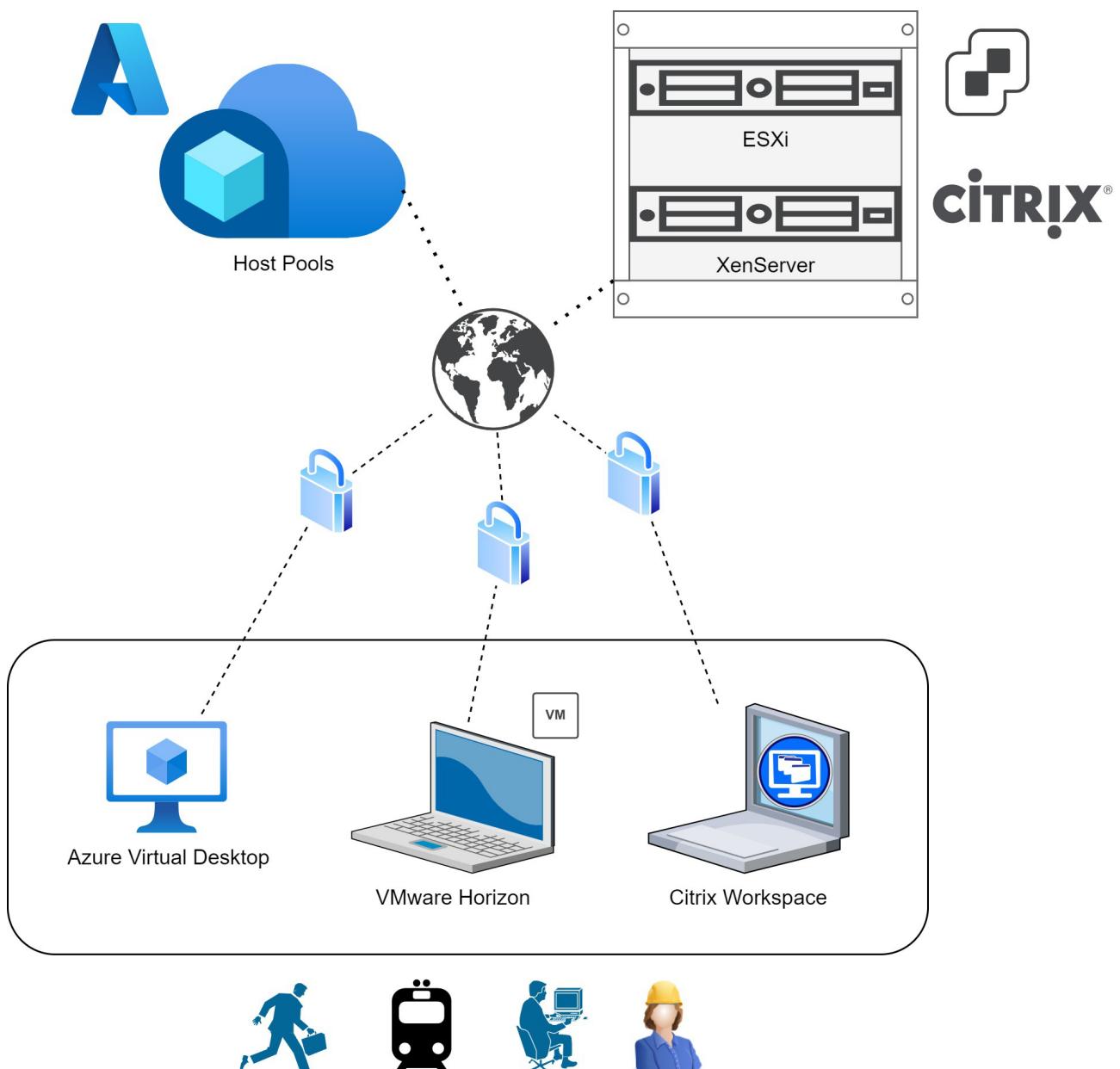


VaaS – VDI as a Service

Shipinyuan Su / Sirak Yosef



1 Management Summary

Die Diplomarbeit "VDI as a Service (VaaS)" beschäftigte sich mit der Entwicklung und Implementierung einer sicheren und effizienten Virtual Desktop Infrastructure (VDI) Lösung, speziell für den Einsatz in sensiblen und geheimen Projekten. Ziel war es, eine flexible, skalierbare und hochsichere Umgebung zu schaffen, die den besonderen Anforderungen solcher Projekte gerecht wurde und gleichzeitig eine hohe Benutzerfreundlichkeit bot.

Dieses Projekt wurde initiiert, weil die aktuelle Arbeitsumgebung in solchen Projekten sehr unflexibel und ineffizient gestaltet war und daher dringend Verbesserungsbedarf bestand. Die bestehenden Systeme waren schwer anpassbar, verwaltbar und mangelten an Benutzerfreundlichkeit.

Zur Verbesserung der Arbeitsumgebung wurde eine VDI-Lösung entwickelt. Dafür wurden drei verschiedene Virtualisierungstechnologien untersucht, die sich grundlegend in ihrer Struktur unterschieden und die gesamte Konzeptionierung erheblich beeinflussten. Jede Technologie bot unterschiedliche Ansätze hinsichtlich Sicherheit, Skalierbarkeit und Benutzerfreundlichkeit, was weitreichende Auswirkungen auf die endgültige Architektur und Implementierung der VDI-Lösung hatte. Die endgültige Wahl fiel auf Citrix, den Marktführer in der Virtualisierung von Desktops und Anwendungen, basierend auf mehreren ausschlaggebenden Faktoren, die durch Analysen ermittelt wurden.

Ein zentrales Ergebnis der Arbeit war die Erstellung einer VDI-Umgebung gemäss dem entwickelten Konzept, die als Proof of Concept diente. Diese Lösung sollte als Vorschlag und Machbarkeitsstudie für die Ablösung der aktuellen Situation in Geheimprojekten dienen. Die funktionsfähige Lösung erfüllte die festgelegten Sicherheits- und Leistungsanforderungen.

Es wurde ausführlich die Wirtschaftlichkeit dieser Lösung geprüft. Analysen zeigten, dass diese Lösung realisierbar ist und einen Gewinn einbringen kann. Eine detaillierte Analyse zeigte, dass die Investition innerhalb von drei Jahren amortisiert werden konnte, wodurch danach Gewinne erzielt würden. Es wurde auch Optimierungspotenzial identifiziert. In Zusammenarbeit mit der Finanzabteilung könnten Strategien entwickelt werden, um die Amortisationszeit auf zwei Jahre zu reduzieren. Dies würde es ermöglichen, bereits nach zwei Jahren Gewinne zu realisieren und ab dem dritten Jahr erneut in neue Hardware zu investieren, um die Infrastruktur weiter zu verbessern.

Für die Implementierung wäre es notwendig gewesen, Pilotnutzer zu definieren, um das Projekt zu testen und zu evaluieren, ob es für den langfristigen Einsatz in sensiblen und geheimen Projekten geeignet ist. Durch ihre Rückmeldungen und Tests hätte sichergestellt werden können, dass die VDI-Umgebung den hohen Sicherheitsstandards entspricht und in der Praxis eine effektive und effiziente Arbeitsumgebung bietet. Mit Demos wurde bewiesen, dass komplexe 3D-Anwendungen stabil und mit hoher Bildfrequenz liefen, sodass diese VDIs mit leistungsstarken Desktop-PCs vergleichbar waren.

Zukünftige Projekte bieten die Möglichkeit, die bestehende VDI-Umgebung weiterzuentwickeln und an spezifische Bedürfnisse anzupassen, um eine noch robustere, sicherere und leistungsfähigere Lösung zu bieten. Diese kontinuierliche Weiterentwicklung könnte den Nutzen und die Akzeptanz der VDI-Umgebung in sensiblen und geheimen Projekten weiter erhöhen.

Inhaltsverzeichnis

1	Management Summary	2
2	Initialisierungsphase.....	6
2.1	Ausgangslage	6
2.2	Projektziele	8
2.3	Projektorganisation.....	9
2.3.1	Rahmenbedingungen.....	9
2.3.2	Projektorganigramm.....	10
2.3.3	Kommunikation.....	11
2.3.4	Datenmanagement.....	11
2.4	Projektplan.....	12
2.5	Lieferergebnisse.....	14
2.6	Ressourcenplan	15
2.6.1	Personalressourcen.....	15
2.6.2	Materialressourcen.....	16
2.7	Risiken.....	17
2.8	Abgrenzungen.....	19
2.9	Studie	20
2.9.1	Ausgangslage.....	20
2.9.2	Standortbestimmung	20
2.9.3	Pflichtenheft.....	23
2.10	Lösungsvarianten	27
2.10.1	Variantenübersicht	27
2.11	Analyse und Bewertung.....	30
2.11.1	SWOT-Analyse	30
2.11.2	Nutzwertanalyse	31
2.12	Variantenentscheid.....	36
2.13	Wirtschaftlichkeit	37
2.13.1	TCO der verschiedenen Varianten.....	37
3	Konzeptphase.....	39
3.1	Lösungsarchitektur	39
3.1.1	Hardwarekomponente	40
3.1.2	Softwaredienste	41
3.1.3	Netzwerk	42
3.1.4	Citrix VDI Service	43
3.2	Technische Umsetzung	44
3.2.1	Implementierungsstrategie	44
3.2.2	Sicherheitsmaßnahmen	46
3.3	Testverfahren	47
3.4	Betrieb der Lösung	48
4	Realisierungsphase.....	49
4.1	Ausführung.....	49
4.2	Prototyp	51
5	Einführungsphase	53
5.1	Einführung des Services	53
5.2	Projektcontrolling / Wirtschaftlichkeit.....	53
6	Schlussbetrachtung.....	55

6.1	Reflexion.....	56
6.2	Dank	56
6.3	Urheberrecht.....	56
7	Authentizität.....	57
8	Anhang.....	58
8.1	Quellenverzeichnis	60
8.2	Abbildungsverzeichnis	61
8.3	Tabellenverzeichnis.....	62

Vorwort

Das Erreichen dieses Meilensteins als Partnerarbeit ist eine aufregende und erfüllende Erfahrung. Es ist ein besonderer Moment, die Ergebnisse unserer harten Arbeit mit Ihnen teilen zu können. Wir sind dankbar, dass uns die Firma Finitia AG die Möglichkeit gegeben hat, uns mit der Entwicklung und Implementierung einer leistungsstarken Virtual Desktop Infrastructure (VDI) zu beschäftigen. Besonders schätzen wir, dass uns als Studenten die Freiheit zur eigenständigen Entscheidungsfindung gegeben wurde.

Während der Arbeit an diesem Projekt gab es sowohl Höhen als auch Tiefen. Doch durch gegenseitige Motivation und Unterstützung konnten wir diese Herausforderungen erfolgreich meistern. Wir haben uns technisch hervorragend ergänzt und konnten in kniffligen Situationen dank der Unterstützung von internen und externen Fachexperten wertvolle Hilfe in Anspruch nehmen.

Diese Zusammenarbeit hat uns nicht nur fachlich weitergebracht, sondern auch gezeigt, wie wichtig Teamarbeit und gegenseitige Unterstützung für den Erfolg eines Projekts sind. Es war eine spannende und herausfordernde Reise, dieses Projekt zu realisieren, und wir sind stolz auf das, was wir erreicht haben. Wir hoffen, dass die Erkenntnisse und Lösungen, die in dieser Arbeit präsentiert werden, einen wertvollen Beitrag zur Weiterentwicklung moderner IT-Infrastrukturen leisten können.

Mit Freude und Stolz präsentieren wir die gewonnenen Erkenntnisse und Ergebnisse.

Einführung

In einer zunehmend digitalisierten Welt gewinnen flexible und sichere Arbeitsmodelle immer mehr an Bedeutung. Die vorliegende Arbeit beleuchtet die Vorteile und Herausforderungen der Implementierung von Virtual Desktop Infrastructure (VDI) as a Service und zeigt, wie diese Technologie die Arbeitsweise moderner Unternehmen verbessern kann. Als angehende diplomierte Informatiker in der Fachrichtung Plattform Engineering haben sie sich das Ziel gesetzt, eine VDI-Umgebung für einen spezifischen Anwendungsfall zu entwickeln. Diese Umgebung soll nicht nur die Flexibilität und Sicherheit erhöhen, sondern auch die Effizienz und Produktivität der Arbeitsprozesse verbessern. Durch die sorgfältige Analyse und Umsetzung dieses Projekts als Proof of Concept hoffen sie, dass diese Lösung die aktuelle Arbeitsweise ablösen kann.

Hinweise

Sofern keine Quellen angegeben sind, stammen die Bilder und Abbildungen aus eigener Erstellung. Quellenangaben werden ansonsten im Quellenverzeichnis und in der Fusszeile angegeben.

Die vollständigen Quellenangaben des Diplomberichtes sind im Anhang A zu finden. Jedes zusätzliche Dokument verfügt über ein eigenes Literaturverzeichnis, in dem die verwendeten Quellen aufgeführt sind.

Zur besseren Lesbarkeit wird in dieser Diplomarbeit das generische Maskulinum verwendet. Die in dieser Arbeit verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter.¹

¹ <https://www.scribbr.ch/hausarbeit-ch/gender-hinweis-hausarbeit-vorlage/>

2 Initialisierungsphase

Die Initialisierungsphase bildet den Grundstein für das gesamte Projekt und umfasst alle wesentlichen Schritte und Informationen, die für den Start erforderlich sind. Eine vollständige Sammlung der Dokumente des Projektinitialisierungsauftrages, einschliesslich der Diplomeingabe, ist im Anhang B zu finden. Im Diplombericht werden lediglich die wichtigsten Punkte hervorgehoben und bei Bedarf auf die detaillierten Informationen im Anhang verwiesen.

2.1 Ausgangslage

In einer Zeit, in der die Arbeitswelt einem rapiden Wandel unterzogen ist, ist es wichtig, diesem Wandel mithalten zu können, um konkurrenzfähig zu bleiben. Dies gilt besonders für ein Unternehmen, das eine breite Kundenbasis von Architekten und Ingenieuren in verschiedenen Teilen der Schweiz bedient. Die Herausforderungen und Veränderungen können wie folgt zusammengefasst werden:

Zunahme von Homeoffice und flexibler Arbeit: Durch die Covid-Pandemie hat sich der Trend zu Homeoffice und flexibler Arbeitsgestaltung verstärkt. An diese neue Arbeitsweise haben sich die Kunden zunehmend gewöhnt, und flexible Arbeitsmodelle werden nun erwartet.

Standortunabhängigkeit: Die geographische Verteilung der Kunden erfordert eine Lösung, die es ermöglicht, effizient und effektiv von verschiedenen Orten aus zu arbeiten. Dies gilt sowohl für die internen Teams als auch für die Interaktion mit den Kunden.

Erhaltung der Arbeitsperformance: Trotz der Notwendigkeit flexibler und ortsunabhängiger Arbeitsmodelle ist es entscheidend, dass die Arbeitseffizienz und -qualität nicht leidet. Zugang zu leistungsfähigen Werkzeugen und Ressourcen wird benötigt, unabhängig vom physischen Standort.

Diese Ausgangslage bildet die Grundlage für die aktuelle Diplomarbeit, bei der es darum geht, die Arbeitsweise des Unternehmens und der Kunden in dieser neuen, flexiblen Arbeitswelt zu unterstützen. Um diese Bedürfnisse zu befriedigen, wurde die Nutzung von Virtual Desktop Infrastructure (VDI) als zentrales Element der IT-Strategie integriert. Mit der Diplomarbeit soll ein spezifischer Anwendungsfall untersucht und gelöst werden. Es bezieht sich auf die Handhabung von sensiblen Projekten, die unter Geheimhaltung stehen. Eine Lösung soll entwickelt werden, die es ermöglicht, die Vorteile von VDI unter Berücksichtigung der Sicherheitsanforderungen zu nutzen. Dabei wird darauf konzentriert, wie VDIs so konfiguriert werden können, dass sie eine sichere, isolierte Arbeitsumgebung für Projekte unter Geheimhaltung bieten, ohne dass auf die Vorteile des flexiblen und standortunabhängigen Arbeitens verzichtet werden muss.

Ein aktuelles Beispiel ist ein Projekt in Lugano, welches unter Geheimhaltung steht. Die Mitarbeiter arbeiten an einem temporären Arbeitsplatz in einem Lager mit einem Notebook, welches nicht mit dem Internet verbunden ist. Bearbeitete Dateien werden auf einen lokalen Network Attached Storage (NAS) gespeichert. Diese Arbeitsweise ist nicht mehr zeitgemäss, um die aktuellen Anforderungen und Bedürfnisse gerecht zu werden.

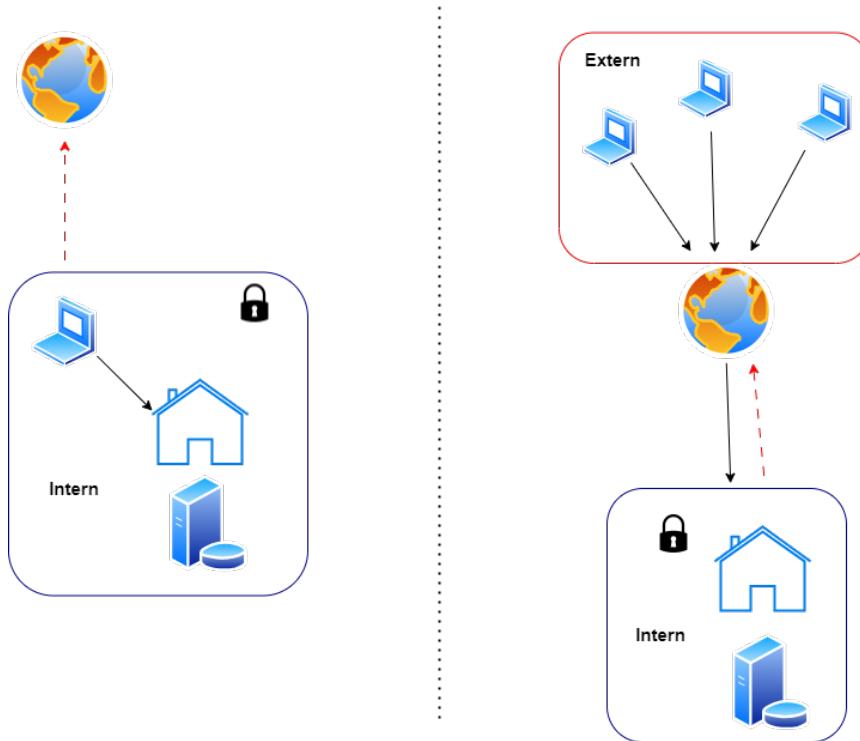


Abbildung 1: Ausgangslage IST/SOLL

Argumente, warum diese Arbeitsweise nicht mehr zeitgemäß ist:

Technologische Entwicklung: die rasche Entwicklung von Cloud-Technologien und virtuellen Arbeitsumgebungen hat effizientere und sicherere Arbeitsmethoden ermöglicht.

Flexibilität und Effizienz: Moderne Arbeitsweisen ermöglichen den Zugriff auf Daten von verschiedenen Standorten und Geräten aus, was die Flexibilität und Effizienz erhöht.

2.2 Projektziele

Folgende Projektziele müssen erreicht werden:

Nr.	Kategorie	Beschreibung	Messgrösse	Priorität*
1	Lieferobjekt	Implementierung einer VDI (Virtual Desktop Infrastructure) -Lösung als PoC, um flexibles Arbeiten zu ermöglichen	Externes verbinden auf die VDI ist möglich	M
2	Betriebliches Ziel	Gewährleistung der kontinuierlichen Verfügbarkeit der VDI-Lösung, durch strategische Lösungen wie Instant Clones oder Redundanz	Uptime der VDI-Lösung in Prozent in Vergleich zur üblichen Lösung	1
3	Technisches Ziel	Implementierung einer VDI-Umgebung, die plattformübergreifend kompatibel ist und die Nutzung auf verschiedenen Geräten, einschliesslich auch Smartphones und Tablets, ermöglicht	Prüfung des Abnahmeprotokolls	1
4	Technisches Ziel	Durch den Einsatz von VDI soll ermöglicht werden, dass auch auf weniger leistungsfähigen Geräten mit hoher Rechenleistung gearbeitet werden kann. Mit der Voraussetzung einer stabilen Internetverbindung.	Zugriffszeiten auf CAD-Programmen: Zeitmessen vom aufstarten von Programmen und öffnen von Dateien sowie das Bearbeiten von Elementen Nutzererfahrung und Reaktionszeit: Feedback von Testusern	1
5	Leistungsziel	Effiziente und Qualitative Leistung von überall	Kein Defizit der Arbeitseffizienz und -qualität, solange eine stabile Internetverbindung vorhanden ist, im Vergleich zu einem PC	1
6	Betriebliches Ziel	Implementierung einer Lösung, die während der Einführungsphase minimale Auswirkungen auf den IT-Betrieb hat	Anzahl Ausfällen und Wartungsarbeiten, die passieren oder gemacht werden müssen während der Implementierung	2
7	Betriebliches Ziel	Reduzierung der Dauer und Erhöhung der Effizienz von Wartungsarbeiten und Änderungsprozesse im IT-Betrieb	Reduzierung der Anzahl Stunden die benötigt werden für einen Change. Analyse der Wiederherstellungszeit des Service	2
8	Technisches Ziel	Projektdaten sind für aussenstehende nicht erreichbar	Daten können nur von bestimmten Personen zugegriffen werden. Es werden mehr als zwei verschiedene Sicherheitsstandards verwendet	M
Priorität: M = Muss, 1 = hoch, 2 = mittel, 3 = tief				

Tabelle 1: Initialisierung - Projektziele

Folgende Ziele sind die Vorgaben für die Phase Initialisierung:

Nr.	Kategorie	Beschreibung	Messgrösse	Priorität*
1	Technisches Ziel	Auswahl und Bewertung geeigneter VDI-Anbieter	Erstellung einer Evaluation der verschiedenen Anbieter	1
2	Technisches Ziel	Definition der technischen Anforderungen für die VDI-Lösung	Fertiggestelltes Anforderungsdokument	1
3	Lieferobjekt	Entwicklung eines zeitlich passenden Projektplans	Fertigstellung und Genehmigung des Projektplans	M
4	Lieferobjekt	Sicherstellung der Finanzierung und Ressourcen für das Projekt	Genehmigung des Projekt-budgets	M
Priorität: M = Muss / 1 = hoch, 2 = mittel, 3 = tief				

Tabelle 2: Ziele der Initialisierung

2.3 Projektorganisation

Dieser Abschnitt bietet einen Überblick über die Struktur und Organisation des Projekts. Es werden die verschiedenen Rollen und Zuständigkeiten der Projektteilnehmer beschrieben, die Kommunikationswege innerhalb des Projekts erläutert und die Verfahren zum Umgang mit Projektänderungen vorgestellt. Darüber hinaus werden die Rahmenbedingungen aufgeführt, die für die praktische Diplomarbeit gelten.

2.3.1 Rahmenbedingungen

In der Diplomarbeit wurden folgende Rahmenbedingungen definiert.

- Anwendung von HERMES Projektmethodik
- Verantwortlichkeiten, Rollen und Kommunikationskanäle definieren
- Definition des Projekts mit Zielen, Umfang und Vorgehen
- Erstellung eines detaillierten Projektplans, welche alle Aktivitäten und Termine aufzeigt
- Projekt wird gemäss den Vorgaben zur Diplomarbeit von der Telematik Schule Bern (TSBE) durchgeführt
- Änderungen im Projekt werden dem Auftraggeber und den Experten kommuniziert

Vorbehalte/Rahmenbedingungen von Prüfungskommission 18.01.2024:

- Überarbeitung der Projektziele, um die Nutzung des Services besser und messbar aufzuzeigen
- In der Studie muss ein Vergleich einer eigenen entwickelten VDI-Lösung vs. Dem MS Azure VDI Service enthalten
- Der Betrieb der Lösung muss definiert und im PoC umgesetzt werden
- Es muss ein Marketing Factsheet inclusive Service SLA und Berechnung der Abopreise erstellt werden
- Es muss aufgezeigt werden wie viele Produkte/Services verkauft werden müssen, um den Break-Even für die Amortisation der Produktentwicklung zu haben (ROI)

2.3.2 Projektorganigramm

Das folgende Organigramm stellt die Organisationsstruktur der Diplomarbeit dar. Es zeigt sowohl die internen als auch die externen Experten, die das gesamte Projekt betreuen und bewerten. Ebenfalls abgebildet ist der Auftraggeber Micha Bucher, der sämtliche Hardware-Ressourcen zur Verfügung stellt und grösstenteils als Schnittstelle zum Kunden dient. Die Studierenden führen das Projekt aus und fungieren auch als Projektleiter.

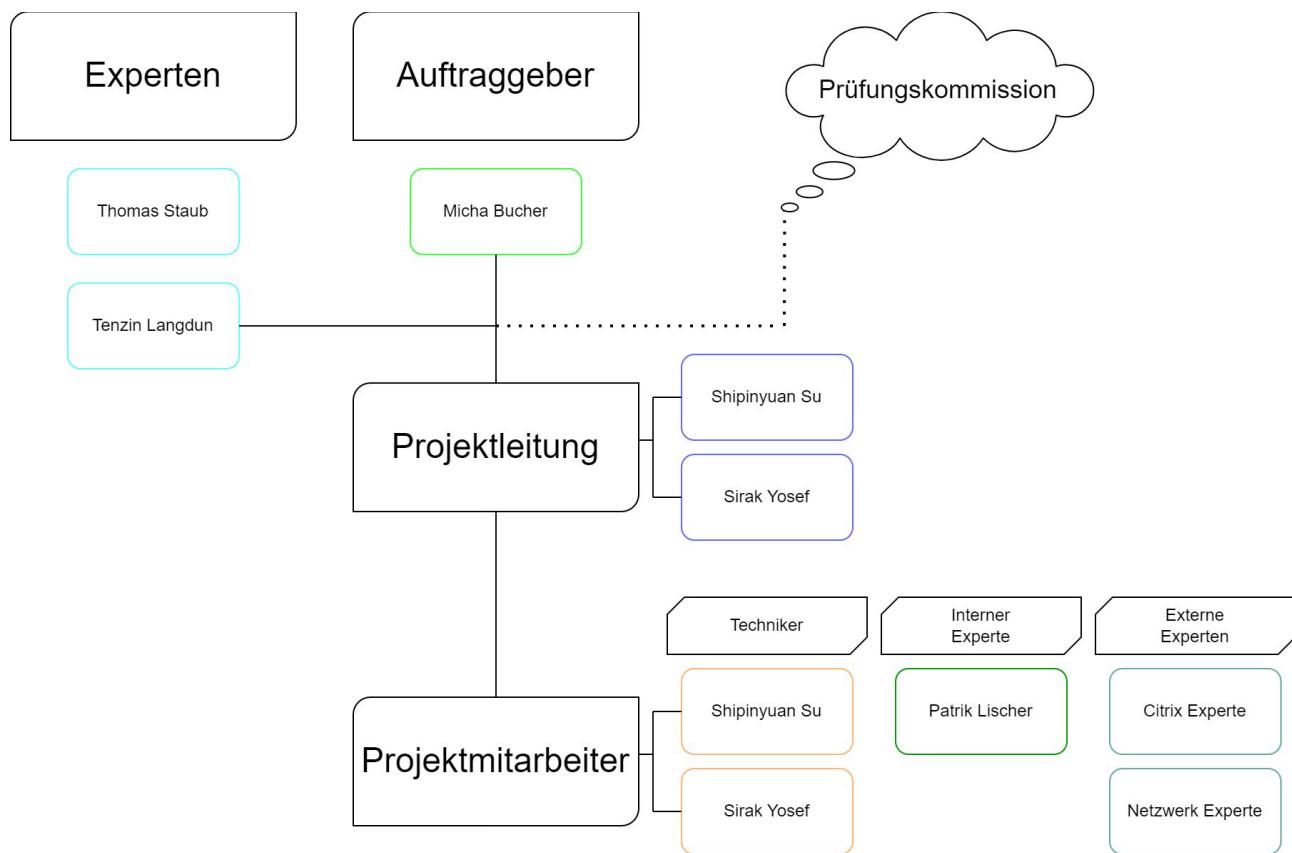


Abbildung 2: Projektorganigramm

2.3.3 Kommunikation

Um eine effektive Kommunikation mit den Experten und dem Auftraggeber zu gewährleisten, wurden spezifische Kommunikationskanäle festgelegt, die in der nachfolgenden Tabelle aufgeführt sind.

