Dell Secured Component Verification version 1.5, 1.5.1, 1.6, 1.7, 1.8 et 1.9

Guide de référence pour les serveurs et les châssis

Septembre 2023
Rév. A00

DELL Technologies

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

1

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

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

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 sera identifiée comme une « non correspondance ».

Remarques :

- 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.
- SCV nécessite une communication NIC USB pour la validation intrabande. Ne désactivez pas la carte NIC USB lors de l'exécution de l'opération SCV.
- 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.

Configuration matérielle

Catégorie	Exigence
Systèmes d'exploitation pris en charge	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 et Windows Server 2022.
Outil SCV	SCV 1.5, 1.5.1, 1.6, 1.7, 1.8 ou 1.9

Catégorie	Exigence
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

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 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

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

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 : Lorsqu'aucun appareil n'est présent pour un composant, l'inventaire SCV affiche une entrée « Inconnu ».

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"
 }
```

2

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

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`.

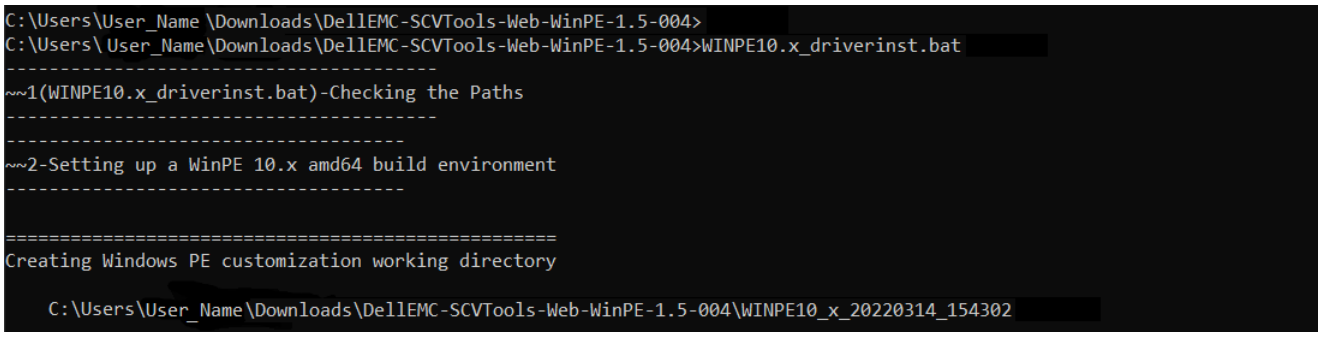

