

Handbuch

Version 2.70 (16.09.2020)

**Published by**

Netree AG

<http://www.netree.ch>

**Copyright © 2020 by Netree AG**

All rights reserved. No part of this manual may be reproduced or transmitted in any form or by any means without the prior written permission of the publisher.

**Warning and Disclaimer**

Every effort has been made to make this manual as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

**Feedback Information**

We like to hear from you! If you have any comments about how we could improve the quality of this book, please don’t hesitate to contact us by visiting [www.netcim.ch](http://www.netcim.ch).

**Inhaltsverzeichnis**

[1 Einleitung 6](#_Toc51157195)

[1.1 Änderungshistorie 6](#_Toc51157196)

[1.2 Definitionen 6](#_Toc51157197)

[1.3 Begriffsdefinition 7](#_Toc51157198)

[1.4 Kompatibilitätsmatrix 8](#_Toc51157199)

[1.4.1 Hinweise 8](#_Toc51157200)

[2 Prerequisites 9](#_Toc51157201)

[2.1 Hardware 9](#_Toc51157202)

[2.1.1 netCIM Server 9](#_Toc51157203)

[2.1.2 netCIM Content Server 9](#_Toc51157204)

[2.1.3 netCIM Boot Image Management Computer 10](#_Toc51157205)

[2.1.4 netCIM vOS Management Computer 10](#_Toc51157206)

[2.1.4.1 Windows Server 2016 / 2019 10](#_Toc51157207)

[2.1.5 Clients 11](#_Toc51157208)

[2.1.6 Netzwerkkomponenten 11](#_Toc51157209)

[2.2 Application Software 12](#_Toc51157210)

[2.2.1 Windows Server 2016 / Windows Server 2019 12](#_Toc51157211)

[2.2.1.1 netCIM Server 12](#_Toc51157212)

[2.2.1.2 netCIM Content Server 12](#_Toc51157213)

[2.2.1.3 netCIM Boot Image Management Computer 12](#_Toc51157214)

[2.2.1.4 netCIM vOS Management Computer 13](#_Toc51157215)

[2.2.1.5 Images 13](#_Toc51157216)

[Installation 14](#_Toc51157217)

[2.3 Installation .NET 3.5 und IIS 14](#_Toc51157218)

[2.3.1 Windows Server 2016 14](#_Toc51157219)

[2.3.2 Windows Server 2019 18](#_Toc51157220)

[2.4 Konfiguration Data Deduplication (Content und netCIM Server) 21](#_Toc51157221)

[2.5 Installation ADK 22](#_Toc51157222)

[2.5.1 Windows Server 2016 / Windows Server 2019 22](#_Toc51157223)

[2.6 Microsoft SQL Server 2019 Express 26](#_Toc51157224)

[2.6.1 Windows Server 2016 / 2019 26](#_Toc51157225)

[2.7 Installation Visual C++ Redist for Visual Studio 2015-2019 x64 und x86 29](#_Toc51157226)

[2.8 Konfiguration Active Directory für Kerberos Authentication 31](#_Toc51157227)

[2.8.1 Vor netCim Version 6.5.7083.0 31](#_Toc51157228)

[2.8.2 Ab netCIM Version 6.5.7083.0 31](#_Toc51157229)

[2.9 Konfiguration Windows Firewall auf dem netCIM Server 31](#_Toc51157230)

[2.10 Installation netCIM 32](#_Toc51157231)

[2.10.1 Windows Server 2016 / Windows Server 2019 32](#_Toc51157232)

[2.11 Konfiguration PXE Boot 37](#_Toc51157233)

[2.11.1 Variante DHCP Server/Optionen 37](#_Toc51157234)

[Windows Server 2016 / 2019 38](#_Toc51157235)

[2.11.2 Variante IP Helper 43](#_Toc51157236)

[2.12 Konfiguration Switches/Router/Firewall 43](#_Toc51157237)

[2.12.1 Benötigte Netzwerk Ports 44](#_Toc51157238)

[3 netCIM aktualisieren 45](#_Toc51157239)

[3.1 Vorbereitungen 45](#_Toc51157240)

[3.2 Neue netCIM Version installieren 45](#_Toc51157241)

[3.2.1 Windows Server 2016 / Windows Server 2019 45](#_Toc51157242)

[3.3 Nachbereitungen 50](#_Toc51157243)

[4 Konfiguration 51](#_Toc51157244)

[4.1 Boot Image generieren und registrieren 51](#_Toc51157245)

[4.1.1 Windows Server 2016 / Windows Server 2019 51](#_Toc51157246)

[4.1.1.1 Create Boot Image 51](#_Toc51157247)

[4.1.1.2 Upload Boot Image 52](#_Toc51157248)

[4.2 vOS Tool 53](#_Toc51157249)

[4.2.1 Vorhandene Befehle 53](#_Toc51157250)

[4.2.2 vOS von einer ISO-Datei erstellen 54](#_Toc51157251)

[4.2.2.1 Windows Server 2016 / Windows Server 2019 54](#_Toc51157252)

[4.2.3 Neue vOS Version erstellen 56](#_Toc51157253)

[4.2.4 Bestehende vOS Version bearbeiten 57](#_Toc51157254)

[4.2.5 Ein vOS kopieren 59](#_Toc51157255)

[4.2.6 vOS Versionen zusammenführen 59](#_Toc51157256)

[4.2.7 vOS Löschen 59](#_Toc51157257)

[4.2.8 vOS Version löschen 59](#_Toc51157258)

[4.2.9 vOS Informationen ergänzen 59](#_Toc51157259)

[4.2.10 vOS Informationen abfragen 59](#_Toc51157260)

[4.2.11 Image Optimierung 60](#_Toc51157261)

[4.2.12 Wichtige Tasks im Imageerstellungsprozess 60](#_Toc51157262)

[4.2.13 Windows 10 Zeitproblematik 60](#_Toc51157263)

[4.3 Deploy Actions 61](#_Toc51157264)

[4.3.1 Allgemeines 61](#_Toc51157265)

[4.3.2 Variablen im PowerShell Code verwenden 61](#_Toc51157266)

[4.3.3 Beispiele 62](#_Toc51157267)

[4.3.3.1 Ausführen einer beliebigen ausführbaren Datei 62](#_Toc51157268)

[4.3.3.2 Ausführen einer MSI Datei 63](#_Toc51157269)

[4.3.3.3 Installation einer Applikation über OneGet 63](#_Toc51157270)

[4.3.3.4 Windows Update mit PowerShell 64](#_Toc51157271)

[4.3.3.5 Installation einer Applikation mit dem netECM:Launcher 65](#_Toc51157272)

[4.3.3.6 Firewall für netCIM auf den Clients konfigurieren 66](#_Toc51157273)

[4.4 Driver Collections 67](#_Toc51157274)

[4.5 OSD Sequence erstellen 67](#_Toc51157275)

[4.5.1 Variablen im Unattend XML 68](#_Toc51157276)

[4.5.2 Konfiguration Join-Domain 69](#_Toc51157277)

[4.5.3 Konfiguration Copy Profile 70](#_Toc51157278)

[4.6 Host Gruppe erstellen 71](#_Toc51157279)

[4.7 Host erfassen 72](#_Toc51157280)

[4.7.1 Unknown Computer Support - Automatisches erfassen 72](#_Toc51157281)

[4.7.2 Unknown Computer Support aus-/einschalten 73](#_Toc51157282)

[4.7.3 Manuelles erfassen 74](#_Toc51157283)

[4.7.4 Host import 76](#_Toc51157284)

[4.8 Berechtigungen 76](#_Toc51157285)

[4.8.1 netCIM Benutzer Rollen 76](#_Toc51157286)

[4.8.2 Best Practice AD Benutzer und Gruppen 76](#_Toc51157287)

[4.8.3 Eigenständige netCIM Content Server 77](#_Toc51157288)

[4.9 Features 78](#_Toc51157289)

[4.9.1 User Logon / Auto Logon 78](#_Toc51157290)

[4.9.2 Mounten der Datenpartition während dem Deployment 81](#_Toc51157291)

[4.9.2.1 Anwendungsbeispiel 81](#_Toc51157292)

[5 Betrieb 82](#_Toc51157293)

[5.1 Jobs auslösen und planen 82](#_Toc51157294)

[5.1.1 Wake On LAN 82](#_Toc51157295)

[5.1.2 Herunterfahren nach Job Verarbeitung 82](#_Toc51157296)

[5.2 Backup und Restore 82](#_Toc51157297)

[5.2.1 Restore SQL Datenbank und netCIM Source 83](#_Toc51157298)

[5.2.1.1 Windows Server 2016 / Windows Server 2019 83](#_Toc51157299)

[5.3 Virenschutz Client 84](#_Toc51157300)

[6 Troubleshooting 85](#_Toc51157301)

[6.1 Allgemein 85](#_Toc51157302)

[6.1.1 Debug Logging aktivieren 85](#_Toc51157303)

[6.1.2 Log Dateien und Speicherorte 86](#_Toc51157304)

[6.1.3 Arbeiten mit dem Log Viewer 86](#_Toc51157305)

[6.2 OS Deployment 87](#_Toc51157306)

[6.2.1 Treiberinstallation im WinPE 87](#_Toc51157307)

[6.2.2 Treiberinstallation im Windows Setup 88](#_Toc51157308)

[6.2.3 Domain Join 88](#_Toc51157309)

[6.2.3.1 Advanced debugging Setupact 89](#_Toc51157310)

[6.2.3.2 Advanced debugging Netsetup 89](#_Toc51157311)

[6.2.3.3 Use another approach to domain join 92](#_Toc51157312)

[6.3 Group Policies 92](#_Toc51157313)

[7 Best Practice – Deploy Actions 93](#_Toc51157314)

[8 Best Practice – Treiber Engineering 94](#_Toc51157315)

[9 Best Practice - Active Directory Machine Password 95](#_Toc51157316)

# Einleitung

Dieses Dokument beschreibt die wichtigsten Punkte von netCIM in Bezug auf die Anforderungen, Installation, Konfiguration und Betrieb. Es enthält zudem Best Practices Informationen und Troubleshooting Ansätze.

Das Dokument wird mit dem Versionszyklus von netCIM aktualisiert und gepflegt.

## Änderungshistorie

|  |  |  |
| --- | --- | --- |
| Version | Autor | Anpassungen |
| 2.62 | Nicola Suter | netCIM Q1 Neuerungen, Windows 10 Secure Time ergänzt |
| 2.63 | Nicola Suter | netCIM Q2 User Logon und Shutdown Feature hinzugefügt, vOS Tool Beispiele ergänzt, Konfiguration Domainjoin und CopyProfile hinzugefügt |
| 2.64 | Sandro Anderes | netCIM Q3 Datenpartition während dem Deployment verwenden hinzugefügt |
| 2.64.1 | Sandro Anderes | Anpassungen vOS Tool Befehle |
| 2.66 | Danilo Dattilo | Anpassung an Server 2016 |
| 2.69 | Sandro Anderes | Anpassungen Copy Profile |
| 2.70 | Remo Schenk / Giuliano Donatiello | Anpassung an Server 2019 und Überarbeitung komplettes Handbuch |

## Definitionen

|  |
| --- |
| Hinweis |
| Zusätzliche Informationen und Links. |

|  |
| --- |
| Wichtig |
| Wichtige Informationen. |

|  |
| --- |
| Schlussfolgerung |
| Gründe für eine gewählte Lösung. |

|  |
| --- |
| Abklärung |
| Muss noch abgeklärt werden. |

## Begriffsdefinition

|  |  |
| --- | --- |
| Begriff | Beschreibung |
| netCIM Server Rolle | Zentraler Server welcher die Source Daten für die Content Server und das netCIM Cockpit bereitstellt. |
| netCIM Content Server Rolle | Diese Rolle stellt den Content für Clients bereit und kann an einem Aussenstandort helfen zur Entlastung der WAN Verbindungen beizutragen. Meist wird diese Rolle auch auf dem zentralen netCIM Server installiert. |
| netCIM Boot Image Management Rolle | Die dadurch zur Verfügung stehenden Tools ermöglichen das Erstellen eines Boot Images (WinPE) für netCIM. |
| netCIM vOS Management Rolle | Diese Rolle muss zwingend auf einem physikalischen Gerät mit aktivierter Hyper-V Rolle installiert werden. Es wird dadurch möglich, neue vOS zu erstellen und bestehende anzupassen. |
| Deploy Action | Eine Deploy Action kann während dem Deployment Prozess (nach dem OS Setup) ausgeführt werden. Sie wird durch ein PowerShell Script definiert und kann Content aufweisen, um beispielsweise ein Programm während dem Deployment zu installieren oder Einstellungen vorzunehmen. |
| Driver Collection | Pro HardwareType, OSVersion und OSArchitektur kann ein Treiber-Paket erstellt werden. Dadurch lässt sich das anzuwendende Treiber-Paket eindeutig identifizieren. |
| vOS | Basis VHD/VHDX eines Betriebssystems oder Version welche nicht generalisiert ist. |
| vOS Generalized Checkpoint | Ein Checkpoint der ein mit Sysprep generalisiertes Betriebssystems enthält. |
| vOS Customized Checkpoint | Ein Checkpoint der ein Betriebssystem enthält, welches den Setup Prozess durchlaufen hat und auf dem alle Deploy Actions ausgeführt wurden. |
| vOS Work Checkpoint | Dieser Checkpoint enthält alle Änderungen seitdem letzten  vOS Customized Checkpoint. Diese werden bei einem Rapid Recovery gelöscht und auf den Stand des Customized Checkpoint zurückgesetzt. |
| OSD Sequence | Definiert den OS Deployment Prozess für ein Image. |
| Host Groups | Logische Gruppierung von mehreren Hosts. Diese Gruppe definiert z.B. die angewendeten OSD Sequenzen und die verwendeten Content Server. |
| Jobs - Full Deployment | Full Deployment oder initiales Deployment. Die Festplatte des Hosts wird neu formatiert und sämtlicher Content wird neu heruntergeladen und eingerichtet. |
| Jobs - Update Deployment | Bei diesem Deployment Typ werden nur die benötigten Daten neu heruntergeladen sowie die Konfigurationsschritte ausgeführt die noch nicht abgeschlossen sind. |
| Jobs - Rapid Recovery | Schnelles zurücksetzen eines Computers. Ist Offline möglich. Es werden nur die Änderungen seit dem letzten Aufsetzen verworfen. |

## Kompatibilitätsmatrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **Windows 10 x86** | **Windows 10 x64** | **Comment** |
| Firmware Type | UEFI |  | X | Limitation by UEFI |
| UEFI Secure Boot |  |  | Not Supported by netCIM |
| Legacy BIOS | X | X |  |
|  |  |  |  |  |
| Harddisk | VHD | X | X |  |
| VHDX | X | X |  |
|  |  |  |  |  |
| VM used for Maintenance | VM Gen 1 | X | X |  |
| VM Gen 2 |  | X |  |
|  |  |  |  |  |
| WinPE | WinPE 10 x86 | x | x | Not Supported on UEFI |
| WinPE 10 x64 |  | x |  |

### Hinweise

|  |
| --- |
| Wichtig |
| **Windows 10 x64/x86**  Windows 10 Pro, Enterprise und Education Editionen werden unterstützt.  **UEFI Compatibility Mode**  Einige Hardwarehersteller bieten im BIOS einen sogenannten „UEFI Compatibility Mode“ an, welcher beim PXE Bootvorgang im Legacy Mode bootet. Diese Einstellung wird von netCIM nicht unterstützt. |

# Prerequisites

## Hardware

Der netCIM Server sollte folgenden Anforderungen genügen um optimale Leistung zu gewährleisten. Je mehr Clients verwaltet werden, desto besser sollte der Server bezüglich Netzwerk- und Harddisk-Performance ausgestattet sein.

Grundsätzlich empfehlen wir die Rollen Server, Content Server und Boot Image Management auf einem Server zu installieren. Sofern dies ein physikalischer Host ist, kann auch die vOS Management Rolle installiert werden.