Adressat der Information	Verantwortlich für die Kommunikation	Inhalt	Ziel	Mittel / Medium	Termin
Interner Expert Thomas Staub	Projektmitarbeiter	Monatlicher Statusbericht	Fortschritt des Projekts an den Experten kommunizieren mit Aussage zu Terminen, Kosten und Änderungen	Status Report	Alle zwei Wochen
Externer Expert Tenzin Langdun	Projektmitarbeiter	Monatlicher Statusbericht	Fortschritt des Projekts an den Experten kommunizieren mit Aussage zu Terminen, Kosten und Änderungen	Status Report	Alle zwei Wochen
Auftraggeber Micha Bucher	Projektmitarbeiter	Ziel und Planung der Projektinitialisierung	Die Abteilung kennt das Vorgehen und die Termine	Meeting	Wöchentlich

Tabelle 3: Kommunikation

Alle Projektänderungen, wie beispielsweise Zieländerungen, werden gemäss den festgelegten Kommunikationswegen zu den definierten Terminen mitgeteilt.

2.3.4 Datenmanagement

Da die Diplomarbeit von zwei Studierenden gemeinsam verfasst wird, ist es von zentraler Bedeutung, dass die Daten so verfügbar sind, dass beide darauf zugreifen und gemeinsam daran arbeiten können. Die Entscheidung fiel dabei auf OneDrive, da dieses Tool bereits in mehreren Projekten erfolgreich genutzt wurde.

Ein Ordner wurde von einem der Studierenden, Sirak, auf OneDrive freigegeben. Innerhalb dieses Ordners wurde eine Struktur erstellt, die sich nach den verschiedenen Phasen der Diplomarbeit richtet. Diese Struktur ermöglicht eine übersichtliche Organisation und Dokumentation der Fortschritte.



Abbildung 3: Datenmanagement - Struktur

	Diplomarbeit		04.03.2024 08:34
	Diplomarbeit_20240325		25.03.2024 10:55
	Diplomarbeit_20240415		22.04.2024 12:20
	Diplomarbeit_20240513		13.05.2024 10:02
	Diplomarbeit_20240519		19.05.2024 16:09

Abbildung 4: Datenmanagement – Backup

Ein weiterer Aspekt des Datenmanagements besteht darin, dass der zweite Studierende, Shinyuan, regelmässig ein Update des gesamten Ordners in seinem eigenen OneDrive erstellt. Dies dient nicht nur als Backup, sondern stellt auch sicher, dass jederzeit auf die aktuelle Version der Arbeit zugegriffen werden kann, selbst bei unerwarteten Problemen.

Durch diese Massnahmen wird eine effiziente und koordinierte Zusammenarbeit gewährleistet, bei der alle Daten stets aktuell und zugänglich bleiben.

2.4 Projektplan

Im Folgenden ist eine Übersicht der Diplomarbeit sowie der wichtigsten Arbeitspakete dargestellt. Die Diplomarbeit wird mithilfe der Projektmethode Hermes 5.1 durchgeführt. Rote Punkte markieren die Meilensteine, darunter ein Meilenstein für das Kickoff-Meeting, ein weiterer für das Zwischenmeeting nach der Initialisierungsphase und schliesslich ein Meilenstein für das Abschlussmeeting. Ziel ist es, die Diplomarbeit zwei Wochen vor der Deadline fertigzustellen, um einen Zeitpuffer von zwei Wochen zu haben.

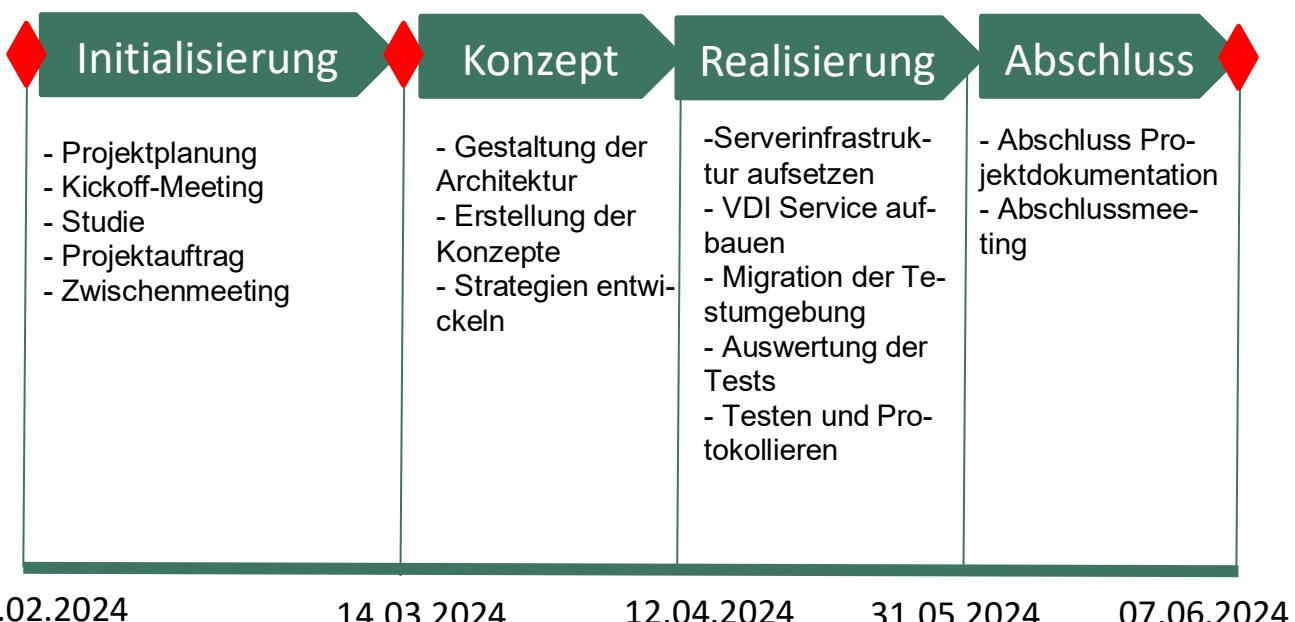


Abbildung 5: Projektübersicht

In dieser Diplomarbeit verlief nicht alles wie ursprünglich geplant. Es kam zu Zeitverschiebungen sowie zu unvorhergesehenen Ereignissen, die den geplanten Ablauf beeinträchtigten. In diesem Abschnitt soll das aktuelle (IST) und das ursprünglich geplante (SOLL) Projektverlauf veranschaulicht werden.

Der komplette Terminplan mit den einzelnen Arbeitspaketen ist im Anhang D aufgeführt. Hier werden die groben Zeitverschiebungen in Wochen dargestellt, einschliesslich der betroffenen Tätigkeiten und der Gründe für die Verzögerungen. Diese Darstellung soll ein klares Bild von den Herausforderungen und Anpassungen vermitteln, die im Laufe des Projekts notwendig wurden.

Phase	Tätigkeit	SOLL Abschluss	IST Abschluss	Bemerkung
Initialisierung	Kickoff-Meeting	21.02.2024	21.02.2024	
	Studie	KW 9	KW 11	Die Studie wurde stark unterschätzt und hat viel mehr Zeit in Anspruch genommen als erwartet.
	Zwischenmeeting	12.03.2024	26.03.2024	Durch die Verzögerung der Studie und der Terminvereinbarung fand das Zwischenmeeting erst zwei Wochen später statt.
Konzept	Detailkonzept	KW 13	KW 16	Durch verschiedene Abhängigkeiten zog sich das Detailkonzept über mehrere Konzepte und konnte erst drei Wochen später abgeschlossen werden.
Realisierung	VDI-Services Aufbauen	KW 19	KW 22	Aufgrund der Unsicherheiten in diesem Bereich war es schwer abzuschätzen, wie lange dieser Prozess dauern würde. Letztendlich konnte hier jedoch Zeit gewonnen werden, trotz der Verzögerung des Abschlusses.
Einführung				Keine Termine
Abschluss	Abschlussmeeting	04.06.2024	04.06.2024	

Tabelle 4: IST / SOLL Verschiebungen

2.5 Lieferergebnisse

In dieser Diplomarbeit werden in den unterschiedlichen Projektphasen verschiedene Lieferergebnisse erstellt. In diesem Abschnitt werden diese Lieferergebnisse aufgelistet und beschrieben.

Initialisierungsphase:

- **Projektplan:** Der Projektplan dient als umfassender Leitfaden für alle Projektaktivitäten und definiert die Meilensteine, Zeitpläne und Ressourcen, die für den erfolgreichen Abschluss des Projekts erforderlich sind.
- **Projektinitialisierungsauftrag:** Der Projektinitialisierungsauftrag stellt die formale Genehmigung dar, das Projekt zu starten, und legt die grundlegenden Ziele, den Umfang und die Projektorganisation fest.
- **Studie:** Die Studie analysiert die relevanten Daten und Informationen, um fundierte Entscheidungen zu treffen und die Grundlagen für die Projektdurchführung zu schaffen.
- **Projektauftrag:** Der Projektauftrag enthält die detaillierte Beschreibung des Projekts, einschließlich der Ziele, des Umfangs, der Zeitpläne und der Verantwortlichkeiten, und dient als verbindliche Vereinbarung zwischen den Projektbeteiligten.

Konzeptphase:

- **Detailkonzept:** Erarbeitung umfassender technischer Spezifikationen und Designprinzipien für die Citrix VDI-Lösung, inklusive einer klaren Definition der technischen Anforderungen und architektonischen Struktur. Jedes Element des Detailkonzepts sollte mit Erfolgskriterien versehen werden, um die Übereinstimmung mit den Projektzielen messbar zu machen.
- **Testkonzept:** Ausarbeitung einer detaillierten Teststrategie, die spezifische Testfälle, Erfolgskriterien für jeden Testfall und die Methodik zu Bewertung der Testergebnisse umfasst.
- **Migrationskonzept:** Detaillierte Planung des Übergangs von der aktuellen Infrastruktur zur neuen VDI-Umgebung, mit klar definierten Schritten und messbaren Erfolgskriterien für jeden wichtigen Schritt der Phase Migration.
- **Betriebskonzept:** Definition der Betriebsprozesse und -richtlinien mit klaren Leistungsindikatoren (KPIs), die den Erfolg des laufenden Betriebs messbar machen.

Realisierungs- und Einführungsphase

- **Arbeitsprotokoll:** Dokumentation des Projektfortschritts, einschließlich Zeitstempel und Verantwortlichkeiten für jede durchgeführte Aktivität, um die Nachvollziehbarkeit zu gewährleisten.
- **Testbericht:** Darstellung der Testergebnisse mit einer klaren Zuordnung zu den im Testkonzept definierten Testfällen und Erfolgskriterien.
- **Auswertung des Nutzerfeedbacks:** Systematische Zusammenfassung des Feedbacks von Pilotbenutzern mit Nutzerzufriedenheit und Verbesserungsvorschlägen, basierend auf vordefinierte Bewertungskriterien.
- **Schulungsunterlagen/Anleitung:** Entwicklung von Schulungsmaterialien mit klar definierten Lernzielen, die den Benutzern nicht nur die Nutzung, sondern auch das Verständnis der VDI-Lösung erleichtern, inklusive Bewertungsmethoden zur Überprüfung des Lernerfolgs.
- **Endabnahmebericht:** Erstellung eines formalen Dokuments zur offiziellen Projektübergabe, inklusive einer detaillierten Überprüfung, ob und wie die definierten Projektziele erreicht wurden.

Abschluss der Diplomarbeit

- **Kostenberechnung:** Aufstellung aller Projektkosten, mit einem Vergleich der geplanten zu den tatsächlich entstandenen Kosten.
- **Abschlussbericht:** Vollständige Dokumentation der Diplomarbeit und Abgabe
Präsentation: Erstellung einer abschliessenden Präsentation, die die Knergebnisse der Diplomarbeit zusammenfasst.

2.6 Ressourcenplan

Dieser Abschnitt widmet sich der detaillierten Analyse der benötigten Mittel und der verfügbaren Ressourcen. Es wird erörtert, welche Infrastruktur und Mittel für die Durchführung des Projekts erforderlich sind, sowie der geschätzte Aufwand und die damit verbundenen internen und externen Kosten.

2.6.1 Personalressourcen

Bei der Schätzung der Personalbedarfs wurden 250 Stunden pro Studenten einberechnet, da das Projekt sehr umfangreich ist. Aufgrund des grossen Arbeitsaufwands wurde die volle Zeit veranschlagt, um sicherzustellen, dass alle notwendigen Aufgaben und potenziellen Herausforderungen bewältigt werden können.

Personalaufwand

Phase	Start	Ende	Ressourcen SOLL			
			Shipinyuan Su	Sirak Yosef	Thomas Staub	Tenzin Langdun
Initialisierung	11.12.2023	14.03.2024	51,5h	51,5h	2h	2h
Konzept	18.03.2024	12.04.2024	44h	44h	0h	0h
Realisierung	15.04.2024	24.05.2024	84h	84h	0h	0h
Einführung	27.05.2024	07.06.2024	8h	8h	0h	0h
Abschluss	11.12.2023	07.06.2024	62h	62h	4h	4h
Total			249.5h	249.5h	6h	6h
Kosten			8'732,50 CHF	8'732,50 CHF		

Tabelle 5: Personalaufwand

2.6.2 Materialressourcen

Es wurden keine neuen Hardwarekäufe getätigt, da die vorhandene Hardware, wie Server und Netzwerkinfrastruktur, genutzt werden konnte. Anbei finden Sie eine Auflistung der verwendeten Hardware. Die detaillierte Beschreibung der aufgelisteten Komponenten ist im Detailkonzept im Anhang E1 zu finden oder in der Studie im Kapitel Wirtschaftlichkeit im Anhang B2 genauer beschrieben.

Materialkosten

Hardware-Komponente	Beschreibung	Kosten (CHF)
Server VDI	Von SuperMicro zusammengestellt	
Gehäuse	SYS-220U-MTNR	
CPUs	2x Intel Xeon Gold 5317 CPU at 3.00 GHz / 12 Cores pro CPU	
RAM	1 TB	
GPUs	2x NVIDIA A16	
SSDs	2x 2 TB SSD	
RAID-Controller	1x	
Netzwerkkarte 10Gbps	1x	
Gesamt Hardware-Kosten		~20'000

Tabelle 6: Materialkosten VDI-Server

Hardware-Komponente	Beschreibung	Kosten (CHF)
Server MGMT	Hardware von SuperMicro, viel selbst umgebaut	
Gehäuse		2'800
CPUs	2x Intel Xeon Silver 2.4GHz 10 Cores	1'000
RAM	768GB	1'800
GPUs	NVIDIA A16	3'200
SSDs	2x 2TB	360
RAID-Controller	1x	550
Netzwerkkarte 10Gbps	1x	350
Gesamt Hardware-Kosten		~9'160

Tabelle 7: Materialkosten MGMT-Server

Hardware-Komponente	Beschreibung	Kosten (CHF)
Synology Nas FS6400	Eine modifizierte Version mit aufgerüsteter Hardware	~15'000
RAM	128 GB	
CPUs	Intel Xeon Silver 4110 2.1GHz 16 Cores	
SSDs	24x	~14'000
Gesamt Hardware-Kosten		~29'000

Tabelle 8: Materialkosten Hauptspeicher

Während der Konzeptionierung wurde zusätzlich ein Desktop-Server integriert, der ursprünglich nicht in die Berechnung aufgenommen wurde, da dieser spontan hinzugefügt wurde. Dieser Server wurde als Testserver verwendet und konnte ohne grosse Kosten als redundanter Server für einige Dienste eingesetzt werden. Im Detailkonzept ist dieser Server mit allen relevanten Details aufgeführt.

Hardware-Komponente	Beschreibung	Kosten (CHF)
Testnotebooks	Ein Lenovo Thinkpad Notebook, welches für die Verbindung und Tests der VDI verwendet wird.	~1'000
RAM	16 GB	
CPUs	Intel Core I7 -10510U, 1.8GHz	
SSDs	500GB	~1'000

Tabelle 9: Materialkosten Testnotebooks

2.7 Risiken

Die nachfolgende Tabelle bietet eine Risikoanalyse potenzieller Risiken, die während der Initialisierungsphase auftreten könnten. Sie beinhaltet eine Einschätzung der Eintrittswahrscheinlichkeit und des Auswirkungsgrads jedes identifizierten Risikos. Dadurch werden präventive Massnahmen festgelegt, um mögliche Hindernisse frühzeitig zu erkennen und proaktiv zu handeln.

Nr.	Risikobeschreibung	EW	AG	RZ	Massnahmen	Verantw.	Termin
1.	Technologische Änderungen	1	2	2	Beobachtung von Markttrends	Projektmitarbeiter	Kontinuierlich während des Projekts
2.	Unzureichende Budgetierung für die vollständige Implementierung der VDI-Lösung	1	3	3	Sicherstellen eines detaillierten und realistischen Kostenvoranschlags und -kontrolle	Projektmitarbeiter	Vor Abschluss der Initialisierungsphase
3	Unterschätzung der Projektressourcen	2	2	4	Detaillierte Ressourcenplanung und regelmässiges Monitoring	Projektmitarbeiter	Vor Abschluss der Initialisierungsphase

Nr.	Risikobeschreibung	EW	AG	RZ	Massnahmen	Verantw.	Termin
					des Ressourcenbedarfs		

EW=Eintretenswahrscheinlichkeit: 1 Niedrig / 2 Mittel / 3 Hoch;
AG=Auswirkungsgrad: 1 Gering / 2 Mittel / 3 Gross;
RZ=Risikozahl: RZ = EW x AG

Tabelle 10: Risikobewertung Initialisierung

Die Risiko Analyse wurde auch für die Phase Migration durchgeführt. Es wurden vier primäre Risiken, definiert als R1 bis R4 und innerhalb der folgenden Risikomatrix dargestellt. Diese Matrix ordnet die Risiken in drei Kategorien ein. Grün symbolisiert ein niedriges Risiko, Gelb ein mittleres Risiko und Rot ein hohes Risiko.

Die beiden grössten Risiken sind R1 und R4, mit Risikozahlen von 4 und 6. R1 betrifft den VDI-Server. Dieses Risiko ist bei der Realisierung eingetreten, weshalb die Umsetzung der VDIs temporär auf dem MGMT-Server aufgesetzt werden musste. R4 war ebenfalls ein Risiko, das die Studenten ständig verfolgte, da eine Verschiebung zu mehreren Zeitverlusten führen konnte. Dies führte dazu, dass die Studenten mehr Freizeit investieren mussten, um dieses Projekt fertigzustellen.

Nr.1	Risiko	Eintrittswahrscheinlichkeit	Auswirkungsgrad	Risikozahl
R1	VDI-Server wird über den ganzen Zeitraum produktiv gebraucht	2	2	4
R2	Defekte Komponente	1	3	3
R3	Personalausfall	2	1	2
R4	Zeitverlust	2	3	6

Tabelle 11: Risikobewertung Migration

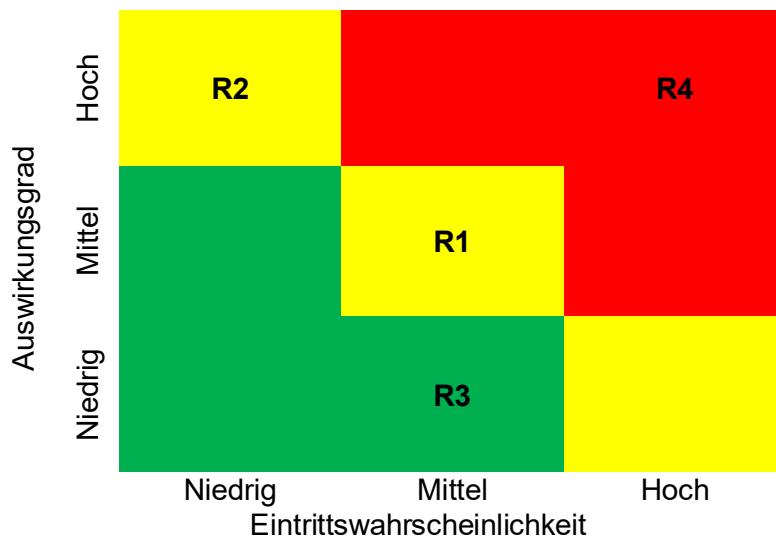


Tabelle 12: Risikomatrix Migration

2.8 Abgrenzungen

Im Rahmen dieser Arbeit liegt der Schwerpunkt auf den Themen und Bereichen, die innerhalb der Box der folgenden Grafik dargestellt sind. Diese Elemente, zu denen die Netzwerkarchitektur, Hardware-Installation, Benutzeranleitungen und VDI-Systeme zählen, definieren den Kern des Projekts. Besondere Bedeutung wird auf die Verfügbarkeit, Sicherheit und Skalierbarkeit des Systems gelegt. Die Themen ausserhalb der Box, obwohl relevant, werden nicht behandelt, um den Fokus und die Grenzen des Projekts klar zu bewahren.

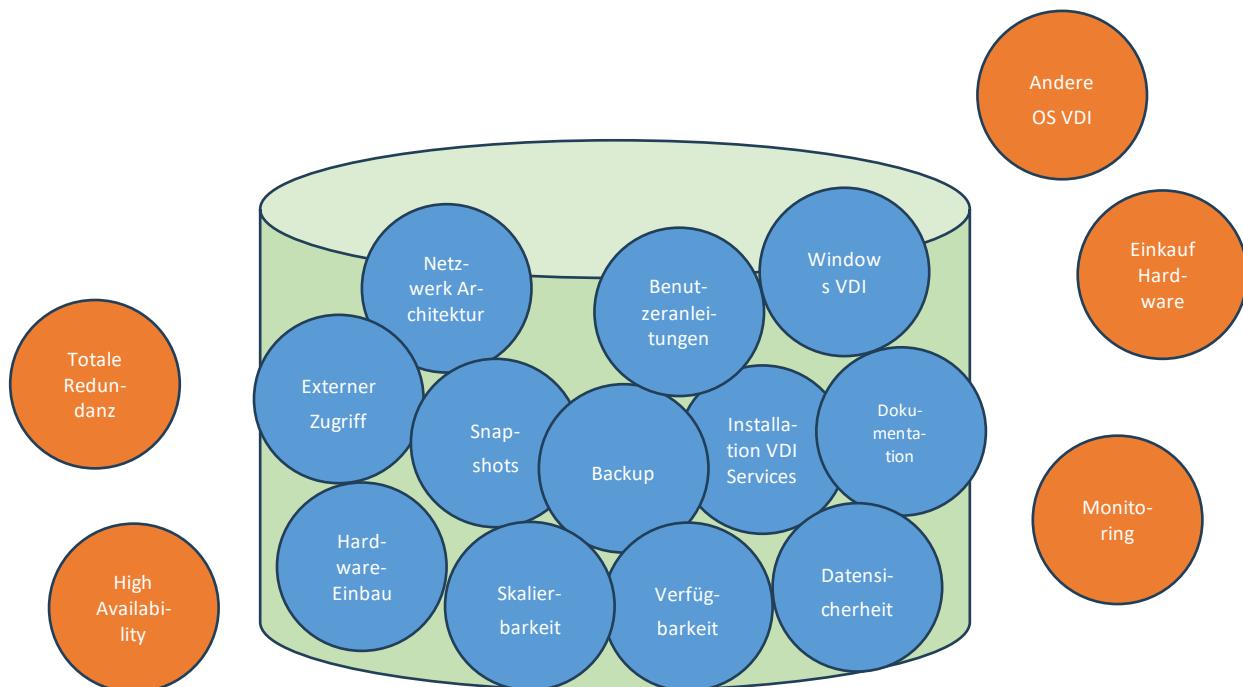


Abbildung 6: Projektabgrenzung

2.9 Studie

In diesem Kapitel werden die wesentlichen Grundsatzentscheidungen der Studie vorgestellt, ohne dabei ins Detail zu gehen. Die vollständige Studie ist im Anhang B2 zu finden. Zunächst wird die aktuelle Situation erfasst und verschiedene Lösungsansätze erarbeitet, gefolgt von der Erstellung eines Katalogs der funktionalen und nicht-funktionalen Anforderungen. Die Lösungsvarianten werden analysiert und evaluiert, um die geeignete Option zu identifizieren, die anschliessend zur Umsetzung des Konzepts ausgewählt wird. Abschliessend wird die Wirtschaftlichkeit der gewählten Variante über den gesamten Lebenszyklus hinweg analysiert, wobei der Total Cost of Ownership (TCO) berücksichtigt wird.

2.9.1 Ausgangslage

Um das Bedürfnis nach flexiblem Arbeiten zu erfüllen, muss eine sichere, effiziente und skalierbare Lösung bereitgestellt werden, die dies nicht nur ermöglicht, sondern auch fördert. Die Studie zielt darauf ab, einen spezifischen Use Case detailliert zu analysieren, die derzeitige Arbeitssituation zu bewerten und die funktionalen sowie nicht-funktionalen Anforderungen der Anwender zu erfassen. Die aktuelle, veraltete und ineffiziente Situation soll durch eine zuverlässige und zukunftssichere Lösung ersetzt werden, die es ermöglicht, von überall aus an Projekten zu arbeiten, ohne die Sicherheitsstandards wie Mehrfaktorauthentifizierung und Systemisolierung zu beeinträchtigen. Dabei muss eine Balance zwischen Sicherheitsmassnahmen und Benutzerfreundlichkeit gefunden werden, um den Zugriff auf Ressourcen in Echtzeit und eine effektive Zusammenarbeit zu gewährleisten.

2.9.2 Standortbestimmung

Um eine präzise Studie zu erarbeiten, muss zunächst eine Standortbestimmung durchgeführt werden, um einen Überblick über die aktuell eingesetzten Sachmittel und notwendigen Verbesserungen zu erhalten. Die Herausforderung besteht darin, dass die betroffenen Parteien in Lugano ansässig sind, während das Projektteam in Bern stationiert ist, was die persönliche Begutachtung der Situation erschwert und durch die Notwendigkeit der Geheimhaltung weiter verkompliziert hat. Das Team verfügt jedoch über eine Kontaktperson in Lugano, die wesentliche Einblicke liefert, und profitiert von den Erfahrungen früherer Geheimhaltungsprojekte in Bern und Zürich, um bewährte Verfahren zu nutzen. Angesichts der strengen Geheimhaltung dürfen keine Informationen preisgegeben werden, und die Projektbeteiligten erhalten nur vom Auftraggeber detaillierte Anforderungen, auf deren Grundlage die Infrastruktur konzipiert und realisiert wird.

Mengen und Häufigkeiten

Projekte dieser Art gibt es nur sehr selten und kann je nach Projekt und Standort unterschiedlich aufgebaut sein. Die Infrastruktur und Anforderungen bleiben jedoch überwiegend konstant. In dieser Analyse liegt der Fokus speziell auf der Situation in Lugano.

Wie das Inventar in Lugano aussieht:



Abbildung 7: NAS in Lugano

Das Synology NAS dient als Speichermedium und wird in Betrieb genommen, sobald es für das Projekt benötigt wird. Alle darauf gespeicherten Daten werden stets verschlüsselt abgelegt, um Sicherheit und Datenschutz zu gewährleisten.



Alle Arbeitsmittel werden sicher in einem verschlossenen Schrank aufbewahrt. Zugang zum Schlüssel haben ausschliesslich befugte Personen, was die Sicherheit der Materialien gewährleistet und unbefugten Zugriff verhindert.

Abbildung 8: Arbeitsmaterialschrank in Lugano



Ein kleines Zimmer dient zunächst als Arbeitsplatz. Es ist jedoch geplant, dieses Zimmer zukünftig als Sitzungszimmer umzugestalten. Dadurch verliert das Projekt seinen bisherigen, festen Standort.

Abbildung 9: Arbeitsplatz in Lugano

Alle verwendete Sachmittel wurden vom Auftraggeber zur Verfügung gestellt. Davon waren einige fest für die Studenten reserviert und freigegeben. Einige waren noch ungewiss oder wurden bei späteren Phasen freigegeben.

Nr.	Typ	Erläuterung
1	Server in verschiedene Formfaktoren	2-3 Server
2	Synology NAS	1-2 Storage FS6400
3	Ein vorhandenes und konfigurierbares Netzwerk	Mit einem externen Partner konfigurierbar
4	Lizenzen	Je nach evaluierte Lösung eine Testlizenz oder Produktive Lizenzen

Abbildung 10: Sachmittel vom Auftraggeber

Informationssicherheit und Datenschutz

Dieses Thema ist von grosser Bedeutung für das Projekt. Da das Projektteam jedoch unabhängig von laufenden Projekten operiert und das System als Proof of Concept (PoC) entwickelt wird, befinden sich keine sensiblen Daten darauf. Die Koordination mit den Stakeholdern erfolgt mündlich, und die Ergebnisse werden in Form von Anforderungen dokumentiert.

Stärken-, Schwächen- und Ursachenanalyse

Bei der Analyse der Stärken sollen die positiven Attribute und Ressourcen hervorgehoben werden, die zur Studie beitragen könnten. Die grösste Stärke besteht im Zugang zu umfangreichem Fachwissen sowie in der finanziellen Unterstützung durch den Auftraggeber. Dadurch wird ein starkes Fundament geboten und ein grosser Spielraum bei der Konzeption unter Einsatz verschiedener Sachmittel, die zur Verfügung stehen, eröffnet.

