Anleitungen

- Installation des Servers
- Computer hinzufügen
- Agent-Installation
- Umzug des Servers auf anderen Computer
- Software Setup-Parameter herausfinden

Installation des Servers

Download

- Das Setup kann unter https://config-hub.de/downloads heruntergeladen werden.

Setup

Login

- Für das Setup wird ein Login benötigt:

image.png
Image not found or type unknown

Komponenten-Auswahl

- Anschließend können die Komponenten ausgewählt werden:

image.png
Image not found or type unknown

Server-Einstellungen

- Kunden -Nummer und -Name: Diese Informationen dienen aktuell nur zur Identifikation der Installation
- Admin-Passwort: Hier wird das Windows-Passwort vom Administrator abgefragt. Dieses Passwort wird für die Installation des Agents (Dienst) an den Computern benötigt

image.png
Image not found or type unknown

Admin-Einstellungen

- Wird der Admin installiert, wird das Verzeichnis C:\ProgramData\ConfigHub\Admin freigegeben (Freigabe-Name ConfigHubAdmin$) und es kann eine UNC-Pfad-Verknüpfung auf dem Desktop abgelegt werden:

image.png
Image not found or type unknown

Zusammenfassung

- Beim Klick auf Installieren starten die Setups:

image.png
Image not found or type unknown

Installations-Fortschritt

image.png
Image not found or type unknown

Installations-Abschluss

> Der Admin sollte einmalig gestartet werden (Login wird nicht benötigt), damit die Server-IP-Adresse konfiguriert wird

image.png
Image not found or type unknown

Computer hinzufügen

Möglichkeit 1: Netzwerk-Scan

Unter Computer / Übersicht lässt sich der Netzwerk-Scan über den Button "NW-Scan" öffnen:

image.png
Image not found or type unknown

Der Scan startet automatisch beim 1. Aufruf. Nach dem Abschluss des Scans können alle gefundenen Computer oder einzelne Computer hinzugefügt werden:

image.png
Image not found or type unknown

Möglichkeit 2: Computer einzeln hinzufügen

Unter Computer / Übersicht lässt sich über den Button "Computer hinzufügen" ein einzelner Computer hinzuzufügen:

image.png
Image not found or type unknown

Es wird eine IP-Adresse oder ein Hostname benötigt:

image.png
Image not found or type unknown

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
Image not found or type unknown

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.

Umzug des Servers auf anderen Computer

Beim Umzug auf einen anderen Server müssen folgende Schritte befolgt werden:

Export der vorhandenen Datenbank

Unter Einstellungen / Server-Datenbank / Exportieren kann die Datenbank exportiert und entschlüsselt werden:

> Die Kennwörter werden in der exportierten Datenbank entschlüsselt gespeichert (sind als Klartext lesbar)

image.png
Image not found or type unknown

Setup am neuen Server

Liegt die exportierte Datenbank neben dem ConfigHub.Setup, wird diese vom Setup kopiert und die Konfiguration bei der Installation wird übersprungen:

image.png
Image not found or type unknown

Bereinigungen

- Die exportierte Datenbank (z.B. neben dem Setup liegend) muss in jedem Fall gelöscht werden, da in dieser die Kennwörter im Klartext lesbar sind
- Der ConfigHub.Server sollte auf dem alten Computer deinstalliert werden

Software Setup-Parameter herausfinden

Um Software silent installieren zu können, werden Aufrufparameter benötigt. Diese sind je nach verwendeter Setup-Software unterschiedlich.

Setup-Software identifizieren

Zunächst muss man herausfinden, welche Setup-Software verwendet wird. Hierzu bietet es sich an, das %temp%-Verzeichnis zu leeren und das Setup zunächst normal zu starten.

Beim Inno-Setup werden im %temp%-Verzeichnis Ordner mit Namen "is-[...].tmp" angelegt.

Inno-Setup

Vollständige Liste aller Setup-Aufrufparameter:

https://jrsoftware.org/ishelp/index.php?topic=consts

Für normale Silent-Installationen reichen normalerweise folgende Parameter aus:

```
/VERYSILENT /NOCANCEL /NORESTART /SUPPRESSMSGBOXES
```

Möchte man innerhalb des Setups z.B. Komponenten auswählen, kann das Setup eine inf-Datei generieren:

```
/SAVEINF="C:\InnoSetup.inf"
```

Aus dieser Datei kann ausgelesen werden, welche zusätzlichen Parameter gesetzt werden können.

MSI-Setups

Vollständige Liste aller Setup-Aufrufparameter: https://learn.microsoft.com/en-us/windows/win32/msi/standard-installer-command-line-options

Für normale Silent-Installationen reichen normalerweise folgende Parameter aus:

```
/quiet /norestart
```

Möchte man innerhalb des Setups z.B. Komponenten auswählen oder den Zielpfad anpassen, kann eine Datei erstellt werden, die beim Setup alle Parameter aufführt:

```
/lp! c:\msi-parameter.txt
```

InstallShield-Setups

Es kann eine Silent-Setup-Datei mit folgendem Befehl erstellt werden:

```
setup.exe /r /f1"C:\setup.iss"
```

Diese kann anschließend zur Silent-Installation mit folgendem Befehl verwendet werden:

```
setup.exe /s /f1"C:\setup.iss"
```