### netCIM Server

|  |  |  |
| --- | --- | --- |
|  | Minimum | Empfohlen |
| Virtualisierung möglich | Ja | Ja |
| Prozessor | 1 Core | 4 Cores |
| Arbeitsspeicher (RAM) | 8GB | 16GB |
| System Disk | 100GB | 100GB Redundant |
| Data Disk | Die Grösse ist abhängig vom Content, welcher durch netCIM verwaltet wird (vOS, Deploy Actions, Driver Collections, usw.) | Die Grösse ist abhängig vom Content, welcher durch netCIM verwaltet wird (vOS, Deploy Actions, Driver Collections, usw.) |
| Netzwerk | 1/Gbits | Mehrere 1/Gbits Netzwerkadapter und teamingfähige Switches |

### netCIM Content Server

|  |  |  |
| --- | --- | --- |
|  | Minimum | Empfohlen |
| Virtualisierung möglich | Ja | Ja |
| Prozessor | 1 Core | 2 Cores |
| Arbeitsspeicher (RAM) | 2GB | 4GB |
| System Disk | 100GB | 100GB Redundant |
| Data Disk | Die Grösse ist abhängig vom Content, welcher durch netCIM verwaltet wird (vOS, Deploy Actions, Driver Collections, usw.) | Die Grösse ist abhängig vom Content, welcher durch netCIM verwaltet wird (vOS, Deploy Actions, Driver Collections, usw.) |
| Netzwerk | 1/Gbits | Mehrere 1/Gbits Netzwerkadapter und teaming fähige Switches |

### netCIM Boot Image Management Computer

|  |  |  |
| --- | --- | --- |
|  | Minimum | Empfohlen |
| Virtualisierung möglich | Ja | Ja |
| Prozessor | 1 Core | 2 Cores |
| Arbeitsspeicher (RAM) | 2GB | 4GB |
| System Disk | 100GB | 100GB Redundant |
| Netzwerk | 1/Gbits | 1/Gbits |

### netCIM vOS Management Computer

#### Windows Server 2016 / 2019

|  |  |  |
| --- | --- | --- |
|  | Minimum | Empfohlen |
| Virtualisierung möglich | Nein | Nein |
| Prozessor | * 4 Cores * Intel VT (Intel Virtualization Technology)- oder AMD-V (AMD Virtualization)-Technologie * Intel XD-Bit (Execute Disable Bit) oder AMD NX-Bit (No Execute Bit) * Hyper-V 2016 / 2019 kompatibel | * 4 Cores * Intel VT (Intel Virtualization Technology)- oder AMD-V (AMD Virtualization)-Technologie * Intel XD-Bit (Execute Disable Bit) oder AMD NX-Bit (No Execute Bit) * Hyper-V 2016 / 2019 kompatibel |
| Arbeitsspeicher (RAM) | 8GB | 16GB |
| System Disk | 100GB | 100GB |
| Data Disk | Die Grösse ist abhängig von der Gesamtgrösse der vOS Daten. | Die Grösse ist abhängig von der Gesamtgrösse der vOS Daten. |
| Netzwerk | 1/Gbits | 1/Gbits |

|  |
| --- |
| Hinweis |
| Es wird empfohlen, diese Rolle nicht auf einem produktiven Hyper-V Server zu installieren, da einige Task (z.B. Image Optimierung) sehr Ressourcen(CPU/Memory/HD) intensiv sind. |

### Clients

|  |  |
| --- | --- |
|  | Minimum |
| Allgemein | Mindestanforderungen der Betriebssysteme |
| Arbeitsspeicher (RAM) | 2GB Ram |
| Motherboard | Legacy BIOS falls 32 Bit Betriebssysteme verteilt werden (Siehe ‎1.4 Kompatibilitätsmatrix). |
| Hard Disk / SSD | Bedingt durch die neue Technologie sollte genügend Platz eingerechnet werden. Dies hängt auch davon ab, wie oft eine neue Version eines Images erstellt wird. Bei geringen Änderungen wird ca. 2GB Speicherplatz benötigt. Daher folgende Rechnung, wenn ein Grundimage mit einer Grösse von 100GB verteilt wird und monatlich Updates eingespielt werden:  100GB + 4 Jahre \* 12 Monate \* 2GB = 196 GB  Daher sollte dieser Client mindestens eine 196GB grosse Hard Disk besitzen.   |  | | --- | | Hinweis | | Es gibt auch die Möglichkeit die Images von Zeit zu Zeit zu optimieren. Dann muss aber einmalig wieder das neue Grundimage verteilt werden. |   Systematische Darstellung, vor- und nach dem Merge-Vorgang: |

### Netzwerkkomponenten

Sollen für den PXE Boot DHCP Optionen verwendet werden, so muss der DHCP Server Custom Vendor und User Classes unterstützen. Für den Microsoft DHCP Server gibt es eine Anleitung und Konfigurationshinweise.

## Application Software

### Windows Server 2016 / Windows Server 2019

#### netCIM Server

|  |  |
| --- | --- |
| Betriebssystem | Windows Server 2016 / 2019 Standard |
| Applikationen | .NET 3.5  IIS 🡪 siehe Prerequisites Installation  MS SQL Server 2014 oder neuer   * Mind. Express Edition * Kann auch auf einem anderen Server sein * (Achtung Speicherplatz für das Logging) |

|  |
| --- |
| Wichtig |
| Wir empfehlen zudem die Konfiguration und den Einsatz des Data Deduplication Features von Windows Server 2016. Dadurch kann mit grosser Wahrscheinlichkeit Speicherplatz eingespart werden. Hinweise zur Konfiguration sind im Kapitel ‎2.4 enthalten. |

#### netCIM Content Server

|  |  |
| --- | --- |
| Betriebssystem | Windows Server 2016 / 2019 Standard |
| Applikationen | IIS 🡪 Siehe Prerequisites Installation  Visual C++ Redistributable Packages for Visual Studio 2015 - 2019 x64 und x86 |

|  |
| --- |
| Wichtig |
| Wir empfehlen zudem die Konfiguration und den Einsatz des Data Deduplication Features von Windows Server 2016 / 2019. Dadurch kann mit grosser Wahrscheinlichkeit Speicherplatz eingespart werden. Hinweise zur Konfiguration sind im Kapitel ‎2.4 enthalten. |

#### netCIM Boot Image Management Computer

|  |  |
| --- | --- |
| Betriebssystem | Windows Server 2016 / 2019 Standard  Windows 10 x64 Pro, Enterprise oder Education |
| Applikationen | **Windows Assessment and Deployment Kit** (ADK) für Windows 10   * Deployment Tools * Windows Preinstallation Environment (Windows PE)   Visual C++ Redistributable Packages for Visual Studio 2015 - 2019 x64 und x86 |

#### netCIM vOS Management Computer

|  |  |
| --- | --- |
| Betriebssystem | Windows Server 2016 / 2019 Standard  Windows 10 x64 Pro, Enterprise oder Education |
| Features | Hyper-V Rolle  Automount |

|  |
| --- |
| Wichtig |
| Automount muss aktiviert sein, damit das vOS Tool die neuen Volume automatisch dem System hinzufügt und ordnet dann dem Laufwerk einen Laufwerksbuchstaben zu. Hier noch den Link dazu, wie man zu den Infos kommt.  <https://technet.microsoft.com/de-ch/library/cc753703(v=ws.11).aspx> |

#### Images

|  |  |
| --- | --- |
| Betriebssystem | **Windows 10** x86/x64 **Pro, Enterprise** oder **Education** |
| Applikationen | Mindestens   * Microsoft .NET 4.5.2 * Microsoft Management Framework 4 |

### Installation

## Installation .NET 3.5 und IIS

### Windows Server 2016

|  |  |
| --- | --- |
|  | Windows Installations-DVD einlegen oder ISO File verbinden. |
|  | Starten sie den „add roles and features“ Prozess. |
|  | Weiter |
|  | “Role-based or feature-based installation“ auswählen |
|  | Weiter |
|  | Wählen sie die Web Server (IIS) Rolle aus. |
|  | Wählen sie die benötigten Features analog dem Bildschirmausschnitt aus.   * .NET Framework 3.5 Features   + .NET Framework 3.5 * .NET Framework 4.6 Features   + .NET Framework 4.6   + ASP.NET 4.6   + WCF Services     - TCP Activation     - HTTP Activation     - TCP PortSharing |
|  | Weiter |
|  | Folgende Unterkomponenten müssen zusätzlich ausgewählt werden:   * Common http Features   + Default Document   + Static Content * Health and Diagnostic   + HTTP Logging * Security   + Request Filtering   + Windows Authentication * Application Development   + .NET Extensibility 3.5   + .NET Extensibility 4.6   + ASP3.5   + ASP4.6   + ISAPI Extensions   + ISAPI Filters * Management Tools   + IIS Management Console |
|  | Wählen sie “Specify an alternate path“ |
|  | Spezifizieren sie nun den Pfad zum SXS Ordner der sich auf dem Windows Installations-Medium befindet.  Anschliessend schliessen Sie das Fenster und starten die Installation. |
|  |  |

### Windows Server 2019

|  |  |
| --- | --- |
|  | Windows Installations-DVD einlegen oder ISO File verbinden. |
|  | Starten sie den „add roles and features“ Prozess. |
|  | Weiter |
|  | “Role-based or feature-based installation“ auswählen |
|  | Weiter |
|  | Wählen sie die Web Server (IIS) Rolle aus. |
|  | Wählen sie die benötigten Features analog dem Bildschirmausschnitt aus.   * .NET Framework 3.5 Features   + .NET Framework 3.5 * .NET Framework 4.7 Features   + .NET Framework 4.7   + ASP.NET 4.   + WCF Services     - TCP Activation     - HTTP Activation     - TCP PortSharing |
|  | Weiter |
|  | Folgende Unterkomponenten müssen zusätzlich ausgewählt werden:   * Common http Features   + Default Document   + Static Content * Health and Diagnostic   + HTTP Logging * Security   + Request Filtering   + Windows Authentication * Application Development   + .NET Extensibility 3.5   + .NET Extensibility 4.6   + ASP3.5   + ASP4.6   + ISAPI Extensions   + ISAPI Filters * Management Tools   + IIS Management Console |
|  | Wählen sie “Specify an alternate path“ |
|  | Spezifizieren sie nun den Pfad zum SXS Ordner der sich auf dem Windows Installations-Medium befindet.  Anschliessend schliessen Sie das Fenster und starten die Installation. |

## Konfiguration Data Deduplication (Content und netCIM Server)

Durch die Konfiguration von Data Deduplication wird verhindert, dass unnötig viel Speicherplatz verwendet wird, da gewisse Daten mehrfach abgespeichert werden. Diese Optimierung findet jeweils in der Nacht statt.

|  |  |
| --- | --- |
|  | PowerShell Konsole als Administrator starten starten. |
| Import-Module ServerManager | PowerShell Modul des Windows Server Managers importieren damit das Feature installiert werden kann. |
| Add-WindowsFeature -name FS-Data-Deduplication | Windows Feature installieren. |
| Import-Module Deduplication | Data Deduplication Modul importieren damit die Konfiguration vorgenommen werden kann. |
| Enable-DedupVolume E: -UsageType Default | Data Deduplication für das Laufwerk E aktivieren. Falls auf dem Site Server der netCIM Content und der netCIM Source Ordner auf unterschiedlichen Laufwerken liegen, sollte die Deduplication auf beiden aktiviert werden. |

## Installation ADK

### Windows Server 2016 / Windows Server 2019

|  |  |
| --- | --- |
|  | Download ADK  Wir empfehlen den ADK 10, Version 2004 Ansonsten sind Konfigurationsanpassungen nötig. Bei der Version 2004 der Download vom ADK und der Download vom Windows PE add-on separat durchgeführt werden.  ADK 10 2004:  <https://go.microsoft.com/fwlink/?linkid=2120254>  Windows PE add-on:  <https://go.microsoft.com/fwlink/?linkid=2120253> |
|  | Zuerst ADK Installation über adksetup.exe starten. Sofern ein anderer als der Standard Pfad gewählt wird, muss dieser Pfad im App Config File(BootImageTool.exe.config) des Boot Image Tools angepasst werden.  <adk installationPath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit"/> |
|  | Am Customer Experience Improvement Program soll nicht teilgenommen werden. |
|  | Die Lizenz muss akzeptiert werden. |
|  | Wählen Sie das Feature «Deployment Tools» aus.  Anschliessend kann die Installation gestartet werden. |
|  | Die Installation wird durchgeführt. |
|  | Nachdem die Installation des AKD abgeschlossen wurde, kann die zweite Installation über adkwinpesetup.exe gestartet werden.  Sofern ein anderer als der Standard Pfad gewählt wird, muss dieser Pfad im App Config File(BootImageTool.exe.config) des Boot Image Tools angepasst werden.  <adk installationPath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit"/> |
|  | Am Customer Experience Improvement Program soll nicht teilgenommen werden. |
|  | Die Lizenz muss akzeptiert werden. |
|  | Nachdem das Feature «Windows Preinstallation Environment (Windows PE) ausgewählt wurde kann die Installation gestartet werden. |

## Microsoft SQL Server 2019 Express

|  |
| --- |
| Wichtig |
| Ab einer Grösse von 500 Endgeräten wird empfohlen Microsoft SQL Server 2019 Standard zu verwenden. |

### Windows Server 2016 / 2019

|  |  |
| --- | --- |
|  | Download SQL Express: <https://go.microsoft.com/fwlink/?linkid=866658>  Installationsdatei SQL2019-SSEI-Expr.exe ausführen, um Installation zu starten.  Installation type Custom auswählen. |
|  | Standardspei Standardspeicherpfad C:\SQL2019 auswählen und installation starten. |
|  | “New SQL Server stand-alone Installation or add features to an existing installation” auswählen. |
|  | Lizenzvereinbarung annehmen. |
|  | Use Microsoft Update to check for updates (recommended)“ auswählen. |
|  | Next, auch wenn ein Fehler dargestellt wird. |
|  | Die folgenden Features müssen installiert werden:   * Database Engine Service |
|  | Default Instanz auswählen. |
|  | Hier sollte als Benutzer für den SQL Service ein eigener Service Benutzer verwendet werden (nicht der netCIM\_Service). Dieser benötigt keine Administratoren Rechte.  Der Dienst SQL Server Browser wird nicht unbedingt benötigt. Deshalb kann dieser auch deaktiviert werden |
|  | Fügen Sie den netCIM Service Benutzer als Administrator hinzu.  Falls unser Berechtigungskonzept aus Kapitel ‎4.8 angewendet wird, müsste hier die netCIM\_Administrators Gruppe sowie der netCIM\_Service Benutzer berechtigt werden.  Wenn die Gruppe sowie Benutzer hinzugefügt sind, dann in der Registerkarte  auf Data Directories wechseln. (siehe unten) |
|  | Nach diesem Schritt startet die Installation vom SQL Server 2019 Express. |

## Installation Visual C++ Redist for Visual Studio 2015-2019 x64 und x86

|  |  |
| --- | --- |
|  | Für die Installation x64 und x86 gibt es zwei verschiedene Setups.  Hier wird der Setup x64 beschrieben, x86 ist jedoch identisch.  Die „Terms and Conditions“ müssen angenommen werden.  x64: <https://aka.ms/vs/16/release/vc_redist.x64.exe>  x86:  <https://aka.ms/vs/16/release/vc_redist.x86.exe> |
|  | Das Setup wurde erfolgreich durchgeführt. Nun kann die Installation der zweiten Architektur durchgeführt werden. |

## Konfiguration Active Directory für Kerberos Authentication

### Vor netCim Version 6.5.7083.0

Damit die verschiedenen Komponenten zusammen kommunizieren können ist es nötig die folgenden SPNs zu registrieren. Diese Befehle müssen als Domain Admin ausgeführt werden und müssen vor der netCIM Installation ausgeführt werden.

setspn -a http/%NETCIMSERVERFQDN% %DOMAIN%\%NETCIMSERVICEUSER%

setspn -a http/%NETCIMSERVERNETBIOSNAME% %DOMAIN%\%NETCIMSERVICEUSER%

Wenn die Variablen angepasst sind sollten die Befehle wie folgt aussehen:

setspn -a http/server01.contoso.local contoso\netCIM\_Service

setspn -a http/server01 contoso\netCIM\_Service

### Ab netCIM Version 6.5.7083.0

Ab dem Release 6.5.7083.0 müssen die bestehenden SPNs gelöscht werden, damit anschliessend die Neuen korrekt funktionieren. Folgende befehle müssen dazu ausgeführt werden:

setspn -D HTTP/%NETCIMSERVERFQDN% %DOMAIN%\%NETCIMSERVICEUSER%

setspn -D HTTP/%NETCIMSERVERNETBIOSNAME% %DOMAIN%\%NETCIMSERVICEUSER%

Anschliessend können die neuen SPNs wie folgt hinzugefügt werden:

setspn -a HTTP/%NETCIMSERVERFQDN%:80/NetCimServer %DOMAIN%\%NETCIMSERVICEUSER%

setspn -a HTTP/%NETCIMSERVERNETBIOSNAME%:80/NetCimServer %DOMAIN%\%NETCIMSERVICEUSER%

Wobei die Werte wie folgt an die Umgebung angepasst werden müssen:

* %NETCIMSERVERFQDN%: Full Qualified Domain Name des netCIM Servers,

z.B. NETCIM-SRV.contoso.local

* %DOMAIN%: Domänenname, z.B. CONTOSO
* %NETCIMSERVICEUSER%: netCIM Service Account, z.B. netcim\_service
* %NETCIMSERVERNETBIOSNAME%: Net Bios Name des netCIM Servers, z.B. NETCIM-SRV

## Konfiguration Windows Firewall auf dem netCIM Server

Die Windows Firewall muss entweder deaktiviert oder es müssen anhand der Tabelle im Kapitel ‎2.12.1 Ausnahmen definiert werden.

## Installation netCIM

### Windows Server 2016 / Windows Server 2019

Vor der Installation sollte man sich im Klaren sein, welches Berechtigungskonzept man verwenden möchte. Ein Vorschlag für die benötigten Benutzer und deren Berechtigungen ist im Kapitel ‎4.8 dokumentiert.

|  |
| --- |
| Wichtig: SQL Instanz |
| Wenn Microsoft SQL Server unter der Default Instanz installiert wurde, darf der Name der Instanz bei der netCIM Server Installation nicht spezifiziert werden.  Falls sich die SQL Server Installation auf dem gleichen Server wie der netCIM Server befindet kann der Standard Wert "." beibehalten werden.  Korrekt: %DBSERVER%  Falsch: %DBSERVER%\MSSQL |

|  |  |
| --- | --- |
|  | Nach dem Starten des netCIM Setups erscheint der Startbildschirm des Installationsdialogs.  Überprüfen Sie vor dem Weiterfahren unbedingt ob sie alle Anforderungen aus Kapitel ‎2 erfüllen. |
|  | Bestätigen Sie den EULA sofern sie Einverstanden sind. |
|  | Wählen sie die gewünschten Rollen aus die auf diesem System installiert werden sollen.  Wichtig ist hier, dass in einer Umgebung als erstes die netCIM Server Rolle installiert wird. |
|  | Dies sind globale Einstellungen für netCIM.  Als netCIM Server Hostname kann der FQDN oder die IP des Hauptservers spezifiziert werden.  Mit dem Enable Debug Logging kann die Granularität der Log Einträge festgelegt werden. Diese Option sollte nur in Testumgebungen verwendet werden. |
|  | Die nachfolgenden Schritte können je nach gewählter Rolle unterschiedlich sein.  In diesem Schritt müssen die Konfigurationsparameter für den netCIM Server spezifiziert werden. |
|  |  |
|  |  |
|  |  |
|  | Die Option „Use DHCP port“ muss deaktiviert werden, wenn die Content Server Rolle auf einem DHCP Server installiert wird. Ansonsten muss die Option aktiviert sein. |
|  |  |
|  |  |
|  | Die Installation kann nun gestartet werden. |
|  |  |
| C:\Users\sut\AppData\Local\Microsoft\Windows\INetCache\Content.Word\final-splash.png | Die Installation wurde erfolgreich beendet.  Im Fehlerfall stehen mehr Informationen in den Logfiles bereit. |
| K:\Bildung\Aarau_Berufsschule\Projekte\netCIM 2016\Screenshots\netcim_cockpit_permissions.png | Nun müssen als erstes die Berechtigungen im Cockpit überprüft werden.  Nach einer Standard Installation haben alle Benutzer Zugriff auf die Webapplikation!  Mehr Informationen finden Sie im Kapitel ‎4.8. |

## Konfiguration PXE Boot

Es gibt zwei verschiedene Möglichkeiten, wie ein netCIM Client im Netzwerk einen PXE Boot Server finden kann.