Die Schwächen in diesem Projekt liegen hauptsächlich in der Transparenz. Die Einschränkungen beim Erhalt und der Weitergabe detaillierter Informationen über die aktuelle Ist-Situation zwingen dazu, sich an die definierten Anforderungen zu halten und diese möglichst präzise zu erfüllen.

Die Ursachen der Stärken und Schwächen sind bekannt, und die Herausforderung wird dennoch gerne angenommen. Da die Lösung als Proof of Concept klassifiziert ist, könnte sie keinen Einsatz im Produktivbetrieb finden. Diese Möglichkeit ist bekannt, dennoch wird der grosse Wert gesehen, diese Lösung zu entwickeln und zu testen. Das Ziel ist es, eine potenzielle Umgebung zu gestalten, die in der Praxis eingesetzt werden könnte. Die Bemühungen bilden eine fundierte Grundlage, die zeigt, wie eine effektive und effiziente Umsetzung in der Zukunft aussehen könnte.

Informationsbeschaffung

Die meisten benötigten Informationen können aus dem engen Kontaktnetz bezogen werden. Dies umfasst sowohl das interne IT-Team als auch externe Partner und Fachexperten, die in grösseren IT-Projekten Unterstützung bieten. Darüber hinaus wird ein direkter Austausch mit den Kunden gepflegt, um Fragen zu stellen oder Feedback einzuholen. Für weitere Informationen wird das Internet herangezogen, beispielsweise, um nach Best Practices der Hersteller zu recherchieren oder Diskussionen in verschiedenen Fachforen zu verfolgen.

2.9.3 Pflichtenheft

Für eine korrekte Evaluierung des Produktes und eine erfolgreiche Konzeptionsphase ist es wichtig, dass die funktionalen und nicht-funktionalen Anforderungen des Kunden genau verstanden werden. Dafür wird mit Hilfe von User Stories ein Anforderungskatalog erstellt. Diese User Stories dienen nicht nur als Grundlage für die Entwicklung, sondern ermöglichen es auch, am Ende des Projekts zu überprüfen, ob alle Anforderungen erfolgreich umgesetzt und erfüllt worden sind.

User Stories

Als...	Möchte ich...	Sodass...
Projektmitarbeiter	Die Möglichkeit auf Homeoffice haben	Ich nicht jeden Tag pendeln muss
Projektmitarbeiter	Von mehreren Standorten aus arbeiten können	Ich auch beim Kunden vor Ort effektiv sein kann

Projektmitarbeiter	Sicherstellen, dass bei Verlust oder Diebstahl meines Arbeitsgerätes keine signifikanten Sicherheitsrisiken entstehen	Der Schutz unserer sensiblen Daten gewährleistet ist
Projektmitarbeiter	Mit meinem Projektteam in Echtzeit kollabrieren können	Die Effizienz unserer Arbeit nicht beeinträchtigt wird
Projektmitarbeiter	Den Arbeitsprozess verstehen und eingeführt bekommen	Ich die Arbeitsumgebung schnell und effektiv nutzen kann
Projektmitarbeiter	Intuitiv Daten bearbeiten und abspeichern können	Ich nicht durch komplizierte Prozesse navigieren muss
Projektmitarbeiter	Trotz der Flexibilität über eine leistungsfähige Umgebung verfügen	Ich weiterhin produktiv und effizient arbeiten kann
Auftragsgeber	den Service auf monatlicher Basis abrechnen können	Wird eine neue Einkommensquelle haben und den Abrechnungsprozess vereinfachen können
IT-Supporter	Benutzermutationen unkompliziert ändern können	Ich Zeit spare und das Wissen schnell weitergeben kann
IT-Supporter	Anpassungen an der Umgebung möglichst einfach und ohne Wartungsarbeiten durchführen können	Die Kundenzufriedenheit hoch bleibt

Tabelle 13: User Stories

Anforderungskatalog

Funktionale Anforderungen:

Die Anforderungen wurden Anhand der User Stories definiert und mit dem Auftragsgeber erweitert. Am Ende der Sammlung wurde das Dokument von den Stakeholdern genehmigt.

Nr.	Anforderung	Kategorie
1	Die Kunden können sich von jedem Ort aus sicher auf ihre VDI verbinden	M
2	Die Remoteverbindung ist durch mindestens zwei Authentifizierungsfaktoren geschützt	M
3	Echtzeit Kollaboration zwischen Nutzern ist möglich	M
4	Eine bereits bekannte und bewährte Dateiallagetechnologie wird für die Dateiverwaltung verwendet	S
5	Der IT-Supporter kann die Leistung (Kerne, RAM, VRAM) der VDI anpassen	S

Nr.	Anforderung	Kategorie
6	IT-Support kann Benutzerkonten in der VDI-Infrastruktur hinzufügen, bearbeiten und löschen	M
7	IT-Support kann Änderungen am VDI-Image vornehmen, ohne den laufenden Betrieb zu stören	S
8	Das Engineering Team kann Anpassung an der Infrastruktur vornehmen, ohne den laufenden Betrieb zu stören	K
9	Sicherheitsfunktionen, wie das Blockieren von Screenshots und Videoaufnahmen der VDI, werden implementiert	K
10	Sensible Daten werden mindestens einmal täglich gesichert	M
11	Das Backup erfolgt automatisch ohne manuellen Eingriff	M
12	Das Benutzerendgerät ist hinsichtlich des Gewichts und Portabilität optimiert	X
13	Das Benutzerendgerät muss in der Lage sein bis zu mindestens vier Sicherheitsfunktionen, wie z.B. sicheres Passwort, Bitlocker, USB Authentifizierung Schlüssel und Deep Freeze ähnliche Produkte zu unterstützen.	X
14	Ein Verlust des Endgerätes führt zu keiner Sicherheitsgefährdung sensibler Daten	X
15	Die VDI-Infrastruktur ist virtuell von der produktiven Umgebung isoliert und unabhängig	M
16	Die Authentifizierung für die VDI erfolgt unabhängig vom produktiven Active Directory	S
17	Eine aktive Verbindung kann in einem Notfall sofort unterbrochen und blockiert werden	M
18	Auf dem Client-Gerät ist eine Endpoint Security Software installiert	M
19	Auf dem VDI-Client läuft ein Antivirus	S
20	Die VDI verfügt über keinen direkten Internetzugang	M
21	Die VDI hat spezifische, vordefinierte Programme installiert	M
22	Die VDI bietet ausreichend Leistung für den reibungslosen Betrieb der erforderlichen CAD-Programme	M
23	Abgespeicherten Dokumente werden verschlüsselt gespeichert	S
24	Wichtige Dienste sind redundant ausgelegt	S
25	Sensible Daten werden ausschliesslich in der vorgesehenen Dateiablage gespeichert, lokale Dateien auf der VDI oder dem Client werden nach jedem Neustart gelöscht	M

Nr.	Anforderung	Kategorie
26	Benutzeranpassung der VDI-Umgebung werden unterstützt und bei einem Neustart beibehalten, sofern sie die Sicherheitsrichtlinie nicht verletzen, wie z.B. CAD-Voreinstellungen	S
27	Die Performance und Verfügbarkeit der VDI wird kontinuierlich überwacht	S
Kategorie: M = Muss, S = Soll, K = Kann, X = wird nicht realisiert		

Tabelle 14: Funktionale Anforderungen

Nicht Funktionale Anforderungen:

Nr.	Anforderung	Beschreibung	Messkriterium	Verifizierung
1	Benutzerfreundlichkeit	Die Arbeitsprozesse sind leichtverständlich. Die Oberfläche ist einfach und intuitiv zu bedienen.	Mehr als 80% der Nutzer geben positives Feedback zur Benutzerfreundlichkeit	Direktes Feedback vom Kunden
2	Sicherheit	Gewährleiste der Datensicherheit und Sicherstellung von einhalten von Sicherheitsstandards	Keine kritischen Schwachstellen bei regelmässigen Tests	Sicherheitsaudits und Penetrations-tests
3	Skalierbarkeit	Das System kann bei steigender oder sinkender Nutzeranzahl effizient Ressourcen zuweisen oder einsparen. Anpassung der Leistung einzelner VDIs möglich	Das System unterstützt ohne Leistungseinbussen die maximale berechnete Anzahl gleichzeitiger Nutzer	Lasttests und Last-monitoring
4	Verfügbarkeit	Das System ist rund um die Uhr verfügbar und kann Ausfälle einzelner Komponenten überstehen	Die Verfügbarkeit des Systems liegt bei 99% über den Monat	Monitoring der Verfügbarkeit
5	Performance	Die VDI-Umgebung bietet eine schnelle Reaktionszeit, vergleichbar mit einem Desktop-PC, auch bei schlechter Internetverbindung	Bietet konstant 30-40 FPS. Automatische Komprimierungen für leistungsschwächere Internetverbindungen sind möglich	Performance-Tests

Nr.	Anforderung	Beschreibung	Messkriterium	Verifizierung
6	Support	Kunden haben während der Geschäftszeiten Zugang zum Support und können Änderungen anfragen	Antwortzeit gemäss Qualität Management Service (QMS)	Rapport des Ticketing

Tabelle 15: Nicht funktionale Anforderungen

2.10 Lösungsvarianten

Für den Variantenentscheid werden drei unterschiedliche VDI-Lösungen analysiert, wobei sowohl technische Merkmale als auch wirtschaftliche Aspekte untersucht werden. Mit Hilfe einer SWOT-Analyse werden die Stärken und Schwächen jeder Lösung identifiziert. Neben der Bewertung der Funktionalitäten wird auch untersucht, inwiefern die drei Produkte die Anforderungen erfüllen, indem eine Nutzwertanalyse durchgeführt wird. Dies ermöglicht eine fundierte Entscheidung zu treffen.

2.10.1 Variantenübersicht

Die Auswahl der passenden Lösung ist entscheidend für das Unternehmen und dessen Zukunftsfähigkeit und muss deshalb sorgfältig evaluiert werden. Als Partner von VMware wurde VMware Horizon zunächst bevorzugt. Jedoch hat die Übernahme von VMware durch Broadcom zu signifikanten Änderungen in der Lizenzierungspolitik geführt, weshalb VMware erneut in unseren Evaluierungsprozess einbezogen wird. Obwohl das Projekt technisch von der aktuellen produktiven VDI-Umgebung unabhängig ist, ist es trotzdem sinnvoll die Produktive Umgebung in dieser Bewertung mit einzubeziehen, vor allem aus wirtschaftlichen Überlegungen wie der Lizenzierung.

Im Kontext der On-Premises VDI-Lösungen stellt Citrix das direkte Äquivalent zu VMware dar und wird daher als eine wichtige Option in der Evaluierung betrachtet. Im Bereich VDI ist Citrix bereits seit längerer Zeit aktiv und etabliert, bevor VMware einen starken Aufschwung auf dem Markt hatte. Citrix bietet mit Citrix Virtual Apps and Desktops Lösungen an, die mit denen von VMware Horizon vergleichbar sind.

Neben den On-Premises Lösungen wird auch die Möglichkeiten einer Cloud-basierten Lösung in Betracht gezogen. Hier liegt der Fokus hauptsächlich auf Microsoft Azure Virtual Desktop (AVD). Azure VDI ermöglicht eine flexible und skalierbare Bereitstellung von virtuellen Desktops und Anwendungen.

Eigenschaften / Lösungen	VMware Horizon	Citrix Virtual Apps and Desktop	Microsoft Azure Virtual Desktop
Grundlegende Architektur	On-Premises, Hybrid, Cloud	On-Premises, Hybrid, Cloud	Cloud, Hybrid
Unterstützte Plattformen	Windows, Linux	Windows, Linux	Windows
Virtualisierungen	Desktops und Anwendungen	Desktops und Anwendungen	Desktops und Anwendungen über Remote-App

Eigenschaften / Lösungen	VMware Horizon	Citrix Virtual Apps and Desktop	Microsoft Azure Virtual Desktop
Managementtools	VMware vCenter, Horizon Console	Citrix Studio, Citrix Director	Azure Portal, Powershell, Microsoft Endpoint Manager
Skalierbarkeit	Hohe Skalierbarkeit Abhängig von Hardware	Hohe Skalierbarkeit Abhängig von Hardware	Hohe Skalierbarkeit
Benutzererfahrung	Blast Extreme Protokoll, bis zu 60 Frames per second (FPS)	HDX-Protokoll, bis zu 120 FPS	RDP und RemoteFX, bis zu 30 FPS
Zugriff von mobilen Endgeräten	VMware Horizon Client	Citrix Receiver / Workspace App	Remote Desktop Client und Web
Implementierungsmodell	On-Premises, Hybrid	On-Premises, Hybrid, Cloud	Primär Cloud
Lizenzmodell	Lizenzkosten abhängig von der Infrastruktur und Partnerschaft	Lizenzkosten abhängig von der Infrastruktur und Partnerschaft	Verbrauchsbasierte Bezahlung, abhängig von der Ressourcenutzung

Tabelle 16: Eigenschaften der Lösungsvarianten

VMware Lösung grafisch

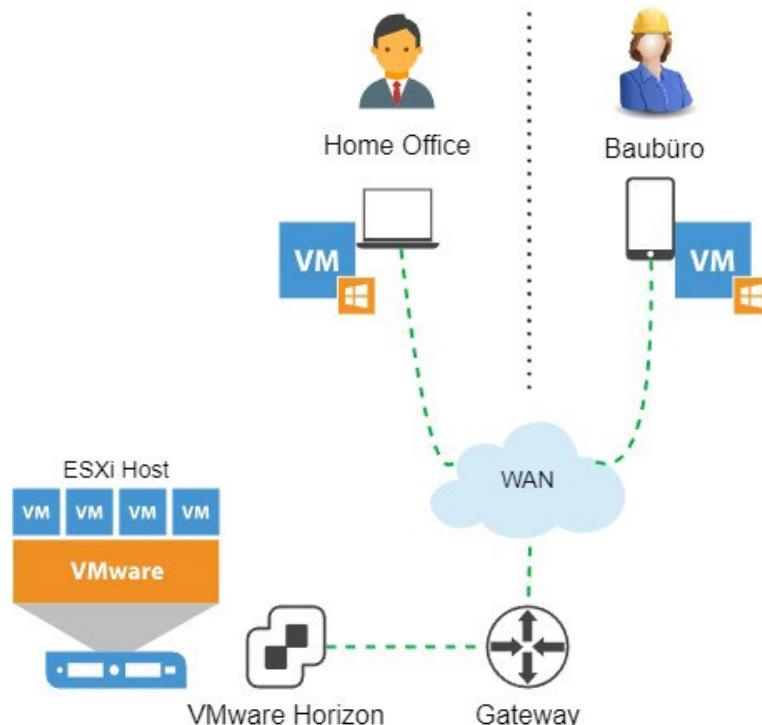


Abbildung 11: VMware Lösung grafisch

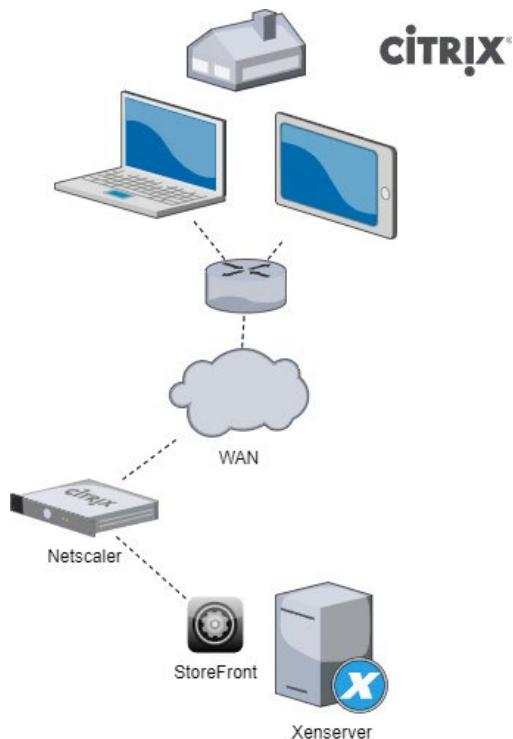
Citrix Lösung grafisch

Abbildung 12: Citrix Lösung grafisch

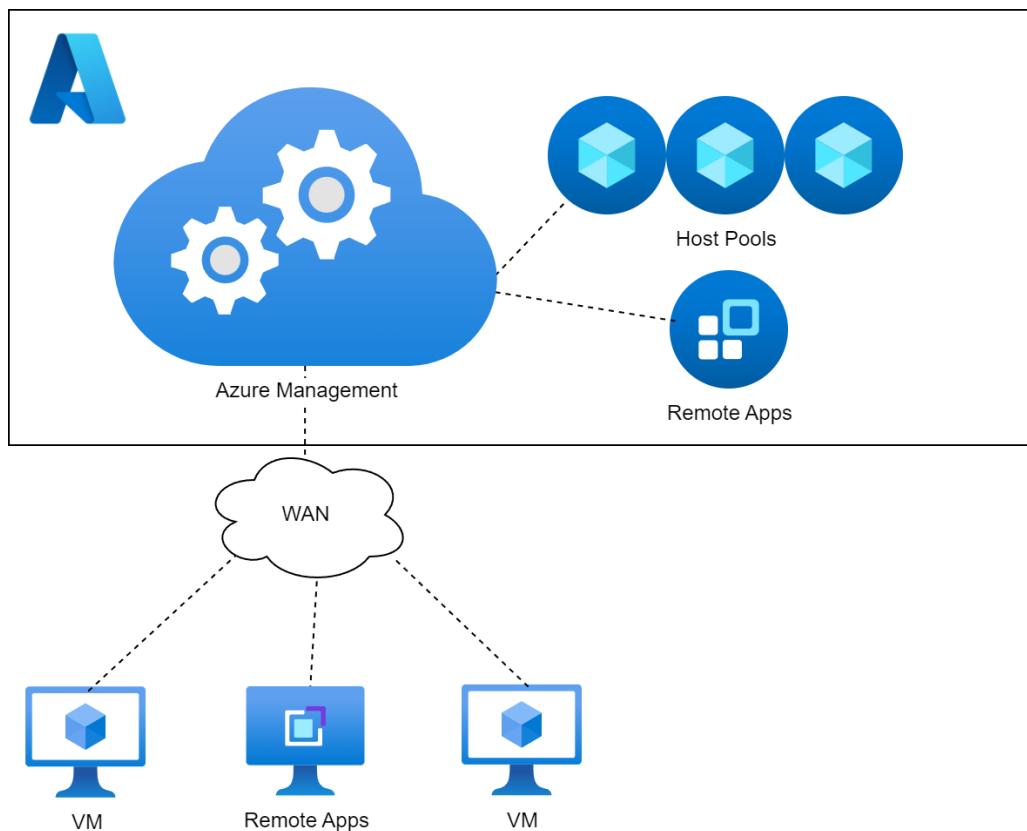
Microsoft Azure Virtual Desktop Lösung grafisch

Abbildung 13: MS AVD Lösung grafisch

Die Kurzbeschreibungen der einzelnen Lösungen findet Ihr in der Studie, im Anhang B2. Für weitere Informationen kann man die Datenblätter der Lösungen im Anhang F4 finden.

2.11 Analyse und Bewertung

Die Auswahl der passenden Lösung ist ein mehrdimensionaler Prozess. Indem unterschiedliche Bewertungskriterien gewichtet werden, entsteht eine ganzheitliche Beurteilung der verschiedenen Optionen.

In der Studie wurde eine detaillierte Anforderungsabdeckung der Lösungen erstellt. Es stellte sich heraus, dass alle Lösungen die Anforderungen erfüllen können, wobei einige Lösungen einfacher umzusetzen sind und andere komplexer. Für eine genaue Abdeckung siehe Anhang der Studie, Kapitel 4.1, Anhang B2.

2.11.1 SWOT-Analyse

Mit dieser Analyse werden die Stärken, Schwächen, Chancen und Risiken jeder Variante bewertet.

		Interne Analyse	
		Stärken	Schwächen
Externe Analyse	Chancen	<ul style="list-style-type: none"> • Skalierbarkeit • Innovativ • Nachhaltigkeit durch zentral verwaltete Ressourcen • Benutzerfreundlichkeit • Steigende Nachfrage • Vielfältig einsetzbar in verschiedene Branchen • Steigerung der Flexibilität und Effizienz 	<ul style="list-style-type: none"> • Abhängigkeiten von Drittanbieter • Komplexität • Veränderung der Arbeitsweise für konservative Kunden • Eher neu auf dem Markt
	Risiken	<ul style="list-style-type: none"> • Marktbedarf ist vorhanden • Akquirieren neuen Kunden • Neue mögliche Partnerschaften 	<ul style="list-style-type: none"> • Änderung der Bedürfnisse • Fehlendes technische Know-how • Konkurrenz auf dem Markt • Grosse Cloud Anbieter mit eigenen Lösungen

Tabelle 17: SWOT-Analyse

2.11.2 Nutzwertanalyse

In der Nutzwertanalyse werden drei verschiedene Lösungsvarianten verglichen, um herauszufinden, welche von ihnen die Anforderungen am besten erfüllt. Dafür werden verschiedene Kriterien verwendet.

Nr.	Kriterium	Beschreibung
1	Kosten	Investitionskosten, Betriebskosten, Wartungskosten
2	Anforderungen	Erfüllung der funktionalen und nicht-funktionalen Anforderungen
3	Komplexität	Schwierigkeit der Implementierung, Konfiguration und Verwaltung der Lösung
4	Kompatibilität	Kompatibilität mit den bestehenden Systemen und Software
5	Benutzerfreundlichkeit	Einfachheit und Intuitivität der Benutzeroberfläche
6	Leistung	Geschwindigkeit, Effizienz und Zuverlässigkeit
7	Skalierbarkeit	Umgang mit wachsenden Anforderungen oder Nutzerzahlen
8	Nachhaltigkeit	Energieeffizienz und Gebrauch von umweltfreundlicheren Materialien
9	Sicherheit	Sicherheitsmassnahmen wie Datenverschlüsselung, Zugriffskontrollen und Compliance mit Sicherheitsstandards
10	Support und Wartung	Verfügbarkeit von Herstellersupport oder Partnerschaften. Regelmäßige Patches

Tabelle 18: Kriterien der Nutzwertanalyse

Gewichtung der Kriterien

Für die Durchführung einer Nutzwertanalyse ist es wichtig, die Bewertungskriterien, die für den Vergleich der verschiedenen Lösungsvarianten herangezogen werden, sorgfältig zu gewichten. Diese Gewichtung reflektiert die relative Bedeutung jedes Kriteriums im Hinblick auf die Gesamtentscheidung. Die Gewichtungsskala erstreckt sich von 0 bis 2, wobei die Bewertung in Schritten von 0,5 erfolgt. Innerhalb dieser Skala repräsentiert ein Wert von 0, dass ein Kriterium relativ zum Gegenstück, völlig unwichtig ist, während ein Wert von 2 anzeigen, dass das Kriterium doppelt so wichtig ist, relativ zum Gegenstück. Eine Standardgewichtung von 1, hat die Bedeutung einer Gleichwertigkeit.

	Kosten	Anforderungen	Komplexität	Kompatibilität	Benutzerfreundlichkeit	Leistung	Skalierbarkeit	Nachhaltigkeit	Sicherheit	Support und Wartung	Punkte	Gewichtung berechnet	Gewichtung für NWA
Kosten	1	1	2	1.5	1	1	1	2	1	1	11.5	13	15
Anforderungen	1	2	1.5	1.5	1	1	1	2	1	1	12	13	15
Komplexität	1	0	1	1	1	0.5	0.5	1.5	0.5	1	7	8	10
Kompatibilität	0	0.5	1	1	1	1	1	2	1	1	8.5	9	10
Benutzerfreundlichkeit	0.5	0.5	1	1	0.5	0.5	0.5	1.5	0.5	0.5	6.5	7	5
Leistung	1	1	1.5	1	1.5	1	1	1.5	1	1	10.5	12	10
Skalierbarkeit	1	1	1.5	1	1.5	1	1.5	1	1	1	10.5	12	10
Nachhaltigkeit	0	0	0.5	0	0.5	0.5	0.5	0	0	0	2	2	5
Sicherheit	1	1	1.5	1	1.5	1	1	2	1	1	11	12	10
Support und Wartung	1	1	1	1	1.5	1	1	2	1	1	10.5	12	10
											90	100	100

Tabelle 19: Gewichtung der Kriterien

Bewertung der Kriterien

Für die Bewertung jedes Kriterium braucht es eine Skala von 0 (ganz schlecht) bis 5 (sehr gut).

		Keine 0	Schlecht 1	Ungenügend 2	Genügend 3	Gut 4	Sehr gut 5
Zuschlagskriterien	Gewicht						
Kosten	15%	Für ein KMU un- erschwinglich	Über dem Budget	leicht über dem Budget	Im Budget	Unter dem Budget	Kostenlos oder nicht Budgetre- levant
Anforderungen	15%	Keine Anforderun- gen erfüllt	Einige wenige Anforderungen erfüllt	Einige wichtige Anfor- derungen erfüllt	Die Mehrheit der Anforderungen erfüllt	Fast alle Anfor- derungen erfüllt	Alle Anforderun- gen erfüllt
Komplexität	10%	Erfordert Schulun- gen und Exper- tenwissen	Spezialwissen nötig	Einstigerfreundlich für Fachpersonal	Handhabbar für Standardfähig- keiten	Benutzerfreund- lich und leicht verständlich	Intuitiv und ohne zusätzliche Hilfe bedienbar
Kompatibilität	10%	Keine Kompatibili- tät mit bestehen- den Systemen und Anwendun- gen	Viele Anpassun- gen nötig	Einige Anpassungen nötig	Geringe Ein- schränkungen	Minimale Anpas- sungen nötig	Nahtlose In- tegration
Benutzerfreundlichkeit	5%	Schwer nutzbar	Ganztägige Schulung erfor- derlich	Kurzer Workshop er- forderlich	Kurze Einfüh- rung erforderlich	Einige Anleitun- gen nötig	Intuitiv ohne Ein- führung nutzbar
Leistung	10%	Produktive Arbeit unmöglich	Erfüllt nicht die Mindestanforde- rungen	Tägliche Abstürze aufgrund unzu- reichender Leistung	Funktioniert mit spürbarer La- tenz	Lauft stabil mit 30 FPS	Lauft stabil mit über 30 FPS
Skalierbarkeit	10%	Nicht skalierbar	Nur durch Hard- ware erweiterbar	Skalierung sind mit Wartungsarbeiten verbunden	Manuelle An- passungen für Skalierung nötig	Schnelle und dy- namische Ska- lierung mit gerin- gen Einschrän- kungen	Schnelle und dy- namische Ska- lierung und Echtzeit Ana- passungen
Nachhaltigkeit	5%	Sehr hoher Ener- gieverbrauch und Nutzung schädli- cher Materialien	Hoher Energie- verbrauch, je- doch gewisse Materialaspekte beachtet	Höherer Energiever- brauch als derzeitiger Standard	Energiever- brauch ent- spricht dem ak- tuellen Standard	Energiever- brauch ent- spricht dem	Hohe Energie- einsparungen und Nutzung nachhaltiger Ressourcen

		Keine 0	Schlecht 1	Ungenügend 2	Genügend 3	Gut 4	Sehr gut 5
Zuschlagskriterien	Gewicht						
						Standard, nachhaltige Produkte im Einsatz	
Sicherheit	10%	Keine Sicherheitsmassnahmen vorhanden	Keine spezifischen Sicherheitsmassnahmen implementierbar	Branchenstandard, mit deutliche Verbesserungsmöglichkeiten	Gute Sicherheitsfeatures implementiert	Mehrere erweiterte Sicherheitsfeatures im Einsatz, Datenverschlüsselung vorhanden	Umfassende Sicherheitsfeatures inklusive Datenverschlüsselung, regelmässige Audits und Compliance-Überprüfungen
Support und Wartung	10%	Kein Support vorhanden	Sehr begrenzter Support, Reaktionszeit über einer Woche	Begrenzter Support, Reaktionszeit über drei Tage	Guter Support, Reaktionszeit von 1-2 Tagen	Direkter Ansprechpartner beim Hersteller oder Partner vorhanden	Direkter Ansprechpartner beim Hersteller oder Partner mit 24/7 Verfügbarkeit und proaktiver Unterstützung

Tabelle 20: Bewertung der Kriterien

Ergebnisse der Nutzwertanalyse

In der Analyse wurden VMware, Citrix und Azure Virtual Desktop umfassend untersucht und anhand von zehn Schlüsselkriterien bewertet, die von Kosten und Anforderungserfüllung bis hin zu Nachhaltigkeit und Support reichen. Die resultierenden Daten ermöglichen es, eine fundierte Entscheidung zu treffen.

