Comment résoudre un échec d'installation de l'agent EDR lorsqu'il y a encore des traces ?

Maxime - 2023-09-26 - N-able EDR

Lorsque vous avez une erreur d'installation de l'agent EDR et que l'agent a déjà été installé par le passé sur cette machine, voici ce qu'il faut faire :

Attention : Ceci est à effectuer si le cleaner n'est pas suffisant (KB : https://watsoft.deskpro.com/kb/articles/comment-faire-un-nettoyage-dune-installation-n-able-edr-ou-edri

Cause :

- Si vous n'avez pas utilisé la fonction de suppression de programmes de Windows, la désinstallation peut être partielle. Si des clés de registre, des pilotes et des fichiers se trouvent sur le terminal, la nouvelle installation de l'agent échoue parce qu'il identifie incorrectement l'agent comme étant installé.

Lorsque vous tentez de supprimer des clés de registre, vous obtenez des erreurs d'autorisation

Pour résoudre le problème de la désinstallation de l'agent :

1. Ouvrez le registre de Windows. Dans le menu Démarrer, entrez : regedit.exe et cliquez sur Exécuter en tant que administrateur.

1. Sauvegardez le registre.

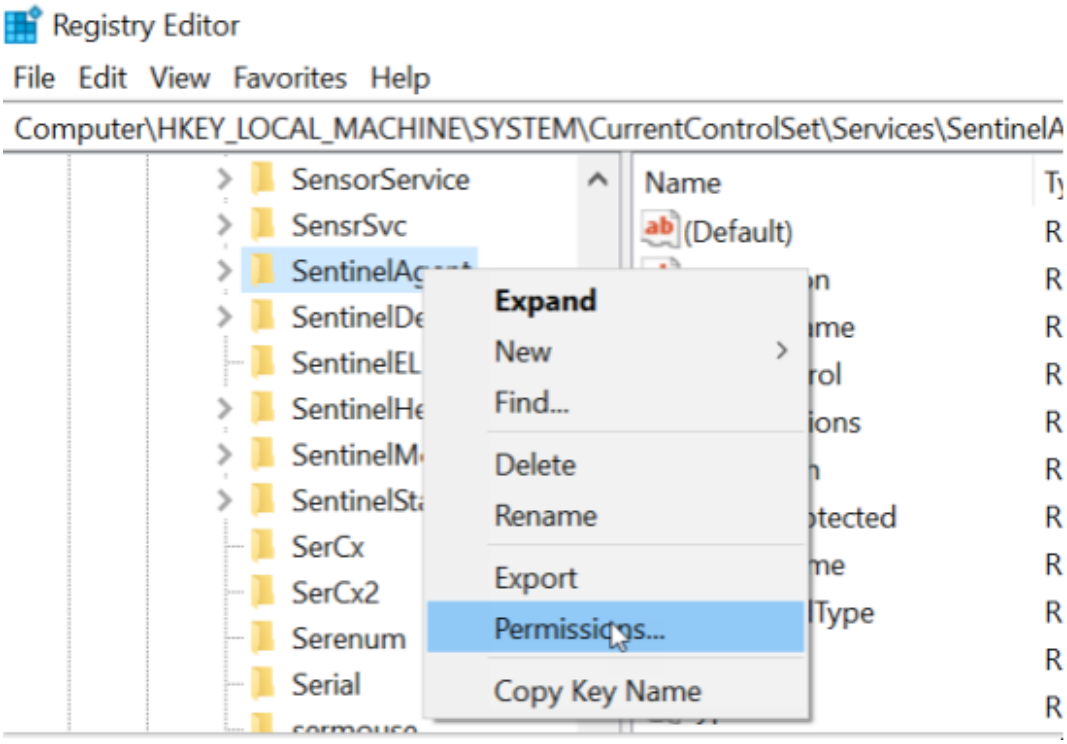
1. Recherchez les dossiers suivants :

```
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SentinelAgent

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
services\SentinelMonitor

Computer\HKEY_CLASSES_ROOT\AppID\SentinelAgent
```

1. Cliquez avec le bouton droit de la souris sur chaque dossier, puis cliquez sur Supprimer.

Si vous obtenez une erreur d'autorisation, modifiez la permissions des clés.

