Hochschule für Technik und Wirtschaft Berlin
University of Applied Sciences

Skriptgesteuerte Erstellung und Konfiguration von Windows-basierten virtuellen Maschinen in Hyper-V mittels PowerShell

Bachelorarbeit

von

Kevin Hübner

Matrikelnummer: 570746

Fachbereich 1: Computer Engineering
Hochschule für Technik und Wirtschaft Berlin

Datum: Berlin, 21.08.2025

Erstgutachten:
Zweitgutachten:

Inhaltsverzeichnis

1 Einleitung

Mit dem fortschreitenden technologischen Wandel stehen Systemadministratoren eine Vielzahl an Werkzeugen zur Verfügung, um ihre Arbeit effizienter zu gestalten. Dazu gehören grafische Benutzeroberflächen, die die Bedienung vereinfachen, Skripte zur Automatisierung wiederkehrender Prozesse sowie zunehmend auch Methoden der Künstlichen Intelligenz. Besonders kleine und mittelständische Unternehmen sind jedoch häufig damit ausgelastet, ihre bestehenden Systeme im täglichen Betrieb zuverlässig zu betreiben. Dadurch geraten neue Technologien, die die Arbeit erleichtern und langfristig effizienter gestalten könnten, oftmals in den Hintergrund.

2 Praxis

Die Idee zu dieser Arbeit entstand aus praktischen Erfahrungen in der Windows-Server-Administration, insbesondere im Umgang mit Hyper-V in Failover-Cluster-Umgebungen. In der bisherigen Vorgehensweise erfolgt die Bereitstellung neuer virtueller Maschinen (VMs) vollständig manuell – von der Erstellung der VM über die Installation des Betriebssystems bis hin zur Konfiguration der benötigten Rollen und Dienste.

Ein typisches Szenario ergibt sich bei der Einrichtung eines neuen Kunden im Rechenzentrum. Standardmäßig werden dabei drei VMs eingerichtet: ein Domänencontroller (DC), ein Dateiserver (FS) sowie ein Terminalserver (TS). Diese klare Trennung der Rollen bietet Vorteile hinsichtlich Übersichtlichkeit, Lastverteilung und Sicherheit. Die manuelle Einrichtung umfasst jedoch zahlreiche wiederkehrende Arbeitsschritte, wie die Vergabe statischer IP-Adressen, die Umbenennung der Rechner, die Einbindung zusätzlicher Festplatten, die Erstellung von Standard-Benutzern und -Gruppen sowie die Konfiguration von Gruppenrichtlinien und Ordnerberechtigungen. Hinzu kommt, dass kundenspezifische Anwendungen wie DATEV besondere Anforderungen stellen, beispielsweise durch den Einsatz von SQL-Datenbanken. Diese zusätzlichen Konfigurationen erhöhen den manuellen Aufwand erheblich.

3 Ziel der Arbeit

Um diesen Herausforderungen zu begegnen, wurde im Rahmen dieser Arbeit ein PowerShell-Skript entwickelt, das die wiederkehrenden Arbeitsschritte bei der Bereitstellung von Windows-Server-VMs weitgehend automatisiert. Das Skript übernimmt unter anderem die Erstellung und Konfiguration von drei VMs (DC, FS, TS), die Einrichtung der grundlegenden Rollen, die Anlage von Standard-Benutzern und -Gruppen, die Vergabe von NTFS-Berechtigungen sowie die Konfiguration von Netzwerkparametern.

Als Grundlage dient ein mit dem Windows-Tool Sysprep generalisiertes VM-Template, das mithilfe einer vorbereiteten Antwortdatei (*unattend.xml*) erstellt wird. Dieses Template ermöglicht es, alle weiteren Konfigurationsschritte skriptgesteuert durchzuführen, wodurch einsatzbereite Systeme mit minimalem manuellem Aufwand bereitgestellt werden können.

Ziel dieser Arbeit ist es daher, ein strukturiertes, skriptbasiertes Vorgehen für die automatisierte Erstellung und Konfiguration von Windows-Server-VMs in Hyper-V zu entwickeln und zu evaluieren. Dadurch soll gezeigt werden, wie sich typische Administrationsaufgaben standardisieren und effizienter gestalten lassen.

4 Theorie

4.1 Sysprep

4.2 Windows Hyper-V

4.3 Windows Powershell

4.3.1 Gültigkeitsbereich von Variablen

4.3.2 Powershell Direct

4.3.3 Kerberos Double Hop Problem

5 Entwicklung des Skripts zur Automatisierung

5.1 Vorbereitung des VM-Templates

Im Rahmen der Skripterstellung wurde zunächst ein VM-Template erstellt. Mit dem VM-Template wird die erneute Installation von Windows in den VMs umgangen, womit es nur noch einmal für das Template selbst installiert werden muss. Ein wesentlicher Bestandteil dieses Schrittes war die Erstellung einer Antwortdatei (Unattend-XML), die im späteren Prozess die automatisierte Erstkonfiguration ermöglicht.