Kriterien	Erläuterung	Gewichtung (G)	VMware		Citrix		Azure	
			Note (W)	G*W	Note (W)	G*W	Note (W)	G*W
Kosten	günstig: 5 / teuer: 0	15	1	15	3	45	1	15
Anforderungen	alle: 5 / keine 0	15	5	75	5	75	5	75
Komplexität	einfach: 5 / komplex 0	10	2	20	2	20	3	30
Kompatibilität	kompatibel: 5 / nicht kompatibel 0	10	4	40	4	40	4	40
Benutzerfreundlichkeit	Intuitiv: 5 / Komplex 0	5	4	20	4	20	4	20
Leistung	Schnell: 5 / langsam 0	10	4	40	5	50	4	40
Skalierbarkeit	Skalierbar: 5 / nicht skalierbar 0	10	4	40	5	50	5	50
Nachhaltigkeit	Nachhaltig: 5 / nicht nachhaltig 0	5	5	25	5	25	5	25
Sicherheit	Compliance: 5 / Sicherheitslücken 0	10	5	50	5	50	4	40
Support und Wartung	innert 24h 5 / mehr als 72h 0	10	3	30	4	40	4	40
Total		100		355		415		375

Tabelle 21: Ergebnisse der Nutzwertanalyse

Die einzelnen Begründungen für die Punktevergabe sind detailliert in der Studie im Anhang B2 beschrieben.

2.12 Variantenentscheid

Nach sorgfältiger Abwägung der verschiedenen Lösungsoptionen und Durchführung einer detaillierten Nutzwertanalyse wurde Citrix Virtual Apps and Desktops als die bevorzugte Lösung entschieden. Die Entscheidung für Citrix wurde durch mehrere ausschlaggebenden Faktoren bestimmt, die im Folgenden erläutert werden:

Kosten: Ein entscheidender Faktor in der Entscheidung für Citrix ist eine bestehende Partnerschaft mit einer vertrauenswürdigen Person, der bereits ein etablierter Citrix-Partner ist. Diese Beziehung ermöglicht es, Citrix-Lizenzen zu vorteilhaften Konditionen zu beziehen, was die Gesamtkosten der Lösung signifikant reduziert. Zudem sind die Standardpreise von Citrix schon sehr wettbewerbsfähig.

Leistung: In der Kategorie Leistung hat Citrix eine Spitzenbewertung erhalten. Insbesondere die Geschwindigkeit der Bereitstellung von Desktops, die für einen dynamischen Betrieb entscheidend ist. Mit Citrix sind wir in der Lage, auch leistungsintensive Anwendungen wie CAD-Tools ohne grosse Latenz oder Performance Einbussen bereitzustellen.

Skalierbarkeit: Die Skalierbarkeit ist für unser Unternehmen von entscheidender Bedeutung, da wir schnell auf Veränderungen in der Arbeitslast reagieren müssen. Citrix ermöglicht eine dynamische Skalierung unserer Ressourcen, was es uns erlaubt, effizient und Energie schonend zu operieren.

Sicherheit: Da alle unserer Projekte unter strengen Vertraulichkeitsvereinbarungen stehen, ist es von entscheidender Bedeutung, eine Lösung zu wählen, die die sichere Handhabung sensibler Daten gewährleisten kann. Citrix ermöglicht nicht nur umfassende Sicherheitsfeatures, sondern bietet auch die Möglichkeit, es als eine komplette On-Premise Lösung zu implementieren. Diese Option ist für uns besonders wichtig, da sie es uns erlaubt, die volle Kontrolle über unsere Daten zu behalten und den Zugriff streng zu regulieren. Durch die Wahl einer On-Premise Konfiguration mit Citrix können wir sicherstellen, dass unsere geheimhaltungsbedürftigen Projekte in einer hochgesicherten Umgebung bearbeitet werden, was ein Schlüsselement unserer IT-Sicherheitsstrategie darstellt.

Support: Durch einen langjährigen Partner besteht eine direkte Ansprechperson für Support und Implementierungsunterstützung. Diese Kontakterson dient als Anlaufstelle für technische Herausforderungen oder Fragen.

In Anbetracht dieser Schlüsselfaktoren und der Tatsache, dass Citrix in der Gesamtbewertung die höchste Punktzahl erreicht hat, ist es zu dem Schluss gekommen, dass Citrix Virtual Apps and Desktops die ideale Lösung für das Unternehmen ist. Es bietet das beste Gleichgewicht zwischen Kosten, Funktionalität und strategischer Ausrichtung für unsere zukünftigen Ziele.

2.13 Wirtschaftlichkeit

Es wurde eine Analyse der Total Cost of Ownership (TCO) der verschiedenen Varianten erstellt. Dies spielt eine zentrale Rolle, um die langfristigen finanziellen Auswirkungen zu verstehen. Diese Analyse zielt darauf ab, nicht nur die direkten Kosten wie Anschaffungs- und Implementierungskosten zu erfassen, sondern auch indirekte Ausgaben, die über die Lebensdauer der Lösung anfallen, wie Betriebskosten und Supportleistungen.

2.13.1 TCO der verschiedenen Varianten

Investitionskosten	VMware	Citrix	Azure
Anschaffungskosten	58'160.-	58'160.-	29'000.- (Speicher)
Implementierungskosten	17'465.-	17'465.-	17'465.-
Schulungskosten	11'000.- ²	9'000.- ³	5'100.- ⁴
Totale Kosten	86'625.-	84'625.-	51'565.-

Tabelle 22: Investitionskosten

Die Anschaffungskosten umfassen die Sachmittel, die für die Umsetzung des Projektes erforderlich sind. Diese Kosten fallen zu Projektbeginn einmalig an. Die Implementierungskosten beziehen sich auf den internen Aufwand für die Realisierung des Projektes, entsprechend dem Personaleinsatz. Die Schulungskosten decken interne Schulungen der Ingenieure ab und sind auf zwei Personen kalkuliert. Die Auflistung der Sachmittel sowie die Personalkosten sind im Kapitel 2.6 Ressourcenplan zu finden oder im Anhang B2, Kapitel 6.

Laufende Kosten	VMware	Citrix	Azure
Lizenzerierung / Monatliche Abrechnungen	~28\$ Pro Benutzer (Partner)	~28\$ Pro Benutzer	~5'000.-
Betriebskosten	200.-	200.-	200.-
Externe Supportkosten	240.-	240.-	240.-
Wartungskosten	240.-	240.-	0
Totale Kosten (Lizenzen auf 15 Personen gerechnet)	1'455.-	1'455.-	5'840.-

Tabelle 23: Laufende Kosten

² <https://www.digicomp.ch/weiterbildung-it-provider/vmware/end-user-computing/kurs-vmware-horizon-deploy-and-manage-v8-8>

³ <https://www.digicomp.ch/weiterbildung-it-provider/citrix/kurs-citrix-virtual-apps-and-desktops-7-administration-on-premises-and-in-citrix-cloud-cws-215>

⁴ <https://www.digicomp.ch/weiterbildung-microsoft-technology/microsoft-azure/kurs-configuring-and-operating-microsoft-azure-virtual-desktop-intensive-training-az-140>

Diese Lizenzpreise sind ohne Währungsschwankungen und Mehrwertsteuer preisgegeben. Für die Berechnung des Azure Virtual Desktop wurde ein virtueller Server ausgewählt, der eine ähnliche Leistung wie eines der aktuellen Sachmittel aufweist. Bei der Ermittlung der Betriebskosten wurden die aktuellen internen Support-Tickets analysiert, die sich auf durchschnittlich etwa 30 Tickets pro Monat belaufen, welche der Kategorie VDI zugeordnet sind. Da die Kundenbasis in der produktiven Umgebung wesentlich grösser sein wird, wurde lediglich einen Bruchteil dieser Basis für diese Berechnungen herangezogen und die Zeit mit einem Stundensatz von 40 CHF veranschlagt. Für externen Support wurden zwei Stunden pro Monat eingeplant, basierend auf einem Stundensatz von 120 CHF. Die Wartungskosten wurden mit einem Aufwand von 2,7 Stunden pro Monat kalkuliert, ebenfalls zu einem internen Stundensatz von 40 CHF

Es ist zu beachten, dass derzeit lediglich **ein** Azure Virtual Desktop ausgewählt wurde. Für einen direkten Vergleich wäre es erforderlich, einen zusätzlichen virtuellen Server hinzuzufügen. Allerdings wurde bewusst darauf verzichtet, den zusätzlichen Server bereits in die Berechnung einzubeziehen, um die Grundlage des Vergleichs zu vereinfachen und die Ergebnisse zunächst isoliert zu betrachten. Auf diese Weise können wir klarer erkennen, wie sich die Leistung und Kosten des Azure Virtual Desktops allein verhalten, bevor weitere Variablen hinzugefügt werden.

Nutzungsdauer	VMware	Citrix	Azure
Jahr 1	88'080.-	84'625.-	57'405.-
Jahr 2	89'535.-	86'080.-	63'245.-
Jahr 3	90'990.-	87'535.-	69'085.-
Jahr 4	92'445.-	88'990.-	74'925.-
Jahr 5	93'900.-	90'445.-	80'765.-

Tabelle 24: Nutzungsdauer auf 5 Jahre

3 Konzeptphase

In diesem Kapitel wird die Konzeptionierung der Diplomarbeit VDI as a Service dargestellt. Die Konzeptphase bietet einen strukturierten Fahrplan für die Realisierung, ermöglicht das frühzeitige Erkennen potenzieller Probleme und die Entwicklung entsprechender Lösungsansätze. Hier werden die Architektur und das Design der Lösung sowie die Implementierungsprozesse und Testverfahren ausführlich beschrieben. Weiterhin wird erläutert, welche Massnahmen und Ressourcen notwendig sind, um die Lösung effektiv zu betreiben. Ziel ist es, eine solide Grundlage für die anschliessende Implementierungsphase zu schaffen. Insgesamt wurden vier Konzepte entwickelt: das Detailkonzept, das Testkonzept, das Migrationskonzept und das Betriebskonzept. Diese sind für weitere Informationen im Anhang E aufgeführt.

3.1 Lösungsarchitektur

Das Ziel dieser Architektur ist es, eine sichere und funktionsfähige VDI-Umgebung (Virtual Desktop Infrastructure) bereitzustellen. Hierzu wurde eine umfassende Infrastruktur entworfen, die sowohl Server- als auch Netzwerkkomponenten umfasst.

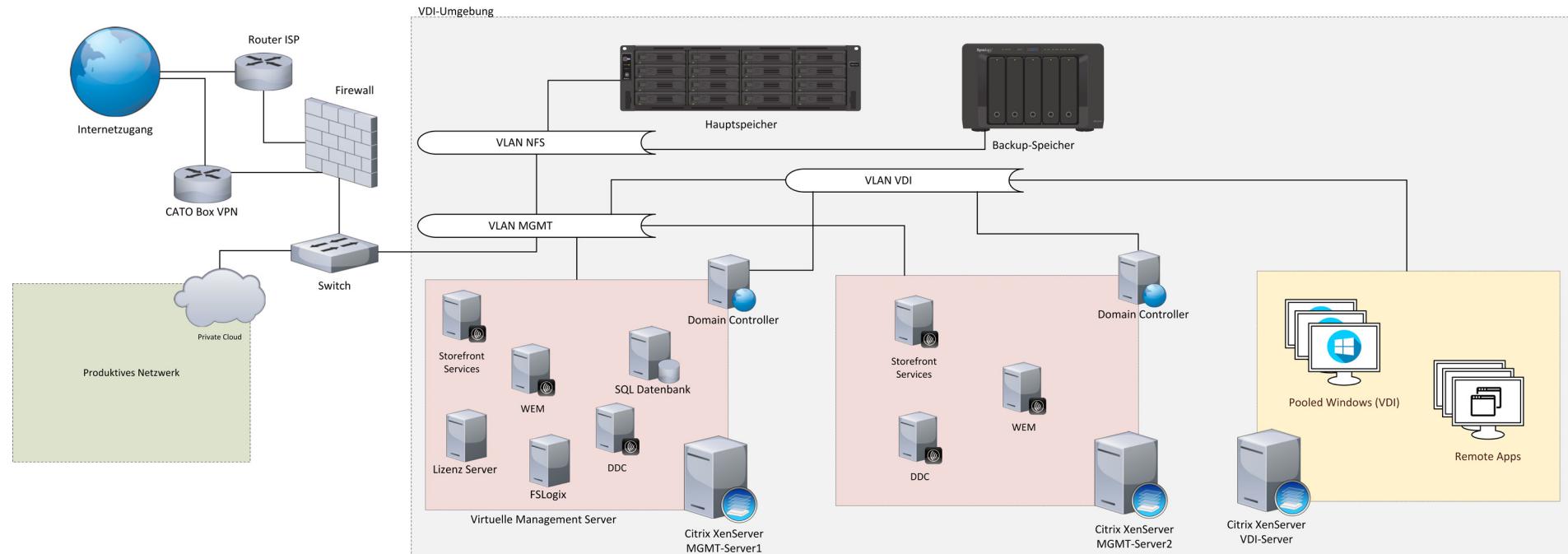


Abbildung 14: Lösungsarchitektur

3.1.1 Hardwarekomponente

Hier werden alle Hardwarekomponenten, die für den Betrieb der Lösung erforderlich sind, detailliert aufgelistet und beschrieben. Dazu gehören Netzwerkgeräte, Server, Desktop-PC und Speichergeräte. Alle Komponenten bis auf den VDI-XenServer konnten für diese Diplomarbeit verwendet werden, da der XenServer in der produktiven Umgebung weiterhin benötigt wurde und für die Diplomarbeit nicht zur Verfügung stand.

Komponente	Funktion	Spezifikationen ⁵	Konfiguration / OS
Firewall (Sophos X430)	Überwacht und steuert den ein- und ausgehenden Datenverkehr	- High Availability (HA) ist eingerichtet (Active-Passive)	Wird vom Dritt-partner verwaltet
Switches (Netgear)	Netzwerkgerät für den Verkehr zwischen verschiedenen Netzwerkkomponenten	- Netgear M4300-96X Modular Managed Switch - Module APM408C - Module für Glas APM408F	Wird vom Dritt-partner verwaltet
XenServer Management 1	Dient als Hypervisor für alle Management VMs, die für die Umgebung benötigt werden	- 2x Intel Xeon Silver 2.4 GHz, 10 Cores - 768GB RAM - 1x NVIDIA A16 - 2x 2TB SSD - 10Gbp/s Netzwerkkarte	XenServer Version 8
XenServer Management 2	Dient als Hypervisor für alle Management VMs, die für die Umgebung benötigt werden	- 2x Intel Xeon Silver 2.4 GHz, 10 Cores - 768GB RAM - 1x NVIDIA A16 - 2x 2TB SSD - 10Gbp/s Netzwerkkarte	XenServer Version 8
XenServer VDI Server	Dient als Hypervisor für alle VDIs, die für die Benutzern zur Verfügung gestellt werden	- 2x Intel Xeon Gold 5317 CPU at 3.00 GHz / 12 Cores pro CPU - 1TB RAM - 2x NVIDIA A16 - 2x 2TB SSD - 1x RAID-Controller - 10Gbp/s Netzwerkkarte	XenServer Version 8
Hauptspeicher (Synology FS6400)	Hauptspeicher für die Datenablage	- INTEL Xeon Silver 4110 at 2.1 GHz / 16 Cores - 128 GB RAM - 24x 3.5 TB SSD - 2x 10Gbp/s Netzwerkkarte	DSM 7.2-64570 Update 1

⁵ <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/1912-ltsr/system-requirements.html>

Backupspeicher (Synology DS1823xs+)	Dient als Backup-Speicher für alle Server	- AMD Ryzen V1780B at 3.35 GHz / 4 Cores - 24 GB RAM - 5x 9.1 TB HDD	DSM 7.2-64570 Update 1
--	---	--	------------------------

Tabelle 25: Hardwarekomponente

3.1.2 Softwaredienste

Wie bei den Hardwarekomponenten werden auch einige wichtige Dienste verwendet, um die VDI-Lösung funktionsfähig zu machen. Die folgende Tabelle gibt einen Überblick über die verwendeten Softwaredienste, ihre Funktionen, Bemerkungen und Hersteller.

Dienst	Funktion	Bemerkung	Hersteller
Desktop Delivery Controller (DDC)	Zuständig für die Zuweisung und Verwaltung von VDIs	Ist das Zentrale Verwaltungssystem für die VDIs	Citrix
SQL-Datenbank	Speichern von Konfigurations- und Sitzungsinformationen	Zentral für die Datenhaltung und Reporting	Microsoft
StoreFront	Dient als Zugangspunkt für Benutzer und verwaltet die Authentifizierung	Bietet eine personalisierbare Benutzeroberfläche	Citrix
Lizenzen Server	Verwaltung von Citrix Lizenzen	Mindestens ein Lizenzserver pro Standort erforderlich	Citrix
Workspace Environment Management (WEM)	Profil- und Umgebungsmanagement	Verbessert die Benutzererfahrung und stellt die korrekten Ressourcen zur Verfügung	Citrix
FSLogix	Profilmanagement in VDI-Umgebungen	Verbessert die Benutzererfahrung	Citrix
VDI-Maschinen	Ressource der virtuellen Desktops	Zentrale Komponente der VDI-Lösung	Citrix Microsoft

Tabelle 26: Softwaredienste

3.1.3 Netzwerk

Auf der linken Seite der Abbildung ist die Netzwerkinfrastruktur dargestellt. Diese zeigt, wie das interne Netzwerk mit dem Internet verbunden ist. Ein zentraler Bestandteil ist der Router des Internet Service Providers (ISP), der den Zugang zum Internet ermöglicht. Der Netzwerkverkehr wird durch eine Firewall geschützt, die unerlaubte Zugriffe verhindert und die Netzwerksicherheit gewährleistet.

Der Switch in der Mitte der Netzwerkinfrastruktur verbindet verschiedene Netzwerkgeräte und sorgt für eine effiziente Datenübertragung innerhalb des Netzwerks. Die Firewall und die Switches sind entscheidend für die Segmentierung des Netzwerks. Durch diese Segmentierung können verschiedene Netzwerksegmente für unterschiedliche Geräte und virtuelle Server geschaffen werden, was die Sicherheit und Verwaltung des Netzwerks verbessert.

Ein weiterer wichtiger Bestandteil ist die CATO Box VPN, die für eine sichere VPN-Verbindung sorgt und den externen Zugriff auf das interne Netzwerk ermöglicht.

Auf der linken Seite ist auch das produktive Netzwerk von Finitia ersichtlich. Dieses Netzwerk läuft zwar ebenfalls über den gleichen Switch, ist aber logisch von der restlichen Umgebung getrennt, um die Sicherheit und Effizienz zu gewährleisten.

Der rechte Bereich (VDI-Umgebung) der Abbildung zeigt die Hardware- und Softwarekomponenten, die für den Betrieb der VDI-Umgebung notwendig sind. Diese Komponenten sind in verschiedenen virtuellen Netzwerken (VLANs) organisiert, die logisch voneinander getrennt sind, um einen kontrollierten und sicheren Netzwerkverkehr zu gewährleisten. Es gibt insgesamt drei VLANs: das MGMT-, VDI- und NFS-Netzwerk.

- **MGMT-Netzwerk (rosa Bereich):** Hier sind der Management-XenServer und alle virtuellen Server untergebracht, die die notwendigen Dienste für die Citrix-Lösung bereitstellen.
- **VDI-Netzwerk (gelber Bereich):** In diesem Netzwerk befindet sich der VDI-XenServer, der die virtuellen Desktops (Pooled Windows VDI) bereitstellt.
- **NFS-Netzwerk:** Dieser Bereich umfasst den Hauptspeicher und den Backup-Speicher, die für die Speicherung und Sicherung der Daten verantwortlich sind.

Die Netzwerkregelungen für die drei Netzwerke wurden so eingerichtet, dass nur das MGMT-Netzwerk eine Internetverbindung hat. Das Management-Netzwerk hat auch Zugriff auf das VDI-Netzwerk, während das VDI-Netzwerk keinen Zugriff auf das Internet hat und nur Zugriff auf die Datenablage hat. Im VDI-Netzwerk befinden sich die VDI-Maschinen, auf denen die Benutzer an den Geheimhaltungsprojekten arbeiten. All diese Regelungen sind auf der Firewall definiert.

Das NFS-Netzwerk ist anders als die beiden anderen Netzwerke eingerichtet. Dieses Netz ist ein Layer-2-Netzwerk, was bedeutet, dass es nicht bis zur Firewall gelangt, sondern nur bis zum Switch und von den anderen Netzwerken abgeschirmt ist. Da es ausschliesslich für Backups und Serverdaten gedacht ist, ist diese Konfiguration vollkommen ausreichend.

Für weitere Informationen zu den Netzwerkregelungen und detaillierten Konfigurationen kann Kapitel 4 des Detailkonzepts (siehe Anhang E1) konsultiert werden.

3.1.4 Citrix VDI Service

Für die ausgewählte Lösung, Citrix, werden verschiedene Servicekomponenten benötigt, damit das Ganze reibungslos funktioniert.⁶

Desktop Delivery Controller (DDC): Ist die zentrale Verwaltungskomponente und muss mindestens auf einem Server pro Standort installiert sein. Man kann den DDC redundant aufbauen, indem man den Kontroller auf verschiedene Server installiert. Mit einem Management Server wird es in dieser Umgebung nicht möglich sein, eine Hardwareredundanz aufzubauen. Der DDC ist zuständig für:

- Verteilung von Desktops und Anwendungen
- Authentifizierung und Verwaltung des Benutzerzugriffs
- Vermittlung von Verbindungen zwischen Benutzern und ihren Desktops und Anwendungen
- Optimierung von Benutzerverbindungen
- Lastausgleich der Verbindungen

Datenbank: Für jeden Standort ist eine Microsoft SQL Datenbank erforderlich, welche die Konfigurations- und Sitzungsinformationen speichert. Die Kontroller müssen eine konsistente Verbindung auf diese Datenbanken haben, da hier die Daten gespeichert sind, die von den Diensten der Kontroller erfasst und verwaltet werden. Diese Datenbank wird standardmäßig auch als Logdatenbank verwendet.

StoreFront: Ist zuständig für die Authentifizierung der Benutzer und verwaltet die Zugriffe von Desktops und Anwendungen, auf denen die Benutzer Zugriff haben. Mit diesem Service haben Benutzer die Möglichkeit auf eine Selbstbedienungszugriff auf Ihre Desktops und Anwendungen. Dies bietet dem Benutzer eine einheitliche Benutzererfahrung über verschiedene Geräte hinweg.

Lizenz Server: Zuständig für die Verwaltung der Citrix-Produktlizenzen. Kommuniziert mit dem Kontroller, um die Lizenzierung für die Sitzungen der einzelnen Benutzer zu verwalten. Auch hier braucht es mindestens einen Lizenz Server pro Standort.

Workspace Environment Management (WEM): Service für die Profilbereitstellung von Ressourcen wie: Anwendungen, Drucker, Netzlaufwerke, Registrierungsschlüssel und mehr.

FSLogix: Ein Microsoft Produkt für das managen von Windows-Benutzerprofile in virtuellen Desktop-Computing-Umgebungen.

⁶ <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/technical-overview.html>

3.2 Technische Umsetzung

Nach der Erstellung der Lösungsarchitektur war es wichtig, die Infrastruktur so zu realisieren, dass diese in einer bestimmten Reihenfolge implementiert wird. Dies stellte sicher, dass man von Grund aus anfängt zu realisieren und keine Blockierungen während der Realisierung auftreten. Eine klare Implementierungsstrategie war hierbei essenziell, um die VDI-Lösung optimal umzusetzen und die Effizienz zu gewährleisten.

3.2.1 Implementierungsstrategie

Die Implementierungsstrategie wird in vier Hauptfaktoren aufgeteilt: Hardware aufsetzen, Netzwerk, Domäne & Dienste und Citrix-Dienste. Diese wurden in der genannten Reihenfolge eingerichtet. Für genauere Informationen zum Vorgehen kann das Migrationskonzept im Anhang E3 konsultiert werden.

Hardware aufsetzen

Als erstes muss das Material geprüft werden, um sicherzustellen, dass alle benötigten Ressourcen auch wirklich vorhanden sind. Da der Management-Server neu geliefert wurde, muss dieser mit den nötigen Komponenten wie CPU, GPU, RAM etc. eingerichtet und mit dem richtigen Betriebssystem gemäss Detailkonzept aufgesetzt werden.

Es gibt aber auch Geräte, die bereits vorhanden sind und übernommen werden, wie die Netzwerkspeicher. Hierbei ist es wichtig zu überprüfen, ob diese noch Daten enthalten und diese bei Bedarf zu löschen oder zu transferieren.

Nachdem alle Hardwarekomponenten einsatzbereit sind, müssen diese im Rack am richtigen Standort im Serverraum installiert werden. Alle Hardwarekomponenten, bis auf den Hauptspeicher, sind bei der Finitia AG im Serverraum untergebracht. Nur der Hauptspeicher ist im Rechenzentrum Wankdorf stationiert. Daher ist es notwendig, für die Einrichtung des Hauptspeichers das Rechenzentrum zu besuchen.

Netzwerk

Als nächstes muss das Netzwerk gemäss dem Detailkonzept eingerichtet werden. Dieses dient als Grundlage für die gesamte VDI-Lösung und alle weiteren Komponenten bauen darauf auf. Nachdem die Netzwerkspeicher und Server konfiguriert und im Serverraum eingerichtet wurden, wurden die Switch-Ports definiert. Anschliessend müssen die VLANs auf der Firewall und den Switches erstellt und die definierten Ports entsprechend konfiguriert werden.

Es ist auch notwendig, die Netzwerkkarten bei den XenServer entsprechen einzurichten. Nachdem dies abgeschlossen wurde, kann mit der Erstellung der Firewall-Richtlinien fortgefahren werden. Hierbei ist es wichtig, alle Kommunikationswege zu verstehen und zu berücksichtigen, um die Richtlinien korrekt einzurichten und die richtigen Ports freizuschalten.

Die Kommunikationsgrafik visualisiert dieses gesamte Setup und zeigt, welche Ports und Protokolle für die Kommunikation zwischen den verschiedenen Komponenten der VDI-Umgebung genutzt werden.

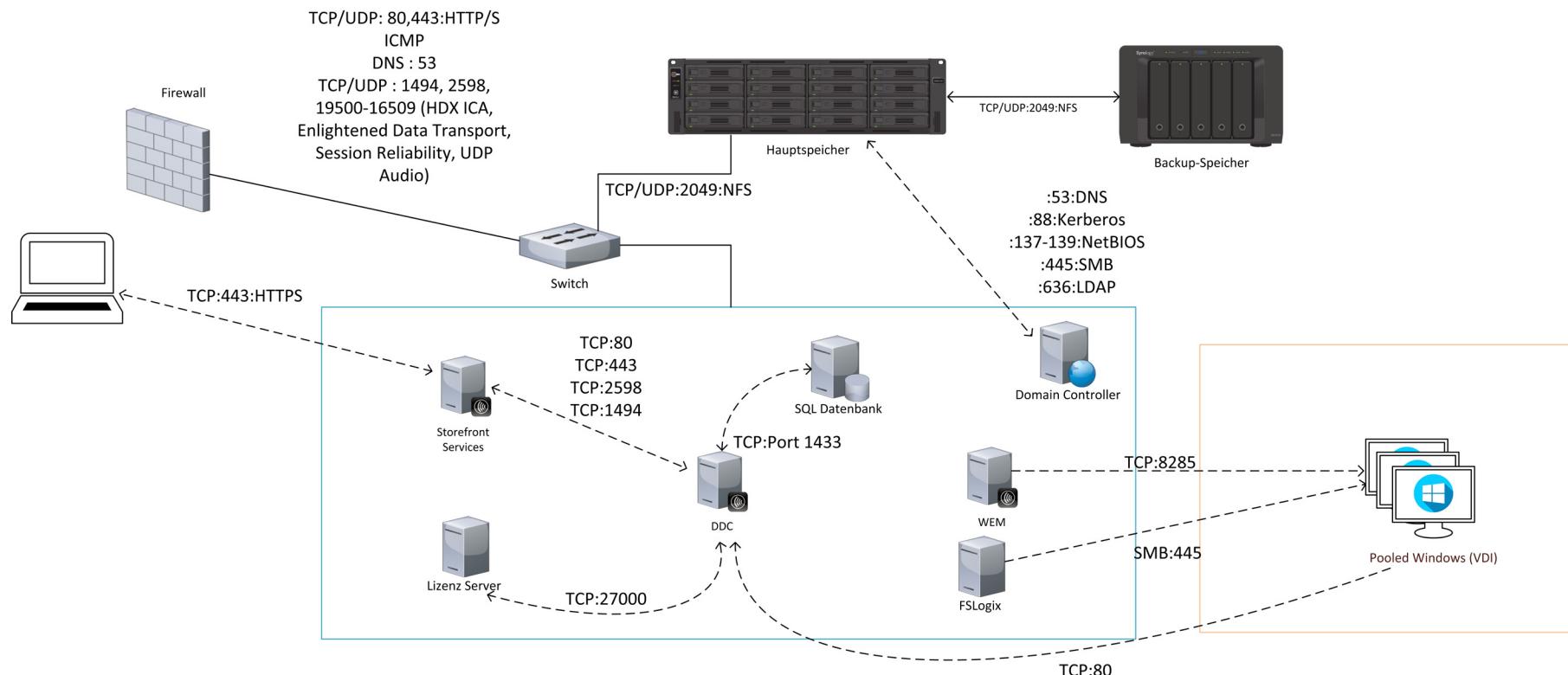


Abbildung 15: Kommunikationsgrafik

Domäne & Dienste

Nachdem der Netzwerkteil abgeschlossen wurde, musste als erstes die neue Domäne gemäss Detailkonzept erstellt werden. Dafür müssen zwei virtuelle Maschinen erstellt werden, die beide als redundante Domain Controller fungieren. Auf den Domain Controllern müssen die Active Directory-Domänendienste installiert und konfiguriert werden.