* Fix definierte DHCP Optionen können auf dem DHCP Server pro DHCP Subnetz definiert werden. Diese legen fest, welcher PXE Boot Server von PXE Clients verwendet werden soll.
* Der PXE Service von netCIM (enthalten in der Content Server Rolle) kann die DHCP Optionen selber versenden, so ist weniger Konfigurationsaufwand. Sofern der netCIM Content Server im selben Subnetz steht wie die Clients funktioniert dies ohne netzwerkseitige Anpassungen. Falls Clients und Content Server in unterschiedlichen Subnetzen stehen, müssen DHCP Broadcasts über Port 67 erlaubt werden oder so genannte IP Helper definiert werden, welche die DHCP Broadcasts aus einem Subnetz an den DHCP Server und den netCIM Content Server weiterleiten.

|  |
| --- |
| Hinweis |
| Die Netree AG empfiehlt die Verwendung der zweiten Variante über IP Helper. |

### Variante DHCP Server/Optionen

Wenn der DHCP eingerichtet ist, müssen noch einige Konfigurationen erledigt werden um netCIM nutzen zu können.

#### Windows Server 2016 / 2019

##### Classes

|  |  |
| --- | --- |
| DHCP_Policies |  |
| Policieshinzufügen | Eine User Class und zwei Vendor Classes gemäss den nachfolgenden Instruktionen erstellen. |
| UEfix64 | UEFI BIOS x64 **Vendor Classes**  Display Name: UEFI BIOS x64  ASCII: PXEClient:Arch:00007 |
| \\hsfp045\FolderRedirection$\DON\Desktop\DHCP\Uefix86.png | UEFI BIOS x86 **Vendor Classes**  Display Name: UEFI BIOS x86  ASCII: PXEClient:Arch:00006 |
| iPXE | iPXE **User Classes**  Display Name: iPXE  ASCII: iPXE |

##### Policies erstellen

Nachdem alle Classes erstellt wurden, können jetzt die Policies erstellt werden.

|  |  |
| --- | --- |
| \\hsfp045\FolderRedirection$\DON\Desktop\DHCP\iPXE1.png | Display Name: iPXE  Condition wie abgebildet. |
| \\hsfp045\FolderRedirection$\DON\Desktop\DHCP\iPXE2.png |  |
| \\hsfp045\FolderRedirection$\DON\Desktop\DHCP\SCope2.png | Option 067 Bootfile Name  Value: http://192.168.2.1/BootScript/Get?u=${uuid:hex}&a=${buildarch}  192.168.2.1 kann mit der IP oder dem FQDN des netCIM Servers ersetzt werden. |
| \\hsfp045\FolderRedirection$\DON\Desktop\DHCP\UEFIBIOSi386.png | Display Name: UEFI BIOS i386  Condition wie abgebildet. |
| \\hsfp045\FolderRedirection$\DON\Desktop\DHCP\UEFIBIOSi386_2.png | Append wildcard einschalten. |
| \\hsfp045\FolderRedirection$\DON\Desktop\DHCP\i386.png | Option 067 Bootfile Name  Value: EFI\i386\snponly.efi |
| uefi bios | Display Name: UEFI BIOS x86\_x64 |
| uefi bios | Append wildcard einschalten, neben dem x64 hat es dann einen \*. |
|  | Option 067 Bootfile Name  Value: EFI\x86\_x64\snponly.efi |

##### Scope Options konfigurieren

|  |  |
| --- | --- |
| ScopeOptions1 | Die bereits konfigurierten Policies werden bereits dargestellt. Nun wird noch die Option 066 und 067 hinzugefügt. |
| Untitled | Option: 066 Boot Server Host Name  Value: IP oder FQDN des netCIM Servers |
| 067 | Option: 067 Bootfile Name  Value: Legacy\undionly.kpxe |

### Variante IP Helper

Sie können die Routingtabellen für die Netzwerkgeräte aktualisieren, um eine ordnungsgemässe Weiterleitung des DHCP-Datenverkehrs sicherzustellen. Sie können z. B. den Befehl "ip helper-address" verwenden, wenn Sie einen Cisco-Router besitzen. Bei einer korrekten Konfiguration werden alle DHCP-Anfragen vom Client an einen DHCP-Server und einen netCIM Content Server geleitet. (Dabei muss das Paket nicht erneut an andere Netzwerksegmente übertragen, sondern nur an angegebene Empfänger weitergeleitet werden.)

Befinden sich der startende Client, der DHCP-Server und der netCIM Content Server im selben Netzwerksegment, muss der Router normalerweise nicht konfiguriert werden. Die DHCP-Anfragen des Clients gehen beim DHCP-Server und beim netCIM Content Server ein. Wenn sich jedoch der DHCP-Server oder der netCIM Content Server in einem anderen Netzwerksegment befindet oder zwar im selben Subnetz aber durch einen Router gesteuert wird, empfiehlt Microsoft eine Anpassung der IP Helper Adressen des Routers. Vom Clientcomputer wird, nachdem er seine IP-Adresse erhalten hat, direkt eine Verbindung mit dem netCIM Content Server hergestellt (erneut mithilfe von DHCP-Paketen), um den Namen und Pfad des herunterzuladenden Netzwerkstartprogramms abzurufen. Sie müssen die folgenden Änderungen vornehmen:

* IP Helper: Alle DHCP-Anfragen von Clients auf UDP-Port 67 sollten direkt zum DHCP-Server und zum netCIM Content Server weitergeleitet werden.
* Firewall: Verfügt der Router über eine integrierte Firewall, müssen Sie zudem die Ports gemäss Kapitel ‎2.12.1 konfigurieren.

|  |
| --- |
| Hinweis |
| Der PXE Server unterstützt nur IPV4 Kommunikation. |

|  |
| --- |
| Wichtig – DHCP Server und netCIM Content Server auf einem Server |
| Beim netCIM Setup muss die Option "Use DHCP Port" auf der PXE Server Konfigurationsseite deaktiviert werden.  Zudem müssen nach dem Setup folgende Befehle auf dem Server ausgeführt werden:  netsh dhcp server \\<DHCPSERVERNAME> add optiondef 60 PXEClient String 0 comment="PXE support"  netsh dhcp server \\<DHCPSERVERNAME> set optionvalue 60 STRING PXEClient |

## Konfiguration Switches/Router/Firewall

Für die korrekte Ausführung von Multicasting müssen alle Router und Switches im Netzwerk für Multicast-Funktionen konfiguriert sein. Andernfalls werden Multicast-Pakete möglicherweise nicht korrekt weitergeleitet.

### Benötigte Netzwerk Ports

|  |  |  |  |
| --- | --- | --- | --- |
| Von | Zu | Ports | Beschreibung |
| netCIM Server | netCIM Content Server | TCP 80 | Content Synchronisation |
| netCIM Boot Image Management Computer | netCIM Server | TCP 80  TCP 445 | Boot Image Upload  SMB Shares |
| netCIM vOS Management Computer | netCIM Server | TCP 80  TCP 445 | Image Upload  SMB Shares |
| Clients | netCIM Server | TCP 80 | Management Traffic |
| netCIM Server | Clients | TCP 80 | Benachrichtigung bei neuen Jobs |
| Clients | netCIM Content Server | UDP 69  UDP 67/4011  TCP 80  TCP 5555 | PXE Boot (TFTP)  PXE Boot  Content Download  Multicast Control |
| netCIM Content Server | Clients | UDP 5556 | Multicast Data |
| netCIM Content Server | netCIM Server | TCP 80 | Content Synchronisation |

# netCIM aktualisieren

Bei der Aktualisierung von netCIM werden die bestehenden Konfigurationen, welche bei der Erstinstallation spezifiziert wurden automatisch ausgelesen.

## Vorbereitungen

Vor einer Aktualisierung muss man folgendes durchführen:

* Backup der Server überprüfen (sofern virtuell, kann ein Snapshot erstellt werden)
* Datenbank sichern
* Überprüfen ob die Passwörter der Service Accounts bekannt sind

## Neue netCIM Version installieren

### Windows Server 2016 / Windows Server 2019

|  |  |
| --- | --- |
|  | Nach dem Starten des netCIM Setups erscheint der Startbildschirm des Installationsdialogs. |
|  | Bestätigen Sie den EULA sofern sie Einverstanden sind. |
| M:\netPRODUCTS\netCIM 2016\Betrieb\Handbuch-Anpassungen-2016Q1Release\Install-Upgrade\components.png | Bei der Auswahl der Komponenten wird dargestellt, für welche Komponenten eine Aktualisierung durchgeführt wird. |
|  | Mit dem Enable Debug Logging kann die Granularität der Log Einträge festgelegt werden. Diese Option sollte nur in Testumgebungen verwendet werden. |
|  | Die nachfolgenden Schritte können je nach gewählter Rolle unterschiedlich sein. |
|  |  |
|  |  |
|  |  |
|  | Die Option „Use DHCP port“ muss deaktiviert werden, wenn die Content Server Rolle auf einem DHCP Server installiert wird. Ansonsten muss die Option aktiviert sein. |
|  |  |
|  |  |
|  | Die Installation kann nun gestartet werden. |
|  |  |
| C:\Users\sut\AppData\Local\Microsoft\Windows\INetCache\Content.Word\final-splash.png | Die Aktualisierung wurde erfolgreich beendet.  Im Fehlerfall stehen mehr Informationen in den Logfiles bereit. |

## Nachbereitungen

Die aktualisierten Programmdateien wurden installiert. Nun muss das Boot Image neu generiert werden. Dies ist nötig, da dort ansonsten nicht die neuesten netCIM Dateien enthalten sind.

# Konfiguration

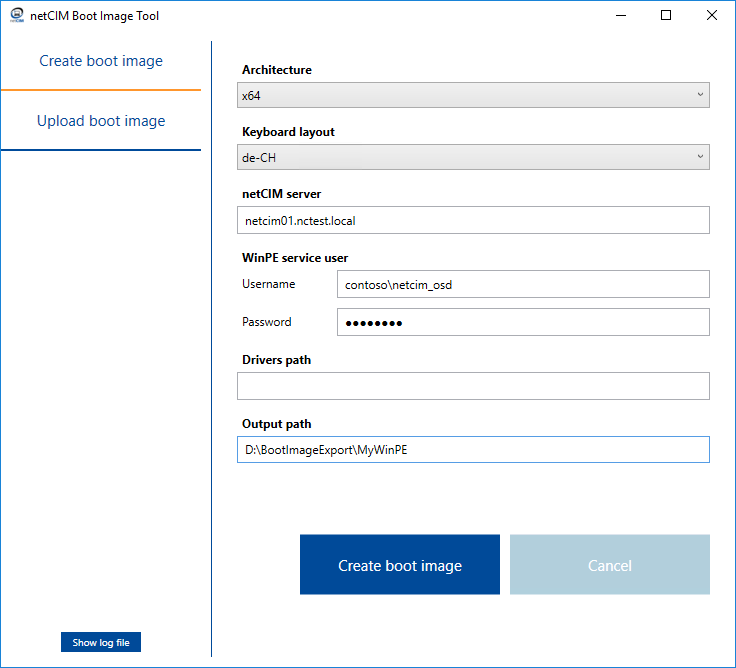
## Boot Image generieren und registrieren

Im Start Menu das netCIM Boot Image Tool als Administrator starten.

### Windows Server 2016 / Windows Server 2019

#### Create Boot Image

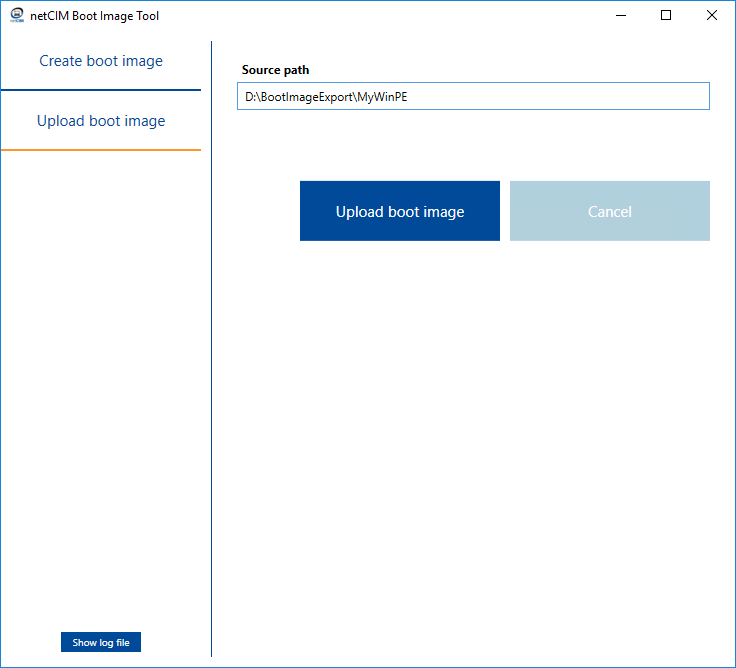
|  |  |
| --- | --- |
| Feld | Wert |
| netCIM Server | Hostname, FQDN oder IP-Adresse des netCIM Servers.  Die Ip-Adresse sollte verwendet werden wenn der Server in einer Workgroup betrieben wird. |
| WinPE Service User | z.B. „contoso\netCIM\_OSD“ 🡪 **Achtung: Dieser Benutzer muss die OSD Rolle im Security Tab im Cockpit zugewiesen haben.** |
| Password | Passwort des WinPE Service Users. |
| Driver Path | Pfad zu einem Ordner der alle Treiber enthält die während der WinPE Phase benötigt werden. Dies sind vor allem Netzwerkkarten und RAID Treiber. Da es nur einen Ordner für alle Hardwaretypen gib welcher alle Treiber (.inf-Dateien) enthält empfehlen wir folgende Struktur pro Architektur und WinPE Version:   * Hardware Model   + LAN   + RAID   Wir empfehlen hier den folgenden Ordner zu verwenden %DataPartition%\Development\WinPEDrivers |
| Output path | Leeren Ordner auswählen z.B. C:\Temp\WinPE |



Anschliessend kann das Boot Image generiert werden.

#### Upload Boot Image

|  |  |
| --- | --- |
| Feld | Wert |
| Source Path | Der Ordner der beim Erstellen als Output Path ausgewählt wurde. |



Anschliessend kann das Boot Image auf den netCIM Server hochgeladen werden.

## vOS Tool

### Vorhandene Befehle

* **New-NetCimVOS**  
  Erstellt ein neues vOS und lokal die Version 1 (nicht generalisiert). Dazu wird eine ISO-, WIM- oder VHD(X)-Datei einer Windows Installation benötigt.
* **New-NetCimVOSVersion**

Erstellt lokal eine neue vOS Version für ein bestehendes vOS.

* **Get-NetCimVOS**  
  Auslesen bestehender vOS vom netCIM Server. Die Funktion ermöglicht ebenfalls das Erstellen eines lokalen Datenstamms eines bestehenden vOS, sollte dieses lokal noch nicht existieren. Ein bestehender lokaler Datenstamm eines vOS kann auch mit den Daten vom netCIM Server überschrieben werden (Download Parameter).
* **Get-NetCimVOSStatus**

Gibt an ob und falls wenn, welche Aktionen für ein vOS ausstehen, damit es deployed werden kann.

* **Invoke-NetCimVOSVersionGeneralization**  
  Generalisiert die ausgewählte lokale Version eines spezifizierten vOS.
* **Submit-NetCimVOS**  
  Gleicht den lokalen Datenstamm eines spezifizierten vOS mit dem netCIM Server ab. Jede lokale Version muss generalisiert werden, bevor sie abgeglichen werden kann.
  + Neue Versionen werden hochgeladen und erstellt.
  + Nicht mehr existierende Versionen werden gelöscht.
  + Veränderte Versionen werden aktualisiert.
* **Set-NetCimVOSVersion**  
  Ermöglicht das Setzen der Beschreibung einer spezifizierte vOS Version. Die Version muss mit dem netCIM Server abgeglichen worden sein bevor die Beschreibung gesetzt werden kann.
* **Set-NetCimVOS**

Ermöglicht das Setzen der Beschreibung eines vOS. Die Version muss mit dem netCIM Server abgeglichen worden sein bevor die Beschreibung gesetzt werden kann.

* **Remove-NetCimVOS**  
  Löscht ein vOS auf dem lokalen Datenstamm und die dedizierte VM, ebenfalls wird es komplett vom netCIM Server entfernt.
* **Remove-NetCimVOSVersion**  
  Löscht die letzte (neuste) lokale vOS Version.
* **Edit-NetCimVOSVersion**

Ermöglicht das Bearbeiten einer bestehenden vOS Version, falls bereits eine generalisierte Version vorliegt, muss der Overwrite Parameter verwendet werden.

