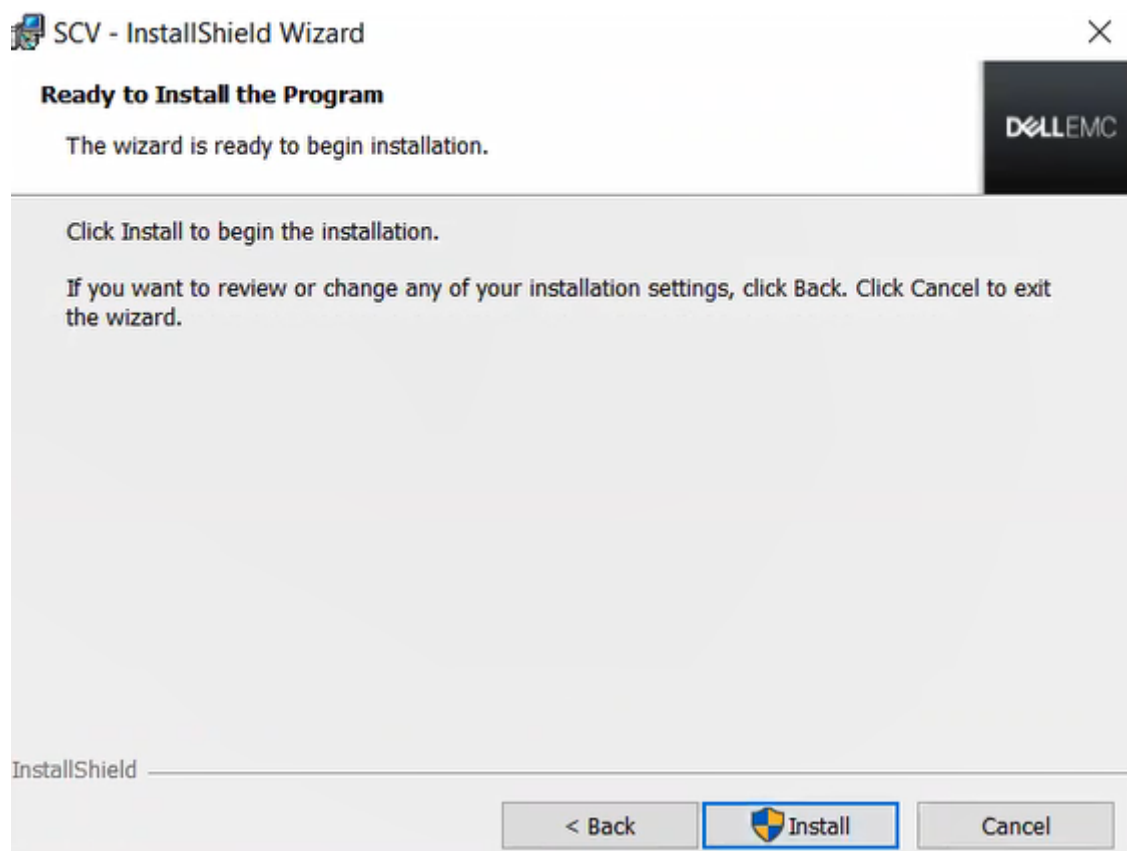


Figure 16. Prêt à installer SCVApp

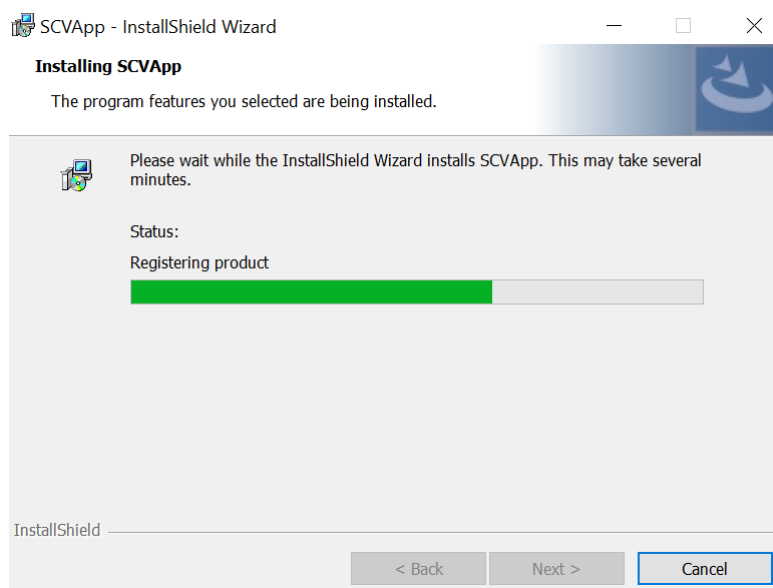


Figure 17. Installation de SCVApp

6. Une fois l'installation terminée, cliquez sur **Terminer** pour quitter l'Assistant InstallShield.

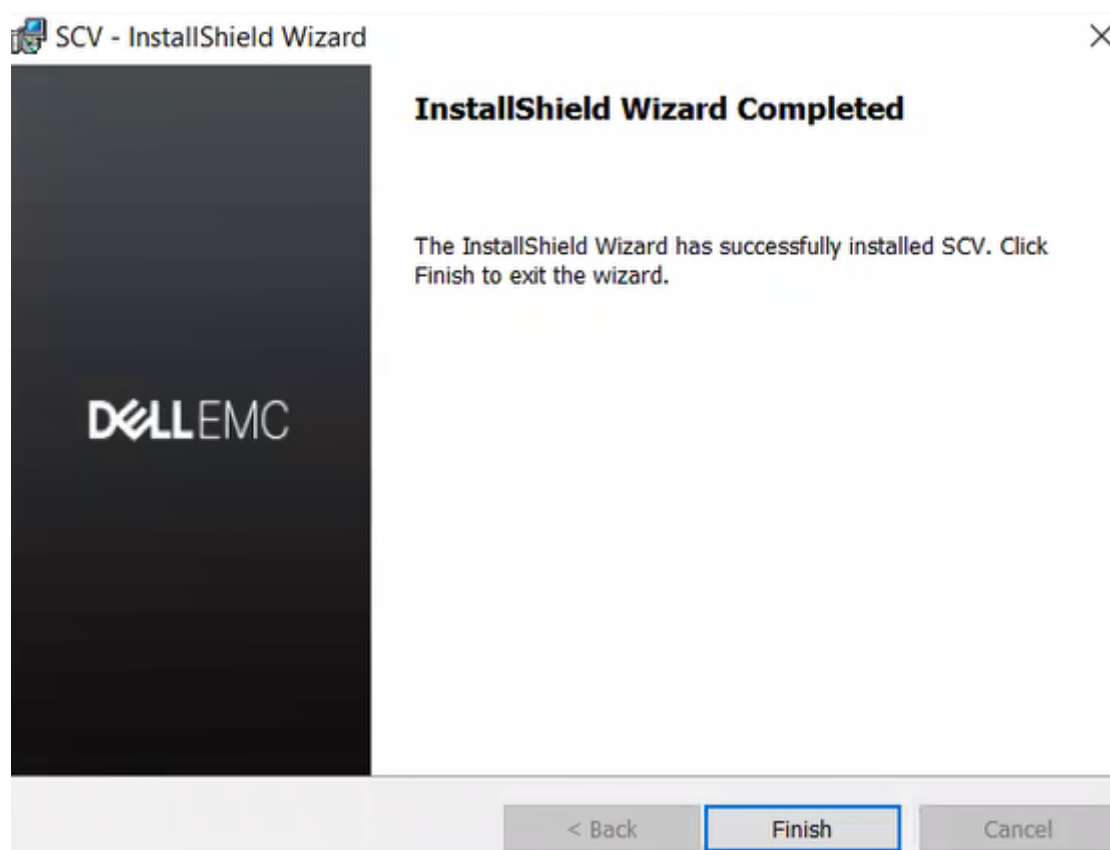


Figure 18. Installation de SCVApp terminée

Exécution de SCV sous Windows Server 2019 et 2022

1. Ouvrez l'invite de commande et accédez au répertoire/dossier SCVTools.
 2. Exécutez la commande `scv validatesysteminventory` pour démarrer le processus de validation.
- REMARQUE :** Lors de l'exécution de SCV sur l'hôte, assurez-vous que l'adresse IP de la carte NIC USB de l'iDRAC est définie sur l'adresse IP par défaut. En outre, assurez-vous que les trois premiers octets de l'adresse IP sont « 169.254.1 ».