Die Dienste, die eingerichtet werden müssen, sind DNS für die Namensauflösung, DHCP für die automatische IP-Vergabe und das Active Directory für die Verwaltung der AD-Objekte wie Benutzer und Computer.

Dieser Schritt war an dieser Stelle notwendig, da die virtuellen Maschinen, die für den Citrix-Dienst benötigt werden, in die neu erstellte Domäne eingebunden werden müssen. Dies stellt sicher, dass die Namensauflösung korrekt funktioniert und die Kerberos-Authentifizierung erfolgreich durchgeführt werden kann.

Für mehr Informationen über die Domäne und Serverrollen kann das Kapitel 5 im Detailkonzept, Anhang E1, konsultiert werden.

Citrix Dienste

Nachdem alle Abhängigkeiten eingerichtet wurden, wie die allgemeine Netzwerkinfrastruktur, die Domäne und die Datenbank, kann das Aufsetzen der Citrix-Dienste beginnen. Es müssen alle Citrix-Dienste eingerichtet werden, die im Kapitel 3.1.4 erwähnt sind.

Für eine erfolgreiche Einrichtung dieser Services sollten externe Hilfsmittel wie Video-Tutorials und Best Practices verwendet werden. Sollte es zu Blockaden kommen, sollte möglichst frühzeitig ein Experte einbezogen werden, um keine wertvolle Zeit zu verlieren.

Das Ziel der erfolgreichen Einrichtung aller dieser Dienste ist es, eine Verbindung auf eine VDI über Citrix Workspace zu ermöglichen. Sobald dies erfolgreich umgesetzt wurde, können alle zusätzlichen Funktionen und Anpassungen vorgenommen werden. Diese sind ebenfalls wichtig, da einige davon zu den definierten Anforderungen gehören.

3.2.2 Sicherheitsmaßnahmen

In diesem Abschnitt werden die wesentlichen Sicherheitsmaßnahmen beschrieben, die notwendig sind, um die Integrität, Verfügbarkeit und Vertraulichkeit der VDI-Umgebung zu gewährleisten.

Netzwerk

Es ist von grosser Bedeutung, dass während der Netzwerkumstellung der laufende Betrieb der produktiven Umgebung nicht gestört wird. Um dies zu gewährleisten, wird die umzustellende Planung als Sicherheitsmaßnahme gemeinsam mit dem Netzwerkanbieter der Finitia AG besprochen. Vor jeder Anpassung am Netzwerk werden die beteiligten Parteien informiert, um sicherzustellen, dass keine Änderungen das produktive Netzwerk beeinträchtigen.

Da die Benutzer auch von aussen auf das Netzwerk zugreifen, wird für die VPN-Verbindung eine Zwei-Faktor-Authentifizierung (2FA) eingerichtet, um die Sicherheit bei der Verbindung zu erhöhen. Diese Maßnahme stellt sicher, dass neben dem Passwort eine zusätzliche Sicherheitsebene vorhanden ist, die unbefugten Zugriff verhindert. Die Zwei-Faktor-Authentifizierung erhöht die Sicherheit erheblich, indem sie die Identität des Benutzers durch einen zweiten Faktor, wie einen Code auf dem Mobiltelefon, überprüft.

Redundanz

Als weitere Sicherheitsmaßnahme werden mehrere Server redundant ausgelegt, um die Ausfallsicherheit zu erhöhen. Zu diesen Servern gehören die beiden XenServer sowie die virtuellen Server

für die Domain Controller, Storefront, WEM und DDC. Diese Redundanz stellt sicher, dass im Falle eines Ausfalls eines dieser Server der gesamte Service weiterhin verfügbar bleibt und nicht beeinträchtigt wird.

Backups

Für den Fall eines Datenverlusts durch unbeabsichtigtes Löschen oder eines Hackingangriffs, der die gesamte Anlage verschlüsselt, sind Backups oft das einzige Mittel, um die Daten wiederherzustellen. Deshalb werden täglich Backups vom Hauptspeicher durchgeführt, um diese Sicherheit zu garantieren. Für detailliertere Informationen zu den Backups kann Kapitel 6 im Detailkonzept im Anhang E1 konsultiert werden.

Security und Datenschutz

Es wird grosser Wert auf Sicherheit und Datenschutz gelegt. Mit einem restriktiven Netzwerk, der Datenverschlüsselung des Hauptspeichers und weiteren Massnahmen ist man gut aufgestellt. Es gibt jedoch einige Aspekte, die von den Diplomanden nicht kontrolliert werden können, wie zum Beispiel das Aufnehmen des Bildschirms über ein Smartphone. Da es sich jedoch um Geheimhaltungsprojekte handelt, auf die nur autorisierte Benutzer Zugriff haben, müssen diese Benutzer strikte Richtlinien befolgen. Die Nichteinhaltung dieser Richtlinien kann Konsequenzen für die Projektmitarbeiter haben.

Diese umfassenden Regeln sind entscheidend, um die Integrität und Vertraulichkeit der in der VDI-Umgebung verarbeiteten Informationen zu schützen und Risiken wie Datenlecks oder unautorisierte Zugriffe effektiv zu minimieren.

Um detaillierte Informationen zu diesen Sicherheitsregeln zu erhalten, kann das Kapitel 3.3 im Betriebskonzept konsultiert werden.

3.3 Testverfahren

Als Grundlage für die systematische Überprüfung der VDI-Lösung, nachdem sie implementiert wurde, wurde das Testkonzept erstellt. Dieses umfasst klare Testziele sowie eine strukturierte Übersicht über die Organisation, Planung, Durchführung, Testrahmen und Testinfrastruktur. Die Testziele sind darauf ausgelegt, die funktionalen und nicht funktionalen Anforderungen zu überprüfen.

Die Testziele des Testverfahrens umfassen:

- **IT-Infrastruktur:** Überprüfung der gesamten Infrastruktur, einschliesslich Server und Netzwerk, um sicherzustellen, dass sie funktionsfähig sind und ihre Aufgaben erledigen.
- **Leistung:** Sicherstellung, dass die VDI die erforderliche Leistung für kritische Anwendungen, insbesondere CAD-Programme, bereitstellt.
- **Anpassungsfähigkeit:** Bewertung der Flexibilität der VDI, um Anpassungen wie Ressourcenverteilung und VDI-Images ohne Beeinträchtigung des laufenden Betriebs vorzunehmen.
- **Datensicherheit:** Überprüfung der täglichen Backups, um den Schutz vor Datenverlust zu garantieren.
- **Sicherheitsrichtlinien:** Gewährleistung der Sicherheit durch spezifische Massnahmen, wie die Verhinderung des Internetzugangs über die VDI.

Folgende Test-Etappen wird die VDI-Lösung durchlaufen.



Abbildung 16: Test-Etappen

Die Ziele werden durch spezifisch erstellte Testfälle adressiert, die sicherstellen, dass die VDI-Lösung den Anforderungen entspricht. Alle Anforderungen und Testfälle sind im Kapitel 8 & 9 im Testkonzept beschrieben.

3.4 Betrieb der Lösung

Klare Betriebsprozesse sind essenziell für den reibungslosen Ablauf des Services. Sie gewährleisten eine kontinuierliche, sichere und effiziente Operation der VDI-Lösung. In diesem Abschnitt werden die Schlüsselprozesse beschrieben, aber für detaillierte Informationen zu den Betriebsprozessen kann das Kapitel 3 im Betriebskonzept konsultiert werden.

Support / Wartung

Der Support ist in 1st, 2nd und 3rd Level unterteilt. Anfragen werden je nach Komplexität an den entsprechenden Support-Level weitergeleitet.

Regelmässige Wartungen sichern Betriebssicherheit und Leistung. Wartungsziele umfassen Systemverfügbarkeit, Performance-Optimierung und Sicherheit. Zwei grosse Wartungsfenster pro Jahr sind eingeplant, unterstützt durch monatliche Updates und regelmässige Überprüfungen.

Management Golden Images

Golden Images sind die Grundlage für alle Desktops und werden als VMs erstellt und konfiguriert. Mit der Snapshot-Technologie können verschiedene Versionen erstellt und bei Bedarf wiederhergestellt werden. Regelmässige Sicherungen und Tests durch Pilotnutzer sind notwendig.

Benutzerverwaltung

Der Service kann parallel zur produktiven VDI-Umgebung angeboten werden. Neue Benutzer werden nach Abschluss des Einführungsprozesses und Unterzeichnung der Geheimhaltungsvereinbarungen ins System aufgenommen. Alle Änderungen werden über ein Ticketing-Tool verwaltet.

Projektnotebook

Notebooks für die VDI-Lösung durchlaufen folgende Schritte: Installation von Windows 10 Pro, BIOS-Verschlüsselung, Aktivierung von BitLocker, Installation von EDR-Programmen, Citrix Workspace und VPN-Einrichtung, sowie Zertifikatsinstallation und optional USB-Authentifizierungsschlüssel. Deep Freeze wird eingesetzt, um lokale Daten zu schützen.

4 Realisierungsphase

In diesem Kapitel werden die ausgearbeiteten Lösungen und deren Implementierung sowie die Reihenfolge, in der diese ausgeführt wurden, dargestellt. Ein wesentlicher Bestandteil des Projekts war die Erstellung eines Prototyps, der im Folgenden erläutert wird. Zudem wurden die notwendigen Marketing- und Finanzdokumente wie Factsheet, Service Level Agreement (SLA) und Business Case erstellt. Diese Themen sind nicht im Diplombericht aufgeführt und verweisen dementsprechend auf die nachfolgenden Anhänge E5 (Factsheet), E4 (Betriebskonzept, Kapitel 4 und 5).

Die Testphase des Projekts umfasste mehrere Schritte, die sorgfältig geplant und dokumentiert wurden. Zunächst wurde festgelegt, was getestet werden sollte und welche Tests durchgeführt werden mussten, indem detaillierte Test-Cases erstellt wurden. Die erwarteten Ergebnisse wurden definiert und ein Testbericht für die Durchführung der Tests wurde erstellt. Die Testanordnung sowie das verwendete Test-Equipment wurden vollständig erfasst und aufgelistet, um die Nachvollziehbarkeit der Tests zu gewährleisten. Die detaillierten Testdokumentationen sind hauptsächlich im Anhang E2 und F2 zu finden, in diesem Bericht wird auf die wichtigsten Aspekte der Tests hingewiesen.

Abschliessend sei erwähnt, dass von der gesamten Realisierung ein ausführlicher Arbeitsbericht erstellt wurde, in dem alle wichtigen Schritte der Realisierung dokumentiert sind. Dieser Arbeitsbericht dient als umfassende Dokumentation und Nachschlagewerk die gesamte Realisierung.

4.1 Ausführung

Die Realisierungsphase stellte einen intensiven Prozess dar, der nicht immer reibungslos verlief. Alle wichtigen Schritte der Realisierung sind im Arbeitsbericht, Anhang F1, detailliert beschrieben. In diesem Abschnitt werden die einzelnen Schritte nochmals chronologisch aufgelistet und erläutert.

Da der Arbeitsbericht thematisch sortiert ist und nicht nach der chronologischen Reihenfolge der Erledigung, bietet dieser Diplombericht einen Rückblick auf die Realisierung in einer chronologischen Abfolge der Tätigkeiten. Zudem wird aufgezeigt, an welchen Stellen es zu Schwierigkeiten kam und wie diese bewältigt wurden.

Vorbereitung

Nach der Erstellung der Konzepte war klar, wie das Projekt realisiert werden sollte. Damit die Realisierung erfolgreich starten konnte, mussten noch einige Vorbereitungen und Abklärungen getroffen werden. Diese waren grösstenteils von Aussenstehende abhängig und mussten daher möglichst früh erledigt werden.

Zu den notwendigen Vorbereitungen zählte beispielsweise die Konfiguration des Netzwerks, einschliesslich der Einrichtung der VLANs, das Patchen der Switch-Ports und die Erstellung der Firewall-Regeln. Da diese Aufgaben von einer externen Person durchgeführt werden mussten, war es wichtig, diese frühzeitig zu beantragen. Diese Beantragung wurde noch während der Konzeptphase vorgenommen, um sicherzustellen, dass bei Beginn der Realisierungsphase sofort mit den Arbeiten gestartet werden konnte.

Des Weiteren mussten Abklärungen bezüglich der Verfügbarkeit der benötigten Hardware und der verfügbaren Lizenzen getroffen werden. Durch diese Vorbereitungen wurde sichergestellt, dass alle notwendigen Ressourcen und Konfigurationen rechtzeitig zur Verfügung standen, um einen reibungslosen Start der Realisierung zu gewährleisten.

Einrichtung der Grundinfrastruktur

Die Einrichtung der Grundinfrastruktur stellte zusammen mit der Einrichtung der Citrix-Services einen der grössten Prozesse der Realisierung dar und war mit verschiedenen Schwierigkeiten verbunden. Die Haupttätigkeiten bei der Einrichtung der Grundinfrastruktur umfassten das Einrichten der Hardware sowie die Herstellung der korrekten Kommunikation zwischen den verschiedenen Komponenten.

Bereits beim Zusammenbau des ersten Management-Servers traten mehrere Schwierigkeiten auf. Die Einzelheiten der Probleme und der durchgeführten Troubleshoots können im Arbeitsbericht oder im Logbuch, Anhang H, nachgelesen werden.

Einrichtung Citrix Dienste

Mit der Unterstützung von YouTube-Tutorials konnten die Studenten die meisten Citrix-Services ohne grössere Probleme einrichten. Dennoch gab es aufgrund der Abhängigkeit der Services von mehreren Diensten häufig aufwendige Troubleshoots, da zahlreiche Fehlerquellen überprüft werden mussten. Neben den verschiedenen Diensten spielten auch Faktoren wie Firewall-Regeln und Lizenzen eine Rolle, die häufig zu weiteren Anpassungen führten.

Die Firewall-Regeln mussten aufgrund unzureichender Recherche mehrfach angepasst werden, bis das gewünschte Endergebnis erreicht wurde. Leider verursachten auch die Lizenzen Schwierigkeiten. Aufgrund der Abwesenheit des Citrix-Experten konnten die produktiven Premium-Lizenzen erst sehr spät eingespielt werden, was zu einer Verzögerung der Implementierung führte.

Schlussendlich konnten die zwei Studenten den Service erfolgreich aufbauen, sodass eine Verbindung zum StoreFront über HTTPS im internen Netz hergestellt und eine VDI-Session gestartet werden konnte.

Diverse Konfigurationen

Nach der erfolgreichen Konfiguration des Grundservices mussten darüber hinaus noch viele weitere Dienste und Konfigurationen eingerichtet werden. Einige dieser Konfigurationen wurden in den benötigten Anforderungen spezifiziert, während andere als zusätzliche Schönheitsanpassungen hinzugefügt wurden. Bei diesen Konfigurationen traten weniger Diskrepanzen auf.

Zu den zusätzlichen Diensten und Konfigurationen gehörten unter anderem Backup-Lösungen, Zwei-Faktor-Authentifizierung (2FA), Sicherheitseinstellungen wie das Deaktivieren von Copy-Paste und Screenshots aus VDI-Sessions sowie die Vereinfachung von Adressen durch DNS-Konfigurationen.

Tests

Dank der Vorteile der Partnerarbeit konnten verschiedene Prozesse parallel durchgeführt werden. Während der eine Student an der Umgebung weiterarbeitete, konnten gleichzeitig verschiedene Tests durchgeführt werden. Diese parallele Arbeitsweise ermöglichte eine effizientere Nutzung der verfügbaren Zeit und Ressourcen.

Abschluss

Mit Abschluss der Realisierung konnten die Studenten einen funktionierenden Service aufbauen, auf den sie beide sehr stolz sind. Durch diese praktische Arbeit konnten sie eine Vielzahl an Fähigkeiten und Wissen erwerben. Sie lernten nicht nur die Produktpalette von Citrix und die Aspekte der Virtualisierung kennen, sondern auch Themenbereiche wie Netzwerk, Domänenadministration, Serverhardware, Sicherheit und Wirtschaftlichkeit.

Auch wenn nicht alle Anforderungen vollständig in der Realisierungsphase erfüllt werden konnten, wurde die Realisierung mit der Testphase abgeschlossen. Anschliessend konnte die Einführungsphase eingeleitet werden. In diesem Rahmen wurde eine Demo durchgeführt und das Abnahmeprotokoll vom Auftraggeber genehmigt.

4.2 Prototyp

Mit Abschluss der Realisierung konnte die VDI-Umgebung erfolgreich als Proof of Concept entwickelt werden. Als eine unabhängige Umgebung im produktiven Netzwerk, ausgestattet mit eigenen Domain Controllern, konnten die Studenten einen voll funktionsfähigen VDI-Service aufbauen. Dabei haben sie eine eigene Infrastruktur entworfen und umgesetzt, welche mehrere Hypervisor-Server umfasst, die über XenCenter verwaltet werden können.

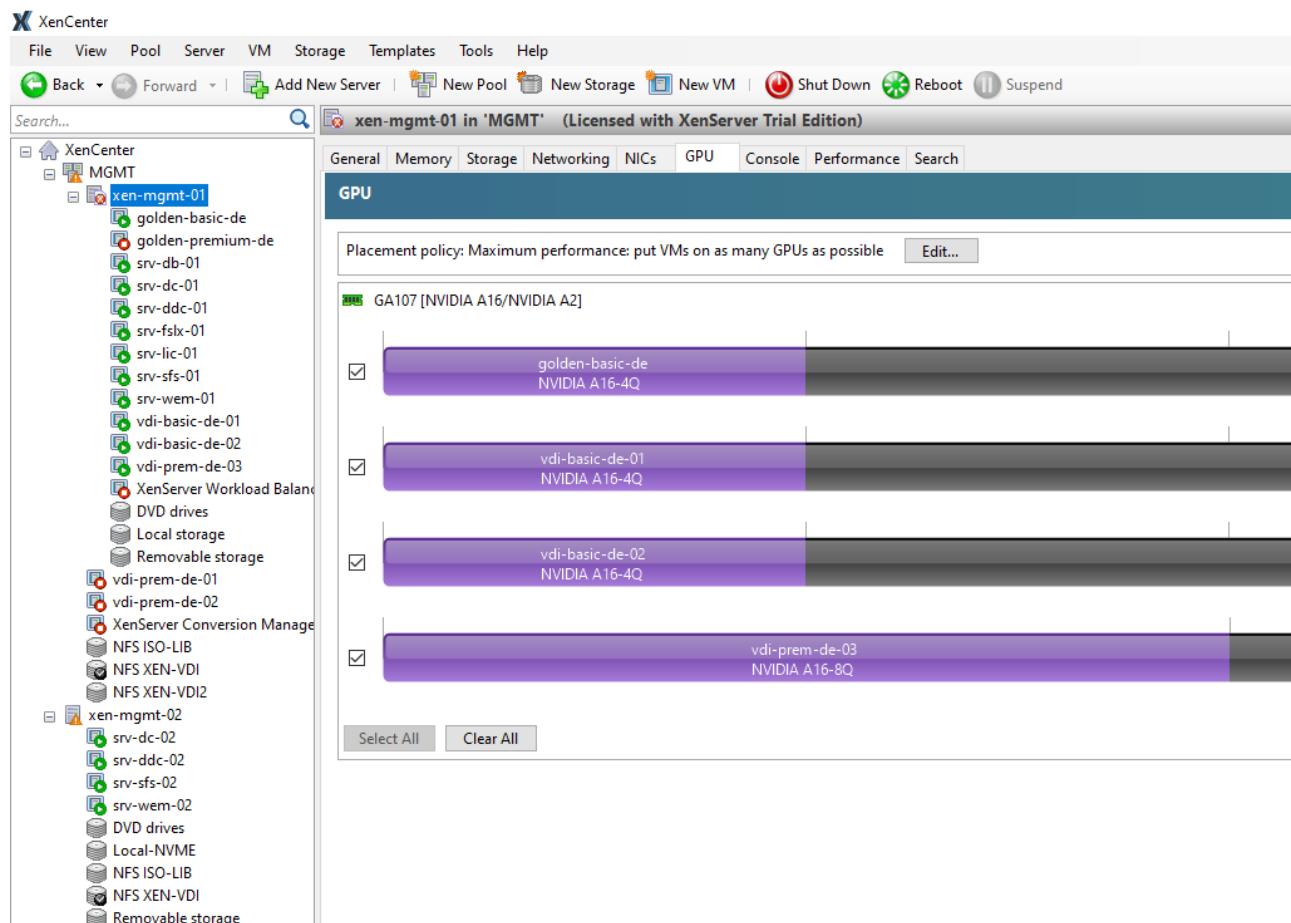


Abbildung 17: XenCenter

Auf diesen Hypervisor-Servern können virtuelle Maschinen erstellt werden, die entweder als virtuelle Server fungieren oder als Golden Image aufgesetzt werden. Diese Golden Images können später auf einem Delivery Controller als VDI bereitgestellt und ausgerollt werden. Die VMs sind auf einem zentralen Hauptspeicher gespeichert, der neben der Lagerung der VMs auch als Datenablage für verschiedene Projekte sowie als Softwareablage für die IT dient.

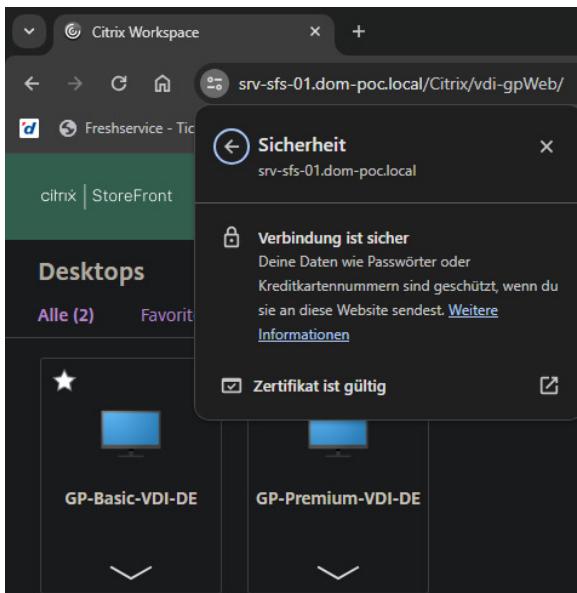


Abbildung 18: Citrix StoreFront Web

Name	Date modified	Type
#recycle	13/05/2024 04:52	File folder
Projekt_xxx1	30/04/2024 09:10	File folder
Projekt_xxxx	30/04/2024 09:09	File folder
Software	22/05/2024 23:52	File folder

Abbildung 19: Datenablage

Der Hauptspeicher ist mit integrierten Backup-Services ausgestattet, einschliesslich Snapshots, Replikationen und Full Backups. Diese Backups ermöglichen es, die verschiedenen Speicherquellen über den Hauptspeicher auf einen standortgetrennten Backup-Speicher zu sichern. Diese Lösung wurde als PoC als vollständig ausreichend empfunden.

Aufgabename	Letzte Sicherung	Status	Versionen
weekly-server-fslogix	Erfolgreich (26.05.2024 02:04:48)	Nächste Sicherung: 02.06.2024 02:00	1
daily-server-fslogix	Erfolgreich (26.05.2024 23:00:24)	Nächste Sicherung: 27.05.2024 23:00	4
Monthly-Server-fslogix	Noch nicht gesichert	Kein Zeitplan	0
Yearly-Server-fslogix	Noch nicht gesichert	Kein Zeitplan	0

Abbildung 20: Synology Active Backup for Business

Alle realisierten Schritte wurden detailliert im Arbeitsbericht, Anhang F1, dokumentiert.

5 Einführungsphase

Die Einführungsphase markiert den Übergang von der Implementierung zur produktiven Nutzung der VDI-Lösung. In dieser Phase werden alle notwendigen Massnahmen getroffen, um die neue Lösung reibungslos in Betrieb nehmen zu können.

5.1 Einführung des Services

Die Einführungsphase ist ein wichtiger Schritt nach der Implementierung der VDI-Lösung. In dieser Phase werden alle notwendigen Massnahmen ergriffen, um die neue Lösung erfolgreich in Betrieb zu nehmen. Ziel ist es, die VDI-Lösung ohne Unterbrechungen des laufenden Betriebs einzuführen.

Um den Service korrekt einzuführen, werden Pilotbenutzer ausgewählt, die die VDI-Lösung anhand der erstellten Benutzeranleitung nutzen sollen. Basierend auf ihren Rückmeldungen, den Testergebnissen, dem Abnahmeprotokoll und dem Projektcontrolling, das im nächsten Unterkapitel erläutert wird, besprechen die Projektleiter gemeinsam mit dem Auftraggeber, ob diese Lösung effektiv umgesetzt werden sollte. Nach der Bestätigung durch den Auftraggeber kann die neue Lösung implementiert werden.

Um Unterbrechungen für die Benutzer zu vermeiden, sollte die Umstellung in einem kontinuierlichen Prozess erfolgen. Alle Benutzerkonten mit den jeweiligen Berechtigungen sollten im Voraus erstellt werden und die Benutzer sollten ihre Zugangsdaten sowie Benutzeranleitung rechtzeitig erhalten.

Da die Daten von der alten Lösung auf dem NAS gespeichert sind und auf den neuen Hauptspeicher migriert werden, dürfen beide Systeme nicht parallel laufen. Andernfalls besteht die Gefahr, dass zwei unterschiedliche Versionen der Daten entstehen, falls jemand weiterhin auf der alten Umgebung arbeiten würde. Daher ist es wichtig, dass die Benutzer richtig informiert werden und das alte NAS zur IT-Abteilung gebracht wird, damit die Daten nach der Migration gelöscht werden können.

5.2 Projektcontrolling / Wirtschaftlichkeit

In diesem Abschnitt wird aufgezeigt, wie die tatsächlichen Kosten nach Abschluss des Projekts ausgefallen sind und ob es Diskrepanzen zur ursprünglichen Budgetplanung gab. Die detaillierte Budgetplanung befindet sich zum einen in der Studie im Anhang B2, Kapitel 6 und zum anderen im Betriebskonzept im Anhang E4, Kapitel 4.

Tatsächliche Kosten

Die tatsächlichen Kosten weichen nicht stark vom geplanten Budget ab. Es gibt Ressourcen, die nicht eingesetzt wurden und eine neue Ressource, die hinzugekommen ist, aber diese führen zu keinen Änderungen bei den Sachmittelkosten. Der XenServer, der nicht eingesetzt wurde, wird in Zukunft eingerichtet, wenn er in der produktiven Umgebung nicht mehr benötigt wird. Der Desktop-PC, der als redundanter XenServer dient, verursacht keine zusätzlichen Kosten, da es sich um einen bereits vorhandenen und nicht genutzten PC der Firma handelt.

Die angefallenen Kosten entsprechen nicht vollständig dem eingeplanten Budget, da sich der Personalaufwand geändert hat. Die ursprünglich geplanten 499 Stunden wurden um 11 Stunden auf insgesamt 510 Stunden überschritten.

Die Kosten für den Personalaufwand belaufen sich daher auf 17'850 CHF anstatt der vorgesehenen 17'465 CHF, was eine Überschreitung von 385 CHF bedeutet. Um das Projekt vollständig abzuschliessen und alle Anforderungen zu erfüllen, die während dieser Diplomarbeit gestellt wurden, würde der Aufwand weiter steigen.

Alle anderen Kosten wie Anschaffungskosten, Betriebskosten und Schulungskosten sind gleichgeblieben und entsprechen dem ursprünglichen Budget.

Abschliessende wirtschaftliche Betrachtung

Aus wirtschaftlicher Sicht kann die Lösung umgesetzt werden. Trotz der Überschreitung der geplanten Stunden bleibt die wirtschaftliche Machbarkeit der Lösung. Die zusätzlichen Kosten durch den erhöhten Personalaufwand sind überschaubar und können durch die langfristigen Vorteile und Effizienzsteigerungen, die die VDI-Lösung bietet, gerechtfertigt werden. Abgesehen davon sind alle anderen Kosten nach der Realisierung gleichgeblieben.