Zur Generierung der Antwortdatei wurde die Windows-Server-ISO eingebunden und mit dem Windows System Image Manager das darin enthaltene Abbild (install.wim) geladen. Anschließend wurde die Zieledition „Server Standard“ ausgewählt, da diese als Grundlage für die Kunden-VMs vorgesehen ist. Vor der Definition der eigentlichen Antwortdatei wurde eine Katalogdatei erzeugt. Innerhalb der Antwortdatei wurden die relevanten Konfigurationsoptionen integriert. Diese sind im Bereich Microsoft-Windows-Shell-Setup zu finden. Dabei lag der Fokus auf dem Abschnitt OOBE, um Ersteinrichtungsoptionen wie Tastaturlayout und Sprache zu überspringen. Zusätzlich wurden noch lokale Benutzerkonten angelegt. Nach Erstellung der XML-Datei wurde diese, der Installation im Audit-Modus hinzugefügt.

Die vollständige XML-Datei wurde im Sysprep Verzeichnis (Sysprep, i.d.R. unter `C:\Windows\System32\Sysprep`) gespeichert. Sysprep ist ein Windows eigenes Tool, welches zur Vorbereitung von Windowssystemen dient.

Anschließend erfolgte die Ausführung von Sysprep mit den Parametern */oobe , /generalize, /shutdown /unattend:(Pfad zur XML−Datei)*. Dadurch wurde die Windows-Installation generalisiert und von der spezifischen VM-Umgebung entkoppelt. Die einmalige Erstellung und Konfiguration beanspruchte auf einem leistungsfähigen System etwa fünf bis zehn Minuten. Das ist die Zeit um Windows-Server auf der VM zu installieren und mit der Tastenkombination STRG+Shift+F3, während der Abfrage des Administratorpassworts, in den Audit-Modus zu wechseln. Dies ermöglichte individuelle Anpassungen sowie die Absicherung des lokalen Administratorkontos während des Bootens in die Windows Umgebung und überspringt die Ersteinrichtung.

Für das Skript war ausschließlich relevant, dass die Passwortvergabe gewährleistet, ein zusätzlicher lokaler Administrator angelegt und Einrichtungsdialoge durch die XML-Datei übersprungen wurden. Ergänzend wurde das Tastaturlayout auf Deutsch gesetzt. Durch die Generalisierung der Windows-Installation wird erreicht, dass die virtuelle Festplatte (VHD/X) einer erstellten VM kopiert und mehrfach wiederverwendet werden kann, ohne dass Konflikte zwischen den Sicherheits-IDs (SIDs) der Administratorbenutzer verschiedener VMs auftreten. Entscheidend ist hierbei, dass die betreffende VM nach der Generalisierung nicht erneut gestartet wird, bevor die VHD(X)-Datei kopiert wurde, da ansonsten die Generalisierung ihre Gültigkeit verliert.
Im Zuge der Experimente mit den VM-Templates zeigte sich jedoch, dass Fehler in der Generalisierung (z. B. durch fehlerhafte Unattend-Dateien) dazu führen können, dass lokale Administratoren auf unterschiedlichen Systemen identische Sicherheits-IDs (SIDs) erhalten. In diesem Fall schlägt der Domänenbeitritt fehl. Daher ist bei der Erstellung der Unattend-Datei besondere Sorgfalt erforderlich. Die Überprüfung der SIDs kann nach der VM-Erstellung über den Befehl *Get−LocalUser −Name Administrator* FL| erfolgen. Werden identische SIDs festgestellt, ist davon auszugehen, dass die Generalisierung mit Sysprep nicht korrekt durchgeführt wurde, was wiederum zum Abbruch des Skripts führen würde.

5.2 Erstellung der VMs mittels PowerShell

Im nächsten Schritt erfolgte die Erstellung von VMs mithilfe von PowerShell. Der grundlegende Ablauf entspricht dabei den Prozessen, die auch aus anderen Virtualisierungslösungen bekannt sind: Jedem virtuellen System werden ein Name, ein Speicherort, Arbeitsspeicher, CPU-Kerne, ein Netzwerkadapter sowie eine Bootfestplatte zugewiesen. Da bereits eine vorbereitete VHDX-Datei für die Bootpartition vorliegt, muss diese lediglich als Bootmedium zugewiesen werden. Dafür muss die vorbereitete VHD(X)-Datei an den vorgesehenen

Speicherort kopiert werden und bei der Erstellung der VM muss der Pfad zu dieser Kopie angegeben werden. Für den Fileserver wurde zusätzlich eine separate Festplatte eingerichtet, die der Speicherung der Nutzerdaten dient und entsprechend in das System eingebunden wird. Die Konfiguration über PowerShell erforderte somit lediglich Schritte, die auch über die grafische Oberfläche ausgeführt werden könnten. Anschließend erfolgt die Zuweisung von Ressourcen wie Arbeitsspeicher und Prozessoranzahl. Für jede neue VM wird dieser Prozess identisch durchgeführt, wodurch sich manuelle Vorgehensweisen mit den PowerShell-basierten Methoden vergleichen lassen. Jedoch wird die Erstellung von mehreren VMs durch ein Skript erheblich vereinfacht, da die Schritte automatisiert und in einer Schleife ausgeführt werden können.