- REMARQUE :** L'erreur Impossible de créer le répertoire scvapp s'affiche lorsque la commande `scv validatesysteminventory` est exécutée sur un répertoire autre que le répertoire qui héberge l'application.
- REMARQUE :** L'erreur Téléchargement du certificat d'usine SCV : Échec s'affiche lorsque la commande `scv validatesysteminventory` est exécutée avec le pare-feu hôte activé. Pour exécuter la commande avec succès, assurez-vous de créer une règle sortante pour l'adresse IP 169.254.1.1.
- REMARQUE :** Après avoir obtenu l'état global « Prêt » dans la sortie `racadm getremoteservicesstatus`, attendez environ 120 secondes avant d'exécuter les commandes `scv`.
- REMARQUE :** une erreur selon laquelle la collecte de l'inventaire du système a échoué peut s'afficher lors de l'exécution de la commande `scv validatesysteminventory` avec l'option `-d <path of the directory>`, si la longueur du chemin d'accès au répertoire dépasse 255 caractères.

```
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
```

Figure 19. Correspondance de l'exécution de la commande de validation et du résultat

3. Si le résultat s'affiche comme `Validating System Inventory: Mismatch`, il indique le composant qui ne correspond pas sous `Mismatch Inventory Summary`.

```
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
```

Figure 20. Non correspondance de l'exécution de la commande de validation et du résultat

```

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

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

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

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

Matched Components
-----
{
  "Baseboard": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00030003",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "X31",
      "Location": "1",
      "Manufacturer": "Dell Inc.",
      "Model": "0M1CC5",
      "SerialNumber": "CN1VC0026T0065"
    }
  ],
  "HardDrive": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "Location": "Disk Bay 0:Enclosure,Internal,0-1",
      "Manufacturer": "Samsung Electronics Co Ltd",
      "Model": "Unknown",
      "SerialNumber": "S6CSNA0RA02805"
    }
  ],
  "Memory": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00060001",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "A1",
      "Manufacturer": "Micron Technology",
      "Model": "DDR5 DIMM",
      "SerialNumber": "3169944A"
    }
  ],
  "Network": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00090002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "NIC.Embedded,2-1-1",
      "Manufacturer": "Broadcom",
      "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:17",
      "SerialNumber": "Unknown",
      "MacAddress": "EC:2A:72:33:06:17"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00090002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "NIC.Embedded,1-1-1",
      "Manufacturer": "Broadcom",
      "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:16",
      "SerialNumber": "Unknown",
      "MacAddress": "EC:2A:72:33:06:16"
    }
  ],
  "PowerSupply": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x000a0002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "A04",
      "Location": "PSU.Slot,1",
      "Manufacturer": "DELL",
      "Model": "PWR SPLY,B00W,RDNT,LTON",
      "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": "MIICVTCcAfuGawIBAgIIAwAAAAAxE+QvCgYIKoZiZj0EAWIwdTELMAKGA1UEBHMCMQ04xETAPBgNVBAGhYNoY5naGFpMREw
    }
  ]
}