Figure 1. Exécution du fichier de commandes via l'invite de commande

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.

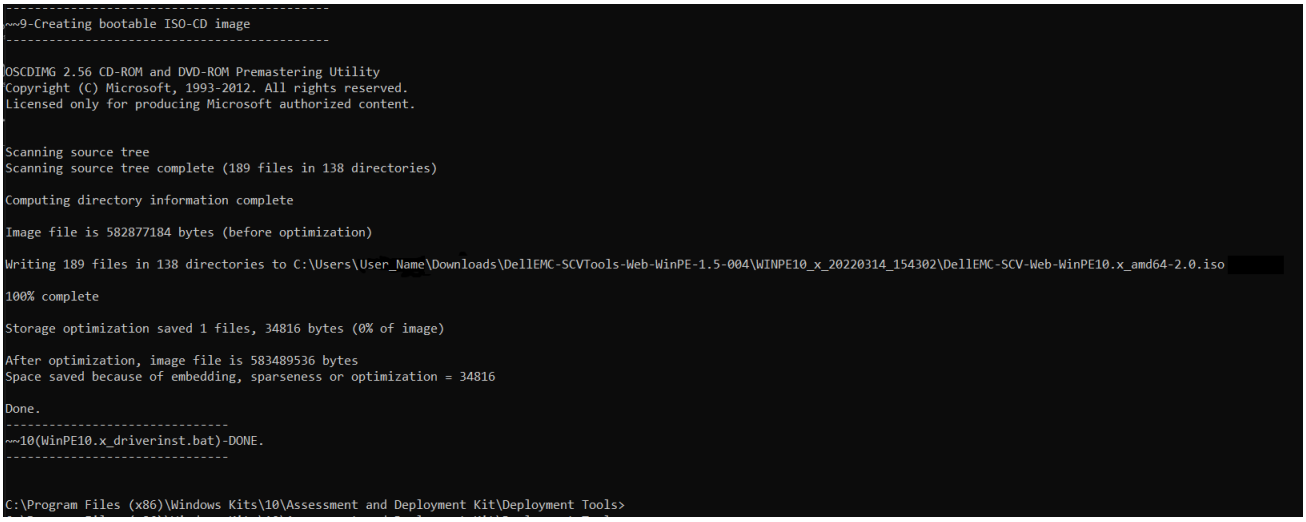

Figure 2. Confirmation de la création de l'image ISO

6. 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 :

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. Copiez les dossiers suivants dans le chemin du dossier correspondant dans l'image ISO personnalisée :
   a. **scv** vers `X:\Dell`
   b. **Toolkit\OpenSSL** pour `X:\Dell\scv`
   c. **Toolkit\DLL** vers `X:\windows\system32`
5. Une fois les fichiers copiés, définissez le chemin du dossier à l'aide de la commande `set PATH=%PATH%;X:\Dell\scv;X:\Dell\scv\openssl;`
6. Le SCV peut désormais être utilisé pour exécuter la validation.

Exécution de SCV sur WinPE

1. Connectez-vous à iDRAC dans le système sur lequel vous souhaitez exécuter l'application SCV.
2. Lancez la console virtuelle, puis cliquez sur **Connecter un média virtuel**.
3. 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.
4. 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.
5. 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 150 caractères.

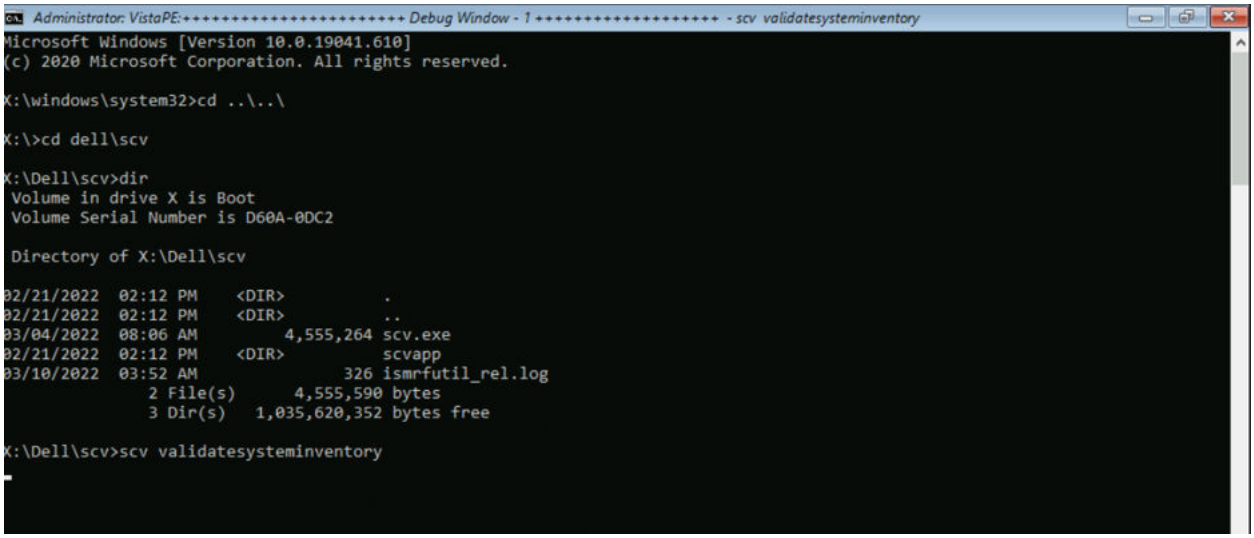

Figure 3. Exécution de la commande de validation

8. Une fois que le système exécute l'application SCV, elle doit donner le résultat `Validating System Inventory: Match`

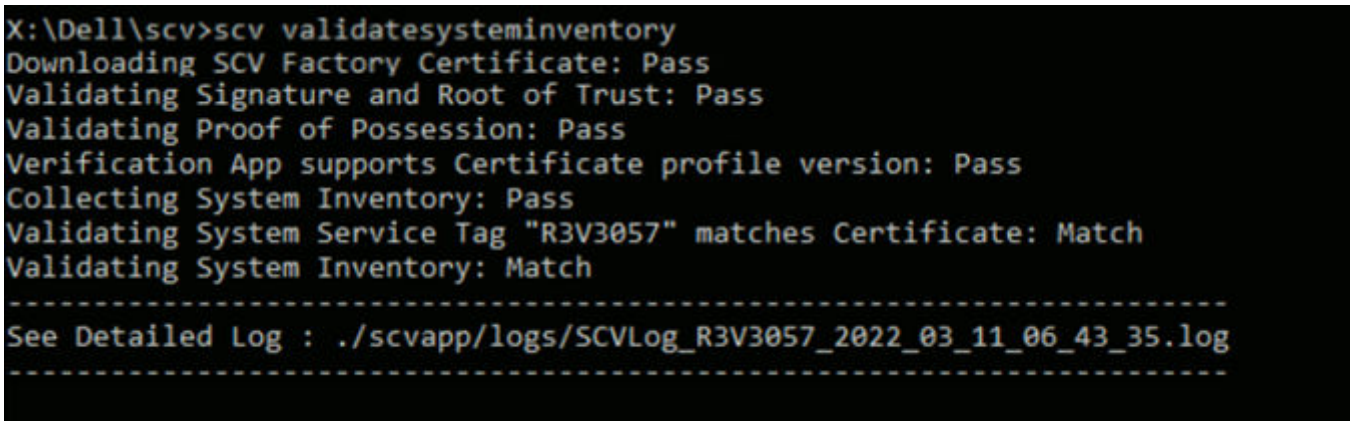

Figure 4. Réussite de l'exécution de la commande de validation et du résultat

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