Vor dem Einstieg in weitere Schritte war eine zusätzliche Anpassung hinsichtlich der Netzwerkadapter erforderlich. Da die Systeme über TeamViewer verwaltet werden, musste für den Netzwerkadapter jeder VM eine statische MAC-Adresse vergeben werden. Dies verhindert, dass die Systeme aus der Geräteliste in TeamViewer verschwinden. Um die MAC-Adresse zuweisen zu können, wird die VM einmalig gestartet, sodass Windows eine temporäre Adresse generiert. Anschließend wird die Maschine heruntergefahren und in Hyper-V die MAC-Adresse auf statisch gesetzt. Danach kann der reguläre Arbeitsablauf fortgesetzt werden.

5.3 Verzeichnisstruktur und Logdateien

Zur Verwaltung der Kunden-VMs wurde eine einheitliche Ordnerstruktur implementiert. Hierfür wurde ein eigenes Skript (FilehandlingFunctions) entwickelt, das für jeden Kunden automatisch identische Verzeichnisse anlegt, wobei die Struktur jeweils unter dem individuellen Kundennamen eingetragen wird. Innerhalb dieser Hierarchie werden die vorbereiteten VHD(X)-Dateien aus dem zentralen Vorbereitungsverzeichnis in die entsprechenden Kundenordner kopiert. Vor der Erstellung überprüft das Skript, ob die betreffende Struktur bereits vorhanden ist, um redundante Duplikate zu vermeiden. Die Umsetzung basiert auf einfachem File Handling, wobei neue Verzeichnisse mit dem PowerShell-Befehl *New−Item* erzeugt werden.

Neben der Verzeichnisstruktur wird für jeden Kunden zusätzlich ein Logfile eingerichtet. Dieses ermöglicht sowohl die Nachverfolgung des Skriptablaufs als auch die Identifikation möglicher Fehlerquellen oder Prozessunterbrechungen. Da das VHD(X)-Template für die VM-Erstellung standardmäßig die Datei unattend.xml enthält, in der Administratorpasswörter hinterlegt sind, entsteht ein nicht zu vernachlässigendes Sicherheitsrisiko. Um dies zu vermeiden, wird

die unattend.xml nach erfolgreicher Erstellung der Kundenordner sowie der zugehörigen VM mithilfe einer im Skript implementierten Funktion wieder gelöscht.

Für die erfolgreiche Automatisierung war es erforderlich, dass bestimmte XML- und Konfigurationsdateien auf den Zielsystemen verfügbar sind. Um dies zu ermöglichen, musste die Gastdienstschnittstelle innerhalb der VMs aktiviert werden, wodurch sich Dateien direkt vom Hostsystem in die Gastsysteme übertragen lassen. Vor dem eigentlichen Transfer wurde in jeder VM ein Ordner angelegt, in den die relevanten Dateien kopiert werden. Für den Domain Controller waren dies Gruppenrichtlinien-Dateien, während für den Fileserver die Installations-XML der entsprechenden Rolle vorgesehen war.

5.4 Konfiguration der virtuellen Maschinen

Vor der Installation von Rollen ist es notwendig, den VMs statische IP-Adressen zuzuweisen und sowohl dem Fileserver als auch dem Terminalserver den Domain Controller als DNS-Server einzutragen. Darüber hinaus erfolgt eine Anpassung der Computernamen zur eindeutigen Identifikation. Für diesen Zweck wurden spezifische kleine Skripte (ChangeIpRenameTs bzw. ChangeIpRenameDc) entwickelt, die die Konfiguration automatisieren. Die Installation der Fileserver-Rolle erfolgt gemeinsam mit der Konfiguration einer statischen IP-Adresse, da diese Rolle unabhängig vom Domain Controller eingerichtet wird (DeployFileServerRole).

Die Einrichtung des Domain Controllers basiert ebenfalls auf PowerShell. Bei einer manuellen Installation lässt sich vor der Heraufstufung ein Skript generieren, das die durchgeführten Arbeitsschritte abbildet. Dieses Vorgehen bietet wertvolle Einblicke in die notwendigen Befehle, zusätzlich stehen umfassende Informationen in der offiziellen Microsoft-Dokumentation zur Verfügung. Für die automatisierte Konfiguration wurde eine Hashmap erstellt, die alle erforderlichen Parameter wie Domänenname, NetBIOS-Name, DSRM-Passwort sowie Pfade für System- und Logdateien enthält. Anschließend wurde die benötigte Rolle installiert und der Domain Controller mittels *Install−ADDSForest* heraufgestuft. Nach einem Neustart stand damit die Grundkonfiguration zur Verfügung. Vor dem Neustart wurde zudem der Google-DNS-Server (8.8.8.8) in die Liste der Weiterleitungen aufgenommen.