* **Merge-NetCimVOSVersion**  
  Fügt mehrere bestehende vOS Versionen zusammen, wobei spezifiziert werden kann, wie viele Versionen zusammengefügt werden.

|  |
| --- |
| Hinweis |
| Die einzelnen PowerShellFunktionen des vOS Tool geben beim Aufruf jeweils die neu erzeugte Version oder den vOS Namen zurück. Dies ist hilfreich, wenn das vOS Tool mit Variablen genutzt wird. |

|  |
| --- |
| Hinweis –VirtualOSName / -ID / VirtualOSID |
| Bei allen vOS Tool Befehlen kann mit dem Namen welcher bei der Erstellung des vOS spezifiziert wurde oder der ID gearbeitet werden. Die ID kann mit dem "*Get-NetCimVOS*" Befehl eruiert werden. |

|  |
| --- |
| Wichtig: Imagegrösse |
| Die mit dem Parameter "-MaximumSizeInGigaBytes " spezifizierte Maximalgrösse bezieht sich auf den Speicherplatz der im Image verfügbar ist. Der tatsächliche Speicherbedarf auf der physischen Festplatte kann höher sein.  Durch das Erzeugen mehrerer Image Versionen kann sich der effektive Speicherbedarf vergrössern. |

### vOS von einer ISO-Datei erstellen

#### Windows Server 2016 / Windows Server 2019

1. Im Start Menu das "netCIM vOS Tool" starten. Achtung, dies muss als Administrator geschehen.
2. Um ein neues vOS von einer ISO Datei zu erstellen, führt man folgendes Kommando aus:

*New-NetCIMVOS –Name "Windows 10" –IsoFilePath "C:\ISO\win10.iso" -MaximumSizeInGigaBytes 100 –AdministratorPassword „Welcome1“ -Verbose*

|  |
| --- |
| Hinweis |
| Mit dem Parameter AdministratorPassword wird das Passwort des lokalen Administrators im Image gesetzt. Nach dem Deployment ist der lokale Administrator Account standardmässig deaktiviert. |

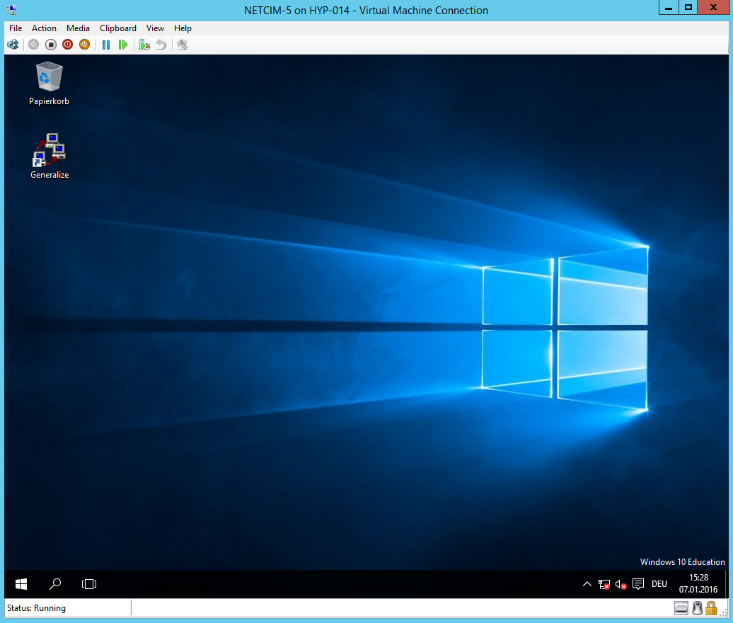
1. Sobald der Vorgang abgeschlossen ist, startet die VM automatisch. Führen sie die Installation durch bis alle Anpassungen wie gewünscht ausgeführt sind.
2. Anschliessend fährt man die Virtuelle Maschine herunter.
3. Um eine vOS Version zu generalisieren, gibt es zwei Varianten, wie der Generalisierungsvorgang vollzogen werden kann.
4. Wenn gewünscht wird, dass während dem Generalisieren noch Änderungen vorgenommen werden können, muss diese Variante angewendet werden. Durch das Ergänzen dieses Parameters, wird der Builtin-Administrator nicht deaktiviert und Änderungen können direkt in der Generalisierungsphase vollzogen werden.

*Invoke-NetCimVOSVersionGeneralization –VirtualOSName "Windows 10" –Version 1* ***–Manual*** *–Verbose*

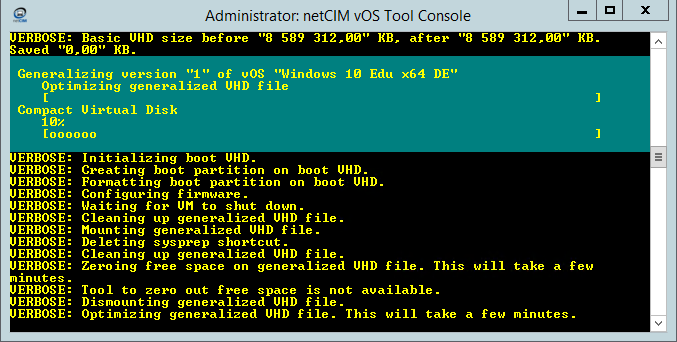
Die angepassten Konfigurationen gelten jedoch nur für den aktuell zu erstellenden „vOS Generalized Checkpoint“.

Nachdem der folgende Parameter angewendet wurde, öffnet sich die virtuelle Maschine und man kann sich mit dem Builtin-Administrator anmelden.

Nachdem die gewünschten Konfigurationen vorgenommen wurden, ist es zwingend notwendig auf das „Generalize“-Desktopsymbol zu klicken. Es ist zu vermeiden, die VM auf herkömmliche Art und Weise herunter zu fahren.



Nachdem die auf dem Desktop vorhandene Verknüpfung aktiviert wurde, fährt der Generalisierungsvorgang eigenständig weiter.



1. Wenn gewünscht ist, dass während dem Generalisieren keine Änderungen und Konfigurationen vorgenommen werden können, muss folgender Befehl angewendet werden:

*Invoke-NetCimVOSVersionGeneralization –VirtualOSName "Windows 10" –Version 1 –Verbose*

1. Zum Schluss, muss das vOS mit dem netCIM Server abgeglichen werden:

*Submit-NetCimVOS -Name "Windows 10" -Verbose*

### Neue vOS Version erstellen

1. Im Start Menu das "netCIM vOS Tool" starten. Achtung, dies muss als Administrator geschehen.

Sofern die VM mit der aktuellen Image Version lokal nicht vorhanden ist, kann diese mit folgendem Befehl vom netCIM Server heruntergeladen werden:

*Get-NetCimVOS -Name "Windows 10" -Download -Verbose*

1. Nun muss eine neue vOS Version erstellen:

*New-NetCimVOSVersion -VirtualOSName "Windows 10"*

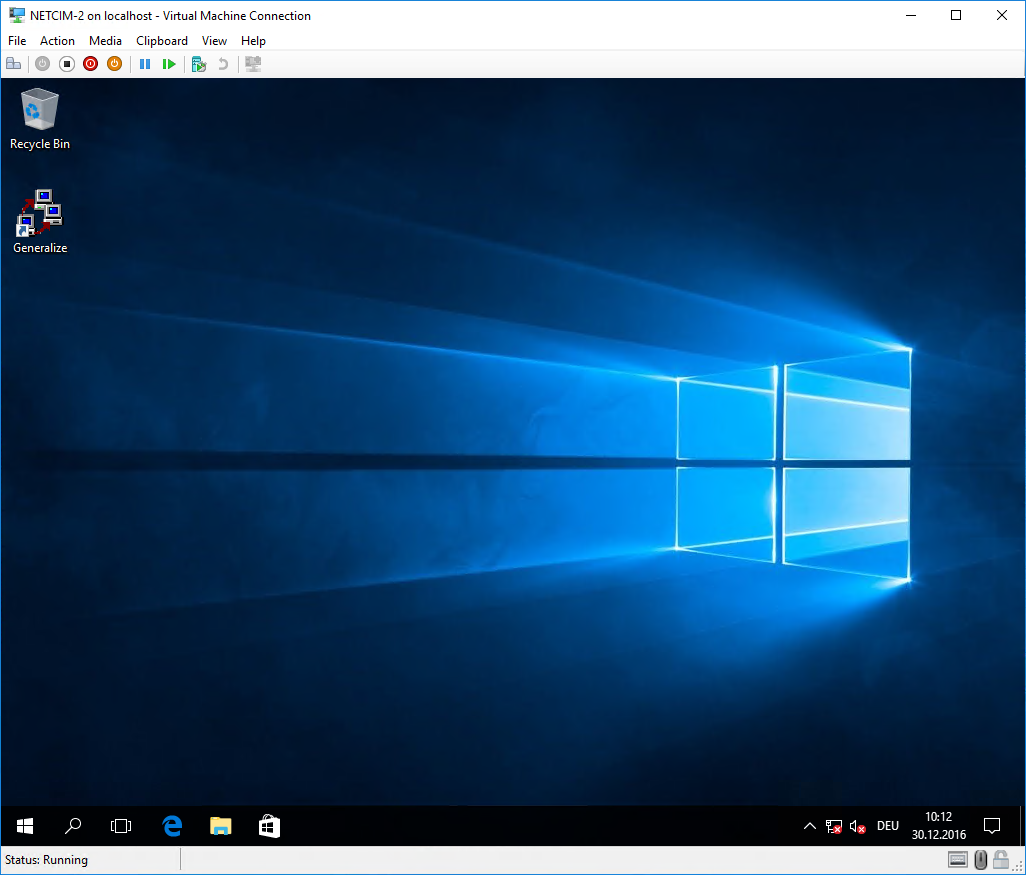
1. Um eine vOS Version zu generalisieren, gibt es zwei Varianten, wie der Generalisierungsvorgang vollzogen werden kann.
2. Wenn gewünscht wird, dass während dem Generalisieren noch Änderungen vorgenommen werden können, muss diese Variante angewendet werden. Durch das Ergänzen dieses Parameters, wird der Builtin-Administrator nicht deaktiviert und Änderungen können direkt in der Generalisierungsphase vollzogen werden.

*Invoke-NetCimVOSVersionGeneralization –VirtualOSName "Windows 10" –Version 1* ***–Manual*** *–Verbose*

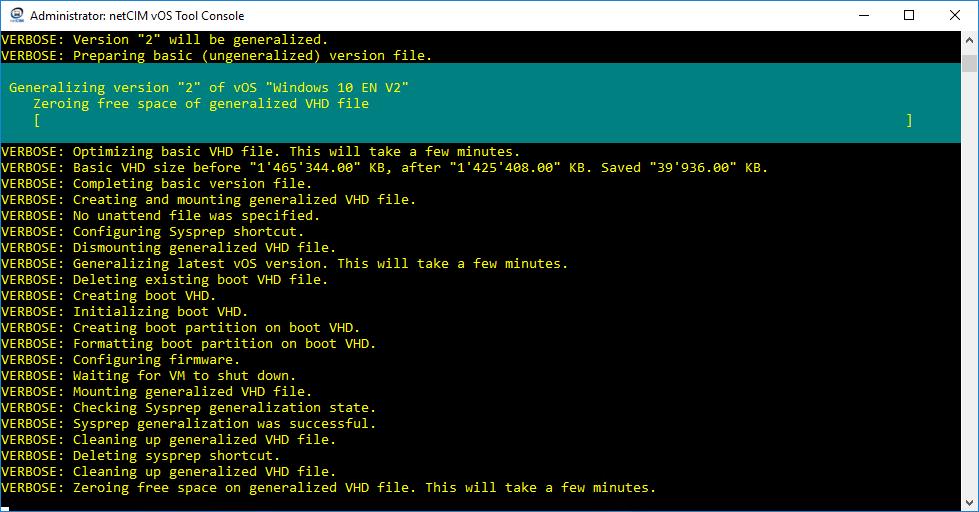
Die angepassten Konfigurationen gelten jedoch nur für den aktuell zu erstellenden „vOS Generalized Checkpoint“.

Nachdem der folgende Parameter angewendet wurde, öffnet sich die virtuelle Maschine und man kann sich mit dem Builtin-Administrator anmelden.

Nachdem die gewünschten Konfigurationen vorgenommen wurden, ist es zwingend notwendig auf das „Generalize“-Desktopsymbol zu klicken. Es ist zu vermeiden, die VM auf herkömmliche Art und Weise herunter zu fahren.



Nachdem die auf dem Desktop vorhandene Verknüpfung aktiviert wurde, fährt der Generalisierungsvorgang eigenständig weiter.



1. Sobald der Vorgang abgeschlossen ist, startet die VM automatisch. Nehmen Sie die gewünschten Anpassungen vor. Nachdem alle gewünschten Anpassungen abgeschlossen sind, Windows herunterfahren. Danach die Generalisierung mit folgendem Befehl starten:

*Invoke-NetCimVOSVersionGeneralization –VirtualOSName "Windows 10" –Verbose*

1. Zum Schluss, muss das vOS mit dem netCIM Server abgeglichen werden:

*Submit-NetCimVOS -Name "Windows 10 " -Verbose*

### Bestehende vOS Version bearbeiten

1. Im Start Menu das "netCIM vOS Tool" starten. Achtung, dies muss als Administrator geschehen.

Sofern die VM mit der aktuellen Image Version lokal nicht vorhanden ist, kann diese mit folgendem Befehl vom netCIM Server heruntergeladen werden:

*Get-NetCimVOS -Name "Windows 10" -Download -Verbose*

1. Damit die Version bearbeitet werden kann, muss folgender Befehl verwendet werden:

Edit-NetCimVOSVersion -VirtualOSName "Windows 10" -Version 1 –Overwrite

Der Overwrite Parameter wird verwendet, wenn die Imageversion bereits generalisiert wurde. Lediglich die aktuellste Imageversion ist editierbar.

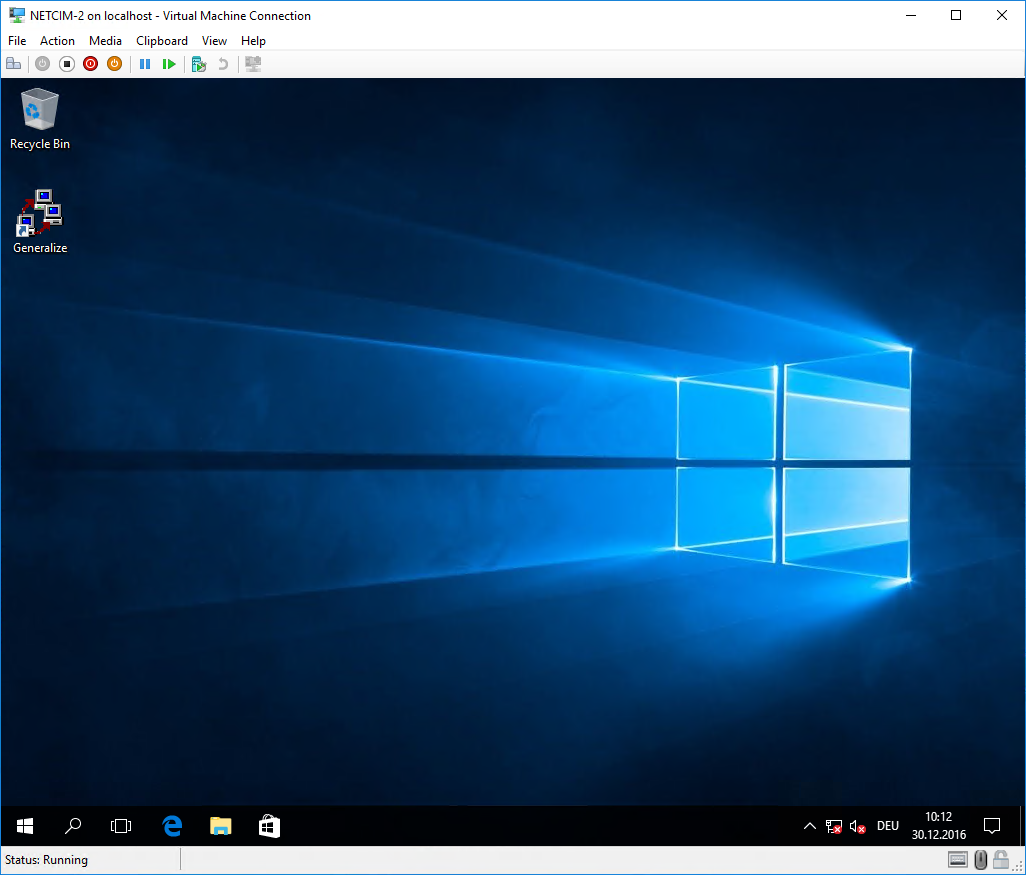
1. Um eine vOS Version zu generalisieren, gibt es zwei Varianten, wie der Generalisierungsvorgang vollzogen werden kann.
2. Wenn gewünscht wird, dass während dem Generalisieren noch Änderungen vorgenommen werden können, muss diese Variante angewendet werden. Durch das Ergänzen dieses Parameters, wird der Builtin-Administrator nicht deaktiviert und Änderungen können direkt in der Generalisierungsphase vollzogen werden.