```
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
--------------------------------------------------------------------------------
```

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

3

Vérification des composants sécurisés sur Linux

Cette section apporte des informations concernant les points suivants :

Sujets :

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@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
```

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@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]#
```

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, elle doit donner le résultat `Validating System Inventory: Match`

```
[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
--------------------------------------------------------------------------------
```

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

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

```
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
--------------------------------------------------------------------------------
```

Figure 10. Détails relatifs aux composants attendus et détectés

Comment vérifier les journaux SCV sous Linux

1. Après l'exécution de la commande SCV dans Linux, les journaux créés sont stockés sous `scvapp\logs`
2. Pour vérifier les journaux, accédez au dossier des journaux et utilisez la commande `vi SCVLog_%service-tag%_%timestamp%.log`

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

Figure 11. Vérification des journaux dans Linux

4

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.

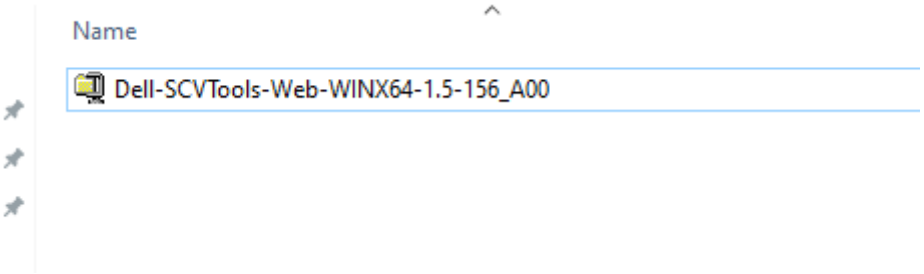

Figure 12. Fichier zip du programme d'installation de SCV

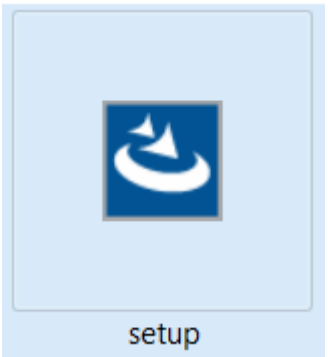