Zum betrachteten Zeitpunkt standen bereits drei VMs zur Verfügung, von denen zwei mit den vorgesehenen Rollen ausgestattet waren und ein funkti-

onsfähiger Domain Controller bereitgestellt war. Der darauffolgende Schritt bestand darin, die verbleibenden Server in die Domäne aufzunehmen, nachdem der Domain Controller vollständig gestartet war. Dies konnte mit einer dedizierten PowerShell-Funktion erreicht werden, die unter Verwendung von *Invoke−Command* den Domänenbeitritt in den VMs remote ausführt.

Nach erfolgreichem Domänenbeitritt der Systeme folgte die Vorbereitung des Fileservers. Hierzu wurde die zusätzliche Festplatte zunächst online geschaltet und mit dem Partitionsstil GPT initialisiert. Anschließend wurde die gesamte Speicherkapazität in einer Partition zusammengefasst, die mit einem Laufwerksbuchstaben (im Skript: D:) und einer eindeutigen Bezeichnung („Daten“) versehen wurde. In diesem Verzeichnis wurden standardisierte Basisordner angelegt, die später als Grundlage für Freigaben dienen. Da Freigaben mit bestimmten Active-Directory-Gruppen verknüpft sind, war zuvor eine grundlegende AD-Struktur zu etablieren.

Die erstellte Active-Directory-Struktur umfasste exemplarische Benutzerkonten (einen Testbenutzer und einen Administrationsaccount), mehrere Standardgruppen (Scan_ LW, Datevuser, Daten_ LW, GF für Geschäftsführung) sowie Organisationseinheiten zur strukturierten Trennung von Benutzern, Gruppen und Computern. Die Benutzer wurden in Form von Hashmaps angelegt, während Gruppen über den Befehl *New−ADGroup* erstellt wurden. Im Anschluss wurden die Benutzer den entsprechenden Gruppen zugeordnet.

Zur Grundstruktur des Active Directory gehören auch Standardrichtlinien, etwa für Netzlaufwerke, Remotedesktop-Einstellungen, Einschränkungen der Eingabeaufforderung und Skriptausführung sowie das Deaktivieren von „New Outlook“. Da viele dieser Gruppenrichtlinien auf Registry-Einträgen basieren, können sie mithilfe von Hashmaps umgesetzt werden. Die benötigten Registry-Keys lassen sich entweder durch das Auslesen bestehender Richtlinien über *Get−GPPrefRegistryValue* oder durch Dokumentationen im Internet identifizieren.

Komplexer gestaltet sich die Abbildung von Netzlaufwerken. Die manuelle Konfiguration eines Netzlaufwerks führt zu einer Vielzahl an Registry-Einträgen. Werden diese als Grundlage für eine neue Gruppenrichtlinie übernommen, schlägt die Umsetzung häufig fehl, sodass die Laufwerke nicht im Explorer angezeigt werden. Dadurch werden sie für Endnutzer unbrauchbar. Um dieses Problem zu umgehen, wurde eine bereits funktionierende Gruppenrichtlinie mit den Netzlaufwerken aus einem bestehenden System exportiert, in die VM des Domain Controllers übertragen, an die SID der neuen Domäne angepasst

und anschließend importiert.

Die importierten Gruppenrichtlinien (GPOs) verhalten sich nach der Anpassung der SIDs wie manuell erstellte Richtlinien. Ein direkter Eingriff in einzelne Registry-Einträge ist damit nicht erforderlich, da die XML-Dateien der GPOs in einer Schleife verarbeitet und die enthaltenen Gruppen angepasst werden können. Mit Abschluss dieser Schritte stand das Grundgerüst des Active Directory bereit, womit lediglich noch wenige Arbeitsschritte bis zur Fertigstellung des Automatisierungsskripts zur Serverstruktur erforderlich waren.

Um den Zugriff auf die Verzeichnisse des Fileservers zu ermöglichen, wurden die Ordner zunächst freigegeben und mit den notwendigen Berechtigungen versehen. Die Freigabe konnte mit dem Befehl *New−SmbShare* umgesetzt werden, wobei mithilfe von Hashmaps und Schleifen Freigabename, Pfad und Berechtigungen automatisiert zugewiesen wurden. Im Anschluss wurden die NTFS-Berechtigungen auf Verzeichnis- und Dateiebene konfiguriert. Hierfür wurden die bestehenden Rechte eines Verzeichnisses zunächst mit *Get−Acl* in einer Variablen gespeichert, anschließend über eine Hashmap neue Einträge definiert (Benutzer bzw. Gruppe, Berechtigungsumfang sowie Anwendungsbereich: Ordner, Unterordner und Dateien). Diese wurden in ein neues ACL-Objekt überführt und mit *Set−Acl* auf das jeweilige Verzeichnis angewendet.