```

Figure 21. Détails relatifs aux composants attendus et détectés

```

-----
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": "0x00090003",
      "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": "S6CSNA0RA02805"
    }
  ],
  "Memory": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00060001",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "A1",
      "Manufacturer": "Micron Technology",
      "Model": "DDR5 DIMM",
      "SerialNumber": "3169944A"
    }
  ],
  "Network": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00090002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "NIC.Embedded.2-1-1",
      "Manufacturer": "Broadcom",
      "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:17",
      "SerialNumber": "Unknown",
      "MacAddress": "EC:2A:72:33:06:17"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00090002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "NIC.Embedded.1-1-1",
      "Manufacturer": "Broadcom",
      "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:16",
      "SerialNumber": "Unknown",
      "MacAddress": "EC:2A:72:33:06:16"
    }
  ],
  "PowerSupply": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x000a0002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "A04",
      "Location": "PSU.Slot.1",
      "Manufacturer": "DELL",
      "Model": "PWR SPLY,800W,RDNT,LTON",
      "SerialNumber": "CNLOD002463504"
    }
  ],
  "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": "1BFCE11FD1C1E363"
    }
  ],
  "iDRAC": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00060003",
      "CertificateIdentifier": "1E1C1VTCCAfuGawIBAgIIAwAAAAAE+QwCgYIKoZIzj0EAwIwdTElMAKGA1UEBHMCOQ8xETAPBgNVBAgMCFN0Yw5naGpPhREwDwYDVQQHDAhTa
    }
  ]
}

```

Figure 22. Détails relatifs aux composants attendus et détectés

Exécution distante de la vérification des composants sécurisés (SCV)

Cette section apporte des informations concernant les points suivants :

Sujets :

- Exécution distante de SCV sous Windows Server 2019 et 2022
- Exécution distante de SCV sur WinPE
- Exécution de SCV sous Linux

Exécution distante de SCV sous Windows Server 2019 et 2022

1. Ouvrez l'invite de commande et accédez au répertoire/dossier SCVTools.
2. Exécutez la commande `scv validatesysteminventory -r <iDRAC IPv4/IPv6[] address> -i` pour démarrer le processus de validation.

```
C:\Users\Administrator>scv validatesysteminventory -r 10.10.10.10 -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 7267YX3 with System Inventory Service Tag: Match
Inventory Comparison Result : Match

Refer Detailed Report File at : C:\Users\Administrator\scvapp\out\SCV_CommandExecutionReport_7267YX3_2024_06_04_18_44_42.txt
```

Figure 23. Correspondance de l'exécution de la commande de validation distante sous Windows et du résultat

Exécution distante de SCV sur WinPE

1. Ouvrez l'invite de commande et accédez au répertoire/dossier SCVTools.
2. Exécutez la commande `scv validatesysteminventory -r <iDRAC IPv4/IPv6[] address> -i` pour démarrer le processus de validation.

```
X:\Dell\scv>scv validatesysteminventory -r 10.10.10.10 -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 : X:\Dell\scv\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2024_06_17_16_38_26.txt
```

Figure 24. Correspondance de l'exécution de la commande de validation distante sous WinPE et du résultat

Exécution de SCV sous Linux

1. Ouvrez l'invite de commande et accédez au répertoire/dossier SCVTools.

2. Exécutez la commande `scv validatesysteminventory -r <iDRAC IPv4/IPv6[] address> -i` pour démarrer le processus de validation.

```
[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
```

Figure 25. Correspondance de l'exécution de la commande de validation distante sous Linux et du résultat

Détails de la commande SCV

Cette section fournit des informations sur certaines commandes scv supplémentaires.

Sujets :

- Obtenir des informations sur l'exécution de SCV
- Obtenir des informations sur la commande `scv validatesysteminventory`
- Connexion distante à une console de gestion et validation de l'inventaire
- Connexion distante à une console de gestion à l'aide d'un port spécifique et validation de l'inventaire
- Vérification de la correspondance de l'emplacement des composants et validation de l'inventaire
- Obtenir la version SCV
- Affichage de la valeur d'un identifiant de certificat sur la console ou redirection de cette valeur vers un fichier

Obtenir des informations sur l'exécution de SCV

Tableau 4. Obtenir plus d'informations sur SCV

scv help	
Description	Utilisez la commande suivante pour obtenir plus d'informations sur SCV et savoir comment l'exécuter.
Synopsis	<pre>scv help</pre>

Sortie

```
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
```

Obtenir des informations sur la commande `scv validatesysteminventory`

Tableau 5. Obtenir plus d'informations sur la commande SCV `validatesysteminventory`

scv help validatesysteminventory	
Description	Utilisez la commande suivante pour obtenir plus d'informations sur la commande SCV <code>validatesysteminventory</code> et savoir comment l'exécuter.