*Invoke-NetCimVOSVersionGeneralization –VirtualOSName "Windows 10" –Version 1* ***–Manual*** *–Verbose*

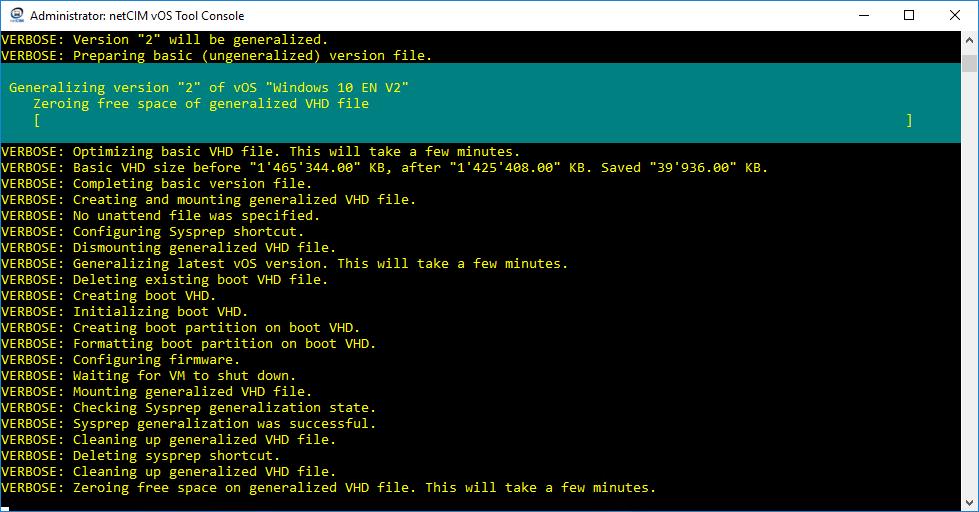
Die angepassten Konfigurationen gelten jedoch nur für den aktuell zu erstellenden „vOS Generalized Checkpoint“.

Nachdem der folgende Parameter angewendet wurde, öffnet sich die virtuelle Maschine und man kann sich mit dem Builtin-Administrator anmelden.

Nachdem die gewünschten Konfigurationen vorgenommen wurden, ist es zwingend notwendig auf das „Generalize“-Desktopsymbol zu klicken. Es ist zu vermeiden, die VM auf herkömmliche Art und Weise herunter zu fahren.



Nachdem die auf dem Desktop vorhandene Verknüpfung aktiviert wurde, fährt der Generalisierungsvorgang eigenständig weiter.



1. Sobald der Vorgang abgeschlossen ist, startet die VM automatisch. Nehmen Sie die gewünschten Anpassungen vor. Nachdem alle gewünschten Anpassungen abgeschlossen sind, Windows herunterfahren. Danach die Generalisierung mit folgendem Befehl starten:

*Invoke-NetCimVOSVersionGeneralization –VirtualOSName "Windows 10" –Verbose*

1. Zum Schluss, muss das vOS mit dem netCIM Server abgeglichen werden:

*Submit-NetCimVOS -Name "Windows 10" -Verbose*

### Ein vOS kopieren

Ein vOS kann mit folgendem Befehl kopiert werden

New-NetCimVOS -Name “Windows 10” –VOSDirectoryPath “D:\netCIM\vOSTool\Work\4”

### vOS Versionen zusammenführen

vOS Versionen werden wie folgt zusammengeführt

Merge-NetCimVOSVersion -VirtualOSName “Windows 10” -Version 5 -DestinationVersion 4

|  |
| --- |
| Hinweis |
| Es lassen sich beliebig viele vOS Versionen zusammenführen. Zu beachten ist, dass immer nur von der neusten Version ausgehend zusammengeführt werden kann. |

### vOS Löschen

Remove-NetCimVOS -Name “Windows 10” -Verbose

### vOS Version löschen

Remove-NetCimVOSVersion -VirtualOSName “Windows 10” -Verbose

### vOS Informationen ergänzen

Die Beschreibung für ein vOS kann wie folgt ergänzt werden:

Set-NetCimVOS –Name “Windows 10” -Description "Beschreibung" -Verbose

Die Beschreibung für eine VOS Version kann mit folgendem Befehl hinzugefügt werden:

Set-NetCimVOSVersion –VirtualOSName "Windows 10" –Version 1 -Description "Beschreibung" –Verbose

Das vOS wird mittes folgendem Befehl umbenannt:

Set-NetCimVOS -Name “Windows 10 Build 1909” –NewName "Windows 10 Build 2004" -Verbose

### vOS Informationen abfragen

Alle vorhandenen vOS abfragen:

Get-NetCimVOS

Status eines vOS Abfragen

Get-NetCimVOSStatus –Name “Windows 10”

### Image Optimierung

Während dem Generalisierungsvorgang wird im vOS zwecks Imageoptimierung das Pagefile gelöscht. Um den Speicherbedarf des Images weiter zu optimieren können nachfolgende Schritte vor dem Generalisierungsprozess ausgeführt werden.

* **Internet Explorer History löschen**

RunDll32.exe InetCpl.cpl,ClearMyTracksByProcess 255

* **Datenträgerbereinigung**

cleanmgr

* **Heruntergeladene Windows Updates löschen**

Stop-Service -Name wuauserv

Get-ChildItem -Path "C:\Windows\SoftwareDistribution\DataStore" –Recurse | Remove-Item –Recurse –Force

Get-ChildItem -Path "C:\Windows\SoftwareDistribution\Download" –Recurse | Remove-Item -Recurse –Force

Start-Service -Name wuauserv

* **Temporäre Ordner bereinigen**

Remove-Item -Path "C:\PerfLogs" -Force

Get-ChildItem -Path "C:\Windows\Temp" –Recurse | Remove-Item -Recurse –Force

* **Event Log bereinigen**

*wevtutil el | foreach {wevtutil cl "$\_"}*

### Wichtige Tasks im Imageerstellungsprozess

Sofern ein Microsoft Office im Image installiert wurde welches über einen KMS Server aktiviert werden soll, ist es unbedingt nötig vor der Generalisierung der vOS Version OSPPREARM auszuführen.

### Windows 10 Zeitproblematik

Das Windows 10 Feature Secure Time kann zu Störungen im Betrieb führen. Dadurch wird die Zeit ggf. falsch synchronisiert. Mit folgendem Registry Eintrag wird die Funktion deaktiviert:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits

"SecureTimeConfidence"=dword:00000000

Dieser Registry Eintrag muss einmalig im Grundimage gesetzt werden.

## Deploy Actions

### Allgemeines

Eine Deploy Action wird nach dem OS Setup ausgeführt und kann mehrere Dateien enthalten. Die Logik der Deploy Action kann mittels PowerShell Code geschrieben werden. Hierzu folgen nun ein paar wichtige Hinweise.

Deploy Actions werden unter dem System Account ausgeführt. Daher besitzen sie die höchsten Rechte auf einem Windows System.

Eine ausführbare Datei kann mit folgendem Befehl ausgeführt werden. Wichtig ist hier, dass man im Anschluss validiert ob der Exit Code eine erfolgreiche Ausführung kennzeichnet oder ob ein Fehler eingetreten ist:

*$process = Start-Process -FilePath "Setup.exe" -ArgumentList @("/sms","/install") -Wait -PassThru*

*do {start-sleep -Milliseconds 500} until ($process.HasExited)*

*if ($process.ExitCode –eq 0) {*

*Write-Debug "Installation Successfull"*

*} else {*

*Throw "Error Occurred. Process has Executed with ExitCode $($process.ExitCode)"*

*}*

Wie bereits erkennbar ist, gibt es die Möglichkeit zur Behandlung von Fehlern und die Möglichkeit Einträge in das Statussystem zurück zu liefern. Um eine Deploy Action abzubrechen und netCIM mitzuteilen, dass ein Fehler aufgetreten ist, kann der Befehl Throw in Verbindung mit einer Nachricht verwendet werden. Z.B.

*Throw "Error Occurred."*

Um nur eine Meldung in das Status System zu schreiben, auch als Fehler, jedoch ohne die Deploy Action abzubrechen, können folgende Befehle verwendet werden:

*Write-Error "Fehlermeldung"*

*Write-Warning "Warnungsmeldung"*

*Write-Verbose "Informationsmeldung"*

*Write-Debug "Debugmeldung"*

### Variablen im PowerShell Code verwenden

Variablen können im PowerShell Code genutzt werden um eine Dynamische Konfiguration zu ermöglichen. Wenn eine Variable z.B. mit dem Namen IsTeacherPC definiert wurde, kann diese wie mit " $NetCimScriptEnvironment.Variables["IsTeacherPC"]" Syntax verwendet werden. Dies könnte in PowerShell wie folgt aussehen:

*Write-Host $NetCimScriptEnvironment.Variables["IsTeacherPC"]*

Wir empfehlen die Verwendung der Variablen über Parameter. Hierzu wird die Zuweisung der netCIM Host Variable zu einer PowerShell Variable in der Parameter Definition des Scripts vorgenommen. Dadurch kann das Script auch mit Kommandozeilenparametern getestet werden, funktioniert aber auch ohne Parameter wenn das NetCimScriptEnvironment existiert. Dadurch ist auch direkt ersichtlich welche netCIM Variablen ein Script braucht.

*[CmdletBinding()]*

*param*

*(*

*[Parameter()]*

*[Bool]*

*$IsTeacherPC = ($NetCimScriptEnvironment.Variables | % {*

*if ($\_ -eq $null -or $\_["IsTeacherPC"] -eq $null) {*

*throw "Required parameter IsTeacherPC is missing."*

*} else {*

*$\_["IsTeacherPC"]*

*}*

*})*

*)*

Folgende Eigenschaften stehen in einer Deploy Action zur Verfügung:

* $NetCimScriptEnvironment.Variables
* $NetCimScriptEnvironment.NetCimServerHostName
* $NetCimScriptEnvironment.NetCimServerPort
* $NetCimScriptEnvironment.LogPath
* $NetCimScriptEnvironment.DeployActionName

### Beispiele

#### Ausführen einer beliebigen ausführbaren Datei

Um eine ausführbare Datei zu starten kann folgendes Script verwendet werden. Wichtig sind die vier Variablen die zu Beginn des Scripts angepasst werden müssen.

*[CmdletBinding()]*

*param*

*(*

*)*

*$Name = $NetCimScriptEnvironment.DeployActionName # Name für Log Einträge*

*$LogDir = $NetCimScriptEnvironment.LogPath*

*$Executable = "Setup.exe" # Path zum Executable Relativ zum Deploy Action Ordner oder Direkt*

*$Arguments = @("/install") # PS Array @() oder @("/Install")*

*$SuccessExitCodes = @(0, 3010)*

*Write-Verbose "Installing $Name"*

*$process = Start-Process -FilePath $Executable -ArgumentList $Arguments -Wait -PassThru*

*do {start-sleep -Milliseconds 500}*

*until ($process.HasExited)*

*$InstallExitCode = $process.ExitCode*

*#Search for Exit Code in Success Exit Code List*

*if($SuccessExitCodes -contains $InstallExitCode){*

*Write-Verbose "Successfully installed $Name with Exit Code $InstallExitCode"*

*} else {*

*Throw "Failed to Install $Name with Exit Code $InstallExitCode"*

*}*

#### Ausführen einer MSI Datei

Um eine MSI Datei zu starten kann folgendes Script verwendet werden. Wichtig sind die vier Variablen die zu Beginn des Scripts angepasst werden müssen.

*[CmdletBinding()]*

*param*

*(*

*)*

*$Name = $NetCimScriptEnvironment.DeployActionName # Name für Log Einträge*

*$LogDir = $NetCimScriptEnvironment.LogPath*

*$MsiFile = "Setup.msi" # Path zum MSI File relativ zum Deploy Action Ordner oder Direkt*

*$Arguments = @("/i",*

*($([char]34) + $MsiFile + $([char]34)),*

*"/qn",*

*"/l\*v $LogDir\$Name\_$(get-date -uformat %Y%m%d-%H%M%S).log"*

*"/Quiet",*

*"/norestart",*

*"ALLUSERS=1")*

*$SuccessExitCodes = @(0, 3010)*

*Write-Verbose "Installing $Name"*

*$process = Start-Process -FilePath "msiexec.exe" -ArgumentList $Arguments -Wait -PassThru*

*do {start-sleep -Milliseconds 500}*

*until ($process.HasExited)*

*$InstallExitCode = $process.ExitCode*

*#Search for Exit Code in Success Exit Code List*

*if($SuccessExitCodes -contains $InstallExitCode){*

*Write-Verbose "Successfully installed $Name with Exit Code $InstallExitCode"*

*} else {*

*Throw "Failed to Install $Name with Exit Code $InstallExitCode"*

*}*

#### Installation einer Applikation über OneGet

OneGet ist eine neue Möglichkeit in Windows 10 Applikationen zu installieren. Eine Community erstellt für diverse Freeware Applikationen Pakete zur Verfügung um diese per PowerShell zu installieren. Diese werden dann vom Internet heruntergeladen. Über Parameter lassen sich jeweils auch diverse Einstellungen vornehmen oder z.B. eine bestimmte Version installieren.

*Get-PackageProvider -Name Chocolatey -Force -verbose*

*set-executionpolicy remotesigned -force*

*Install-Package adobereader -Verbose –force*

Der Paketname, hier adobereader kann mit jedem Beliebigen ersetzt werden der auf <https://chocolatey.org/packages> verfügbar ist.

|  |
| --- |
| Hinweis |
| Dies ist nur mit Windows 10 und neuer möglich. |

#### Windows Update mit PowerShell

Um alle aktuellen Updates die auf der konfigurierten Windows Update Quelle (WSUS/Internet) verfügbar sind zu installieren, kann folgender Befehl genutzt werden:

*$UpdateSession = New-Object -Com Microsoft.Update.Session*

*$UpdateSearcher = $UpdateSession.CreateUpdateSearcher()*

*Write-Verbose("Searching for applicable updates...")*

*$SearchResult = $UpdateSearcher.Search("IsInstalled=0 and Type='Software'")*

*Write-Verbose("List of applicable items on the machine:")*

*For ($X = 0; $X -lt $SearchResult.Updates.Count; $X++){*

*$Update = $SearchResult.Updates.Item($X)*

*Write-Verbose( ($X + 1).ToString() + "&gt; " + $Update.Title)*

*}*

*If ($SearchResult.Updates.Count -eq 0) {*

*Write-Verbose("There are no applicable updates.")*

*} else {*

*$UpdatesToDownload = New-Object -Com Microsoft.Update.UpdateColl*

*For ($X = 0; $X -lt $SearchResult.Updates.Count; $X++){*

*$Update = $SearchResult.Updates.Item($X)*

*$Null = $UpdatesToDownload.Add($Update)*

*}*

*Write-Verbose("Downloading Updates...")*

*$Downloader = $UpdateSession.CreateUpdateDownloader()*

*$Downloader.Updates = $UpdatesToDownload*

*$DownloadResult = $Downloader.Download()*

*Write-Verbose $DownloadResult*

*$UpdatesToInstall = New-Object -Com Microsoft.Update.UpdateColl*

*For ($X = 0; $X -lt $SearchResult.Updates.Count; $X++){*

*$Update = $SearchResult.Updates.Item($X)*

*If ($Update.IsDownloaded) {*

*#Write-Verbose( ($X + 1).ToString() + "&gt; " + $Update.Title)*

*$Null = $UpdatesToInstall.Add($Update)*

*}*

*}*

*Write-Verbose("Installing Updates...")*

*$Installer = $UpdateSession.CreateUpdateInstaller()*

*$Installer.Updates = $UpdatesToInstall*

*$InstallationResult = $Installer.Install()*

*Write-Verbose("List of Updates Installed with Results:")*

*For ($X = 0; $X -lt $UpdatesToInstall.Count; $X++){*

*Write-Verbose($UpdatesToInstall.Item($X).Title + ": " + $InstallationResult.GetUpdateResult($X).ResultCode)*

*}*

*Write-Verbose("Installation Result: " + $InstallationResult.ResultCode)*

*Write-Verbose(" Reboot Required: " + $InstallationResult.RebootRequired)*

*If ($InstallationResult.RebootRequire -eq $True){*

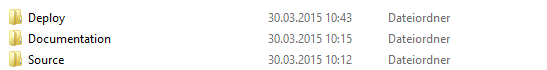
*Write-Warning "Reboot Required"*

*}*

*}*

#### Installation einer Applikation mit dem netECM:Launcher

**Schritt 1:**

Ordnerstruktur erstellen: 

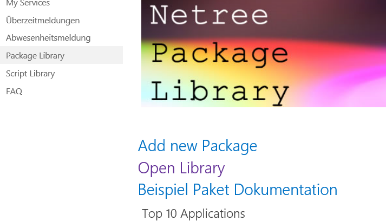
**Schritt 2:**

Source Ordner: Hersteller Datei vom Download



**Schritt 3:**

Dokumentation Ordner: Downloaden von Intranet.netree.ch🡪



**Schritt 4:**

**Deploy Ordner:** RunLauncher Downloaden von netecm.netree.ch 🡪 Products/netecm Launcher/RunLauncher + Die Config Datei für (.net Framework)  
Von Source Ordner die Hersteller Datei kopieren.  
XML-Datei (launcherConfig) anpassen.  
Beim Ausführen des RunLauncher immer als ADMIN! 🡪 Schritt 5 beachten für DeployAction  
Am Schluss LOGS anschauen: C:\Windows\Logs\SCCM\Apps  
**Troubleshooting**: <http://netecm.netree.ch/wiki/Pages/netECMLauncher_Troubleshooting.aspx>

**Schritt 5:**

1.Ordner Struktur hinaufladen und aktualisieren

2.PowerShell Code suchen für RunLauncher

#### Firewall für netCIM auf den Clients konfigurieren

Um die Clients zu benachrichtigen, wenn neue Jobs verfügbar sind oder den Onlinestatus zu überprüfen benötigt netCIM zwei Firewall Exceptions.