Ein Problem dieser Vorgehensweise besteht darin, dass Rechte jeweils nur für einen Ordner und eine Gruppe gleichzeitig gesetzt werden können. Der Versuch, mehrere Einträge parallel zu übernehmen, führte entweder zu fehlerhaften Berechtigungen oder zu fehlenden Fehlermeldungen, sodass die Rechtevergabe stets einzeln vorgenommen werden musste. Nach der Umsetzung der Freigaben und NTFS-Berechtigungen verblieb als letzter Bestandteil die Einrichtung des Terminalservers.

Die Installation der dazugehörigen Rollen konnte nicht vollständig über PowerShell-Kommandos innerhalb des Gastesystems erfolgen. Stattdessen wurden die Rollen mithilfe von PowerShell Direct über den Hyper-V-Host remote in die VM installiert und anschließend konfiguriert. Damit konnte eine funktionsfähige Terminalserver-Umgebung bereitgestellt werden, wenngleich die Lizenzierungskonfiguration nicht Teil des Skripts war. Auch ohne diese Konfiguration ist eine Anmeldung mittels Remotedesktop für einzelne Benutzer möglich, wodurch Kernfunktionen des Terminalservers zur Verfügung stehen.

Zum Abschluss wurden sämtliche VMs einmalig neu gestartet, um einen einheitlichen Betriebszustand herzustellen und alle Konfigurationen sowie Änderungen, die einen Neustart erforderten, gültig zu machen. Lediglich beim Terminalserver besteht eine geringe Wahrscheinlichkeit, dass der Dienst "Remotedesktopverwaltung"nach dem Neustart nicht ordnungsgemäß ausgeführt wird. Da im Anschluss an die Grundkonfiguration jedoch weitere Installationen und Anpassungen erfolgen, wird dieses Restrisiko als vernachlässigbar eingestuft.

Das Skript verfügt darüber hinaus über ein grafisches Benutzerinterface (GUI), welches die zu Beginn der Einrichtung erforderlichen Eingaben für die Erstellung der virtuellen Maschinen zentral abfragt. Dadurch werden die notwendigen Informationen bereits im Vorfeld gesammelt und automatisch in den weiteren Prozess eingebunden. Dies führt zu einer deutlichen Zeitersparnis im Vergleich zur manuellen Erstellung, da Verzögerungen durch unbeaufsichtigte Eingabefenster, beispielsweise wenn parallel andere Tätigkeiten ausgeführt werden, vermieden werden können.

6 Testumgebungen

Zur Validierung des entwickelten Skripts wurden Testdurchläufe in zwei unterschiedlichen Umgebungen durchgeführt. Dadurch kann die Stabilität und Portabilität der Lösung besser eingeschätzt werden, da sowohl die eingesetzte Hardware als auch die Software variieren.

Hardware- und Softwarekonfiguration

Tabelle 1: Hardware- und Softwarekonfiguration der Testumgebungen

Komponente	**Testumgebung Home**	**Testumgebung Server 1**	**Testumgebung Server 2**
CPU	AMD Ryzen 7 7800X3D, 8 Kerne / 16 Threads, 4,3–4,5 GHz	Intel Xeon E3-1230 v5, 4 Kerne / 8 Threads, 3,7 GHz	2× Intel Xeon E5-2643 v3, 6 Kerne / 12 Threads
RAM	32 GB DDR5-6000	64 GB DDR4-2133	256 GB DDR4-2133
PowerShell-Version	7.5.2	5.1	5.1
Windows-Version	Windows 11 Pro	Windows Server 2025 Standard	Windows Server 2019 Standard

Virtuelle Maschinen

Die virtuellen Maschinen wurden in beiden Testumgebungen identisch konfiguriert:

- **CPU-Kerne:** 2
- **RAM:** 2GB pro VM
- **Zusätzliche VHDX:** 35MB auf dem File Server

Testmethodik und Testergebnisse

Zur Überprüfung des entwickelten Skripts wurden mehrere Testdurchläufe auf den beschriebenen Umgebungen durchgeführt. Ziel war die Validierung der Funktionsfähigkeit, Stabilität und Ausführungsdauer des Automatisierungsprozesses. Der Fokus lag dabei nicht auf einer detaillierten funktionalen Prüfung der konfigurierten Dienste, sondern auf der wiederholbaren und automatisierten Erstellung der virtuellen Maschinen. Trotzdem wurde darauf geachtet, dass die grundlegenden Konfigurationen wie Domänenbeitritt, Netzwerkanpassungen und Freigaben korrekt umgesetzt wurden und funktionsfähig sind.