Figure 13. Programme d'installation de SCV

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

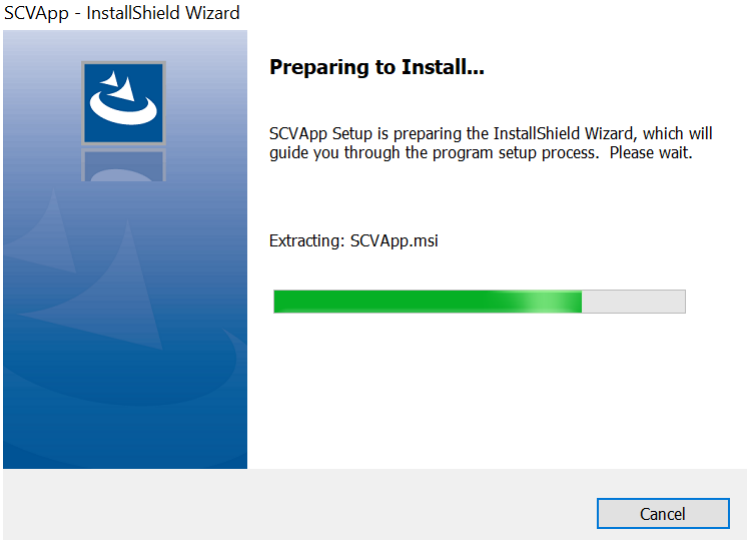

Figure 14. Exécution du programme d'installation de SCV

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.

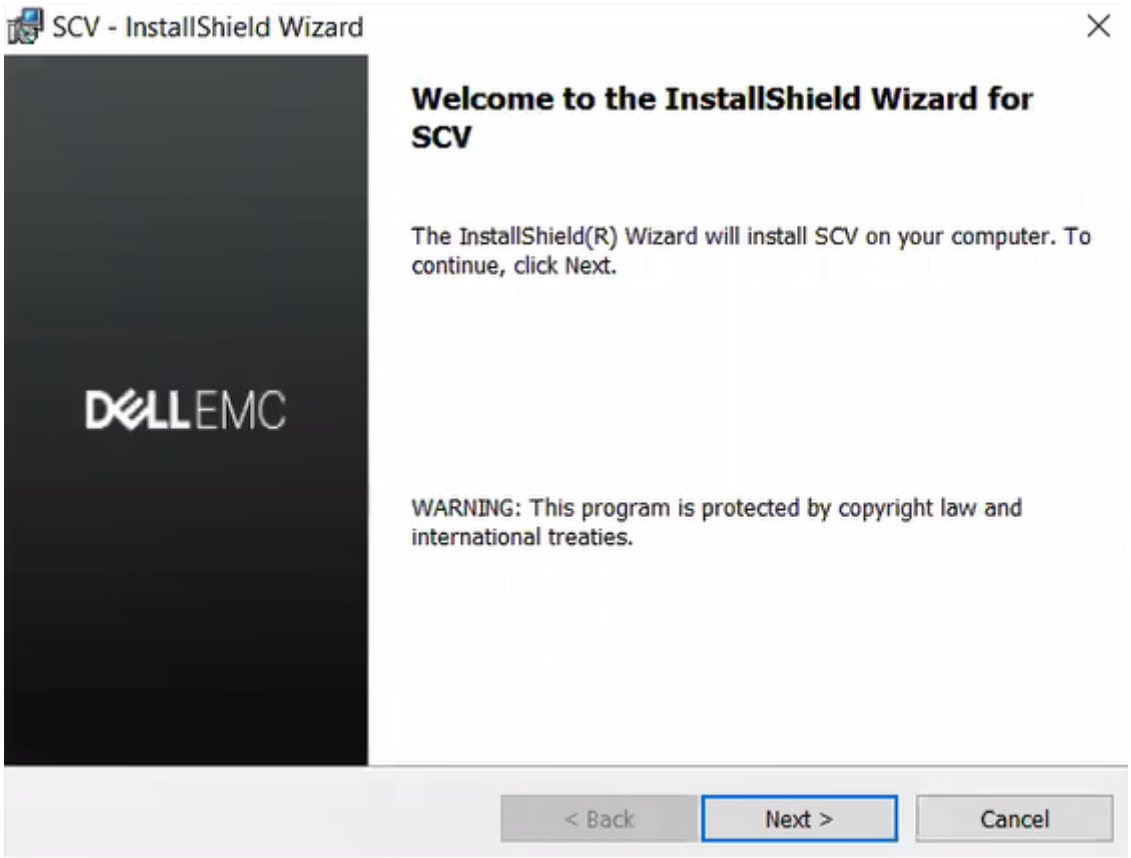

Figure 15. Assistant InstallShield pour SCVApp

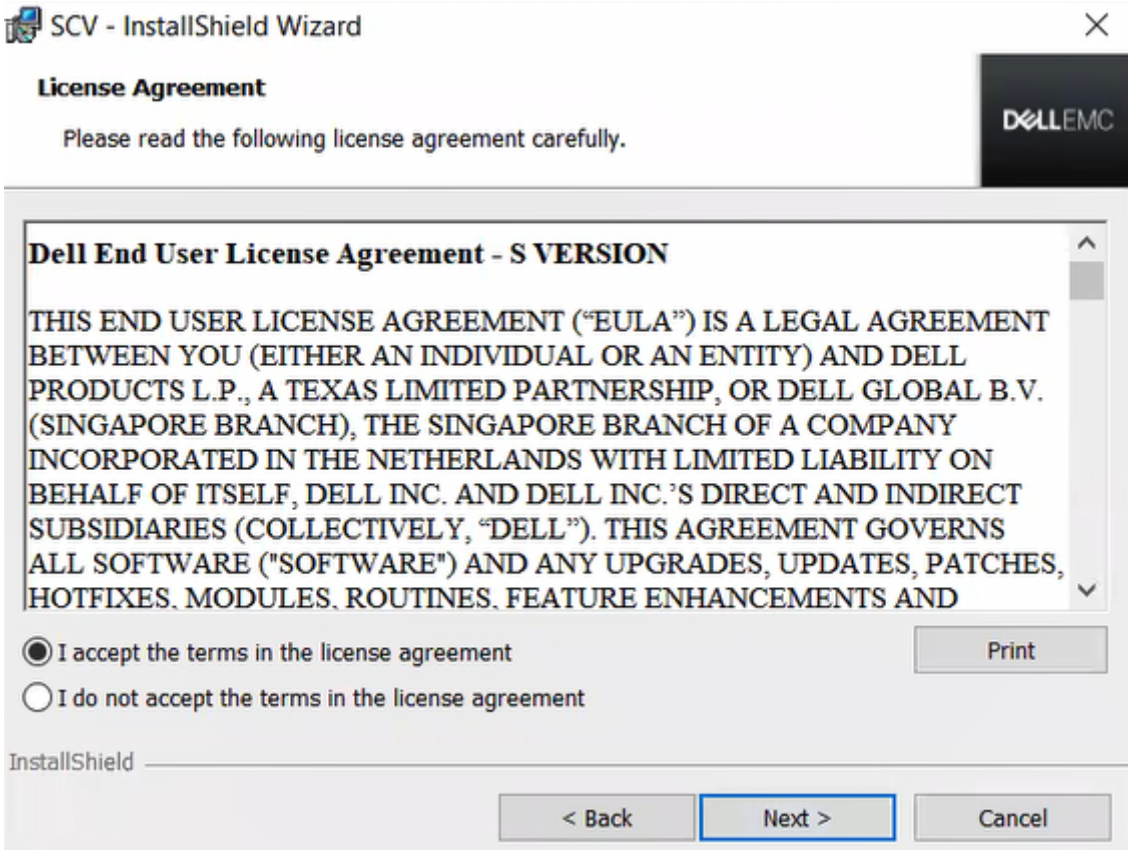

Figure 16. Contrat de licence pour SCVApp

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

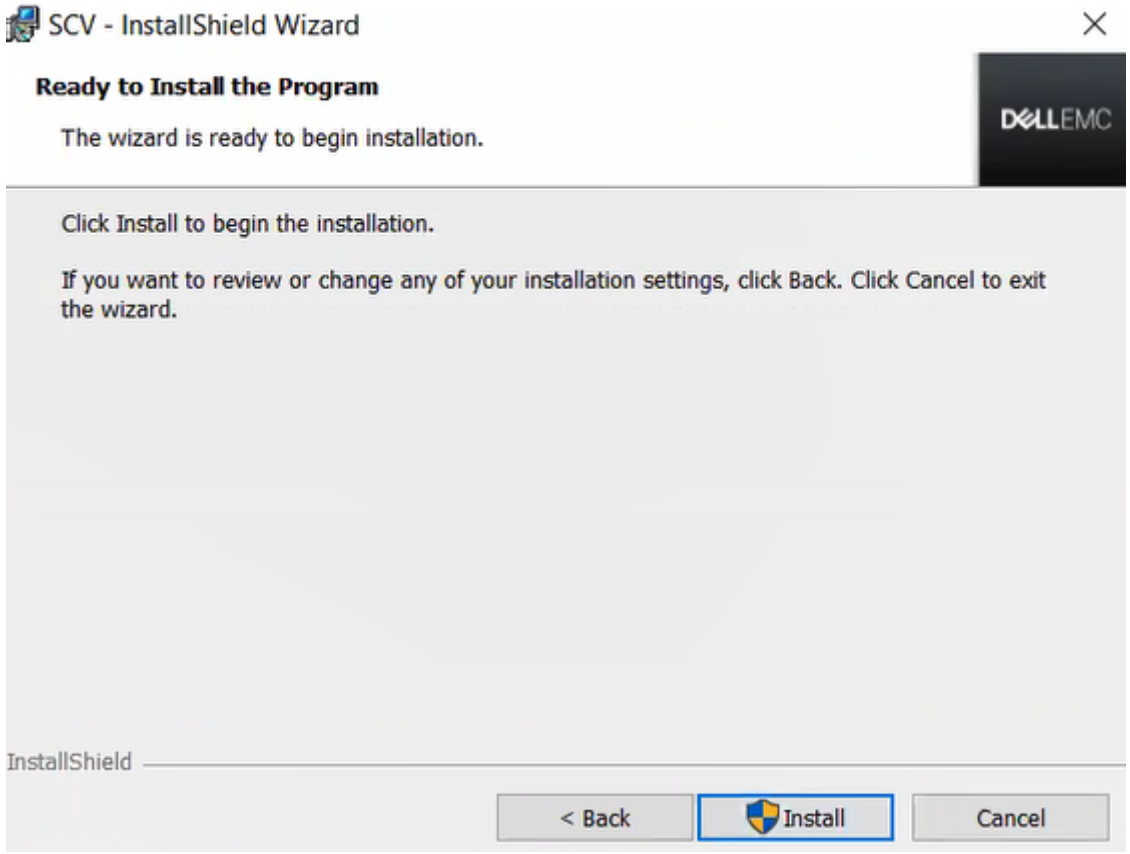

Figure 17. Prêt à installer SCVApp

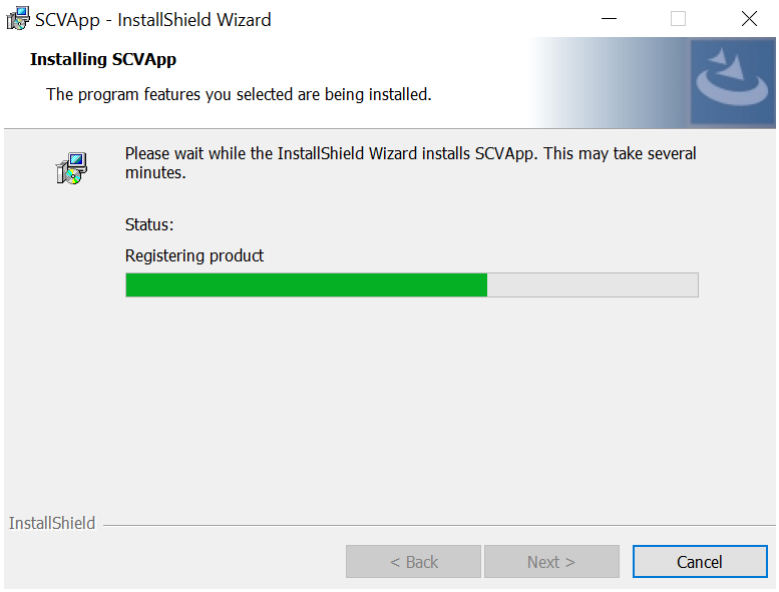