Import-Module NetSecurity -ErrorAction SilentlyContinue

if (Get-Command "New-NetFirewallRule" -errorAction SilentlyContinue)

{

Write-Verbose "Add netCIM - Allow Ping Rule"

New-NetFirewallRule -Name Allow\_Ping -DisplayName "netCIM - Allow Ping" -Description "ICMP Allow incoming V4 echo request" -Protocol ICMPv4 -IcmpType 8 -Enabled True -Profile Any -Action Allow -ErrorAction Stop

Write-Verbose "Add netCIM - Job Notification Rule"

New-NetFirewallRule -Name "Custom App Rule (in)" -Description "Allows the netCIM Server to contact the clients an tell them when a new Job is available." -DisplayName "netCIM Job Notification" -Enabled:True -Profile Any -Direction Inbound -Action Allow -Protocol TCP -LocalPort 80 -ErrorAction Stop

} else {

Write-Verbose "Add netCIM - Allow Ping Rule"

$process = Start-Process -FilePath "netsh.exe" -ArgumentList 'advfirewall firewall add rule name="netCIM - Allow Ping" description="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow' -Wait -PassThru

do {start-sleep -Milliseconds 500}

until ($process.HasExited)

$InstallExitCode = $process.ExitCode

if($InstallExitCode -eq 0){

Write-Verbose "Successfully added netCIM - Allow Ping Rule with Exit Code $InstallExitCode"

} else {

Throw "Failed to add netCIM - Allow Ping Rule with Exit Code $InstallExitCode"

}

Write-Verbose "Add netCIM - Job Notification Rule"

$process = Start-Process -FilePath "netsh.exe" -ArgumentList 'advfirewall firewall add rule name="netCIM - Job Notification" description="Allows the netCIM Server to contact the clients an tell them when a new Job is available." dir=in action=allow protocol=TCP localport=80' -Wait -PassThru

do {start-sleep -Milliseconds 500}

until ($process.HasExited)

$InstallExitCode = $process.ExitCode

if($InstallExitCode -eq 0){

Write-Verbose "Successfully added netCIM - Job Notification Rule with Exit Code $InstallExitCode"

} else {

Throw "Failed to add netCIM - Job Notification Rule with Exit Code $InstallExitCode"

}

}

## Driver Collections

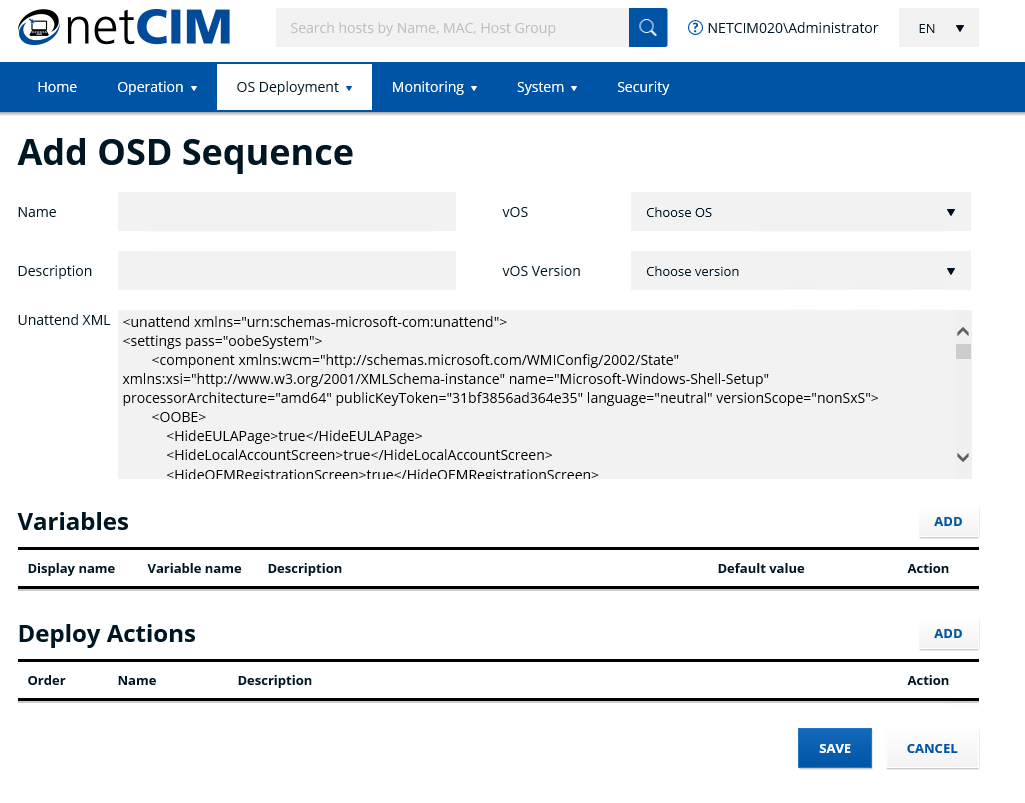
Eine Driver Collection enthält alle Treiber für eine bestimmte "Hardware Modell – Betriebssystem – Architektur" Kombination. Im Best Practice Abschnitt ist definiert, wie die Treiber (INF Files) am besten innerhalb eines Pakets abgespeichert werden sollten und nach welchem Prozess gearbeitet werden soll.

Eine neue Driver Collection kann über das OS Deployment Menu – Drivers hinzugefügt werden.



Sofern es sich jedoch um einen komplett neuen Hardware Typ handelt muss vorgängig unter OS Deployment 🡪 Hardware ein neuer Hardware Typ erfasst werden.

## OSD Sequence erstellen



Die OSD Sequence definiert den kompletten Ablauf des Deployments für ein vOS. Besonders wichtig ist das Unattend XML. Sofern wichtige Einstellungen fehlen wird das Setup nicht im Zero Touch Modus ausgeführt. Andererseits kann ein inkorrektes Unattend XML bedeuten, dass Windows Setup ohne entsprechende Fehlermeldung stehen bleibt oder abbricht.

Damit netCIM den Client später im Betrieb über neue Jobs informieren und den Onlinestatus überprüfen kann, ist es wichtig, dass die Firewall wie im Kapitel ‎4.3.3.6 beschrieben konfiguriert wird.

Zudem muss sichergestellt werden, dass die Computer, welche Rapid Recovery verwenden, sofern Sie in eine Domäne hinzugefügt werden, ihr Maschinen Passwort nicht wechseln. Dies kann über einen Registry Eintrag mit einer Deploy Action oder über eine Group Policy erreicht werden. Die nötige Konfiguration ist im Kapitel ‎9 erklärt.

### Variablen im Unattend XML

Variablen können im Unattend XML genutzt werden um eine dynamische Konfiguration zu ermöglichen. Wenn eine Variable z.B. mit dem Namen KeyboardLayout definiert wurde, kann diese wie mit "%NETCIM.Variable.KeyboardLayout%" Syntax verwendet werden. Dies könnte im XML wie folgt aussehen:

*<InputLocale>%NETCIM.Variable.KeyboardLayout%</InputLocale>*

Zudem kann im XML File auch immer die Variable mit dem aktuellen Hostnamen verwendet werden:

*%NETCIM.HostName%*

Im Minimum muss der folgende Abschnitt im Unattend XML vorhanden sein um ein korrektes Staging gewährleisten zu können:

*<settings pass="specialize">*

*<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">*

*<ComputerName>%NETCIM.HostName%</ComputerName>*

*</component>*

*</settings>*

### Konfiguration Join-Domain

Damit Clients während dem Deployment automatisch in die Domäne aufgenommen werden, muss das Unattend XML folgendermassen ergänzt werden:

|  |
| --- |
| <settings pass="specialize">  <!-- Domain Join -->  <component name="Microsoft-Windows-UnattendedJoin" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">  <Identification>  <Credentials>  <Username>**%Join-Domain-User%**</Username>  <Domain>**%NetBIOSName%**</Domain>  <Password>**%Join-Domain-User-PW%**</Password>  </Credentials>  <JoinDomain>**%Domain%**</JoinDomain>  <MachineObjectOU>**%CLIENT-OU%**</MachineObjectOU>  <DebugJoin>True</DebugJoin>  </Identification>  </component>  <component xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS">  <ComputerName>%NETCIM.HostName%</ComputerName>  </component> |

|  |  |
| --- | --- |
| Platzhalter | Beschreibung |
| **%Join-Domain-User%** | Benutzer welcher für den Domainjoin verwendet wird. Der Benutzer muss Mitglied der Default Ad-Gruppe "Account Operators" sein, damit er die benötigten Berechtigungen, für das Erstellen von AD Objekten besitzt. |
| **%NetBIOSName%** | NetBIOS Name der Domäne, z.b. "CONTOSO" |
| **%Join-Domain-User-PW%** | Passwort des zuvor spezifizierten Domainjoin Users |
| **%Domain%** | Domänenname, z.b. "CONTOSO.LOCAL" |
| **%CLIENT-OU%** | OU in welcher der Client während dem Client Aufgenommen wird, kann über das AD Attribut "distinguishedName" ausgelesen werden.  Z.b. "OU=Client, OU=netCIM2016, DC=CONTOSO,DC=LOCAL" |

### Konfiguration Copy Profile

|  |
| --- |
| Wichtig |
| Seit der Windows Version 1703 (OS Build 15063.296) können beim Copy Profile Probleme auftreten. Es wird daher empfohlen vorübergehend auf diese Funktion zu verzichten und den Eintrag im Unattend-File auf “false” zu setzen oder komplett zu entfernen! |

Mithilfe der Copy-Profile Funktion wird aus dem zuletzt angemeldeten Benutzer im netCIM vOS das Default Profil erstellt. Für die Konfiguration sind folgende Schritte notwendig:

* Generalisierung des vOS mit dem "–Manual" Parameter (siehe Kapitel: 5.2 vOS Tool)
  + Gewünschte Anpassungen für das zukünftige Default Profil vornehmen
* Anpassen des Unattend XML im Pass specialize:

|  |
| --- |
| <settings pass="specialize">  <component xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS">  <ComputerName>%NETCIM.HostName%</ComputerName>  **<CopyProfile>true</CopyProfile>**  </component>  </settings> |

## Host Gruppe erstellen

Wenn Add gedrückt wird kann eine Host-Gruppe erstellt werden.

|  |  |
| --- | --- |
| Name | Dies kann ein sprechender Name sein. Wobei wir keine sehr langen Namen empfehlen. |
| Management Password | Das Management Passwort ist optional. Dieses Passwort wird auf den Clients benötigt sofern ein Benutzer lokal den Computer mit Rapid Recovery zurücksetzen möchte. Sofern kein Passwort definiert wurde, kann er dies ohne Passworteingabe erledigen. |
| Native Boot | Sofern aktiviert, kann nur eine OSD Sequenz Ausgewählt werden und es steht kein Rapid Recovery und keine Update Möglichkeit zur Verfügung. Der Vorteil liegt hier dabei, dass dann ein ganz normales Betriebssystem-Deployment durchgeführt wird. |
| Boot Menu Timeout | Darstellungsdauer des Boot Menus in Sekunden. Bevor das Timeout abläuft hat der Benutzer die Möglichkeit, das zu startende Betriebssystem auszuwählen. |
| OSD Sequence Assignments | |  |  | | --- | --- | | **Order** | Reihenfolge im Boot Menu.  Die erste OSD Sequenz ist standardmässig ausgewählt und wird nach Ablauf des Timeouts automatisch gestartet. | | **Sequence Name** | Die OSD Sequenz. | | **Data Partition Drive Letter** | Sofern eine Datenpartition erstellt werden soll, welche bei einem Rapid Recovery nicht gelöscht werden soll, kann hier der Laufwerksbuchstabe spezifiziert werden. Die Datenpartition wird während dem Deployment als neue Deploy Action im Hostmenü angezeigt und kann anschliessen während dem Deployment bereits beschrieben werden. | | **Data Partition size** | Grösse der Data Partition in GB. | | **Enable Auto Recovery** | Sofern aktiviert, wird bei jedem Computer Start zuerst ein Rapid Recovery für dieses vOS vorgenommen. | | **Host Name Prefix/Suffix** | Dieser Eintrag wird an den Hostnamen angehängt. Sofern Domain Joins vorgenommen werden müssen alle vOS auf einem Host unterschiedliche Hostnamen aufweisen. Dies wird mit dieser Eigenschaft sichergestellt. | |
| Content Server | Hier können die Content Server ausgewählt werden, welche von den Clients genutzt werden dürfen. |

|  |
| --- |
| Wichtig |
| Wenn die Datenpartitionsgrösse verändert wird, wird diese gelöscht und neu erstellt. Die Daten gehen verloren.    Die Datenpartition wird ansonsten nur zurückgesetzt wenn die ganze Festplatte formatiert wird (Full Deployment). |

## Host erfassen

Hosts können über mehrere Optionen hinzugefügt werden. Es gibt die Möglichkeit die Funktion Unknown Computer Support zu nutzen, welche für einzelne Geräte einfach funktioniert, da man keine GUID abschreiben muss. Weiter können mehrere Hosts über eine Excel Datei importiert werden. Diese Methode eignet sich bestens, wenn man vom Hersteller eine Liste der gelieferten Geräte inklusive der BIOS GUID’s erhalten hat. Die dritte Variante ist das manuelle Erfassen eines Hosts über das Cockpit.

|  |
| --- |
| Hinweis |
| Die MAC Adresse muss beim Erfassen von Hosts nicht angegeben werden. Der netCIM Agent übermittelt nach der Installation die MAC Adresse des Clients automatisch an den netCIM Server und ermöglich so das Wake On LAN. |

### Unknown Computer Support - Automatisches erfassen

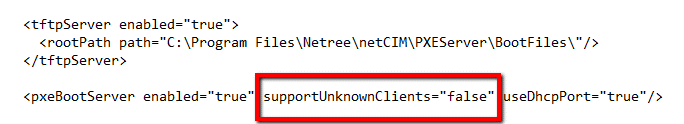
|  |  |
| --- | --- |
| C:\Users\sut\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Screenshot (1).png | Während dem PXE Boot erscheint die Meldung „Unknown host“. Durch Betätigen der Taste „b“ kann die Host Registrierung gestartet werden. |
| \\hsfp045\FolderRedirection$\sut\Desktop\Screenshots\Screenshot (4).png | Credentials eines netCIM Administrator Accounts angeben. |
| \\hsfp045\FolderRedirection$\sut\Desktop\Screenshots\Screenshot (5).png | Den Hostnamen, Hardware Typ und die Hostgruppe spezifizieren. Per Klick auf „**Save and Start Deployment**“ die Erfassung abschliessen. |

### Unknown Computer Support aus-/einschalten

Falls der Unknown Computer Support im Nachhinein noch ein oder ausgeschaltet werden möchte, z.B. aufgrund eines Parallelbetriebes, muss dies im entsprechenden Config-File angepasst werden.

Diese Datei befindet sich unter folgendem Pfad:

**%systemdrive%\ProgramFiles\Netree\netCIM\PXEServer\PxeService.exe.config**

Darin muss die Zeile **supportUnknownClients =“false“** dementsprechend angepasst werden.

### Manuelles erfassen

Wichtig beim Erfassen eines neuen Hosts ist, dass die korrekt formatierte GUID verwendet wird. Am besten ist, wenn die GUID verwendet wird, welche beim PXE Boot im Abschnitt netCIM dargestellt wird.

|  |
| --- |
| Hinweis |
| Dies kommt daher, dass es zwei Formate der GUID gibt und leider werden von diese von unterschiedlichen Programmen unterschiedlich genutzt.  Die Formate heissen "Pretty Print" und "Raw Byte Order". In netCIM wird die "Pretty Print" Schreibweise genutzt. Anhand der Schreibweise ist nicht erkennbar welches Format eingesetzt wird.  **Wie unterscheiden sich diese Formate?**  Beide bestehen aus 32 Hexadezimalen Zeichen (0-9 und A-F).  Pretty Print: 12345678-1234-1234-1234-1234567890AB  Raw Byte Order: 78563412-3412-3412-1234-1234567890AB  Wie man erkennen kann, sind im Raw Byte Order Format die Zeichen der ersten drei Blocks in umgekehrter Reihenfolge.  **Wie kann ich eine GUID einfach konvertieren?**  PowerShell Function  function Convert-GUID {  Param (  [Parameter(Mandatory=$True)]  [String]  $GUID  )  #Clean Up GUID  $GUID = $GUID -replace " " -replace "-"    # Create an array of two-charactere byte  $b = $GUID -split '(..)' | ? { $\_ }  # Build the final string, piecing together byte by byte  $convertedGUID = $b[3] + $b[2] + $b[1] + $b[0] + "-" + $b[5] + $b[4] + "-" + $b[7] + $b[6] + "-" + $b[8] + $b[9] + "-" + $b[10] + $b[11] + $b[12] + $b[13] + $b[14] + $b[15]  return $convertedGUID  }  Diese kann wie folgt aufgerufen werden:  Convert-GUID –GUID 12345678-1234-1234-1234-1234567890AB |

|  |  |
| --- | --- |
| cid:image001.png@01D0991C.104ED440 | Während dem PXE Boot ist die korrekte GUID im netCIM Abschnitt ersichtlich. |
|  | Die Clients können im Abschnitt „**Hosts**“ verwaltet werden. |
|  | Unter „**ADD**“ einen neuen Host erfassen. |
|  | Die verlangten Informationen wie im Bild eingeben. |

### Host import

|  |  |
| --- | --- |
| \\hsfp045\FolderRedirection$\DON\Desktop\Unbenannt.png | Die Hostdaten können im Tab Hosts per Klick auf **IMPORT** importiert werden. |
|  | Unter **DOWNLOAD TEMPLATE FILE** die Beispieldatei für den Import downloaden. |
|  | Nun die betreffenden Zeilen gemäss den Spaltenüberschriften in die Beispieldatei einfügen. |
|  | Anschliessend mit „**UPLOAD AND VALIDATE IMPORT FILE**“ die Importdatei validieren. |

## Berechtigungen

Wichtig ist, dass nicht nur die Benutzer welche auf das Cockpit zugreifen im netCIM berechtigt werden müssen, sondern auch alle Benutzer welche z.B. als Service Account im PXE, Content Server sowie im Boot Image Tool verwendet werden.