6.0.1 Testumgebung Zuhause

Tabelle 2: Zeitübersicht der Testdurchläufe – Server 1

Schritt	**Log 1 (hh:mm:ss)**	**Log 2 (hh:mm:ss)**	**Log 3 (hh:mm:ss)**	**Log 4 (hh:mm:ss)**	**Log 5 (hh:mm:ss)**
Skript-Start	0:00:00	0:00:00	0:00:00	0:00:00	0:00:00
Kopieren fertig	0:00:26	0:00:31	0:00:32	0:00:31	0:00:32
VMs erstellt	0:00:30	0:00:36	0:00:36	0:00:34	0:00:36
VMs angepasst	0:00:31	0:00:36	0:00:36	0:00:35	0:00:37
VMs gestartet	0:00:34	0:00:39	0:00:39	0:00:37	0:00:40
Windows initialisierung fertig	0:01:13	0:01:34	0:01:30	0:01:28	0:01:32
Kopieren fertig	0:01:44	0:02:04	0:01:56	0:02:01	0:02:04
Löschen von Dateien fertig	0:01:52	0:02:14	0:02:08	0:02:10	0:02:14
MAC umgestellt	0:02:05	0:02:36	0:02:21	0:02:23	0:02:24
static IP	0:02:32	0:03:03	0:02:46	0:02:49	0:02:50
DC installiert	0:04:21	0:04:52	0:05:08	0:04:48	0:05:16
Domain beigetreten	0:10:01	0:11:32	0:11:48	0:11:28	0:11:56
Ordnerstruktur FS	0:11:56	0:12:57	0:12:43	0:12:21	0:12:52
AD Struktur erstellt	0:12:19	0:13:20	0:13:06	0:12:44	0:13:15
Freigaben Ordner	0:12:25	0:13:24	0:13:13	0:12:51	0:13:24
TS installiert	0:18:13	0:18:14	0:19:09	0:18:32	0:19:04
Skript-Ende	0:18:40	0:18:43	0:19:10	0:18:33	0:19:04
Gesamtzeit	0:18:40	0:18:43	0:19:10	0:18:33	0:19:04

6.0.2 Testumgebung Server 1

Tabelle 3: Zeitübersicht der Testdurchläufe – Server 1

Schritt	**Log 1 (hh:mm:ss)**	**Log 2 (hh:mm:ss)**	**Log 3 (hh:mm:ss)**	**Log 4 (hh:mm:ss)**	**Log 5 (hh:mm:ss)**
Skript-Start	0:00:00	0:00:00	0:00:00	0:00:00	0:00:00
Kopieren fertig	0:06:02	0:06:03	0:04:53	0:04:53	0:04:52
VMs erstellt	0:06:15	0:06:14	0:05:03	0:05:04	0:05:04
VMs angepasst	0:06:15	0:06:14	0:05:04	0:05:04	0:05:04
VMs gestartet	0:06:20	0:06:19	0:05:09	0:05:09	0:05:09
Windows initialisierung fertig	0:10:52	0:12:12	0:09:52	0:11:17	0:10:21
Kopieren fertig	0:12:30	0:13:33	0:11:28	0:12:37	0:12:14
Löschen von Dateien fertig	0:13:00	0:13:51	0:11:45	0:13:58	0:12:34
MAC umgestellt	0:14:34	0:15:31	0:13:23	0:14:06	0:13:39
static IP	0:16:30	0:17:28	0:15:14	0:16:07	0:15:28
DC installiert	0:21:01	0:22:47	0:19:56	0:20:50	0:20:33
Domain beigetreten	0:27:52	0:29:31	0:26:38	0:27:37	0:27:26
Ordnerstruktur FS	0:29:12	0:30:55	0:28:03	0:29:12	0:29:20
AD Struktur erstellt	0:29:53	0:31:41	0:28:42	0:30:10	0:30:06
Freigaben Ordner	0:30:03	0:31:51	0:28:52	0:30:22	0:30:17
TS installiert	0:42:19	0:43:29	0:40:47	0:43:08	0:41:37
Skript-Ende	0:43:11	0:43:29	1:09:41	0:43:08	0:41:37
Gesamtzeit	0:43:11	0:43:29	1:09:41	0:43:08	0:41:37

Ebenfalls wurde die Einrichtung der VMs auf der Testumgebung mit dem Server 1 manuell getestet. Der erste, manuelle, Test wurde von einer Praktikantin mit begleitender Unterstützung durchgeführt. In etwas 2 Stunden war das System aus 3 VMs genauso einsatzfähig wie die Serverstruktur, die durch das Skript automatisiert erstellt wurde. Drei weitere manuelle Test wurden vom Autor dieser Arbeit durchgeführt. Durch die Erfahrungen, die während der Entwicklung des Skripts gesammelt wurden, konnte die Zeit der manuelle Einrichtung merkbar reduziert werden. Anfangs war die manuelle Einrichtung der VMs langsamer und mit 1 Stunde und 33 Minuten deutlisch länger als die automatisierte Variante. Doch mit der wachsenden Routine, durch die gleichen Abläufe, konnte die Zeit im dritten Durchlauf auf 1 Stunde und 8 Minuten reduziert werden.