Wenn das Projekt jedoch anders als in dieser PoC-Umgebung vollständig mit kompletter Ausfallsicherheit aller Komponenten eingerichtet werden soll, würden die Kosten deutlich höher ausfallen als die im PoC angefallenen. Es müssten diverse Hardwarekomponenten redundant ausgelegt werden und dafür müsste man diese erst noch beschaffen. Dazu gehören ein zweiter VDI XenServer oder Netzwerkkarten, um die Netzwerkverbindung der physischen Server redundant auszulegen. Es gibt auch einige virtuelle Server in der PoC-Lösung, die nicht redundant ausgelegt wurden und diese müssten ebenfalls redundant ausgelegt werden. Dementsprechend würden nicht nur die Sachmittelkosten steigen, sondern auch der Personalaufwand.

Zusammenfassend lässt sich sagen, dass die tatsächlichen Kosten im Rahmen des Budgets geblieben sind und die Investition in die VDI-Lösung wirtschaftlich sinnvoll ist. Die Lösung bietet eine erhöhte Effizienz, Flexibilität und Sicherheit im Betrieb. Wenn jedoch eine vollständige Ausfallsicherheit gefordert ist, müssen die zusätzlichen Kosten für die redundante Auslegung der Komponenten und den erhöhten Personalaufwand berücksichtigt werden.

6 Schlussbetrachtung

Die Diplomarbeit ist abgeschlossen, und die VDI-Lösung ist funktionsfähig und stellt einen überzeugenden Proof of Concept dar, der den gestellten Anforderungen gerecht wird. Dieses umfangreiche Projekt deckte verschiedene Aspekte wie Netzwerk, Server, Virtualisierung, Backups und viele weitere Bereiche ab. Während der Diplomarbeit gab es Höhen und Tiefen: Einige Dinge funktionierten problemlos, während andere viel Zeit und Mühe zur Lösung erforderten. Insgesamt war es jedoch ein erfolgreiches und lehrreiches Projekt.

Ein besonderer Aspekt dieses Projekts und auch der persönliche Beitrag der Diplomanden ist die Entwicklung einer einzigartigen VDI-Lösung, die speziell für Geheimhaltungsprojekte entworfen und realisiert wurde. Diese Lösung wurde genau auf die Probleme der aktuellen Umgebung zugeschnitten. Die Studenten hatten die komplette Freiheit, eine eigenständige Umgebung zu gestalten und zu realisieren, und zwar übergreifend über die verschiedenen Bereiche, wie oben erwähnt.

Ob dieses Projekt nun tatsächlich als Lösung von der IT an die Kunden der Finitia AG vorgestellt wird, hängt vom Auftraggeber und der Nachfrage nach einer flexiblen, sicheren VDI-Umgebung ab. Es ist jedoch nun bewiesen, dass die Realisierung eines solchen Projekts nach gründlicher Planung möglich ist. Durch die bereits vorhandene Verwendung solcher VDIs in der produktiven Umgebung wird das Potenzial als praktikable Arbeitsumgebung bestätigt. Dieses Projekt ist jedoch noch lange nicht vollständig und perfekt. Es gibt viele Anpassungen und Optimierungen, die vorgenommen werden könnten, um die Sicherheit, Verfügbarkeit und Effizienz weiter zu verbessern. Aufgrund des zeitlichen Rahmens und der Kosten dieses Projekts war es jedoch nicht möglich, alle möglichen Verbesserungen umzusetzen.

Es gab immer wieder fachliche Diskussionen mit dem internen Experten, bei denen Themen wie Sicherheit und Verfügbarkeit der zukünftigen Umgebung erörtert wurden und welche zusätzlichen Massnahmen realisiert werden könnten. Die Studenten mussten diese Ideen jedoch bremsen, da diese Anpassungen nicht im zeitlichen Rahmen durchgeführt werden konnten. Schlussendlich kann diese Lösung als Vorschlag und Machbarkeitsstudie beim nächsten Projekt vorgestellt werden. Ob diese Lösung angenommen wird, ist noch ungewiss. Abschliessend kann man sagen, dass dieses Projekt einen grossen Einfluss auf die Entwicklung solcher VDI-Umgebungen in zukünftigen Projekten haben wird.

6.1 Reflexion

Zu Beginn des Projekts herrschte eine gewisse Unsicherheit, da die Diplomanden nicht sicher waren, ob die geplante Zeit ausreichen würde. Spätestens mit Beginn der Realisierung merkten sie jedoch, dass es umsetzbar sein würde. Die Diplomanden sind sehr stolz auf die geleistete Arbeit und das Endergebnis.

Rückblickend gibt es immer einige Aspekte, die man hätte besser machen können, insbesondere in Bezug auf den Überblick, da während des Projekts neue Aufgaben hinzukamen oder zusätzliche Aspekte berücksichtigt werden mussten. Durch die breitgefächerten Themenbereiche wäre es umso wichtiger gewesen, die Abgrenzungen genauer zu definieren.

Die Freiheiten und die eher groben Anforderungen führten dazu, dass unzählige Erweiterungen vorgenommen werden konnten, um diese Anforderungen zu erfüllen, was viel Zeit in Anspruch nahm. Diese Anforderungen hätten genauer definiert werden sollen und mit weniger Muss-Kriterien. Damit haben sich die Studenten ein wenig selbst ein Bein gestellt, obwohl sie explizit darauf hingewiesen wurden, wenige Muss-Kriterien zu wählen.

Ausserdem gab es zu viele Abhängigkeiten, die sich immer wieder als Hindernisse darstellten, die entweder das geplante Vorgehen verhinderten oder zu Zeitverschiebungen führten. Beim nächsten Projekt müssen solche Abklärungen intensiver durchgeführt werden.

Abklärungen und Diskussionen wurden mehrheitlich nur mündlich geführt, was bei der Dokumentation verloren gehen könnte. Daher wäre es von Vorteil, solche Abklärungen schriftlich festzuhalten, um sicherzustellen, dass alle wichtigen Informationen und Entscheidungen dokumentiert und nachverfolgt werden können. Das Projekt verlief nicht perfekt, was jedoch normal ist; das Wichtigste ist, dass Erfahrungen gesammelt werden konnten.

Dieses Projekt hat gezeigt, dass durch Engagement und Durchhaltevermögen auch komplexe Herausforderungen gemeistert werden können. Die Diplomanden haben nicht nur ihre technischen Fähigkeiten weiterentwickelt, sondern auch gelernt, wie wichtig Planung, Kommunikation und Problemlösungsfähigkeiten in einem Projekt sind.

6.2 Dank

An dieser Stelle möchten sich die Diplomanden bei der Firma Finitia AG und dem IT-Leiter Micha Bucher für die Bereitstellung der Ressourcen und die Nutzung der Einrichtungen für die Diplomarbeit bedanken. Ein besonderer Dank gilt den beiden externen Experten und dem Netzwerkdienstleister, die bei Fragen oder Unklarheiten zur Verfügung standen. Zudem geht auch ein Dankeschön an die Betreuer der Diplomarbeit Thomas Staub und Tenzin Langdun, die bei Unklarheiten zum Diplomprozess weiterhelfen konnten.

6.3 Urheberrecht

Da in dieser Diplomarbeit vertrauliche Informationen der Firma Finitia AG verwendet werden, unterliegt sie dem Urheberrecht. Jegliche Veröffentlichung oder Vervielfältigung dieser Arbeit ist ohne ausdrückliche vorherige schriftliche Genehmigung der Verfasser nicht gestattet.

7 Authentizität

Mit unseren Unterschriften bestätigen wir, die vorliegende Diplomarbeit selbstständig, ohne Hilfe Dritter und nur unter Benutzung der angegebenen Quellen ohne Copyright-Verletzung, erstellt zu haben.

Ort / Datum

31.05.2024

Unterschrift

Shipinyuan Su

Shipinyuan Su

Ort / Datum

31.05.2024

Unterschrift

Sirak Yosef

Sirak Yosef

8 Anhang

Im folgenden Anhang sind sämtliche Dokumente aufgeführt, die im Rahmen dieser Diplomarbeit erstellt wurden. Die Dokumente sind alphabetisch und farblich voneinander getrennt, um eine bessere Übersichtlichkeit zu gewährleisten. Diese Materialien stellen eine bedeutende Ergänzung zum Diplombericht dar und bieten einen detaillierten Einblick in die Arbeit sowie die erzielten Ergebnisse.

Anhang A

8.1 Quellenverzeichnis

- Digicomp. (25. 03 2024). *Digicomp*. Abgerufen am 25. 03 2024 von
<https://www.digicomp.ch/weiterbildung-it-provider/citrix/kurs-citrix-virtual-apps-and-desktops-7-administration-on-premises-and-in-citrix-cloud-cws-215>
- Digicomp. (25. 03 2024). *Digicomp*. Abgerufen am 25. 03 2024 von
<https://www.digicomp.ch/weiterbildung-microsoft-technology/microsoft-azure/kurs-configuring-and-operating-microsoft-azure-virtual-desktop-intensive-training-az-140>
- Digicomp. (25. 03 2024). *Digicomp*. Abgerufen am 25. 03 2024 von
<https://www.digicomp.ch/weiterbildung-it-provider/vmware/end-user-computing/kurs-vmware-horizon-deploy-and-manage-v8-8>
- Ostler, U. (06. 12 2011). *Datacenter-insider*. Abgerufen am 12. 04 2024 von Datacenter-insider:
<https://www.datacenter-insider.de/von-tier1-bis-tier-4-die-vier-qualitaetsstufen-eines-rechenzentrums-a-341120/>
- Schrader, T. (11. 08 2022). *Scribbr*. Abgerufen am 20. 05 2024 von Scribbr:
<https://www.scribbr.ch/hausarbeit-ch/gender-hinweis-hausarbeit-vorlage/>
- Staff, C. (10. 11 2022). *Citrix Docs*. Abgerufen am 15. 04 2024 von Citrix Docs:
<https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/1912-ltsr/system-requirements.html>
- Wang, B. (08. 06 2023). *Citrix Docs*. Abgerufen am 12. 04 2024 von Citrix Docs:
<https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/technical-overview.html>

8.2 Abbildungsverzeichnis

Abbildung 1: Ausgangslage IST/SOLL.....	7
Abbildung 2: Projektorganigramm.....	10
Abbildung 3: Datenmanagement - Struktur.....	11
Abbildung 4: Datenmanagement – Backup	12
Abbildung 5: Projektübersicht.....	12
Abbildung 6: Projektabgrenzung.....	19
Abbildung 7: NAS in Lugano	21
Abbildung 8: Arbeitsmaterialschrank in Lugano.....	21
Abbildung 9: Arbeitsplatz in Lugano.....	22
Abbildung 10: Sachmittel vom Auftraggeber.....	22
Abbildung 11: VMware Lösung grafisch.....	28
Abbildung 12: Citrix Lösung grafisch.....	29
Abbildung 13: MS AVD Lösung grafisch	29
Abbildung 14: Lösungsarchitektur.....	39
Abbildung 15: Kommunikationsgrafik	45
Abbildung 16: Test-Etappen	48
Abbildung 17: XenCenter	51
Abbildung 18: Citrix StoreFront Web.....	52
Abbildung 19: Datenablage	52
Abbildung 20: Synology Active Backup for Business	52

8.3 Tabellenverzeichnis

Tabelle 1: Initialisierung - Projektziele.....	8
Tabelle 2: Ziele der Initialisierung	9
Tabelle 3: Kommunikation.....	11
Tabelle 4: IST / SOLL Verschiebungen.....	13
Tabelle 5: Personalaufwand.....	15
Tabelle 6: Materialkosten VDI-Server.....	16
Tabelle 7: Materialkosten MGMT-Server.....	16
Tabelle 8: Materialkosten Hauptspeicher	17
Tabelle 9: Materialkosten Testnotebooks	17
Tabelle 10: Risikobewertung Initialisierung.....	18
Tabelle 11: Risikobewertung Migration	18
Tabelle 12: Risikomatrix Migration	19
Tabelle 13: User Stories.....	24
Tabelle 14: Funktionale Anforderungen	26
Tabelle 15: Nicht funktionale Anforderungen.....	27
Tabelle 16: Eigenschaften der Lösungsvarianten	28
Tabelle 17: SWOT-Analyse	30
Tabelle 18: Kriterien der Nutzwertanalyse.....	31
Tabelle 19: Gewichtung der Kriterien.....	32
Tabelle 20: Bewertung der Kriterien.....	34
Tabelle 21: Ergebnisse der Nutzwertanalyse.....	35
Tabelle 22: Investitionskosten	37
Tabelle 23: Laufende Kosten.....	37
Tabelle 24: Nutzungsdauer auf 5 Jahre	38
Tabelle 25: Hardwarekomponente	41
Tabelle 26: Softwaredienste	41

Anhang B1



Projektinitialisierungsauftrag

VDI as a Service

Auftraggeber	Micha Bucher
Projektleiter	Shipinyuan Su, Sirak Yosef
Autor	Shipinyuan Su, Sirak Yosef
Klassifizierung	Intern
Status	Abgegeben

Änderungsverzeichnis

Datum	Version	Änderung	Autor
11.12.2023	0.1	Dokument erstellt	Shipinyuan Su, Sirak Yosef
12.12.2023	1.0	Fertigstellung Kapiteln	Shipinyuan Su, Sirak Yosef
16.12.2023	1.1	Eintrag Experte & Korrektur	Shipinyuan Su, Sirak Yosef
15.02.2024	1.2	Bearbeitung Projektziele, Ergänzung der Projektorganisation	Shipinyuan Su, Sirak Yosef
21.02.2024	1.3	Anpassung nach Kick-Off Meeting: Ausgangslage und Projektziele	Shipinyuan Su, Sirak Yosef

Tabelle 1: Änderungsverzeichnis

Inhaltsverzeichnis

1	Ausgangslage.....	3
2	Projektziele	5
3	Projektorganisation	7
4	Lieferobjekte	8
5	Rahmenbedingungen	9
6	Kommunikation	10
7	Projektplan.....	10
8	Termine	12
9	Kosten	12
10	Ressourcen	12
11	Risiken	13
12	Projektabgrenzung	14
13	Abbildungsverzeichnis.....	15
14	Tabellenverzeichnis.....	15

1 Ausgangslage

Wir befinden uns in einer Zeit, in der die Arbeitswelt einem rapiden Wandel unterzogen ist. Dies betrifft besonders unser Unternehmen, das eine breite Kundenbasis von Architekten und Ingenieuren in verschiedenen Teilen der Schweiz bedient. Die Herausforderungen und Veränderungen können wie folgt zusammengefasst werden:

Zunahme von Homeoffice und flexibler Arbeit: Durch die Covid-Pandemie hat sich der Trend zu Homeoffice und flexibler Arbeitsgestaltung verstärkt. Unsere Kunden haben sich zunehmend an diese neue Arbeitsweise gewöhnt und erwarten nun flexible Arbeitsmodelle.

Standortunabhängigkeit: Die geographische Verteilung unserer Kunden erfordert eine Lösung, die es ermöglicht, effizient und effektiv von verschiedenen Orten aus zu arbeiten. Dies gilt sowohl für unsere internen Teams als auch für die Interaktion mit unseren Kunden.

Erhaltung der Arbeitsperformance: Trotz der Notwendigkeit flexibler und ortsunabhängiger Arbeitsmodelle ist es entscheidend, dass die Arbeitseffizienz und -qualität nicht leidet. Unsere Kunden benötigen Zugang zu leistungsfähigen Werkzeugen und Ressourcen, unabhängig von ihrem physischen Standort.

Diese Ausgangslage bildet die Grundlage für unsere aktuelle Diplomarbeit, bei dem es darum geht, die Arbeitsweise unseres Unternehmens und unserer Kunden in dieser neuen, flexiblen Arbeitswelt zu unterstützen.

Um diese Bedürfnisse zu befriedigen hat unser Unternehmen die Nutzung von Virtual Desktop Infrastruktur integriert als zentrales Element unserer IT-Strategie. Mit unserer Diplomarbeit wollen wir ein spezifischer Anwendungsfall untersuchen und lösen. Es bezieht sich auf die Handhabung von sensiblen Projekten, die unter einer Geheimhaltung stehen. Unsere Arbeit ziel darauf ab, eine Lösung zu entwickeln, die es ermöglicht, die Vorteile von VDI unter Berücksichtigung der Sicherheitsanforderungen zu nutzen. Hierbei konzentrieren wir uns darauf, wie VDIs so konfiguriert werden können, dass sie eine sichere, isolierte Arbeitsumgebung für Projekte unter Geheimhaltung bieten, ohne dass die Mitarbeitenden auf die Vorteile des flexiblen und standortunabhängigen Arbeitens verzichten müssen.

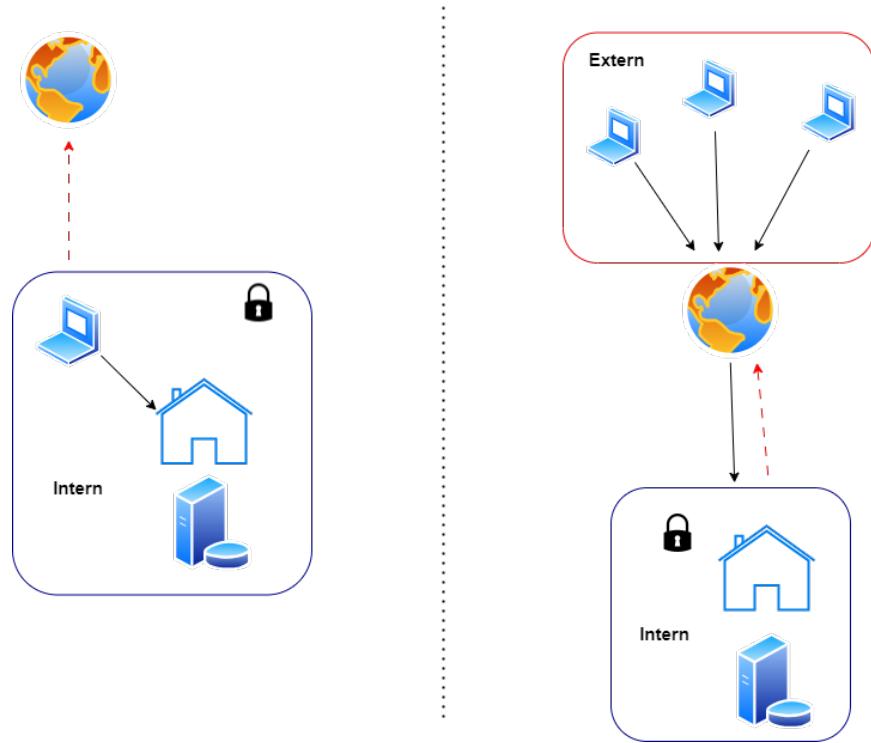


Abbildung 1: Grafik IST/SOLL

Ein aktuelles Beispiel ist ein Projekt in Lugano, welches unter Geheimhaltung steht. Die Mitarbeitende arbeiten an einem temporären Arbeitsplatz in einem Lager mit einem Notebook, welches nicht mit dem Internet verbunden ist. Bearbeitete Dateien werden auf einen lokalen Network Attached Storage (NAS) gespeichert. Diese Arbeitsweise ist nicht mehr zeitgemäß, um die aktuellen Anforderungen und Bedürfnisse gerecht zu werden.

2 Projektziele

Folgende Projektziele müssen erreicht werden:

Nr.	Kategorie	Beschreibung	Messgrösse	Priorität
1	Lieferobjekt	Implementierung einer VDI (Virtual Desktop Infrastructure) -Lösung als PoC, um flexibles Arbeiten zu ermöglichen	Externes verbinden auf die VDI ist möglich	M
2	Betriebliches Ziel	Gewährleistung der kontinuierlichen Verfügbarkeit der VDI-Lösung, durch strategische Lösungen wie Instant Clones oder Redundanz	Uptime der VDI-Lösung in Prozent in Vergleich zur üblichen Lösung	1
3	Technisches Ziel	Implementierung einer VDI-Umgebung, die plattformübergreifend kompatibel ist und die Nutzung auf verschiedenen Geräten, einschliesslich auch Smartphones und Tablets, ermöglicht	Prüfung des Abnahmeprotokolls	1
4	Technisches Ziel	Durch den Einsatz von VDI soll ermöglicht werden, dass auch auf weniger leistungsfähigen Geräten mit hoher Rechenleistung gearbeitet werden kann. Mit der Voraussetzung einer stabilen Internetverbindung.	Zugriffszeiten auf CAD-Programmen: Zeitmessen vom aufstarten von Programmen und öffnen von Dateien sowie das Bearbeiten von Elementen Nutzererfahrung und Reaktionszeit: Feedback von Testusern	1
5	Leistungsziel	Effiziente und qualitative Leistung von überall	Kein Defizit der Arbeitseffizienz und -qualität, solange eine stabile Internetverbindung vorhanden ist, im Vergleich zu einem PC	1
6	Betriebliches Ziel	Implementierung einer Lösung, die während der Einführungsphase minimale Auswirkungen auf den IT-Betrieb hat	Anzahl Ausfällen und Wartungsarbeiten, die passieren oder gemacht werden müssen während der Implementierung	2
7	Betriebliches Ziel	Reduzierung der Dauer und Erhöhung der Effizienz von Wartungsarbeiten und Änderungsprozesse im IT-Betrieb	Reduzierung der Anzahl Stunden die benötigt werden für einen Change. Analyse der Wiederherstellungszeit des Service	2
8	Technisches Ziel	Projektdaten sind für aussenstehende nicht erreichbar	Daten können nur von bestimmten Personen zugegriffen werden. Es werden mehr als zwei verschiedene Sicherheitsstandards verwendet	M

Priorität: M = Muss / 1 = hoch, 2 = mittel, 3 = tief

Tabelle 2: Projektziele

Folgende Ziele sind die Vorgaben für die Phase Initialisierung:

Nr.	Kategorie	Beschreibung	Messgrösse	Priorität
1	Technisches Ziel	Auswahl und Bewertung geeigneter VDI-Anbieter	Erstellung einer Evaluation der verschiedenen Anbieter	1
2	Technisches Ziel	Definition der technischen Anforderungen für die VDI-Lösung	Fertiggestelltes Anforderungsdokument	1
3	Lieferobjekt	Entwicklung eines zeitlich passenden Projektplans	Fertigstellung und Genehmigung des Projektplans	M
4	Lieferobjekt	Sicherstellung der Finanzierung und Ressourcen für das Projekt	Genehmigung des Projektbudgets	M
Priorität: M = Muss / 1 = hoch, 2 = mittel, 3 = tief				

Tabelle 3: Ziele Initialisierungsphase

3 Projektorganisation

Das folgende Organigramm stellt die Organisationsstruktur der Diplomarbeit dar. Es zeigt sowohl die internen als auch die externen Experten, die das gesamte Projekt betreuen. Ebenfalls abgebildet ist der Auftraggeber Micha Bucher, der uns sämtliche Hardware-Ressourcen zur Verfügung stellt. Wir führen das Projekt aus und fungieren auch als Projektleiter.

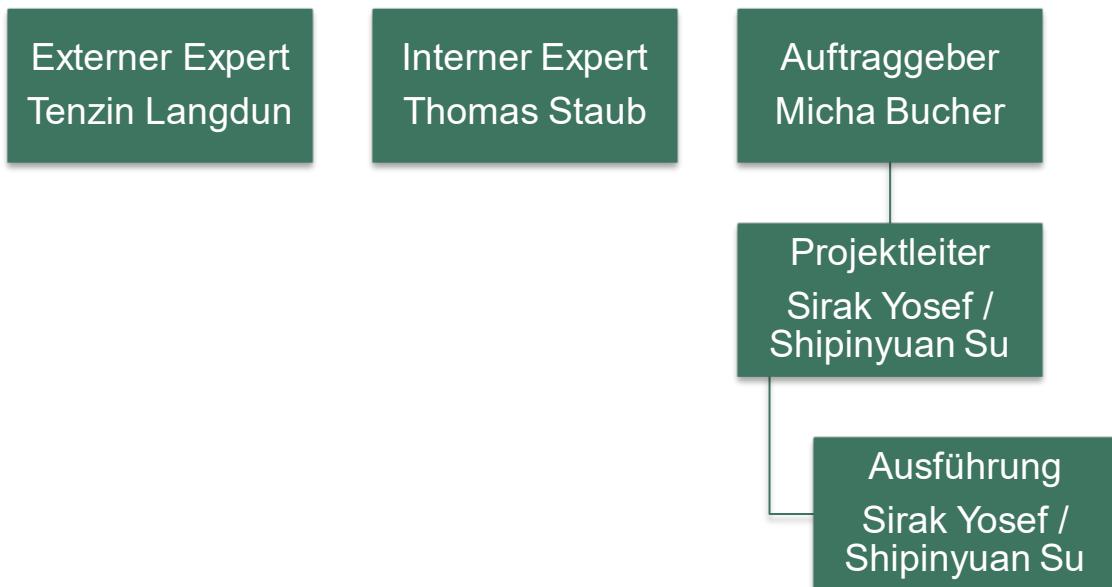


Abbildung 2: Projektorganisation

4 Lieferobjekte

In der folgenden Tabelle wird aufgezeigt, welche Ergebnisse zu jeder Phase während der Diplomarbeit erarbeite werden.

Phase	Lieferobjekte
Initialisierung	<ul style="list-style-type: none">• Projektplan• Präsentation für Kick-off-Meeting• Projektinitialisierungsauftrag• Studie• Projektauftrag
Konzept	<ul style="list-style-type: none">• Detailkonzept• Testkonzept• Migrationskonzept• Betriebskonzept• Präsentation mit den wichtigsten Phasenergebnissen
Realisierung & Einführung	<ul style="list-style-type: none">• Testbericht• Arbeitsprotokoll• Schriftliche Auswertung vom Feedback der Pilotbenutzer• Schulung• Anleitung• Endabnahme
Abschluss	<ul style="list-style-type: none">• Finaler Abschluss der Aufwand und Kostenberechnungen• Abschlussbericht• Präsentation

Tabelle 4: Lieferobjekte

5 Rahmenbedingungen

In der Diplomarbeit wurden folgende Rahmenbedingungen definiert.

- Anwendung von HERMES Projektmethodik
- Verantwortlichkeiten, Rollen und Kommunikationskanäle definieren
- Definition des Projekts mit Zielen, Umfang und Vorgehen
- Erstellung eines detaillierten Projektplans, welche alle Aktivitäten und Termine aufzeigt
- Projekt wird gemäss den Vorgaben zur Diplomarbeit von der Telematik Schule Bern (TSBE) durchgeführt
- Änderungen im Projekt werden dem Auftraggeber und den Experten kommuniziert

Vorbehalte/Rahmenbedingungen von Prüfungskommission 18.01.2024:

- Überarbeitung der Projektziele, um Nutzen des Services besser und messbar aufzuzeigen
- In der Studie muss ein Vergleich einer eigenen entwickelten VDI-Lösung vs. Dem MS Azure VDI Service enthalten
- Der Betrieb der Lösung muss definiert und im PoC umgesetzt werden
- Es muss ein Marketing Factsheet inclusive Service SLA und Berechnung der Abopreise erstellt werden
- Es muss aufgezeigt werden wie viele Produkte/Services verkauft werden müssen, um den Break-Even für die Amortisation der Produktentwicklung zu haben (ROI)

6 Kommunikation

Um eine effektive Kommunikation mit den Experten und dem Auftraggeber zu gewährleisten, wurden spezifische Kommunikationskanäle festgelegt, die in der nachfolgenden Tabelle aufgeführt sind.

Adressat der Information	Verantwortlich für die Kommunikation	Inhalt	Ziel	Mittel / Medium	Termin
Interner Expert Thomas Staub	Projektmitarbeiter	Monatlicher Statusbericht	Vorschritt des Projekts an Expert kommunizieren mit Aussage zu Termin, Kosten	Status Report	Alle zwei Wochen
Externer Expert Tenzin Langdun	Projektmitarbeiter	Monatlicher Statusbericht	Vorschritt des Projekts an Expert kommunizieren mit Aussage zu Termin, Kosten	Status Report	Alle zwei Wochen
Auftraggeber Micha Bucher	Projektmitarbeiter	Ziel und Planung der Projektinitialisierung	Die Abteilung kennt das Vorgehen und die Termine	Meeting	Wöchentlich

Tabelle 5: Kommunikation

7 Projektplan

Im Folgenden ist eine Übersicht der Diplomarbeit sowie der wichtigsten Arbeitspakete dargestellt. Die Diplomarbeit wird mithilfe der Projektmethode Hermes 5.1 durchgeführt. Rote Punkte markieren die Meilensteine, darunter ein Meilenstein für das Kickoff-Meeting, ein weiterer für das Zwischenmeeting nach der Initialisierungsphase und schliesslich ein Meilenstein für das Abschlussmeeting. Ziel ist es, die Diplomarbeit zwei Wochen vor der Deadline fertigzustellen, um einen Zeitpuffer von zwei Wochen zu haben.

