



Distributeur de
valeur ajoutée
watsoft.com - 05 56 15 01 01
Solutions logicielles pour les professionnels de l'IT

Base de connaissances > N-able EDR > Comment résoudre une erreur de signature invalide ?

Comment résoudre une erreur de signature invalide ?

Thibaut - 2024-01-05 - N-able EDR

Comment résoudre une erreur de signature invalide ?

Problème :

Error

Erreur de signature non valide.

Contexte :

Des mises à jour du certificat Windows sont nécessaires.

Causes possibles :

- Ce paramètre de stratégie de groupe
https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.InternetCommunicationManagement::CertMgr_DisableAutoRootUpdates bloque les mises à jour de la racine d'authentification.

- L'accès à l'URL de mise à jour de la racine d'authentification est bloqué par le pare-feu de l'entreprise.

L'accès à ctldl.windowsupdate.com doit être débloqué pour que l'installation fonctionne.

Certificats requis :

Actuellement, l'agent requiert ces certificats racine :

- **Microsoft Azure Code Signing (ACS) root**

Pour l'installation, nous vous recommandons d'avoir des patches plus récents que ceux

mentionnés ici

<https://support.microsoft.com/en-gb/topic/kb5022661-windows-support-for-the-azure-code-signing-program-4b505a31-fa1e-4ea6-85dd-6630229e8ef4>

- **DigiCert root**

Pour l'installation, assurez-vous que vous êtes synchronisé avec les dernières listes de confiance et listes de révocation de certificats.

Configurer un partage réseau pour récupérer les mises à jour de certificats dans les scénarios avec pare-feu et hors ligne (voir les instructions de Microsoft

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn265983\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn265983(v=ws.11))

Autre solution :

Mettez à jour les certificats à partir du site de mise à jour de la racine d'authentification sur Windows 10. Exécutez :

```
certutil -verifyCTL -f AuthRootWU
```

```
certutil -verifyCTL -f DisallowedWU
```

```
certutil -verifyCTL -f PinRulesWU
```

Si ces commandes ne fonctionnent pas en raison d'un pare-feu, créez un fichier SST sur un ordinateur :

```
certutil -generateSSTFromWU C:\roots.sst
```

puis, dans PowerShell, importer ce fichier sur l'ordinateur protégé par un pare-feu :

```
Import-Certificate -FilePath C:\roots.sst -CertStoreLocation Cert:\LocalMachine\Root
```

Pour installer manuellement des certificats numériques :

Si vous ne pouvez pas mettre à jour les certificats expliqués dans les méthodes précédentes, vous pouvez les importer manuellement à partir des fichiers signés sur votre ordinateur.

les importer à partir des fichiers signés dans le magasin de l'autorité de certification racine de confiance de votre point

de votre point d'accès local.

Warning

L'installation manuelle des certificats racine ne résout que les problèmes de signature de l'agent et de son installateur. L'agent s'appuie sur le fait que le système d'exploitation des racines peuplées pour la validation de la signature des logiciels exécutés par l'utilisateur. Si vous ne déployez pas les mises à jour CTL de Microsoft, les certificats malveillants connus qui ont été révoqués ne le sont pas sur votre système.

1 - Cliquez droit sur **SentinelAgent.exe** .

2 - Ouvrez les **propriétés**.

3 - Cliquez sur l'onglet **Signatures numériques / Digital Signatures**.

4 - Sélectionnez chacune des deux signatures qu'elle possède actuellement, puis cliquez sur **Détails > Voir la certification / View Certificate**.

5 - Cliquez sur le **Chemin de certification / Certification Path** pour voir la chaîne exacte de certificats utilisée.

6 - Cliquez sur le bouton **général** et **Installer le certificat**.

7 - Sélectionner **Machine locale / Local Machine** comme emplacement.

8 - Sélectionner **Veillez sélectionner tous les certificats dans le magasin / Please all certificates in the following store** suivant et cliquez sur **Parcourir / Browse**.

9 - Sélectionnez **Autorités de certification racine de confiance / Trusted Root Certification Authorities** comme emplacement du certificat, puis cliquez sur **OK**.

10 - Cliquez sur **Finir**

N'hésitez pas à nous contacter en cas de difficultés.

Vous retrouverez la documentation original ci-joint :

Pièce jointes

- [How To Solve an Invalid Signature Error \(1\).pdf \(286.49 KB\)](#)