Figure 18. Installation de SCVApp

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

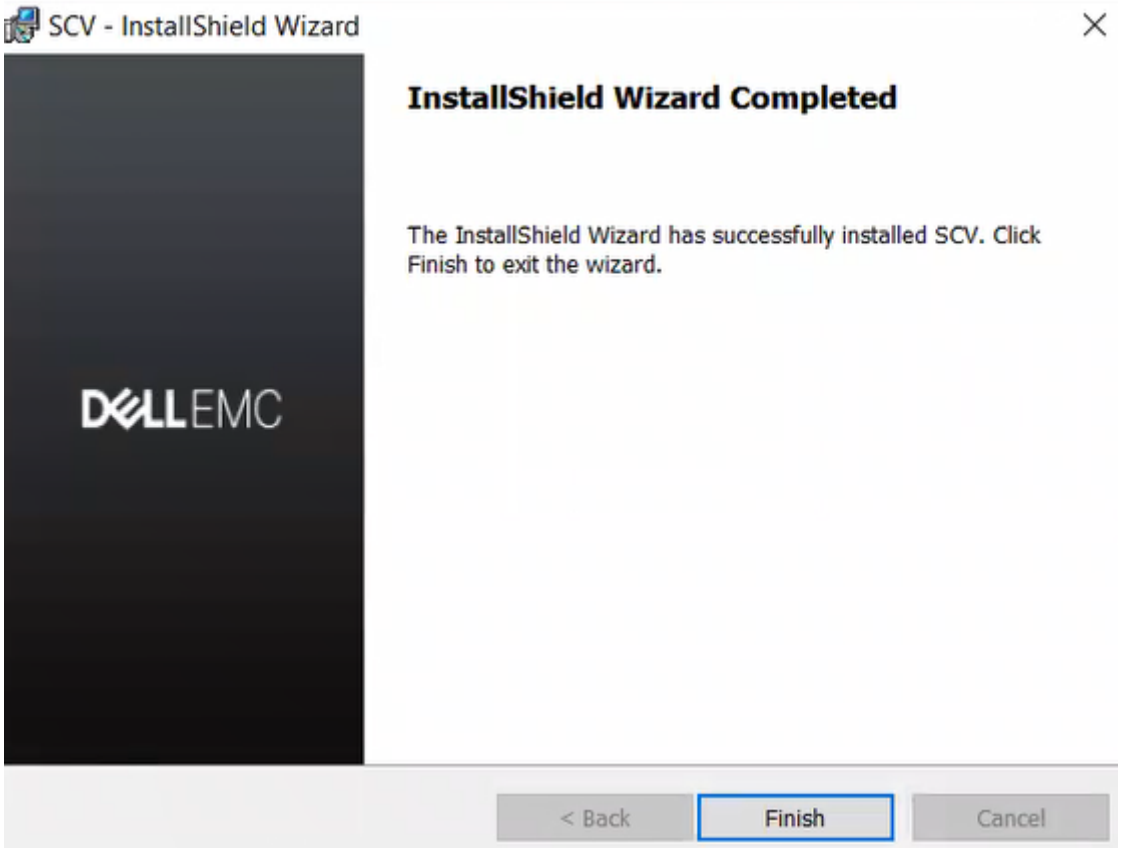

Figure 19. Installation de SCVApp terminée

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 « 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 150 caractères.

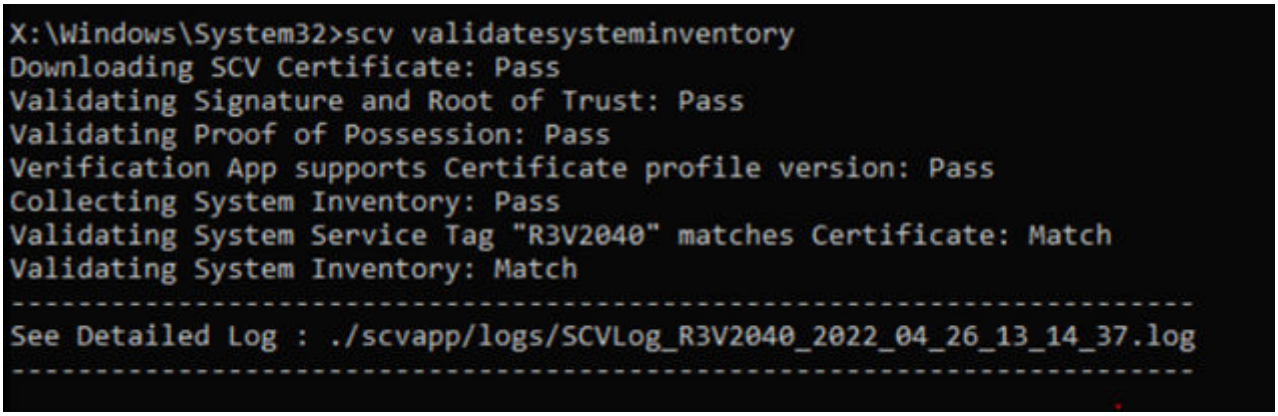

Figure 20. Réussite de l'exécution de la commande de validation et du résultat

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

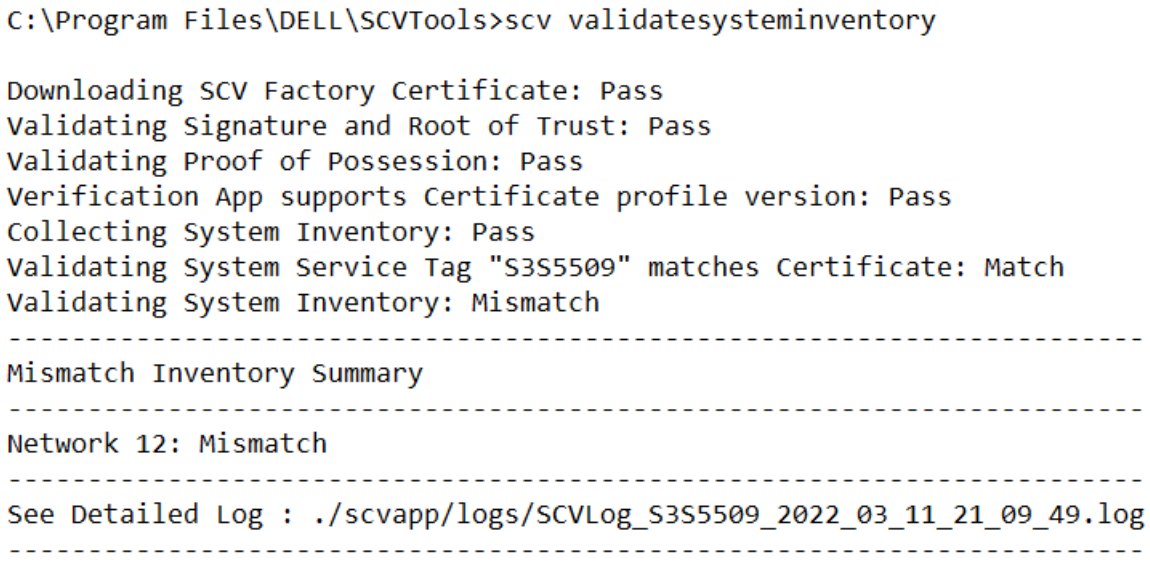

Figure 21. Échec de la validation et du résultat