Die Arbeitspakete und Termine sind in dem Zeitplan (ist im Anhang) genauer definiert.

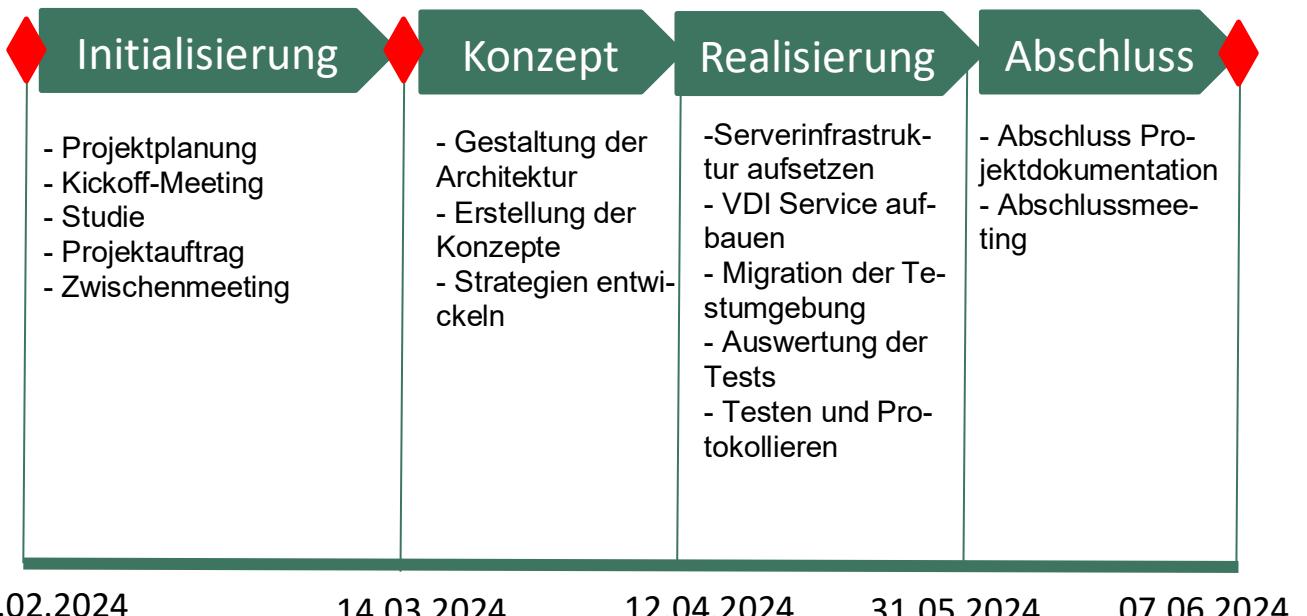


Abbildung 3: Projektübersicht

8 Termine

Die folgenden Lieferergebnisse werden in der Phase Initialisierung erstellt.

Nr.	Ergebnis	Termin
1	<i>Projektplan</i>	11.02.2024
2	<i>Studie</i>	03.03.2024
3	<i>Projektauftrag</i>	10.03.2024

Tabelle 6: Termine Initialisierungsphase

9 Kosten

Der geschätzte interne Personalaufwand für die Initialisierungsphase beläuft sich auf etwa 5'600 CHF. Diese Schätzung basiert auf einem durchschnittlichen internen Stundensatz von 35 CHF. Weitere Details zu den Personalkosten und den Sachkosten für das gesamte Projekt finden sich in der Studie.

Phase	Geplant
Initialisierung	5'600sFr

Tabelle 7: Kosten

10 Ressourcen

In diesem Kapitel werden die für die Initialisierungsphase benötigten Personal- und Sachressourcen beschrieben.

Personalressourcen

Rolle / Person	Februar	März	April	Total	Bestätigung Vorgesetzter
Shipinyuan Su	20h	30h	30h	80h	Erteilt
Sirak Yosef	20h	30h	30h	80h	Erteilt
Diverse	0h	0h	0h	0h	

Tabelle 8: Personalressourcen

Sachmittel

Es besteht für die Initialisierungsphase kein Bedarf an materiellen Ressourcen wie Räumlichkeiten, IT-Infrastruktur, spezialisierter Software und ähnlichen, die zusätzliche externe Kosten verursachen würden.

11 Risiken

Die nachfolgende Tabelle bietet eine Risikoanalyse potenzieller Risiken, die während der Initialisierungsphase auftreten könnten. Sie beinhaltet eine Einschätzung der Eintrittswahrscheinlichkeit und des Auswirkungsgrads jedes identifizierten Risikos. Dies ermöglicht es uns, präventive Massnahmen festzulegen, um mögliche Hindernisse frühzeitig zu erkennen und proaktiv zu handeln.

Nr.	Risikobeschreibung	EW	AG	RZ	Massnahmen	Verantw.	Termin
1.	Technologische Änderungen	1	2	2	Beobachtung von Markttrends	Projektmitarbeiter	Kontinuierlich während des Projekts
2.	Unzureichende Budgetierung für die vollständige Implementierung der VDI-Lösung	1	3	3	Sicherstellen eines detaillierten und realistischen Kostenvoranschlags und -kontrolle	Projektmitarbeiter	Vor Abschluss der Initialisierungsphase
3	Unterschätzung der Projektressourcen	2	2	4	Detaillierte Ressourcenplanung und regelmäßiges Monitoring des Ressourcenbedarfs	Projektmitarbeiter	Vor Abschluss der Initialisierungsphase

EW=Eintretenswahrscheinlichkeit: 1 Niedrig / 2 Mittel / 3 Hoch;

AG=Auswirkungsgrad: 1 Gering / 2 Mittel / 3 Gross;

RZ=Risikozahl: RZ = EW x AG

Tabelle 9: Risiken

12 Projektabgrenzung

Im Rahmen dieser Arbeit werden wir uns auf die Themen und Bereiche konzentrieren, die innerhalb der Box der folgenden Grafik dargestellt sind. Diese Elemente, einschliesslich Netzwerkarchitektur, Hardware-Installation, Benutzeranleitungen und VDI-Systeme, definieren den Kern unseres Projekts. Wir legen besonderen Wert auf die Verfügbarkeit, Sicherheit und Skalierbarkeit unseres Systems. Die Themen ausserhalb der Box, obwohl sie relevant sind, werden in dieser Arbeit nicht behandelt, um den Fokus und die Grenzen des Projekts klar zu bewahren.

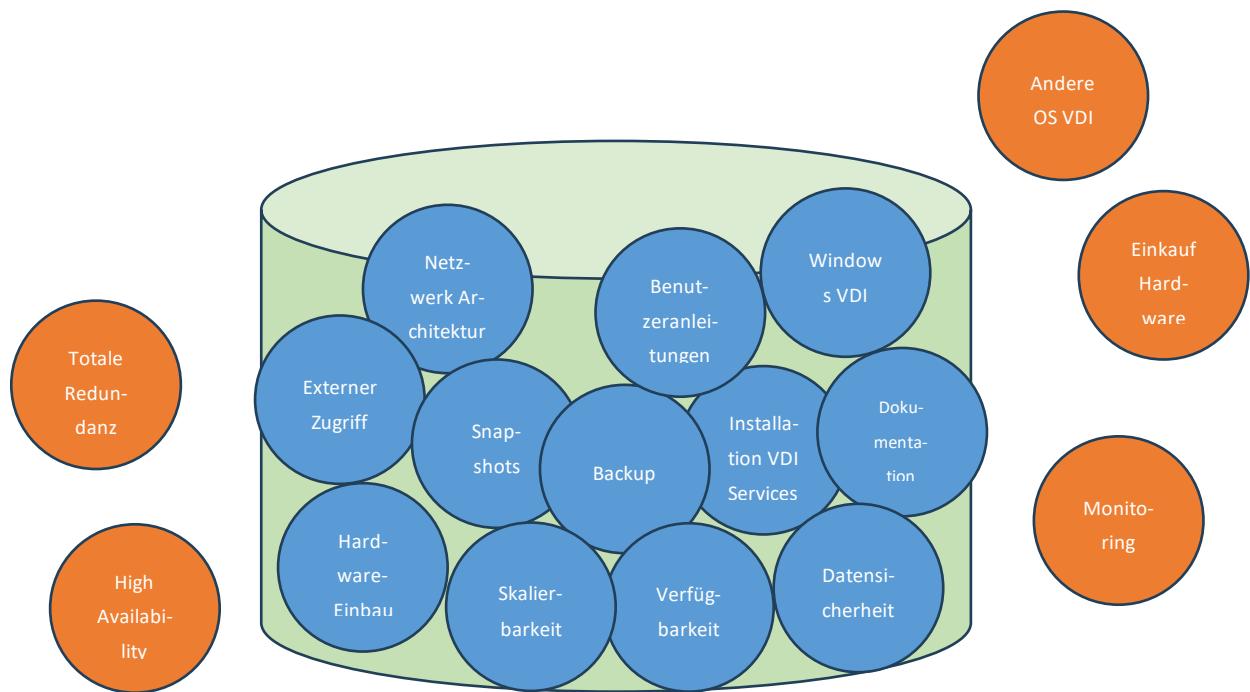


Abbildung 4: Projektabgrenzung

13 Abbildungsverzeichnis

Abbildung 1: Grafik IST/SOLL	4
Abbildung 2: Projektorganisation	7
Abbildung 3: Projektübersicht.....	11
Abbildung 4: Projektabgrenzung.....	14

14 Tabellenverzeichnis

Tabelle 1: Änderungsverzeichnis.....	1
Tabelle 2: Projektziele.....	5
Tabelle 3: Ziele Initialisierungsphase	6
Tabelle 4: Lieferobjekte.....	8
Tabelle 5: Kommunikation.....	10
Tabelle 6: Termine Initialisierungsphase	12
Tabelle 7: Kosten.....	12
Tabelle 8: Personalressourcen	12
Tabelle 9: Risiken	13

Anhang B2



Studie

VDI as a Service

Auftraggeber	Micha Bucher
Projektleiter	Shipinyuan Su, Sirak Yosef
Autor	Shipinyuan Su, Sirak Yosef
Klassifizierung	Intern
Status	Abgesegnet

Änderungsverzeichnis

Datum	Version	Änderung	Autor
25.02.2024	0.1	Dokument erstellt	Shipinyuan Su, Sirak Yosef
10.03.2024	1.1	Stärken, Schwächen Analyse	Shipinyuan Su, Sirak Yosef
14.03.2024	1.2	Pflichtenheft	Shipinyuan Su, Sirak Yosef
17.03.2024	1.3	Variantenentscheid	Shipinyuan Su, Sirak Yosef
22.03.2024	1.4	Studie fertig machen – Nutzwertanalyse, Variantenentscheid und Wirtschaftlichkeit	Shipinyuan Su, Sirak Yosef
11.04.2024	1.5	Korrekturen nach Zwischenmeeting	Shipinyuan Su, Sirak Yosef

Tabelle 1: Änderungsverzeichnis

Inhaltsverzeichnis

1	Studie.....	3
1.1	Ausgangslage.....	3
1.2	Standortsbestimmung	4
2	Pflichtenheft.....	8
2.1	User Stories.....	8
2.2	Anforderungskatalog	9
3	Lösungsvarianten.....	12
3.1	Variantenübersicht	12
4	Analyse und Bewertung.....	18
4.1	Anforderungsabdeckung	18
4.2	SWOT-Analyse	20
4.3	Nutzwertanalyse	21
5	Variantenentscheid	29
6	Wirtschaftlichkeit	30
6.1	TCO der verschiedenen Varianten.....	32
7	Glossar.....	35
8	Quellenverzeichnis.....	36

1 Studie

Diese Studie untersucht die Möglichkeiten von Virtual Desktop Infrastructure (VDI) als Dienstleistung. Das Thema ist aktuell sehr wichtig, da die Nachfrage nach flexiblen und sicheren Arbeitsumgebungen wächst. Im Mittelpunkt stehen bekannte Technologien wie MS Azure VDI, Citrix VDI und VMware. Es wird geprüft, was diese leisten können und wie die Kosten aussehen.

Zunächst wird der Bedarf für VDI und die damit verbundenen Ziele geklärt. Es folgt eine gründliche Informationssuche, um einen Überblick über bestehende Angebote und Anforderungen zu erhalten. Daraus entsteht eine Liste mit wichtigen Kriterien, die sowohl technische Aspekte als auch Sicherheit und Kosten umfasst.

Mit dieser Liste werden verschiedene VDI-Lösungen bewertet. Es findet ein Vergleich statt, um Stärken und Schwächen jeder Option zu identifizieren. Dabei werden nicht nur die sofortigen technischen Möglichkeiten und Kosten berücksichtigt, sondern auch die langfristige Perspektive.

Die Entscheidung für eine bestimmte Lösung basiert auf einer umfassenden Analyse, die alle wichtigen Faktoren einbezieht. Es wird auch geprüft, ob die Investition sich finanziell lohnt, also ob die Vorteile die Kosten übersteigen.

Das Ziel dieser Studie ist es, eine klare Orientierung für die Nutzung von VDI zu bieten. So kann eine fundierte Entscheidung getroffen werden, die den individuellen Anforderungen gerecht wird.

1.1 Ausgangslage

Mit dem Bedürfnis flexibel arbeiten zu wollen, muss eine sichere, effiziente und skalierbare Lösung bereitgestellt werden, welche das flexible Arbeiten nicht nur ermöglicht, sondern auch fördert. In der Studie wird drauf abgezielt, einen spezifischen Use Case detailliert zu analysieren. Dabei wird ein Überblick verschafft, wie die Arbeit derzeit gestaltet ist und die Bedürfnisse der Anwender werden erfasst, als auch deren funktionale und nicht-funktionale Anforderungen.

Die aktuelle Situation ist nicht mehr zeitgemäß und bedarf der Ablösung durch eine zuverlässige und zukunftssichere Lösung. Das stationierte arbeiten ist ineffizient, zudem ist das Dateimanagement veraltet, umständlich und nicht benutzerfreundlich.

Es besteht das Bedürfnis von überall an Projekten arbeiten zu können. In diesem Zusammenhang müssen Sicherheitsstandards berücksichtigt werden, wie Mehrfaktorauthentifizierung sowie physische und logische Isolierung des Systems, wobei die Benutzerfreundlichkeit nicht beeinträchtigt werden darf.

Um dieses Ziel zu erreichen, ist es wichtig, eine Balance zwischen Sicherheitsmaßnahmen und Benutzerfreundlichkeit zu finden. Dabei spielt es auch eine Rolle wie der Zugriff auf Ressourcen in Echtzeit, um eine reibungslose und effektive Zusammenarbeit zu gewährleisten.

1.2 Standortsbestimmung

Um eine präzise Studie erarbeiten zu können, muss zunächst eine Standortbestimmung durchgeführt werden. Dies ermöglicht, einen Überblick zu verschaffen, welche Sachmittel aktuell eingesetzt werden und in welchen Bereichen Verbesserungen notwendig sind. Die Erstellung einer Inventarliste der gegenwärtigen Situation ist essenziell, damit realistische Lösungsvarianten evaluiert werden können.

Die Herausforderung besteht darin, dass die betroffenen Parteien in Lugano ansässig sind, während das Projektteam in Bern stationiert ist. Dies erschwert es, sich persönlich ein Bild von der Situation zu machen. Hinzu kommt, dass die Notwendigkeit der Geheimhaltung zusätzliche Komplikationen mit sich bringen könnte. Um diese Hürde zu überwinden, verfügt das Team über eine Kontaktperson in Lugano, die wesentliche Einblicke und Informationen bereitstellt. Darüber hinaus ist das Team bestrebt, von den Erfahrungen früherer Geheimhaltungsprojekte in Bern und Zürich zu profitieren, um einen umfassenderen Überblick über die Abwicklung solcher Projekte zu erlangen. Diese Erfahrungen gewähren Einblicke in bewährte Verfahren und Veranschaulichen, wie ähnliche Anforderungen in der Vergangenheit bewältigt wurden.

Angesichts der strengen Geheimhaltung des Projektes dürfen keine Informationen darüber preisgegeben werden. Selbst die Projektbeteiligten haben keinen Zugang zu sensiblen Informationen über die Projekte. Stattdessen erhalten sie direkt vom Auftraggeber detaillierte Anforderungen, auf deren Grundlage die Infrastruktur konzipiert und realisiert wird.

Mengen und Häufigkeiten

Projekte dieser Art gibt es nur sehr selten und kann je nach Projekt und Standort unterschiedlich aufgebaut sein. Die Infrastruktur und Anforderungen bleiben jedoch überwiegend konstant. In dieser Analyse liegt der Fokus speziell auf der Situation in Lugano.

Inventar in Lugano:

Nr.	Typ	Erläuterung
1	Lenovo Notebooks	2 Notebooks
2	Synology NAS	1 Storage

Tabelle 2: Inventar Lugano



Das Synology NAS dient als Speichermedium und wird in Betrieb genommen, sobald es für das Projekt benötigt wird. Alle darauf gespeicherten Daten werden stets verschlüsselt abgelegt, um Sicherheit und Datenschutz zu gewährleisten.

Abbildung 1: NAS von Lugano



Alle Arbeitsmittel werden sicher in einem verschlossenen Schrank aufbewahrt. Zugang zum Schlüssel haben ausschliesslich befugte Personen, was die Sicherheit der Materialien gewährleistet und unbefugten Zugriff verhindert.

Abbildung 2: Arbeitsmaterial Lugano



Ein kleines Zimmer dient zunächst als Arbeitsplatz. Es ist jedoch geplant, dieses Zimmer zukünftig als Sitzungszimmer umzugestalten. Dadurch verliert das Projekt seinen bisherigen, festen Standort.

Abbildung 3: Arbeitsplatz Lugano

Zur Verfügung gestellte Sachmittel vom Auftraggeber:

Nr.	Typ	Erläuterung
1	Server in verschiedene Formfaktoren	2-3 Server
2	Synology NAS	1-2 Storage FS6400
3	Ein vorhandenes und konfigurierbares Netzwerk	Mit einem externen Partner konfigurierbar
4	Lizenzen	Je nach evaluierte Lösung eine Testlizenz oder Produktive Lizenzen

Tabelle 3: Zur Verfügung gestellte Sachmittel

Informationssicherheit und Datenschutz

Dieses Thema ist von grosser Bedeutung für das Projekt. Da das Projektteam jedoch unabhängig von laufenden Projekten operiert und das System als Proof of Concept (PoC) entwickelt wird, befinden sich keine sensiblen Daten darauf. Die Koordination mit den Stakeholdern erfolgt mündlich, und die Ergebnisse werden in Form von Anforderungen dokumentiert.

Stärken-, Schwächen- und Ursachenanalyse

Bei der Analyse der Stärken sollen die positiven Attribute und Ressourcen hervorgehoben werden, die zur Studie beitragen könnten. Die grösste Stärke besteht im Zugang zu umfangreichem Fachwissen sowie in der finanziellen Unterstützung durch den Auftraggeber. Dadurch wird ein starkes Fundament geboten und ein grosser Spielraum bei der Konzeption unter Einsatz verschiedener Sachmittel, die zur Verfügung stehen, eröffnet.

Die Schwächen in diesem Projekt liegen hauptsächlich in der Transparenz. Die Einschränkungen beim Erhalt und der Weitergabe detaillierter Informationen über die aktuelle Ist-Situation zwingen dazu, sich an die definierten Anforderungen zu halten und diese möglichst präzise zu erfüllen.

Die Ursachen der Stärken und Schwächen sind bekannt, und die Herausforderung wird dennoch gerne angenommen. Da die Lösung als Proof of Concept klassifiziert ist, könnte sie keinen Einsatz im Produktivbetrieb finden. Diese Möglichkeit ist bekannt, dennoch wird der grosse Wert gesehen, diese Lösung zu entwickeln und zu testen. Das Ziel ist es, eine potenzielle Umgebung zu gestalten, die in der Praxis eingesetzt werden könnte. Die Bemühungen bilden eine fundierte Grundlage, die zeigt, wie eine effektive und effiziente Umsetzung in der Zukunft aussehen könnte.

Informationsbeschaffung

Die meisten benötigten Informationen können aus dem engen Kontaktnetz bezogen werden. Dies umfasst sowohl das interne IT-Team als auch externe Partner und Fachexperten, die in grösseren IT-Projekten Unterstützung bieten. Darüber hinaus wird ein direkter Austausch mit den Kunden gepflegt, um Fragen zu stellen oder Feedback einzuholen. Für weitere Informationen wird das Internet herangezogen, beispielsweise, um nach Best Practices der Hersteller zu recherchieren oder Diskussionen in verschiedenen Fachforen zu verfolgen.

Analyse und Bewertung

Ein umfassender Überblick über die Studie konnte verschafft werden. Die Stärken und Schwächen sind bewusst, was eine klare Einschätzung der Ausgangslage ermöglicht. Das Projekt erfordert einen erheblichen Personaleinsatz sowie spezifisches Fachwissen und birgt Risiken in Bezug auf die Kosten für Sachmittel und den damit verbundenen Aufwand. Die Analyse dieser Aspekte ist somit unerlässlich.

2 Pflichtenheft

Für eine korrekte Evaluierung des Produktes und eine erfolgreiche Konzeptionierungsphase ist es wichtig, dass die funktionalen und nicht-funktionalen Anforderungen des Kunden genau verstanden werden. Dafür wird mit Hilfe von User Stories ein Anforderungskatalog erstellt. Diese User Stories dienen nicht nur als Grundlage für die Entwicklung, sondern ermöglichen es auch, am Ende des Projekts zu überprüfen, ob alle Anforderungen erfolgreich umgesetzt und erfüllt worden sind.

2.1 User Stories

Als...	Möchte ich...	Sodass...
Projektmitarbeiter	Die Möglichkeit auf Homeoffice haben	Ich nicht jeden Tag pendeln muss
Projektmitarbeiter	Von mehreren Standorten aus arbeiten können	Ich auch beim Kunden vor Ort effektiv sein kann
Projektmitarbeiter	Sicherstellen, dass bei Verlust oder Diebstahl meines Arbeitsgerätes keine signifikanten Sicherheitsrisiken entstehen	Der Schutz unserer sensiblen Daten gewährleistet ist
Projektmitarbeiter	Mit meinem Projektteam in Echtzeit kollabrieren können	Die Effizienz unserer Arbeit nicht beeinträchtigt wird
Projektmitarbeiter	Den Arbeitsprozess verstehen und eingeführt bekommen	Ich die Arbeitsumgebung schnell und effektiv nutzen kann
Projektmitarbeiter	Intuitiv Daten bearbeiten und abspeichern können	Ich nicht durch komplizierte Prozesse navigieren muss
Projektmitarbeiter	Trotz der Flexibilität über eine leistungsfähige Umgebung verfügen	Ich weiterhin produktiv und effizient arbeiten kann
Auftragsgeber	den Service auf monatlicher Basis abrechnen können	Wir eine neue Einkommensquelle haben und den Abrechnungsprozess vereinfachen können
IT-Supporter	Benutzermutationen unkompliziert ändern können	Ich Zeit spare und das Wissen schnell weitergeben kann
IT-Supporter	Anpassungen an der Umgebung möglichst einfach und ohne Wartungsarbeiten durchführen können	Die Kundenzufriedenheit hoch bleibt

Tabelle 4: User Stories

2.2 Anforderungskatalog

Funktionale Anforderungen

Die Anforderungen wurden Anhand der User Stories definiert und mit dem Auftragsgeber erweitert. Am Ende der Sammlung wurde das Dokument von den Stakeholdern genehmigt.

Nr.	Anforderung	Kategorie
1	Die Kunden können sich von jedem Ort aus sicher auf ihre VDI verbinden	M
2	Die Remoteverbindung ist durch mindestens zwei Authentifizierungsfaktoren geschützt	M
3	Echtzeit Kollaboration zwischen Nutzern ist möglich	M
4	Eine bereits bekannte und bewährte Dateiallagetechnologie wird für die Dateiverwaltung verwendet	S
5	Der IT-Supporter kann die Leistung (Kerne, RAM, VRAM) der VDI anpassen	S
6	IT-Support kann Benutzerkonten in der VDI-Infrastruktur hinzufügen, bearbeiten und löschen	M
7	IT-Support kann Änderungen am VDI-Image vornehmen, ohne den laufenden Betrieb zu stören	S
8	Das Engineering Team kann Anpassung an der Infrastruktur vornehmen, ohne den laufenden Betrieb zu stören	K
9	Sicherheitsfunktionen, wie das Blockieren von Screenshots und Videoaufnahmen der VDI, werden implementiert	K
10	Sensiblen Daten werden mindestens einmal täglich gesichert	M
11	Das Backup erfolgt automatisch ohne manuellen Eingriff	M
12	Das Benutzerendgerät ist hinsichtlich des Gewichts und Portabilität optimiert	X
13	Das Benutzerendgerät muss in der Lage sein bis zu mindestens vier Sicherheitsfunktionen, wie z.B. sicheres Passwort, Bitlocker, USB Authentifizierung Schlüssel, Deep Freeze ähnliche Produkte zu unterstützen.	X
14	Ein Verlust des Endgerätes führt zu keiner Sicherheitsgefährdung sensibler Daten	X
15	Die VDI-Infrastruktur ist virtuell von der produktiven Umgebung isoliert und unabhängig	M
16	Die Authentifizierung für die VDI erfolgt unabhängig vom produktiven Active Directory	S
17	Eine aktive Verbindung kann in einem Notfall sofort unterbrochen und blockiert werden	M

Nr.	Anforderung	Kategorie
18	Auf dem Client-Gerät ist eine Endpoint Security Software installiert	M
19	Auf dem VDI-Client läuft ein Antivirus	S
20	Die VDI verfügt über keinen direkten Internetzugang	M
21	Die VDI hat spezifische, vordefinierte Programme installiert	M
22	Die VDI bietet ausreichend Leistung für den reibungslosen Betrieb der erforderlichen CAD-Programme	M
23	Abgespeicherten Dokumente werden verschlüsselt gespeichert	S
24	Wichtige Dienste sind redundant ausgelegt	S
25	Sensible Daten werden ausschliesslich in der vorgesehenen Dateiablage gespeichert, lokale Dateien auf der VDI oder dem Client werden nach jedem Neustart gelöscht	M
26	Benutzeranpassung der VDI-Umgebung werden unterstützt und bei einem Neustart beibehalten, sofern sie die Sicherheitsrichtlinie nicht verletzen, wie z.B. CAD-Voreinstellungen	S
27	Die Performance und Verfügbarkeit der VDI wird kontinuierlich überwacht	S
Kategorie: M = Muss, S = Soll, K = Kann, X = wird nicht realisiert		

Tabelle 5: Funktionale Anforderungen

Nicht-funktionale Anforderungen

Nr.	Anforderung	Beschreibung	Messkriterium	Verifizierung
1	Benutzerfreundlichkeit	Die Arbeitsprozesse sind leichtverständlich. Die Oberfläche ist einfach und intuitiv zu bedienen.	Mehr als 80% der Nutzer geben positives Feedback zur Benutzerfreundlichkeit	Direktes Feedback vom Kunden
2	Sicherheit	Gewährleiste der Datensicherheit und Sicherstellung von einhalten von Sicherheitsstandards	Keine kritischen Schwachstellen bei regelmässigen Tests	Sicherheitsaudits und Penetrations-tests
3	Skalierbarkeit	Das System kann bei steigender oder sinkender Nutzeranzahl effizient Ressourcen zuweisen oder einsparen. Anpassung der Leistung einzelner VDIs möglich	Das System unterstützt ohne Leistungseinbussen die maximale berechnete Anzahl gleichzeitiger Nutzer	Lasttests und Last-monitoring
4	Verfügbarkeit	Das System ist rund um die Uhr verfügbar und kann Ausfälle einzelner Komponenten überstehen	Die Verfügbarkeit des Systems liegt bei 99% über den Monat	Monitoring der Verfügbarkeit
5	Performance	Die VDI-Umgebung bietet eine schnelle Reaktionszeit, vergleichbar mit einem Desktop-PC, auch bei schlechter Internetverbindung	Bietet konstant 30-40 FPS. Automatische Komprimierungen für leistungsschwächere Internetverbindungen sind möglich	Performance-Tests
6	Support	Kunden haben während der Geschäftzeiten Zugang zum Support und können Änderungen anfragen	Antwortzeit gemäss Qualität Management Service (QMS)	Rapport des Ticketing

Tabelle 6: Nicht-funktionale Anforderungen

3 Lösungsvarianten

Für den Variantenentscheid werden drei unterschiedliche VDI-Lösungen analysiert, wobei sowohl technische Merkmale als auch wirtschaftliche Aspekte untersucht werden. Mit Hilfe einer SWOT-Analyse werden die Stärken und Schwächen jeder Lösung identifiziert. Neben der Bewertung der Funktionalitäten wird auch untersucht, inwiefern die drei Produkte die Anforderungen erfüllen, indem eine Nutzwertanalyse durchgeführt wird. Dies ermöglicht eine fundierte Entscheidung zu treffen.

