Agent-Installation

> Die Agent-Installation wird für hinzugefügte Computer automatisch versucht

CMD-Skript für Voraussetzungen 2, 3 und 4:

```
:: Ping zulassen
netsh advfirewall firewall add rule name="Ping ICMPv4 zulassen" protocol=icmpv4:8,any dir=in
action=allow

:: c$-Freigabe zulassen (damit das Setup kopiert werden kann)
netsh advfirewall firewall set rule name="Datei- und Druckerfreigabe (SMB eingehend)" new
enable=yes

:: Remote-WMI erlauben (damit das Setup ausgeführt werden kann)
netsh advfirewall firewall set rule group="Windows-Verwaltungsinstrumentation (WMI)" new
enable=yes

:: UAC-Beschränkung aufheben (in Arbeitsgruppen benötigt, falls die UAC aktiv ist)
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

Voraussetzung 1: Gültiger Windows-Login

Damit das Agent-Setup zum Computer kopiert und remote ausgeführt werden kann, benötigt der ConfigHub unter Organisation einen gültigen Windows-Login, welcher über lokale Administratoren-Rechte verfügt.

image.png

Voraussetzung 2: Ping ist möglich

Der Ping sollte zu Computern möglich sein (außer dies ist explizit nicht erwünscht - hierfür gibt es die Server-Einstellung "Ping zu Agents ist erlaubt").

Details zum Ping

Überprüfung

Über eine Eingabeaufforderung den Befehl **ping [IP-Adresse] -4** ausführen

Windows-Defender-Firewall

Die entsprechende Windows-Defender-Firewall-Regel heißt "**Kernnetzwerkdiagnose - ICMP-Echoanforderung (ICMPv4 eingehend)**" und ist standardmäßig deaktiviert.

Leider kann die Firewall-Regel über folgenden CMD-Befehl (erfordert Admin-Rechte) nicht immer aktiviert werden (da sie unter dem Namen nicht immer gefunden wird):

```
netsh advfirewall firewall set rule name="Kernnetzwerkdiagnose - ICMP-Echoanforderung (ICMPv4 eingehend)" new enable=yes
```

Voraussetzung 3: c$-Freigabe ist erreichbar

Die c$-Freigabe (SMB Port 445) muss erreichbar sein, damit das Setup über die c$-Freigabe (nach C:\ProgramData\ConfigHub\Agent) kopiert werden kann.

Details zur c$-Freigabe

Überprüfung

Der Zugriff kann getestet werden, ob die c$-Freigabe über den Windows-Explorer geöffnet werden kann.
Hierbei muss einer der Windows-Logins aus der ConfigHub Organisation verwendet werden.

Windows-Defender-Firewall

Die entsprechende Windows-Defender-Firewall heißt "**Datei- und Druckerfreigabe (SMB eingehend)**" und ist standardmäßig deaktiviert.

Die Firewall-Regel kann über folgenden CMD-Befehl (erfordert Admin-Rechte) aktiviert werden:

```
netsh advfirewall firewall set rule name="Datei- und Druckerfreigabe (SMB eingehend)" new enable=yes
```

Voraussetzung 4: Setup lässt sich remote ausführen

Damit das Setup remote gestartet werden kann, muss entweder

- Remote-WMI (Port 135) erreichbar sein
- oder die Admin$ - Freigabe für PsExec erreichbar sein

Bei aktiver Benutzerkontensteuerung (UAC)

Damit das Setup über die WMI (Windows Management Instrumentation) oder PsExec ausgeführt werden, muss bei aktiver Benutzerkontensteuerung folgender Registry-Wert gesetzt werden, damit der Zugriff auf die WMI oder die Admin$-Freigabe gewährt wird:

Registry-Pfad:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Registry-Wertname: LocalAccountTokenFilterPolicy
Registry-Werttyp: DWORD
Registry-Wert: 1

Es kann folgender CMD-Befehl (mit Admin-Rechten) ausgeführt werden (überschreiben mit ja bestätigen):

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1
```

Alternativ kann auch eine .reg-Datei mit folgendem Inhalt ausgeführt werden:

```
Windows Registry Editor Version 5.00


[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"LocalAccountTokenFilterPolicy"=dword:00000001
```

Einstellungen für WMI (Windows Management Instrumentation)

Windows-Defender-Firewall

Die entsprechenden Windows-Defender-Firewall heißen "**Windows-Verwaltungsinstrumentation (DCOM eingehend)**" und "**Windows-Verwaltungsinstrumentation (WMI eingehend)**". Diese sind standardmäßig deaktiviert.

Die Firewall-Regeln können über folgenden CMD-Befehl (erfordert Admin-Rechte) aktiviert werden:

```
netsh advfirewall firewall set rule group="Windows-Verwaltungsinstrumentation (WMI)" new enable=yes
```

Alternative: Agent-Setup manuell ausführen

Das Setup kann auch manuell ausgeführt werden.

Der ConfigHub Server lädt die aktuelle Version nach **C:\Programdata\ConfigHub\Server\Downloads** herunter.

Revision #13
Created 15 October 2022 06:53:39 by Dennis Hempel
Updated 21 February 2023 20:41:16 by Dennis Hempel