7 Technische Erkenntnisse der Skripterstellung

Während der Entwicklung und Umsetzung des Automatisierungsskripts für Hyper-V traten eine Vielzahl technischer Besonderheiten und Fallstricke auf, die bei zukünftigen Projekten berücksichtigt werden sollten. Eine grundlegende Voraussetzung für bestimmte Aktionen, wie beispielsweise den Domänenbeitritt, ist die Verwendung eindeutiger SIDs. Dies wurde durch den Einsatz von *sysprep* in Verbindung mit einer funktionierenden Antwortdatei sichergestellt. Dabei zeigte sich, dass die Antwortdatei strikt in der Reihenfolge von oben

nach unten abgearbeitet wird, weshalb der *OOBE*-Abschnitt möglichst früh platziert werden sollte.

Im Bereich der Skripterstellung mit PowerShell war besonders bei der Arbeit mit GUIs und Benutzerinteraktionen Aufmerksamkeit erforderlich. So erwies es sich als sinnvoll, beim Aufbau einer RAM-Auswahl Integer-Werte in Byte-Form anzugeben, da Strings in Arrays nicht zuverlässig verarbeitet wurden. Das Rückgabeverhalten wurde über *return* angepasst, um korrekte Werte zu liefern. Außerdem zeigte sich, dass in PowerShell die Überprüfung auf *NULL* konsistent mit der Schreibweise *NULL −eq \$Variable* erfolgen sollte, um logische Fehler, insbesondere bei Array-Prüfungen,zu vermeiden.

GUI-Fenster verhielten sich in Bezug auf die Anzeige im Vordergrund nicht immer wie erwartet, selbst wenn die Eigenschaft *TopMost* gesetzt war. Dieses Problem wurde durch die Definition eines Mutterfensters und die gezielte Anzeige untergeordneter Fenster mit *.Add_Shown()* gelöst. Passworteingaben ließen sich in der GUI zwar ausblenden, mussten jedoch für die weitere Verarbeitung mittels *ConvertTo−SecureString −PlainText* in ein SecureString-Format konvertiert werden. Beim Auswählen von Verzeichnissen war zu beachten, dass der Pfad über die Eigenschaft *InitialDirectory* und nicht *RootFolder* festgelegt werden muss.

Für die Eingabevalidierung, beispielsweise bei IP-Adressen, bot sich die Nutzung regulärer Ausdrücke wie *"[0−9]+\textbackslash.[0−9]+\textbackslash .[0−9]+\textbackslash.[0−9]+"* an. Variablen, die innerhalb von Remote-Jobs oder Sessions genutzt werden, mussten mit dem Präfix *Using:* übergeben werden – auch dann, wenn sie zuvor global deklariert wurden. Innerhalb von Strings war eine Variablenersetzung nur mit der Schreibweise *\$(Variable)* möglich. Bei Abfragen, die einen String erfordern, erwies sich die Verwendung des Parameters *−ExpandProperty* als notwendig, um Objektrückgaben zu vermeiden.

Das Ausführen von Befehlen mit dem Parameter *−AsJob* startete Prozesse im Hintergrund, was problematisch sein konnte, wenn das Ergebnis sofort benötigt wurde. In solchen Fällen war es erforderlich, den Job aktiv zu überwachen, das Ende der Ausführung abzuwarten und anschließend den Job zu entfernen. Beim Einsatz von *Invoke−Command* konnte entweder direkt mit VM-Namen oder mit zuvor erstellten Sessions gearbeitet werden; letztere mussten nach Abschluss wieder geschlossen werden. Um Anmeldevorgänge zu vermeiden, konnten Anmeldeinformationen als *PSCredential*-Objekte hinterlegt werden. Diese wurden über *New−Object* erstellt, wobei das Passwort

als SecureString abgefragt und zusammen mit dem Benutzernamen in einer Variablen gespeichert wurde.

Vor der Ausführung des Skripts wurde geprüft, ob es in einer administrativen Sitzung lief. Falls nicht, wurde es über *Start−Process* mit dem Verb *RunAs* neu gestartet. Für eine einheitliche Protokollierung wurde eine Log-Funktion erstellt, die Zeitstempel im Format *"[dd/MM/yy HH:mm:ss]"* generierte. Nicht benötigte Ausgaben wurden konsequent mit Out-Null| unterdrückt.

Netzwerkanpassungen innerhalb von Windows-VMs erfolgten mit *New−\ allowbreak Net\allowbreak IPAddress* anstelle von *Set−NetIPAddress*. Um Dateien vom Hyper-V-Host auf eine VM zu übertragen, musste die Gastdienstschnittstelle aktiviert werden, was über *Enable−VMIntegrationService* möglich war. Anschließend konnte der Kopiervorgang mit *Copy−VMFile* durchgeführt werden, wobei Systempfade nur indirekt beschreibbar waren.