Tableau 5. Obtenir plus d'informations sur la commande SCV validatesysteminventory (suite)

scv help validatesysteminventory	
Synopsis	scv help validatesysteminventory

Sortie

```
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.
```

Connexion distante à une console de gestion et validation de l’inventaire

Tableau 6. Validation distante d'un inventaire spécifique

scv validatesysteminventory -r <adresse IPv4/IPv6> -i	
Description	Utilisez la commande suivante pour vous connecter à distance à une adresse IP de console de gestion spécifique et valider l’inventaire.
Synopsis	scv validatesysteminventory -r <IPv4/IPv6 address> -i
Entrée	-r <IPV4/IPV6 address>

Sortie

```
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
```

Connexion distante à une console de gestion à l'aide d'un port spécifique et validation de l'inventaire

Tableau 7. Validation de l'inventaire à l'aide d'un port spécifique

scv validatesysteminventory -r <adresse IPv4/IPv6:Port> -i	
Description	Utilisez la commande suivante pour vous connecter à une adresse IP de console de gestion à l'aide d'un port spécifique et valider l'inventaire.
Synopsis	scv validatesysteminventory -r <IPv4/IPv6 address:Port> -i
Entrée	-r <IPV4/IPV6 address>

Vérification de la correspondance de l'emplacement des composants et validation de l'inventaire

Tableau 8. Vérification de la correspondance de l'emplacement des composants

scv validatesysteminventory --enforceorder	
Description	Utilisez la commande suivante pour vous assurer que l'emplacement des composants correspond, tout en validant l'inventaire. REMARQUE : Tout remplacement de composant est identifié comme « non correspondant » lors de l'utilisation de la commande --enforceorder.
Synopsis	scv validatesysteminventory --enforceorder

Sortie

```
(C:\Users\Administrator>scv validatesysteminventory -r 10.10.10.10 -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
```

Obtenir la version SCV

Tableau 9. Obtenir la version SCV

version scv	
Description	Utilisez la commande suivante pour afficher la version actuelle de l'application SCV.
Synopsis	scv version

Sortie

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

Affichage de la valeur d'un identifiant de certificat sur la console ou redirection de cette valeur vers un fichier

Tableau 10. Affichage ou redirection de la valeur d'un identifiant de certificat

scv extractcert	
Description	Utilisez la commande suivante pour afficher la valeur d'un identifiant de certificat sur la console ou pour rediriger cette valeur vers un fichier.
Synopsis	<pre>scv extractcert -r <IPv4/IPv6 address> -i -c <Component Name> -l <Location> -f <File Name> -d <Directory Name></pre>
Entrée	● <code>--remoteip <IPV4/IPV6 address></code> ● <code>--component <Component_name></code> ● <code>--location <Location_name></code> ● <code>--file <File_name></code> ● <code>--directory <Directory_name></code>