Pour chaque dossier : Cliquez avec le bouton droit de la souris, puis cliquez sur Permissions.



Dans la fenêtre Autorisations, cliquez sur Avancé.

Dans la fenêtre qui s'ouvre, s'il existe un onglet Propriétaire, cliquez sur le nom d'utilisateur Administrateurs.

S'il n'y a pas d'onglet Propriétaire, le nom du propriétaire est du texte dans la fenêtre.

Cliquez sur Modifier. Dans la fenêtre qui s'ouvre, entrez Administrateurs. Cliquez sur OK.

Cliquez sur OK.

Dans la fenêtre Permissions, sélectionnez Administrateurs puis, dans la colonne colonne Autoriser, cliquez sur Contrôle total.

Cliquez sur OK.

Supprimez le dossier de clés

1. Recherchez sentinel dans le registre. Si la désinstallation a eu des problèmes, vous pouvez voir plus de registres à supprimer.

Computer\HKEY_CLASSES_ROOT\AppID\SentinelHelperService
Computer\HKEY_CLASSES_ROOT\SentinelAgent
Computer\HKEY_CLASSES_ROOT\SentinelHelper
Computer\HKEY_CLASSES_ROOT\SentinelOneLog
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\SentinelHelper Service
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SentinelAgent
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SentinelHelper
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SentinelOneLog
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\App ID\SentinelHelperService
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentV ersion\Uninstall\Sentinel Agent
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SentinelAgent.exe
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SentinelCtl.exe Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SentinelHelperService.exe
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SentinelRemediation.exe
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SentinelServiceHost.exe
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SentinelStaticEngine.exe
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SentinelStaticEngineScanner.exe
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\SentinelOneLog
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\ Windows NT\CurrentVersion\Image File

Execution Options\SentinelAgent.exe
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\ Windows NT\CurrentVersion\Image File Execution Options\SentinelCtl.exe Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\ Windows NT\CurrentVersion\Image File Execution Options\SentinelHelperService.exe
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\ Windows NT\CurrentVersion\Image File Execution Options\SentinelRemediation.exe
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\ WindowsNT\CurrentVersion\Image File Execution Options\SentinelServiceHost.exe
- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\ WindowsNT\CurrentVersion\Image File ExecutionOptions\SentinelStaticEngine.exe
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\ WindowsNT\CurrentVersion\Image File Execution Options\SentinelStaticEngineScanner.exe
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\WMI\Autologger\SentinelLogger
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\WMI\Autologger\SentinelLogSession0
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\WMI\Autologger\SentinelStatic
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\LogProcessorService
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SentinelAgent
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SentinelHelperService
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SentinelMonitor
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SentinelStaticEngine
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\SentinelLogger
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\SentinelLogSession0
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\SentinelStatic
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LogProcessorService
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SentinelAgent
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SentinelHelperService
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SentinelMonitor
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SentinelStaticEngine
Computer\HKEY_LOCAL_MACHINE\SYSTEM\Setup\FirstBoot\Services\LogProcessorService
Computer\HKEY_LOCAL_MACHINE\SYSTEM\Setup\FirstBoot\Services\SentinelAgent
Computer\HKEY_LOCAL_MACHINE\SYSTEM\Setup\FirstBoot\Services\SentinelHelperService
Computer\HKEY_LOCAL_MACHINE\SYSTEM\Setup\FirstBoot\Services\SentinelMonitor
Computer\HKEY_LOCAL_MACHINE\SYSTEM\Setup\FirstBoot\Services\SentinelStaticEngine

Supprimer uniquement le dernier DWORD SentinelOneLog_.binlog de
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ApplicationAssociationToasts\SentinelOneLog_.binlog
Supprimez uniquement la dernière valeur binaire "Sentinel Agent" de
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
Ne supprimer que le dernier REG_SZ "Sentinel Agent" de
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

1. Si les dossiers d'installation subsistent, supprimez-les ainsi que leur contenu. Il s'agit des chemins par défaut :

```
C:\Windows\System32\drivers\SentinelOne\

C:\ProgramData\Sentinel\

C:\Program Files\SentinelOne\
```

1. Redémarrez pour appliquer les modifications du registre.