### netCIM Benutzer Rollen

Es gibt nur zwei Rollen in netCIM, der Administrator hat komplette Rechte über die Infrastruktur. Ein Benutzer kann keine Konfigurationen vornehmen und der Zugriff kann auf einzelne Host Gruppen eingeschränkt werden. So können Benutzer Deployments auslösen, und neue Hosts erfassen aber zum Beispiel keine neuen vOS erstellen und Deploy Actions modifizieren.

### Best Practice AD Benutzer und Gruppen

Wir empfehlen in einer Domain mit mindestens zwei Benutzern und einer Gruppe zu arbeiten. Zudem sollte für den SQL Server ein SQL Service Account erstellt werden, sofern nicht bereits einer vorhanden ist.

|  |  |  |
| --- | --- | --- |
| Vorgeschlagener Name | Typ | Beschreibung |
| netCIM\_Service | AD Benutzer | Dieser Benutzer Account muss im Cockpit die Rolle Content Server und PXE Server zugewiesen erhalten. Zudem muss dieser Account in der lokalen Administrator Gruppe des netCIM Servers sein. Dieser Benutzer muss Vollzugriff auf den SQL Server erhalten. |
| netCIM\_OSD | AD Benutzer | Der Benutzer Account muss im Cockpit die Rolle OSD zugewiesen erhalten bekommen. |

|  |  |  |
| --- | --- | --- |
| netCIM\_Administrators | AD Gruppe | Diese Gruppe erhält Zugriff auf das Cockpit von netCIM und auf dem netCIM Server muss diese in die lokale Gruppe "netCIM Package Source Administrators" hinzugefügt werden. Zudem sollte dieser Benutzer Vollzugriff auf den SQL Server erhalten. |

### Eigenständige netCIM Content Server

Sofern ein Content Server auf einem eigenen Server z.B. in einem Remote Standort betrieben wird, muss sichergestellt sein, dass der verwendete Service Benutzer auf dem Content Server in der Gruppe "netCIM Content Administrators" befindet sofern er nicht bereits in der Administratoren Gruppe ist. Zudem muss er die netCIM Rollen Content Server und PXE Server besitzen.

Sofern der netCIM Content Server nicht in derselben Domain betrieben wird, kann auch ein lokaler Benutzer verwendet werden, welcher auch auf dem netCIM Server existiert und die Content Server und PXE Server Rolle zugewiesen hat.

## Features

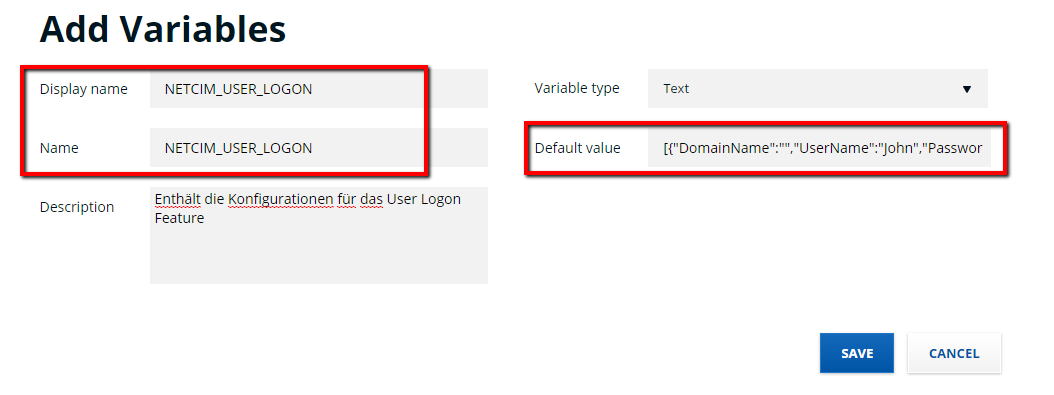
### User Logon / Auto Logon

Das User Logon Feature ermöglicht das Anmelden von Benutzern während dem Deployment. Dies hat den Vorteil, dass die Benutzerprofile bereits generiert wurden und die Anmeldung im Betrieb schneller erfolgt.

Ebenfalls kann die Autologon Option aktiviert werden, damit beim Starten des Betriebssystems ein Benutzer automatisch angemeldet wird.

|  |
| --- |
| Wichtige Hinweise |
| * Benutzer werden durch die Anmeldekonfiguration nicht erzeugt und müssen bereits existieren. Lokale Benutzer müssen entweder über das Unattend XML oder eine Deploy Action erstellt werden * Anmeldungen werden nach der letzten Deploy Action durchgeführt. * Passwörter werden Klartext abgespeichert und übertragen |

Alle Konfigurationen für das User Logon werden über eine netCIM Variable auf den jeweiligen OSD Sequenzen vorgenommen. Die Variable muss folgendermassen erstellt werden:



Der Wert der Variable kann entweder einen Eintrag für ein User Logon enthalten oder Leer sein. Die Variable kann auf Host ebene überschrieben werden. Wenn kein Wert spezifiziert wird, werden auch keine User Logons durchgeführt.

**Beispiele**

Benutzer John soll während dem Deployment angemeldet werden (wird kein DomainName spezifiziert, kann es sich um einen lokalen oder einen Domänenbenutzer handeln):

|  |
| --- |
| [{"DomainName":"","UserName":"John","Password":"Welcome1"}] |

Benutzer John der Domäne CONTOSO soll während dem Deployment angemeldet werden (DomainName spezifiziert, es wird spezifisch der Benutzer John der Domäne CONTOSO eingeloggt. Der DomainName kann auch der Computername sein um sicherzustellen, dass ein lokaler Benutzer eingeloggt wird):

|  |
| --- |
| [{"DomainName":"CONTOSO","UserName":"John","Password":"Welcome1"}] |

Der lokale Benutzer John soll während dem Deployment angemeldet werden (DomainName= Hostname. Benutzer John ist ein lokaler Benutzer. Die Eigenschaften DomainNameund UserName können die Variable %NETCIM.HostName% enthalten, welche während dem Deployment mit dem Hostnamen des jeweiligen Betriebssystems ersetzt wird):

|  |
| --- |
| [{"DomainName":"%NETCIM.HostName%","UserName":"John","Password":"Welcome1"}] |

Zuerst soll der lokale Benutzer John und anschliessend der lokale Benutzer Jane während dem Deployment angemeldet werden (Es können mehrere Benutzer spezifiziert werden, welche während dem Deployment angemeldet werden sollen):

|  |
| --- |
| [{"DomainName":"%NETCIM.HostName%","UserName":"John","Password":"Welcome1"},{"DomainName":"%NETCIM.HostName%","UserName":"Jane","Password":"Welcome1"}] |

Der lokale Benutzer John soll während dem Deployment angemeldet werden und nach dem Deployment bei jedem Computerstart automatisch angemeldet werden. Dies wird mit der Eigenschaft EnableForAutoLogon festgelegt (Standardwert: false). Es kann nur eine automatische Anmeldung Benutzer pro Betriebssystem festgelegt werden:

|  |
| --- |
| [{"DomainName":"%NETCIM.HostName%","UserName":"John","Password":"Welcome1","EnableForAutoLogon":"true"}] |

Der lokale Benutzer John soll während dem Deployment angemeldet werden. Für die Anmeldung wird ein Timeout von 30 Sekunden festgelegt. War die Anmeldung erfolgreich, wird 10min gewartet, bis der Benutzer abgemeldet und das Deployment fortgesetzt wird (LogonTimeout = Zeit in Millisekunden bevor die Anmeldung abgebrochen wird (Standardwert: 60000 Millisekunden was 1 Minute entspricht). LogonSuccessWaitTime = Zeit in Millisekunden die gewartet wird, bis der Benutzer nach einer erfolgreichen Anmeldung wieder abgemeldet wird (Standardwert: 300000 Millisekunden was 5 Minuten entspricht):

|  |
| --- |
| [{"DomainName":"%NETCIM.HostName%","UserName":"John","Password":"Welcome1","LogonTimeout":"30000","LogonSuccessWaitTime":"600000"}] |

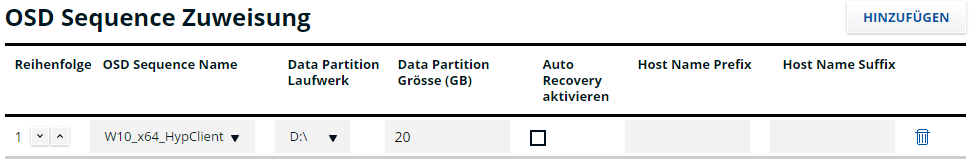
|  |
| --- |
| Hinweise |
| * Der Wert der Variable NETCIM\_USER\_LOGON  ist JSON formatiert. Der [ ] Block enthält eine Liste von { } Blöcken und innerhalb jedem { } Block befinden sich die Eigenschaften für einen Benutzer. Für mehrere Benutzer werden mehrere { } Blöcke kommagetrennt innerhalb [ ] aufgelistet * Eine minimale Anmeldekonfiguration besteht aus den Eigenschaften DomainName, UserName und Password pro Benutzer. Alle weiteren Eigenschaften sind optional. Werden die optionalen Eigenschaften nicht angegeben, gelten die Standardwerte * Existiert die Variable NETCIM\_USER\_LOGON nicht oder hat diese einen leeren Wert, entspricht dies einer leeren Anmeldekonfiguration. Während dem Deployment werden keine Anmeldungen durchgeführt. * Hat die Variable NETCIM\_USER\_LOGON einen ungültigen Wert, der nicht den Vorgaben entspricht schlagen Deployments fehl |

|  |
| --- |
| Wichtig: Spezifizierung des Domänennamens |
| Für das User Logon muss der Domänennamen im NetBIOS Format spezifiziert werden, das heisst:  "CONTOSO" und nicht "CONTOSO.LOCAL" |

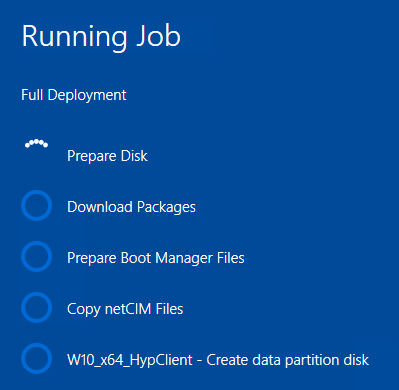
### Mounten der Datenpartition während dem Deployment

Ab dem Q3 Release ist es möglich, während dem Deployment eine Datenpartition zu erstellen, diese zu mounten und anschliessen direkt zu beschreiben. Es ist somit möglich, dass nach dem Aufsetzen des Computers bereits eine Datenpartition mit bestehenden Daten vorhanden ist oder, dass während dem Deployment Deploy Actions ausgeführt werden können, welche auf die Partition zugreifen.

Die Datenpartition wird wie gewohnt im netCIM Cockpit unter der Hostgruppe erstellt.



Während des Deployments wird ausserdem eine neue Deploy Action mit dem Namen «Create data partition disk» angezeigt.



#### Anwendungsbeispiel

Falls wir nun während des Deployments eine Anwendung vom Laufwerk «C:\» auf die Datenpartition kopieren möchte, könnte die Deploy Action wie folgt aussehen:

#Variabel für die Datenpartition (in diesem Fall Laufwerk "D:\"

$Datenpartition = "D:\"

#Variabel für den zu testenden Pfad

$Path = Test-Path -Path $Datenpartition

#Überprüfen ob der Pfad vorhanden ist

If ($Path -eq "True"){

#Ordner "C:\Software" auf die Datenpartition kopieren

Copy-Item -Path C:\Software -Destination $Datenpartition -Recurse -Force

}

# Betrieb

## Jobs auslösen und planen

Es können verschiedene Jobs mit unterschiedlichen Parametern gestartet werden. Die Job Typen Full, Update und Rapid Recovery können verzögert gestartet werden. Damit die Computer den Job auch wirklich durchführen können und automatisch gestartet werden, kann die Option Wake On LAN aktiviert werden. Sofern mehrere Computer von derselben Host Gruppe gestartet werden kann es Sinn machen, wenn Multicast aktiviert wird. Multicast reduziert die Netzwerklast erheblich.

|  |
| --- |
| Wichtig |
| Wenn die Datenpartitionsgrösse verändert wird, wird diese gelöscht und neu erstellt. Die Daten gehen verloren.    Die Datenpartition wird ansonsten nur zurückgesetzt wenn die ganze Festplatte formatiert wird. |

### Wake On LAN

Für die Funktionalität Wake On LAN wird in einem Netzwerk die MAC Adresse des Empfängers benötigt. Da ein Netzwerk viele Subnetze enthalten kann, wird zusätzlich die Subnetz Adresse benötigt. Da diese Information dynamisch sein kann und somit vom Administrator nur schwer vordefiniert werden kann, werden die Subnetz und MAC Adressen automatisch von den Clients an den netCIM Server übermittelt. Das bedeutet aber auch, dass der erste Start nach dem Erfassen nicht per Wake On LAN geschehen kann.

### Herunterfahren nach Job Verarbeitung

Beim Erstellen eines Jobs kann die Option "Herunterfahren nach Job Verarbeitung" ausgewählt werden. Das heisst, der Client fährt nach Abschluss der Verarbeitung herunter. Falls der Job nicht erfolgreich war und ein Fehler auftritt, wird der Host nicht heruntergefahren, damit mittels Fehlermeldung weiteres Troubleshooting durchgeführt werden kann.

## Backup und Restore

Für ein Backup des Systems müssen folgende Komponenten gesichert werden:

* netCIM Source Share
* SQL Datenbank

### Restore SQL Datenbank und netCIM Source

#### Windows Server 2016 / Windows Server 2019

|  |  |
| --- | --- |
|  | Erstellen eines Systems mit demselben Hostnamen |
|  | Installation netCIM |
|  | Stoppen der Services: netCIM Server, netCIM Content Server |
|  | Microsoft SQL Datenbank aus Backup wiederherstellen auswählen |
|  | Per Klick auf „Add“ den Pfad zum \*.bak File der Datenbank angeben |
|  | Inhalt in den netCIM Source Ordner zurück kopieren |
|  | Jedes Package manuell per „Distribute“ Button aktualisieren oder automatisch mit folgendem Script: |
| $cse = (Get-WmiObject win32\_service | ?{$\_.Name -like 'NetCimContentServer'})  $cse = $cse.PathName.Replace("`"","")  $csp = $cse | Split-Path -Parent  Add-Type -Path “$csp\Netree.NetCim6.Client.dll"  $c = New-Object Netree.NetCim6.Client.NetCimServerProxy("localhost")  foreach($pkg in $c.PackageDistributionManager.ListDistributedPackages().Items){  $c.PackageDistributionManager.Distribute($pkg.ID)  } | |

## Virenschutz Client

Wenn eine Antivirensoftware auf den Clients eingesetzt wird, empfehlen wir folgendes:

* Ausschluss des netCIM Ordners welcher die VHDX Files enthält %SYSTEMROOT%\netCIM.

Ansonsten gelten die normalen Empfehlungen für Windows Systeme gemäss den Best Practice Angaben von Microsoft und den Virenschutzherstellern.

# Troubleshooting

## Allgemein

Alle netCIM Log Einträge werden zentral in der netCIM Datenbank abgespeichert. Zudem werden alle Log Einträge lokal in einer Datei abgespeichert. Sofern keine Netzwerkverbindung vorhanden ist, werden die Log Einträge verzögert übermittelt.

### Debug Logging aktivieren

Grundsätzlich ist das Debug Logging (Detailliertester Log Level) in netCIM deaktiviert. Dies kann bei der ersten Installation aktiviert werden. Dieses Vorgehen wird jedoch nur für explizite Testumgebungen empfohlen. Daher sollte das Debug Logging bei Problemen pro Komponente aktiviert werden. Dies geschieht über die entsprechenden App.Config Files der jeweiligen Komponenten.

|  |  |  |
| --- | --- | --- |
| Pfad der Datei | Komponente | Hinweis |
| %InstDir%\OSDHandlerBinaries\x64\OsdHandler.exe.config | OSD Handler | Nach der Anpassung muss das Boot Image neu erstellt werden! |
| %InstDir%\OSDHandlerBinaries\x86\OsdHandler.exe.config | OSD Handler |
| %InstDir%\BootImageTool\BootImageTool.exe.config | Boot Image Tool | Tool muss neu gestartet werden. |
| %InstDir%\ContentServer\NetCimContentService.exe.config | Content Server | Service muss neu gestartet werden. |
| %InstDir%\PXEServer\PxeService.exe.config | PXE Service | Service muss neu gestartet werden. |
| %InstDir%\Server\NetCimService.exe.config | Service | Service muss neu gestartet werden. |
| %InstDir%\WebConsole\Web.config | Cockpit | IIS Reset muss durchgeführt werden. |

Die Veränderung in den Config Files beschränkt sich darauf, den hier folgenden Abschnitt zu suchen und den Value auf „ALL“ zu setzen. Um das Debug Logging wieder zu deaktivieren muss der Wert wieder auf „INFO“ zurückgeändert werden.