Die Installation bestimmter Serverrollen, wie des Dateiservers, war nur über XML-basierte Konfigurationen möglich. Remote Desktop Services (RDS) konnten vom Domänencontroller auf den Terminalserver installiert werden, wobei zusätzliche Konfigurationen – etwa Session Collections, RDS-Lizenzierung und Neustarts des Verwaltungsdienstes – direkt auf dem TS erfolgten.
Weitere Besonderheiten betrafen die Handhabung von Strings, Hash-Tabellen und VM-Eigenschaften: Beim Splitten eines Strings am Punkt musste der Punkt mit *"\textbackslash."* escaped werden. VMs konnten vollständig aus Hash-Tabellen heraus erstellt werden, wobei CPU-Anpassungen erst nach der Erstellung und MAC-Adressänderungen nur nach dem ersten Start möglich waren. Neue virtuelle Festplatten wurden per *Add−VMHardDiskDrive* angebunden, anschließend online geschaltet, benannt, mit einem Laufwerksbuchstaben versehen und formatiert.

Passwörter von Active-Directory-Konten ließen sich nicht ohne Weiteres zurücksetzen, während lokale Passwörter per Remote- oder PowerShell-Direct-Zugriff problemlos geändert werden konnten. Bestimmte Installationsfehlermeldungen bei RDS ließen sich möglicherweise auf fehlende Lizenzserverkonfigurationen zurückführen.

8 Fazit

Das Zield er Arbeit war die Erstellung und Konfiguration von Windows-basierten virtuellen Maschinen in Hyper-V durch den Einsatz von PowerShell zu automatisieren. Ausgangspunkt war die übliche manuelle Vorgehensweise, bei der zahlreiche wiederkehrende Schritte erforderlich sind, um Domänencontroller, Dateiserver und Terminalserver bereitzustellen.

Das entwickelte Powershell-Skript übernimmt die wesentliche Aufgaben der Systemeinrichtung. Dazu zählen die automatisierte Erstellung von VMs auf Basis eines vorbereiteten Windows-Server-Templates, die Vergabe statischer IP-Adressen und Computernamen, die Konfiguration von Active Directory auf einemdem dazu Eingerichteten Domain Controller, die Einrichtung eines Fileserver und die dazugehörigen Freigaben sowie die Zuweisung von NTFS-Berechtigungen. Ergänzend wurde die Konfiguration des Terminalservers einschließlich der benötigten Rollenkomponenten umgesetzt. Durch diese Automatisierung konnte der manuelle Aufwand erheblich reduziert und die Gefahr von Fehlern in der Einrichtung minimiert werden.

Die Tabellen zur Umsetzung verdeutlichen, dass ein hoher Automatisierungsgrad erreicht wurde. Dennoch bleiben einzelne manuelle Nacharbeiten, wie etwa die Aktivierung des Betriebssystems oder die finale Lizenzierung des Terminalservers, notwendig. Dies stellt eine Grenze der aktuellen Lösung dar, die in zukünftigen Weiterentwicklungen durch zusätzliche Skriptmodule oder den Einsatz weiterführender Tools adressiert werden könnte.

Zusammenfassend zeigt die Arbeit, dass der Einsatz von PowerShell ein effizientes Mittel darstellt, um wiederkehrende und fehleranfällige Administrationsaufgaben in Hyper-V-Umgebungen zu automatisieren. Damit leistet sie einen Beitrag zur Standardisierung von Abläufen in der Windows-Server-Administration, insbesondere für kleine und mittlere Unternehmen.

Darüber hinaus ergeben sich aus der Arbeit verschiedene Ansätze zur Weiterentwicklung des Skripts. So wäre es sinnvoll, die Funktionalität dahingehend zu erweitern, dass optional auch nur zwei oder eine virtuelle Maschine erstellt werden kann, um die Lösung besser an kleinere Kundenszenarien anzupassen. Ebenso könnte eine flexible Erweiterung des Speichers einzelner VMs implementiert werden, idealerweise über eine grafische Oberfläche zur vereinfachten Bedienung.

Weitere Verbesserungsmöglichkeiten bestehen insbesondere im Bereich der Terminalserver-Konfiguration, beispielsweise durch die automatische Einbindung des Lizenzservers. Auch die Anpassung des Skripts an Failover-Cluster stellt einen relevanten nächsten Schritt dar, da die aktuelle Entwicklung ausschließlich in einer Standalone-Hyper-V-Umgebung getestet wurde und cluster-spezifische Rollen und Eigenschaften noch nicht berücksichtigt werden.

Ein weiterer Optimierungsbedarf betrifft die derzeit implementierte Wartezeit nach der Installation des Domänencontrollers. Momentan wird hierfür ein statisches Zeitintervall von 6,5 Minuten per sleep-Befehl genutzt. Dieses Vorgehen ist zwar funktional, jedoch unflexibel und wenig professionell. Eine zuverlässigere Methode zur Erkennung des erfolgreichen Systemstarts wäre hier wünschenswert, auch wenn die Beobachtung und zeitliche Abschätzung des Bootvorgangs von Windows-Servern eine gewisse Herausforderung darstellt.

Schließlich könnte die Benutzerverwaltung verbessert werden, indem Benutzerkonten und Gruppen über eine XML-Datei definiert und direkt nach der Erstellung automatisch verarbeitet werden. Auf diese Weise ließe sich der Grad der Standardisierung und Automatisierung nochmals erhöhen.