```
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
--------------------------------------------------------------------------------
```

Figure 22. Détails relatifs aux composants attendus et détectés

5

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

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

```
C:\>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_51_50.log
--------------------------------------------------------------------------
```

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

REMARQUE : L'exemple ci-dessus est destiné à l'exécution de la commande de validation en mode interactif, elle ne nécessite pas de paramètre `-u` et `-p`.

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> -u <iDRAC username> -p <iDRAC password>` pour démarrer le processus de validation.

```
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
```

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

REMARQUE : L'exemple ci-dessus est destiné à l'exécution de la commande de validation en mode interactif, elle ne nécessite pas de paramètre `-u` et `-p`.

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> -u <iDRAC username> -p <iDRAC password>` pour démarrer le processus de validation.

```
[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
--------------------------------------------------------------------------
```

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

REMARQUE : L'exemple ci-dessus est destiné à l'exécution de la commande de validation en mode interactif, elle ne nécessite pas de paramètre `-u` et `-p`.

6

Détails de la commande SCV

Cette section fournit des informations sur certaines commandes scv supplémentaires.

Sujets :

Obtenir des informations sur l'exécution de SCV

Tableau 1. Obtenir plus d'informations sur SCV

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

Sortie

```
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>
```

Obtenir des informations sur la commande scv validatesysteminventory

Tableau 2. Obtenir plus d'informations sur la commande SCV validatesysteminventory

Description	Utilisez la commande suivante pour obtenir plus d'informations sur la commande SCV `validatesysteminventory` et savoir comment l'exécuter.
Synopsis	`scv help validatesysteminventory`

Sortie

```
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.
```

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

Tableau 3. Validation distante d'un inventaire spécifique

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> -u <UserName> -p <Password>`
Entrée	• - `r` — Adresse IPv4/IPv6 • - `u`— Nom d'utilisateur • - `p`— Mot de passe

Sortie

```
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
---------------------------------------------------------------------
```

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

Tableau 4. Validation de l'inventaire à l'aide d'un port spécifique

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> -u <UserName> -p <Password>`
Entrée	• `-r` — Adresse IPv4/IPv6 • `-u`— Nom d'utilisateur • `-p`— Mot de passe

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

Tableau 5. Vérification de la correspondance de l'emplacement des composants

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 <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
---------------------------------------------------------------------
```

Obtenir la version SCV

Tableau 6. Obtenir la 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 1.5 (Build 156)
Copyright(c) 2020 - 2022 Dell, Inc.
All Rights Reserved

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

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

Tableau 7. Affichage ou redirection de la valeur d'un identifiant de certificat

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	`scv extractcert -r <IPv4/IPv6 address> -u <UserName> -p <Password> -component <Component Name> -l <Location> -f <File Name>`
Entrée	• `-r` — Adresse IPv4/IPv6 • `-u`— Nom d'utilisateur • `-p`— Mot de passe • `-component`— Nom du composant • `-l`— Emplacement • `-f`— Nom du fichier

Sortie

```
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==
```

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

```
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
```

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

7

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%20A00.zip

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

MD5 : edb649dbf130e43aeaf5358f1186d312

SHA1 : a92d23c8e9e61fd5c4e568cb23be3024df3f886f

SHA-256 : c947162dc67f5d441ff22b063d7566c52db23cc0c51746455e492c60943f8165

8

Codes de retour

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

Tableau 8. 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 indiquée est hors de la 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/la plate-forme actuelle.
14	La syntaxe de la commande est incorrecte.
15	Commande à exécuter en mode usine (SSM).
16	SCV n'a pas de 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/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.

9

Obtenir de l'aide

Sujets :

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 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 www.dell.com/support/home.
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.