Sortie

```
X:\Dell\scv>scv extractcert -r ██████████ --component iDRAC --location 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-----MIICXzCCAgaAwIBAgIIBAaaaaaahswCgYIKoZIzj0EAwIwCjELMAkGA1UEBhMCQ04xEDAOBgNVBAgMB1RyYW5qaW4xEDAOBgNV
BAMCB1RyYW5qaW4xEDAOBgNVBAoMB0ZveG9vbW4xDTALBgNVBAsMBFBSST00XHJAcBgNVBAMFTBQ1aWMc05NzQxLTc0QkItMjMzNzAeFw0yMzA0MTIwMDI0MzJaF
w0yMjA0MTIwMDI0MzJaMH8xCzAJBgNVBAYTA1VTM04wDAYDVQQIDAVUZDhzcjEETMBEGA1UEBwwKUm91bmQgUm9jaZEFMB0GA1UECgwWRGV5bC8BUZwNobm9sb2dpZXh
wSjEjZ0E0AaG1UECgwFSURS00mXgJAyBGNVBAhMEWlj0j3h0jCyOmK0xIz0ME4MFkwEYyRKoZIZj0CAQYIKoZIzj0DAQoDQgAEAxz0MoFlb7Ar1FFImSXkR4/r
c5L+7p2ziHmLSMDKU2eqFHCn6I05KxKbrCgky0wVvxrhUATSSdBUrAEYynS+6N5MHcwCQYDVR0TBAlwADALBgNVHQ8EBAMCBwAeHQYDVR0LBBywFAyIKwYBBQUHwE
GCC3QAQUFBwMCMCBGGA1UddGQNBQ0/g68BLUQ1ReExQMNBwYupAEK631TAFBgNVHSMEGDAwBgRyuNpu7GgYOVwI1MaBV8If/Pxx/ETAKBggqhkJpQQQDagNHADBEA1Ayp
ODJ32+nu3j1cZ2/W49RFpQUh8Cxfv6pAhWkHhLntwI9nKwR48X501Pmk47N09S1MwsUHF50FQE7j1hTSvtu6ow=-----END CERTIFICATE-----

X:\Dell\scv>
```

Figure 26. Affichage de la valeur d'un identifiant de certificat sur la console

```
C:\Users\Administrator>scv extractcert -r 1999.1999.12.31 -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
```

Figure 27. Écriture de la valeur d'un identifiant de certificat dans un fichier

Fonctionnalité SCVApp MARS

MARS (MAC Address Reporting Service) est une nouvelle offre qui fournit l'adresse MAC de l'iDRAC, le port LOM 0 et l'étiquette de service du serveur correspondant.

SCVApp extrait l'adresse MAC de l'inventaire du certificat pour le composant réseau et iDRAC.

Les commandes SCVApp suivantes sont utiles :

Tableau 11. Obtention des informations sur MARS

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

Tableau 12. Exécution de la commande MARS pour extraire les détails MARS et créer le fichier marsreport.csv

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

Tableau 12. Exécution de la commande MARS pour extraire les détails MARS et créer le fichier marsreport.csv (suite)

scv mars	
	93:53 <ServiceTag>,iDRAC,c8:4b:d6:98:93:4c

Fonctionnalité SPDM

SPDM (Security Protocol and Data Model) est un protocole utilisé pour établir les fonctionnalités de sécurité et l'authenticité entre les composants matériels. SPDM permet l'échange de messages entre l'iDRAC et les appareils distants tels que les contrôleurs de stockage et les contrôleurs NIC. Cela inclut les certificats d'identité du matériel.

L'application SCV prend en charge la découverte des certificats d'identité matériels pour les appareils distants compatibles SPDM. L'application SCV exporte l'identité matérielle des appareils SPDM compatibles dans le certificat SCV.

SCV 1.93.0 prend en charge PERC 12.2.

Certificat CA racine SCV

 **REMARQUE :** Cette section fournit des détails sur le certificat CA racine SCV.

Format de fichier : extrait les fichiers directement sur le disque local

Nom du fichier : Certificate A00.zip

Taille du fichier : 929 octets

Description du format : ce format de fichier se compose d'une archive de fichiers qui peut être décompressée dans un répertoire du disque dur. L'installation peut ensuite être effectuée à partir de ce répertoire.

Lien de téléchargement : [https://dl.dell.com/FOLDER06748569M/1/Certificate A00.zip](https://dl.dell.com/FOLDER06748569M/1/Certificate_A00.zip)

Pour garantir l'intégrité de votre téléchargement, veuillez vérifier la valeur de la somme de contrôle.