<log4net>

<root>

<level value="ALL"/>

<appender-ref ref="LogFileAppender"/>

</root>

### Log Dateien und Speicherorte

Wichtig ist zu beachten, dass der Temp Ordner je nach Benutzer an einem anderen Speicherort abgelegt ist. Daher ist immer wichtig zu überprüfen unter welchem Kontext der jeweilige Service oder die jeweilige Applikation ausgeführt wird.

|  |  |  |
| --- | --- | --- |
| Datei | Rolle | Beschreibung |
| %TEMP%\NetCimWebConsole.log | netCIM Server |  |
| %TEMP%\NetCimContentService.log | netCIM Content Server | Beinhaltet alle Informationen welche mit der Content Distribution zusammenhängen. |
| %TEMP%\NetCimBootImageTool.log | netCIM Boot Image Management Computer |  |
| %TEMP%\NetCimPxeService.log | netCIM Content Server | Beinhaltet alle Informationen welche in Bezug mit dem PXE Boot stehen. |
| %TEMP%\NetCimService.log | netCIM Server | Beinhaltet alle Informationen über den die Aktionen die auf dem zentralen Service ausgeführt wurden. |
| %SYSTEMROOT%  \NetCim\Log\OsdHandler.log | netCIM Clients | Beinhaltet alle Informationen welche während dem Ausführen der OSD Sequence auftreten. |
| %SYSTEMROOT%  \NetCim\Log\dismApplyDrivers\_s10.log | netCIM Clients | DISM Log File des Apply Driver Steps. Die Nummer hinter S entspricht der ID der OSD Sequence. |
| %SYSTEMROOT%  \NetCim\Log\dismCreateImage.log | netCIM Clients | DISM Log File für Konvertierung der VHDX zu einem WIM File (Nur Native Boot). |
| %SYSTEMROOT%  \NetCim\Log\dismApplyImage.log | netCIM Clients | DISM Log File für WIM File Anwendung auf die physikalische Festplatte (Nur Native Boot). |
| %SYSTEMROOT%  \NetCim\Log\netCIMAgent.log | netCIM Clients | netCIM Agent Log File. |
| %TEMP%\NetCimAgent.install.log | netCIM Clients | MSI Log File der Agent Installation. |

### Arbeiten mit dem Log Viewer

Der Log Viewer ermöglich das zentrale Betrachten aller netCIM Log Files. Der Log Viewer kann über die Navigation (Monitoring 🡪 Log Viewer) oder über den Job Status erreicht werden. Da diese Datenbank sehr viele Informationen enthält, ist es sehr wichtig korrekt zu filtern.

Die wichtigsten Filterkriterien sind:

* System 🡪 Host auf welchem die Aktion stattgefunden hat.
* Datum und Zeit 🡪 Wann wurde die Aktion ca. durchgeführt.
* Logger 🡪 Welche Komponente hat die Aktion ausgeführt. Standardmässig sind die wichtigsten Logger für ein OS Deployment ausgewählt.
* Level 🡪 Der Level bestimmt wie wichtig der Eintrag ist. Diese Levels werden in der folgenden Reihenfolge immer wie detaillierter: Fatal 🡪 Error 🡪 Warning 🡪 Information 🡪 Debug

## OS Deployment

Grundsätzlich arbeitet netCIM nach dem folgenden Prozess beim OS Deployment. Dieser muss verstanden werden um beim Troubleshooting die richtigen Log Files zu analysieren.



### Treiberinstallation im WinPE

|  |  |
| --- | --- |
| Log file | Description |
| X:\$WINDOWS.~BT\Sources\Panther\setupact.log | Contains information about setup actions during the installation. |
| X:\$WINDOWS.~BT\Sources\Panther\setuperr.log | Contains information about setup errors during the installation. |
| X:\$WINDOWS.~BT\Sources\Panther\miglog.xml | Contains information about the user directory structure. This information includes security identifiers (SIDs). |
| X:\$WINDOWS.~BT\Sources\Panther\PreGatherPnPList.log | Contains information about the initial capture of devices that are on the system during the downlevel phase. |

### Treiberinstallation im Windows Setup

This phase is the first boot phase that starts when you receive the message to wait while Windows prepares to start for the first time. During this boot phase, basic hardware support is installed. The following table lists the log files that are important during this setup phase.

|  |  |
| --- | --- |
| Log File | Description |
| C:\WINDOWS\PANTHER\setupact.log | Contains information about setup actions during the installation. |
| C:\WINDOWS\PANTHER\setuperr.log | Contains information about setup errors during the installation. |
| C:\WINDOWS\PANTHER\miglog.xml | Contains information about the user directory structure. This information includes security identifiers (SIDs). |
| C:\WINDOWS\INF\setupapi.dev.log | Contains information about Plug and Play devices and driver installation. |
| C:\WINDOWS\INF\setupapi.app.log | Contains information about application installation. |
| C:\WINDOWS\Panther\PostGatherPnPList.log | Contains information about the capture of devices that are on the system after the online configuration phase. |
| C:\WINDOWS\Panther\PreGatherPnPList.log | Contains information about the initial capture of devices that are on the system during the downlevel phase. |

### Domain Join

When a Windows 7 desktop is created in netCIM it runs through the Microsoft Windows mini-setup process which uses a file called unattend.xml to configure a variety of desktop settings. If your desktop is not joining the domain correctly, here are some common issues and how to solve them.

Check your unattend file for issues. For example, let’s assume that you have this configuration:

fully qualified domain name: vdidomain.acme.com or vdidomain.local

short domain name: vdi

OU: acmegrp1

Domain account: Administrator

Open the unattend file on the desktop and check for some common problems. The unattend file is located in c:\windows\panther.

Search for the <JoinDomain> tag and check the fully qualified domain name. It should look like this:

<JoinDomain>vdidomain.local</JoinDomain> or

<JoinDomain>vdidomain.acme.com</JoinDomain>

Check the domain specification by searching for the Domain tag: <Domain>. The Domain tag must be the short domain name, not the fully qualified domain name.It should look like this:

Correct: <Domain>vdi<Domain>

Incorrect: <Domain>vdidomain.acme.com<Domain>

Check the Username specification. It should look like this:

Correct: <Username>Administrator</Username>

Incorrect:<Username>vdi\Administrator<\Username>

Check the processor architecture

Edit the unattend.xml to fix problems

#### Advanced debugging Setupact

The following log file details the progress of the mini-setup process, including a summary line for each domain attempt. Check this log file for errors:

C:\Windows\Panther\UnattendGC\setupact.log

Note: Be sure you are not looking at the setupact.log in C:\Windows\Panther. You want the log file that's in C:\Windows\Panther\UnattendGC.

Search for DJoin.exe to see a log of the domain join operations:

*DsGetDCName failed: 0x54b … check your fully qualified domain name*

NetJoinDomain attempt failed: 0x89a … check your domain join credentials

*NetJoinDomain attempt failed 0x2: check your OU specification*

Still stumped? For other log files to check, go to the section on Advanced debugging later in this document.

#### Advanced debugging Netsetup

One log file details the entire process of joining the domain: C:\Windows\debug\NetSetup.log. Look for the section with today's date to watch the process from the beginning, or go to the bottom of the file to see the last attempt and why it failed. If an attempt fails, Windows makes another attempt every five seconds, up to 80 times, as a result, your log may contains many duplicate failure messages.

A successful domain join displays the following message:

05/01/2012 09:28:01:740 NetpDoDomainJoin: status: 0x0

This line appears at the bottom of the last attempt, and denotes that the domain join process succeeded. Any return status other than 0x0 denotes a failure. You may also see the following lines above it, which also show success:

05/01/2012 09:28:01:740 NetpCompleteOfflineDomainJoin: status: 0x0

05/01/2012 09:28:01:740 NetpJoinDomain: NetpCompleteOfflineDomainJoin SUCCESS: Requested a reboot :0x0

Failure, again, is a non-zero return code:

01/20/2012 10:53:01:232 NetpDoDomainJoin: status: 0x2

One of the most common failures is an error attempting to connect to the IPC$ share on the domain controller. It will look like this:

05/02/2012 23:14:21:057 NetUseAdd to \\DC1.company.local\IPC$ returned XXXX

Get the returned message (XXXX) and run net helpmsg XXXX from a command prompt to see the specific error. The following are common domain join errors and solutions to those errors.

**Failure 1231**

07/12/2012 14:38:52:122 NetUseAdd to \\DC1.company.local\IPC$ returned 1231

07/12/2012 14:38:52:122 NetpJoinDomain: status of connecting to dc '\\TDC1.company.local': 0x4cf

07/12/2012 14:38:52:122 NetpJoinDomainOnDs: Function exits with status of: 0x4cf

07/12/2012 14:38:52:122 NetpDoDomainJoin: status: 0x4cf

The server could not be reached. Is a network connection available?

**Failure 1326**

05/02/2012 23:07:31:696 NetUseAdd to \\DC1.company.local\IPC$ returned 1326

05/02/2012 23:07:31:696 NetpJoinDomain: status of connecting to dc '\\DC1.company.local': 0x52e

05/02/2012 23:07:31:696 NetpJoinDomainOnDs: Function exits with status of: 0x52e

05/02/2012 23:07:31:696 NetpDoDomainJoin: status: 0x52e

Failure 1326 is a straightforward password error, "Logon failure: unknown user name or bad password." Double-check the username and password in your unattend.xml file.

**Failure 1909**

05/02/2012 23:14:21:057 NetUseAdd to \\DC1.company.local\IPC$ returned 1909

05/02/2012 23:14:21:057 NetpJoinDomain: status of connecting to dc '\\DC1.company.local': 0x775

05/02/2012 23:14:21:057 NetpJoinDomainOnDs: Function exits with status of: 0x775

05/02/2012 23:14:21:057 NetpDoDomainJoin: status: 0x775

A 1909 error means "The referenced account is currently locked out and may not be logged on to." Go to your Active Directory and unlock the account. You should also determine how the account got locked. Often the account becomes locked because the unattend.xml has an incorrect password. Attempting to join a domain retries dozens of times. If the password is incorrect, you might get three password failures and dozens of "account locked" failures.

**Bad OU specified**

01/20/2012 10:53:01:232 NetpCreateComputerObjectInDs: NetpGetComputerObjectDn failed: 0x2

01/20/2012 10:53:01:232 NetpProvisionComputerAccount: LDAP creation failed: 0x2

01/20/2012 10:53:01:232 NetpProvisionComputerAccount: Cannot retry downlevel, specifying OU is not supported

01/20/2012 10:53:01:232 ldap\_unbind status: 0x0

01/20/2012 10:53:01:232 NetpJoinDomainOnDs: Function exits with status of: 0x2

01/20/2012 10:53:01:232 NetpJoinDomainOnDs: status of disconnecting from '\\DC1.company.local': 0x0

01/20/2012 10:53:01:232 NetpDoDomainJoin: status: 0x2

The message "Cannot retry downlevel, specifying OU is not supported" means that the specified OU is invalid. This error could indicate that the OU does not exist within the AD, or that you are attempting to specify the default Computers container. Windows requires that the default OU be left unspecified, so if you want to put new desktops into the default Computers OU, you must delete the <MachineObjectOU> line entirely. Look further up the log file for what the specified OU is:

01/20/2012 10:53:01:123 lpMachineAccountOU: OU=Computers,OU=VDI,DC=company,DC=local

Verify the existence of the specified OU and confirm that it is not the top-level Computers container.

**Bad domain specified**

If the domain name itself is invalid, a domain join makes no entries to NetSetup.log and does not create a log file. In this situation, look in C:\Windows\Panther\UnattendGC\setupact.log for lines like this:

2012-07-13 16:11:15, Warning [DJOIN.EXE] Unattended Join: DsGetDcName failed: 0x54b, last error is 0x0, will retry in 5 seconds...

The error text for 0x54b (1355) is "The specified domain either does not exist or could not be contacted." You can look further up in the setupact.log to see exactly what domain you were trying to join. Note that this is an error with the "JoinDomain" tag, not the credentials.

**Insufficient user rights**

07/17/2012 13:26:47:524 NetpMapGetLdapExtendedError: Parsed [0x5] from server extended error string: 00000005: SecErr: DSID-03152492, problem 4003 (INSUFF\_ACCESS\_RIGHTS), data 0

07/17/2012 13:26:47:524 NetpModifyComputerObjectInDs: ldap\_add\_s failed: 0x32 0x5

07/17/2012 13:26:47:524 NetpCreateComputerObjectInDs: NetpModifyComputerObjectInDs failed: 0x5

07/17/2012 13:26:47:524 NetpProvisionComputerAccount: LDAP creation failed: 0x5

...

07/17/2012 13:26:47:539 NetpDoDomainJoin: status: 0x5

The user account you specify must have rights to add machine accounts to the domain in the specified OU. This error appears when you have a valid account with insufficient privileges. Either try a different account or adjust the account privileges in the domain.

#### Use another approach to domain join

If you are unable to make your domain join work automatically via the unattend file, you can try adding a Deploy Action to the deployment process to do the domain join. For more information, see the PowerShell Command Add-Computer.

## Group Policies

Sofern Group Policies nicht erfolgreich angewendet werden, sollten folgende Punkte überprüft werden:

1. Windows Event Viewer 🡪 Windows Logs – System: Basis Informationen zu Fehlern sowie jede Aktualisierung im Hintergrund wird dargestellt.
2. Windows Event Viewer 🡪 Applications and Services Logs – Microsoft – Windows – GroupPolicy – Operational
3. Sofern keine Fehler auftreten, sollte überprüft werden ob die GPO’s erkannt werden oder von einer anderen Policy überschrieben werden. Dies geschieht am einfachsten mit dem folgenden Befehl, welcher einen HTML Report erstellt und darstellt welche Einstellungen aus welcher Policy angewendet werden:

gpresult /H c:\temp\result.html

Sofern diese Analysen keine weiteren Erkenntnisse aufzeigen kann das erweiterte GPO Logging (Gpsvc.log) wie folgt aktiviert werden:

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and then click the following registry subkey:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion

1. On the Edit menu, point to New, and then click Key.
2. Type Diagnostics, and then press ENTER.
3. Right-click the Diagnostics subkey, point to New, and then click DWORD Value.
4. Type GPSvcDebugLevel, and then press ENTER.
5. Right-click GPSvcDebugLevel, and then click Modify.
6. In the Value data box, type 00030002, and then click OK.
7. Exit Registry Editor.
8. At a command prompt, type the following command, and then press ENTER:

gpupdate /force

1. View the Gpsvc.log file in the following folder:

%windir%\debug\usermode

|  |
| --- |
| Hinweis Usermode Folder |
| If the usermode folder does not exist under %windir%\debug\ the gpsvc.log file will not be created. If the usermode folder does not exist, create it under %windir%\debug |

# Best Practice – Deploy Actions

Für die Deploy Actions empfiehlt es sich eine lokale Ablage Struktur anzulegen, welche mehr Informationen enthält als die Deploy Action selbst. Diese Ablage wird im Normalfall Development Ordner genannt und sollte auf der Datenpartition des Servers liegen.

|  |  |  |  |
| --- | --- | --- | --- |
| <Manufacturer>\_<Product>\_<Version>\_<PackageVersion>\_<Typ>\_<Sprache>\_<Architecture> | | | Pro Application und Version existiert ein Verzeichnis. Dieser Name ist auch zugleich der Deploy Action Name. |
| | | Deploy | | Enthält das fertige Paket, welches in die Deploy Action kopiert wird. |
| | | | Source | Enthält die Source Dateien welche verwendet werden. |
| | | | Documentation | Enthält die Dokumentationen zu diesem Software Paket inkl. dem PowerShell Command welcher in netCIM benötigt wird. |

Wenn die Deploy Actions im netCIM erfasst werden, sollte als Deploy Action Name der Name des Hauptordners verwendet werden:

<Manufacturer>\_<Product>\_<Version>\_<PackageVersion>\_<Typ>\_<Sprache>\_<Architecture>

Der Typ kann folgende Werte enthalten:

* P für physikalisches Paket
* V für eine virtuelle Applikation

Nur der Inhalt des Ordners Deploy wird als Content in eine netCIM Deploy Action übernommen.

# Best Practice – Treiber Engineering

Die Paket Struktur für eine Driver Collection und den Boot Image Treiber Ordner sollte wie folgt sein:

|  |  |  |
| --- | --- | --- |
| <Category> | | Folgende Kategorien sind erlaubt: LAN, WWAN, WLAN, CHIPSET, DISPLAY, CAMERA, SOL, GRAPHIC, RAID, AUDIO, MEI, OTHERS  Alle Treiber die nicht explizit in eine dieser Kategorien zugeordnet werden können, werden im Ordner OTHERS abgespeichert. |
| | | <DeviceManufacturer>\_<DeviceName>\_<Version>\_<Language>\_<Architecture> | Für jedes Gerät innerhalb der Kategorien wird ein Ordner erstellt. |

Grundsätzlich sollte nach folgendem Prozess gearbeitet werden, wenn ein neues Hardware Modell integriert werden muss:



# Best Practice - Active Directory Machine Password

Active Directory benötigt eine spezielle Einstellung damit die Funktion Rapid Recovery verwendet werden kann. Standardmässig aktualisiert ein Computer, welcher Mitglied in einer Domäne ist, sein Passwort periodisch. Dies muss verhindert werden, da sich sonst ein Computer nach einem Rapid Recovery nicht mehr in der Domäne authentifizieren kann.

|  |
| --- |
| Hinweis |
| Wie der Prozess des Computer Passwortwechsel abläuft ist hier detailliert beschrieben:  <http://blogs.technet.com/b/askds/archive/2009/02/15/test2.aspx> |

Die Anpassung kann über GPO’s oder über die Registry auf dem Client vorgenommen werden.

**Registry**

Key: HKLM\SYSTEM\CurrentControlSet\Services\NetLogon\Parameters

Name: DisablePasswordChange

Typ: REG\_DWORD

Wert: 1

**Group Policy Object**

Ort: Computer Configuration\windows Settings\Security settings\Local Policies\Security Options

Name: Domain member: Disable machine account Password changes