MD5 : edb649dbf130e43aeaf5358f1186d312

SHA1 : a92d23c8e9e61fd5c4e568cb23be3024df3f886f

SHA-256 : c947162dc67f5d441ff22b063d7566c52db23cc0c51746455e492c60943f8165

Codes de retour

Vous trouverez ci-dessous la liste des codes de retour pour l'opération SCV :

Tableau 13. Codes de retour SCV

Code	Description
0	Toutes les opérations ont réussi et l'inventaire a été mis en correspondance.
1	Défaillance générique.
2	Une autre instance de l'opération SCV est en cours d'exécution.
3	L'autorisation n'est pas appropriée pour l'utilisateur.
4	L'opération SCV n'a pas pu démarrer, les conditions préalables ne sont pas remplies.
5	Échec du téléchargement du certificat à partir de l'iDRAC.
6	Échec de la validation de la signature et de la racine de confiance.
7	Échec de la validation de la preuve de possession.
8	Le profil n'est pas pris en charge pour les détails de la version, comme indiqué dans le certificat.
9	Le profil, les sous-schémas/utilitaires sont altérés, la signature du profil ne correspond pas.
10	Impossible de collecter les données en raison d'une défaillance de l'utilitaire.
11	Non-correspondance dans l'inventaire.
12	La valeur spécifiée est hors plage. La longueur de l'argument est plus grande ou plus courte que celle autorisée.
13	Commande SCV saisie non valide ou incorrecte. Toute commande ou option saisie n'est pas prise en charge sur l'interface ou la plateforme actuelle.
14	La syntaxe de la commande est incorrecte.
16	SCV ne dispose pas d'une licence requise installée.
17	L'iDRAC ne dispose pas de suffisamment de ressources (p. ex. : mémoire).
18	Service indisponible/occupé.
19	Problème de transfert de fichiers (intrabande).
20	Le mode de verrouillage activé ou les attributs dépendants ne sont pas valides ou ne sont pas configurés.
21	Impossible de se connecter (hors bande)
22	Dépendance non respectée pour une spécification
23	Problèmes liés à la session.
24	Échec en raison d'une erreur de clé, de certificat ou de signature non valides.
25	Échec du téléchargement de certificat.

Obtenir de l'aide

Sujets :

- [Contacter Dell](#)
- [Documents et ressources de support](#)
- [Commentaires sur la documentation](#)

Contacter Dell

Dell propose plusieurs possibilités de maintenance et de support en ligne ou par téléphone. Si vous ne disposez pas d'une connexion Internet fonctionnelle, consultez votre facture, le bordereau de marchandises ou le catalogue des produits Dell pour trouver les informations de contact. La disponibilité des services varie selon le pays et le produit. Certains services peuvent ne pas être disponibles dans votre zone géographique. Pour prendre contact avec Dell pour des questions commerciales, de support technique ou de service client :

Étapes

1. Rendez-vous sur Page de [support Dell](#).
2. Sélectionnez votre pays dans le menu déroulant située dans le coin inférieur droit de la page.
3. Pour obtenir une assistance personnalisée :
 - a. Saisissez le numéro de série de votre système dans le champ **Saisissez votre numéro de série**.
 - b. Cliquez sur **Envoyer**.
La page de support qui répertorie les différentes catégories de supports s'affiche.
4. Pour une assistance générale :
 - a. Sélectionnez la catégorie de votre produit.
 - b. Sélectionnez la gamme de votre produit.
 - c. Sélectionnez votre produit.
La page de support qui répertorie les différentes catégories de supports s'affiche.
5. Pour savoir comment contacter le support technique mondial Dell :
 - a. Cliquez sur [Contacter le support technique](#).
 - b. Saisissez le numéro de série de votre système dans le champ **Saisissez votre numéro de série** sur la page Web Nous contacter.

Documents et ressources de support

- La page d'accueil du support iDRAC permet d'accéder à des documents sur les produits, des livres blancs techniques, des vidéos d'instructions, et plus encore :
 - www.dell.com/support/idrac
- Guide de l'utilisateur de l'iDRAC et autres manuels :
 - www.dell.com/idracmanuals
- Pour plus d'informations sur les serveurs PowerEdge, voir la documentation sur :
 - www.dell.com/poweredgemanuals
- Support technique Dell :
 - www.dell.com/support

Commentaires sur la documentation

Vous pouvez évaluer la documentation ou rédiger vos commentaires sur n'importe laquelle de nos pages de documentation Dell et cliquer sur **Envoyer des commentaires** pour envoyer vos commentaires.