3.1 Variantenübersicht

Die Auswahl der passenden Lösung ist entscheidend für das Unternehmen und dessen Zukunftsfähigkeit und muss deshalb sorgfältig evaluiert werden. Als Partner von VMware wurde VMware Horizon zunächst bevorzugt. Jedoch hat die Übernahme von VMware durch Broadcom zu signifikanten Änderungen in der Lizenzierungspolitik geführt, weshalb VMware erneut in unseren Evaluierungsprozess einbezogen wird. Obwohl das Projekt technisch von der aktuellen produktiven VDI-Umgebung unabhängig ist, ist es trotzdem sinnvoll die Produktive Umgebung in dieser Bewertung mit einzubeziehen, vor allem aus wirtschaftlichen Überlegungen wie der Lizenzierung.

Im Kontext der On-Premises VDI-Lösungen stellt Citrix das direkte Äquivalent zu VMware dar und wird daher als eine wichtige Option in der Evaluierung betrachtet. Im Bereich VDI ist Citrix bereits seit längerer Zeit aktiv und etabliert, bevor VMware einen starken Aufschwung auf dem Markt hatte. Citrix bietet mit Citrix Virtual Apps and Desktops Lösungen an, die mit denen von VMware Horizon vergleichbar sind.

Neben den On-Premises Lösungen wird auch die Möglichkeiten einer Cloud-basierten Lösung in Betracht gezogen. Hier liegt der Fokus hauptsächlich auf Microsoft Azure Virtual Desktop (AVD). Azure VDI ermöglicht eine flexible und skalierbare Bereitstellung von virtuellen Desktops und Anwendungen.

Eigenschaften / Lösungen	VMware Horizon	Citrix Virtual Apps and Desktop	Microsoft Azure Virtual Desktop
Grundlegende Architektur	On-Premises, Hybrid, Cloud	On-Premises, Hybrid, Cloud	Cloud, Hybrid
Unterstützte Plattformen	Windows, Linux	Windows, Linux	Windows
Virtualisierungen	Desktops und Anwendungen	Desktops und Anwendungen	Desktops und Anwendungen über Remote-App
Managementtools	VMware vCenter, Horizon Console	Citrix Studio, Citrix Director	Azure Portal, Powershell, Microsoft Endpoint Manager
Skalierbarkeit	Hohe Skalierbarkeit Abhängig von Hardware	Hohe Skalierbarkeit Abhängig von Hardware	Hohe Skalierbarkeit

Eigenschaften / Lösungen	VMware Horizon	Citrix Virtual Apps and Desktop	Microsoft Azure Virtual Desktop
Benutzererfahrung	Blast Extreme Protokoll, bis zu 60 Frames per second (FPS)	HDX-Protokoll, bis zu 120 FPS	RDP und RemoteFX, bis zu 30 FPS
Zugriff von mobilen Endgeräten	VMware Horizon Client	Citrix Receiver / Workspace App	Remote Desktop Client und Web
Implementierungsmodell	On-Premises, Hybrid	On-Premises, Hybrid, Cloud	Primär Cloud
Lizenzmodell	Lizenzkosten abhängig von der Infrastruktur und Partnerschaft	Lizenzkosten abhängig von der Infrastruktur und Partnerschaft	Verbrauchsbasierte Bezahlung, abhängig von der Ressourcenutzung

Tabelle 7: Eigenschaften der Lösungsvarianten

VMware Lösung grafisch

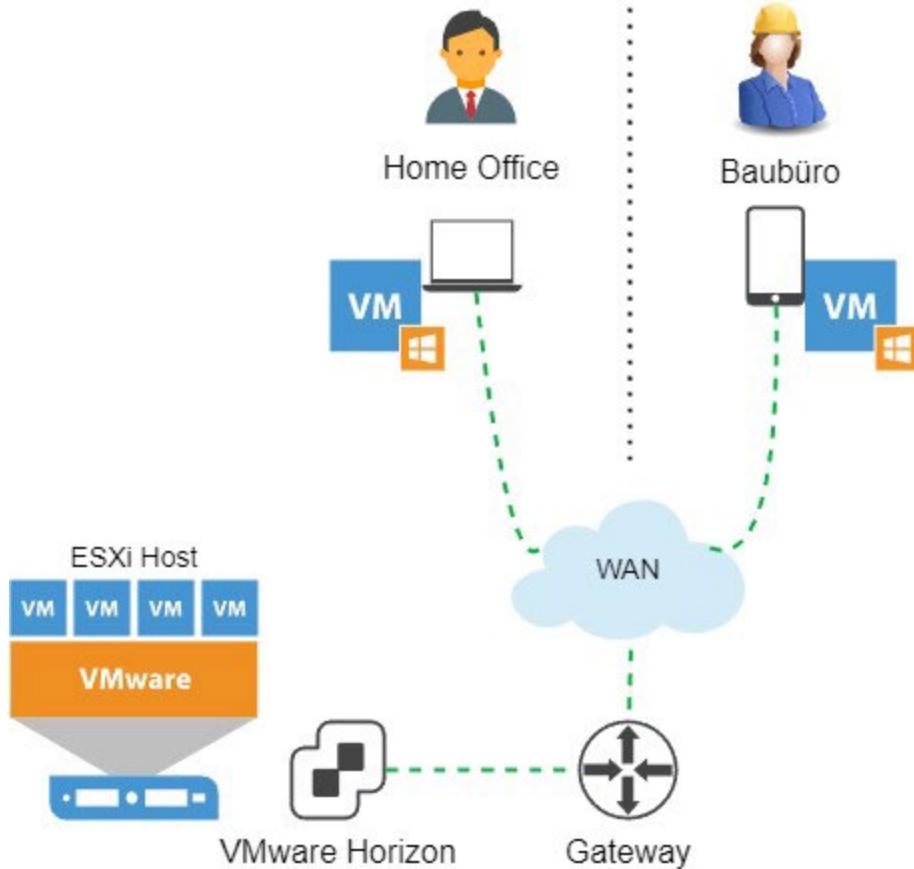


Abbildung 4: VMware Lösung grafisch

Citrix Lösung grafisch

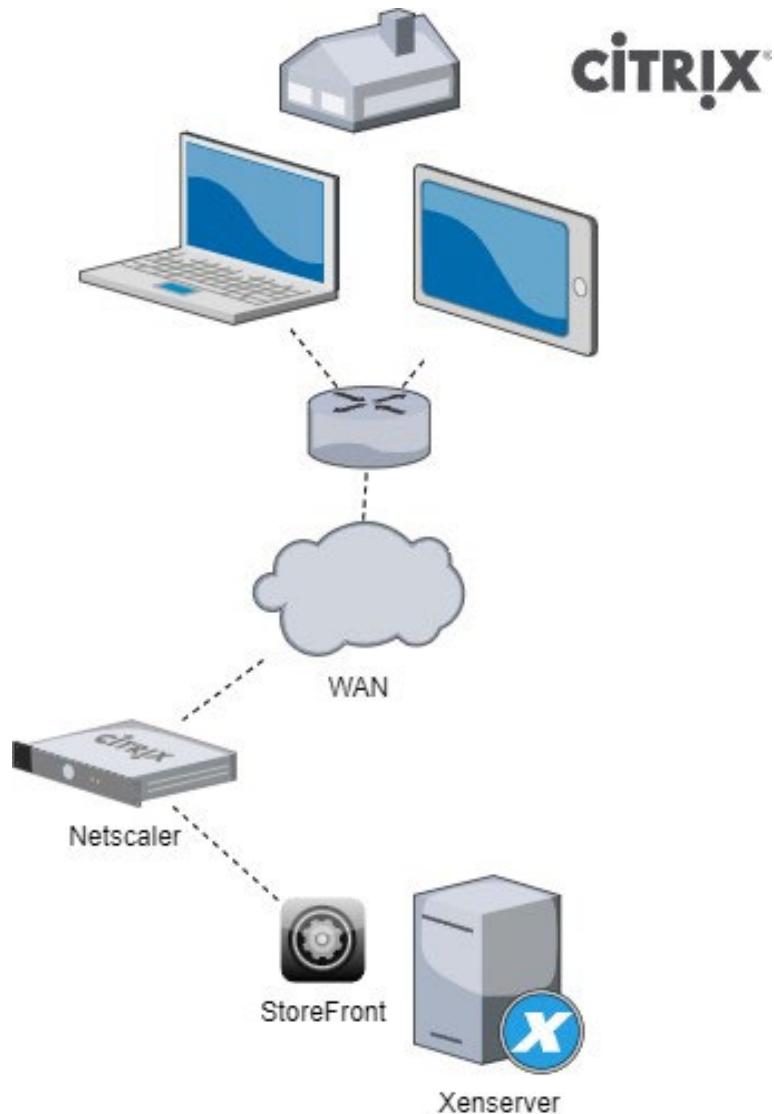


Abbildung 5: Citrix Lösung grafisch

Microsoft Azure Virtual Desktop Lösung grafisch

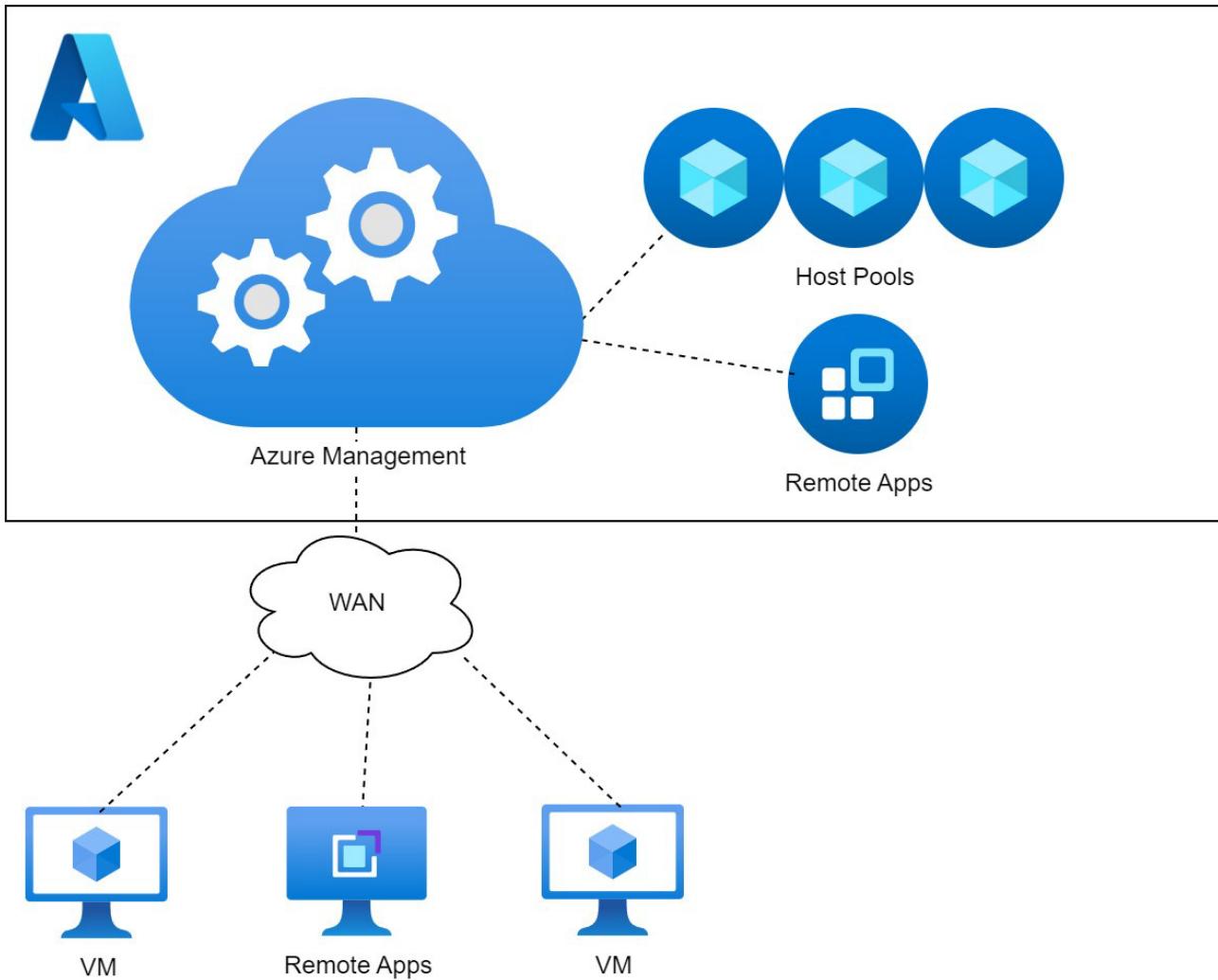


Abbildung 6: MS AVD Lösung grafisch

Kurzbeschreibung

VMware Horizon

Diese Variante, welche schon in der produktiven Umgebung verwendet wird, hat in den letzten Jahren eine Menge an Beliebtheit gewonnen.¹ Bei dieser Entscheidung würde es heissen, die VMware Palette zu verwenden. Vom Hypervisor ESXi bis zum vCenter bis zum VMware Horizon. VMware hat neben Horizon noch viele andere Produkte um seine Umgebung gestalten und managen zu können. VMware wurde Ende 2023 von Broadcom übernommen, was zu grossen Änderungen der Lizenzierung führt.² Für weitere Informationen siehe Datenblatt im Anhang F.

Citrix Virtual Apps and Desktops

Citrix ist eine bewährte Lösung, die in vielen aktiven Umgebungen eingesetzt wird. Citrix wurde im Jahr 1989 gegründet und akquirierte zwischen 2005 und 2012 viele Firmen, was zur Expansion in neuen Märkten führte.³ Ähnlich wie VMware hat Citrix ein grosses Portfolio an Technologien und Services zu Bereitstellung virtueller Anwendungen und Desktops. Im Gegensatz zu VMware, bleibt Citrix ein unabhängiges Unternehmen, das kontinuierlich Innovation und Entwicklung seiner Lösungen investiert. Für weitere Informationen siehe Datenblatt im Anhang F.

¹ <https://blogs.vmware.com/euc/2020/08/vmware-horizon-8-generally-available.html>

² <https://www.broadcom.com/blog/broadcom-announces-successful-acquisition-of-vmware>

³ <https://www.networkworld.com/article/865742/software-gaining-speed-citrix-buys-netscaler.html>

MS Azure Virtual Desktop

Azure Virtual Desktop, auch bekannt als MS AVD, ist ein von Microsoft entwickelter Dienst zur Virtualisierung von Desktops und Anwendungen. AVD ermöglicht es, Endbenutzern eine vollständige Desktopumgebung auf Basis von Windows 10/11 oder Remote-Anwendungen zur Verfügung stellen. Eine Schlüsselfunktion von AVD umfasst die Erstellung einer vollständigen Desktop-Virtualisierungsumgebung ohne die Notwendigkeit einer eigenen Infrastruktur. Dies macht AVD zu einer flexiblen Lösung für Unternehmen verschiedener Größen. Wie die anderen zwei Lösungen bietet AVD viele verschiedene Funktionen an, um die Benutzererfahrung zu optimieren. Sowohl auch Optimierungen in Ressourcen Nutzung. Mit der Möglichkeit von Multisession auf einer VM ist es möglich die Ressourcen auf mehreren VMs aufzuteilen, somit muss man VMs nicht personalisieren. Das Load-balancing kann auf verschiedene Weisen angepasst werden. Sowohl unterstützt es auch Funktionen wie FSLogix, wo man VM unabhängig immer das gleiche User Profil hat. Sicherheitstechnisch gibt es auch eine grosse Anzahl Möglichkeiten.⁴ Unterschiedlich zu den anderen Lösungen wird bei AVD nur die effektive Ausführungszeit verrechnet. Dabei spielen Faktoren mit, wie Komponentenleistungen wie z.B. vCPUs, RAM und Bandbreite. Für weitere Informationen siehe Datenblatt im Anhang F.

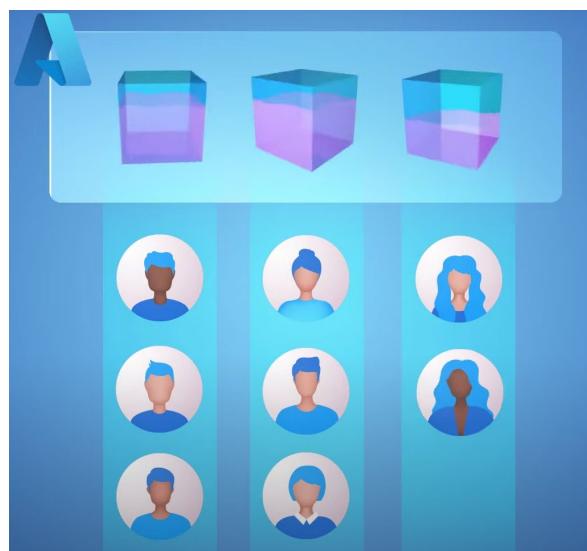


Abbildung 7: MS AVD Multisession

⁴ https://www.youtube.com/watch?v=aPEibGMvxZw&ab_channel=MicrosoftMechanics

4 Analyse und Bewertung

Die Auswahl der passenden Lösung ist ein mehrdimensionaler Prozess. Indem unterschiedliche Bewertungskriterien gewichtet werden, entsteht eine ganzheitliche Beurteilung der verschiedenen Optionen.

4.1 Anforderungsabdeckung

Nr.	Anforderungsbeschreibung	Kategorie	VMware	Citrix	Azure
1	Die Kunden können sich von jedem Ort aus sicher auf ihre VDI verbinden	M	Ja	Ja	Ja
2	Die Remoteverbindung ist durch mindestens zwei Authentifizierungsfaktoren geschützt	M	Ja	Ja	Ja
3	Echtzeit Kollaboration zwischen Nutzern ist möglich	M	Ja	Ja	Ja
4	Eine bereits bekannte und bewährte Dateiallagetechnologie wird für die Dateiverwaltung verwendet	S	Ja	Ja	Ja
5	Die VDI bietet eine Leistung vergleichbar mit einem Desktop-PC, der über 8 Kernen, 16 GB RAM und 4 GB VRAM verfügt	S	Ja	Ja	Ja
6	IT-Support kann Benutzerkonten in der VDI-Infrastruktur hinzufügen, bearbeiten und löschen	M	Ja	Ja	Ja
7	IT-Support kann Änderungen am VDI-Image vornehmen, ohne den laufenden Betrieb zu stören	S	Ja	Ja	Ja
8	Das Engineering Team kann Anpassung an der Infrastruktur vornehmen, ohne den laufenden Betrieb zu stören	K	Ja	Ja	Ja
9	Sicherheitsfunktionen, wie das Blockieren von Screenshots und Videoaufnahmen der VDI, werden implementiert	K	Ja	Ja	Ja
12	Die VDI-Infrastruktur ist virtuell von der produktiven Umgebung isoliert und unabhängig	M	Ja	Ja	Ja
13	Die Authentifizierung für die VDI erfolgt unabhängig vom produktiven Active Directory	M	Ja	Ja	Ja*
14	Eine aktive Verbindung kann in einem Notfall sofort unterbrochen und blockiert werden	M	Ja	Ja	Ja

Nr.	Anforderungsbeschreibung	Kategorie	VMware	Citrix	Azure
15	Auf dem Client-Gerät ist eine Endpoint Security Software installiert	M	Ja	Ja	Ja
16	Auf dem VDI-Client läuft ein Antivirus	S	Ja	Ja	Ja
17	Die VDI verfügt über keinen direkten Internetzugang	M	Ja	Ja	Ja
18	Die VDI hat spezifische, vordefinierte Programme installiert	M	Ja	Ja	Ja
19	Die VDI bietet ausreichend Leistung für den reibungslosen Betrieb der erforderlichen CAD-Programme	M	Ja	Ja	Ja
20	Abgespeicherten Dokumente werden verschlüsselt gespeichert	S	Ja	Ja	Ja
21	Wichtige Dienste sind redundant ausgelegt	S	Ja	Ja	Ja
22	Sensible Daten werden ausschliesslich in der vorgesehenen Dateiablage gespeichert, lokale Dateien auf der VDI oder dem Client werden nach jedem Neustart gelöscht	M	Ja	Ja	Ja
23	Benutzeranpassung der VDI-Umgebung werden unterstützt und bei einem Neustart beibehalten, sofern sie die Sicherheitsrichtlinie nicht verletzen, wie z.B. CAD-Voreinstellungen	S	Ja	Ja	Ja
24	Die Performance und Verfügbarkeit der VDI wird kontinuierlich überwacht	S	Ja	Ja	Ja
Kategorie: M = Muss, S = Soll, K = Kann					

Tabelle 8: Anforderungsabdeckung

Die Authentifizierung der Azure Virtual Desktop erfolgt in erster Linie über das Azure Active Directory (Azure AD, neu MS Entra ID). Für die Unabhängigkeit dieser Authentifizierung wäre der Aufbau eines neuen Tenant notwendig.

4.2 SWOT-Analyse

Mit dieser Analyse werden die Stärken, Schwächen, Chancen und Risiken jeder Variante bewertet.

		Interne Analyse	
		Stärken	Schwächen
Externe Analyse	Chancen	<ul style="list-style-type: none">• Skalierbarkeit• Innovativ• Nachhaltigkeit durch zentral verwaltete Ressourcen• Benutzerfreundlichkeit• Steigende Nachfrage• Vielfältig einsetzbar in verschiedene Branchen• Steigerung der Flexibilität und Effizienz	<ul style="list-style-type: none">• Abhängigkeiten von Drittanbieter• Komplexität• Veränderung der Arbeitsweise für konservative Kunden• Eher neu auf dem Markt
	Risiken	<ul style="list-style-type: none">• Marktbedarf ist vorhanden• Akquirieren neuen Kunden• Neue mögliche Partnerschaften	<ul style="list-style-type: none">• Änderung der Bedürfnisse• Fehlendes technische Know-how• Konkurrenz auf dem Markt• Grosse Cloud Anbieter mit eigenen Lösungen

Tabelle 9: SWOT-Analyse

4.3 Nutzwertanalyse

In der Nutzwertanalyse werden drei verschiedene Lösungsvarianten verglichen, um herauszufinden, welche von ihnen die Anforderungen am besten erfüllt. Dafür werden verschiedene Kriterien verwendet.

Nr.	Kriterium	Beschreibung
1	Kosten	Investitionskosten, Betriebskosten, Wartungskosten
2	Anforderungen	Erfüllung der funktionalen und nicht-funktionalen Anforderungen
3	Komplexität	Schwierigkeit der Implementierung, Konfiguration und Verwaltung der Lösung
4	Kompatibilität	Kompatibilität mit den bestehenden Systemen und Software
5	Benutzerfreundlichkeit	Einfachheit und Intuitivität der Benutzeroberfläche
6	Leistung	Geschwindigkeit, Effizienz und Zuverlässigkeit
7	Skalierbarkeit	Umgang mit wachsenden Anforderungen oder Nutzerzahlen
8	Nachhaltigkeit	Energieeffizienz und Gebrauch von umweltfreundlicheren Materialien
9	Sicherheit	Sicherheitsmaßnahmen wie Datenverschlüsselung, Zugriffskontrollen und Compliance mit Sicherheitsstandards
10	Support und Wartung	Verfügbarkeit von Herstellersupport oder Partnerschaften. Regelmäßige Patches

Tabelle 10: Kriterien der Nutzwertanalyse

Gewichtung der Kriterien

Für die Durchführung einer Nutzwertanalyse ist es wichtig, die Bewertungskriterien, die für den Vergleich der verschiedenen Lösungsvarianten herangezogen werden, sorgfältig zu gewichten. Diese Gewichtung reflektiert die relative Bedeutung jedes Kriteriums im Hinblick auf die Gesamtentscheidung. Die Gewichtungsskala erstreckt sich von 0 bis 2, wobei die Bewertung in Schritten von 0,5 erfolgt. Innerhalb dieser Skala repräsentiert ein Wert von 0, dass ein Kriterium relativ zum Gegenstück, völlig unwichtig ist, während ein Wert von 2 anzeigt, dass das Kriterium doppelt so wichtig ist, relativ zum Gegenstück. Eine Standardgewichtung von 1, hat die Bedeutung einer Gleichwertigkeit.

	Kosten	Anforderungen	Komplexität	Kompatibilität	Benutzerfreundlichkeit	Leistung	Skalierbarkeit	Nachhaltigkeit	Sicherheit	Support und Wartung	Punkte	Gewichtung berechnet	Gewichtung für NWA
Kosten	1	1	2	1.5	1	1	1	2	1	1	11.5	13	15
Anforderungen	1	2	1.5	1.5	1	1	1	2	1	1	12	13	15
Komplexität	1	0	1	1	1	0.5	0.5	1.5	0.5	1	7	8	10
Kompatibilität	0	0.5	1	1	1	1	1	2	1	1	8.5	9	10
Benutzerfreundlichkeit	0.5	0.5	1	1	0.5	0.5	0.5	1.5	0.5	0.5	6.5	7	5
Leistung	1	1	1.5	1	1.5	1	1	1.5	1	1	10.5	12	10
Skalierbarkeit	1	1	1.5	1	1.5	1	1.5	1	1	1	10.5	12	10
Nachhaltigkeit	0	0	0.5	0	0.5	0.5	0.5	0	0	0	2	2	5
Sicherheit	1	1	1.5	1	1.5	1	1	2	1	1	11	12	10
Support und Wartung	1	1	1	1	1.5	1	1	2	1	1	10.5	12	10
											90	100	100

Tabelle 11: Gewichtung der Kriterien

Bewertung der Kriterien

Für die Bewertung jedes Kriterium braucht es eine Skala von 0 (ganz schlecht) bis 5 (sehr gut).

Zuschlagskriterien	Gewicht	Keine 0	Schlecht 1	Ungenügend 2	Genügend 3	Gut 4	Sehr gut 5
Kosten	15%	Für ein KMU unerschwinglich	Über dem Budget	leicht über dem Budget	Im Budget	Unter dem Budget	Kostenlos oder nicht Budgetrelevant
Anforderungen	15%	Keine Anforderungen erfüllt	Einige wenige Anforderungen erfüllt	Einige wichtige Anforderungen erfüllt	Die Mehrheit der Anforderungen erfüllt	Fast alle Anforderungen erfüllt	Alle Anforderungen erfüllt
Komplexität	10%	Erfordert Schulungen und Expertenwissen	Spezialwissen nötig	Einstiegerfreundlich für Fachpersonal	Handhabbar für Standardfähigkeiten	Benutzerfreundlich und leicht verständlich	Intuitiv und ohne zusätzliche Hilfe bedienbar
Kompatibilität	10%	Keine Kompatibilität mit bestehenden Systemen und Anwendungen	Viele Anpassungen nötig	Einige Anpassungen nötig	Geringe Einschränkungen	Minimale Anpassungen nötig	Nahtlose Integration
Benutzerfreundlichkeit	5%	Schwer nutzbar	Ganztägige Schulung erforderlich	Kurzer Workshop erforderlich	Kurze Einführung erforderlich	Einige Anleitungen nötig	Intuitiv ohne Einführung nutzbar
Leistung	10%	Produktive Arbeit unmöglich	Erfüllt nicht die Mindestanforderungen	Tägliche Abstürze aufgrund unzureichender Leistung	Funktioniert mit spürbarer Latenz	Lauft stabil mit 30 FPS	Lauft stabil mit über 30 FPS
Skalierbarkeit	10%	Nicht skalierbar	Nur durch Hardware erweiterbar	Skalierung sind mit Wartungsarbeiten verbunden	Manuelle Anpassungen für Skalierung nötig	Schnelle und dynamische Skalierung mit geringen Einschränkungen	Schnelle und dynamische Skalierung und Echtzeit Anpassungen
Nachhaltigkeit	5%	Sehr hoher Energieverbrauch und Nutzung schädlicher Materialien	Hoher Energieverbrauch, jedoch gewisse Materialaspekte beachtet	Höherer Energieverbrauch als derzeitiger Standard	Energieverbrauch entspricht dem aktuellen Standard	Energieverbrauch entspricht dem	Hohe Energieeinsparungen und Nutzung nachhaltiger Ressourcen

		Keine 0	Schlecht 1	Ungenügend 2	Genügend 3	Gut 4	Sehr gut 5
Zuschlagskriterien	Gewicht						
						Standard, nachhaltige Produkte im Einsatz	
Sicherheit	10%	Keine Sicherheitsmassnahmen vorhanden	Keine spezifischen Sicherheitsmassnahmen implementierbar	Branchenstandard, mit deutliche Verbesserungsmöglichkeiten	Gute Sicherheitsfeatures implementiert	Mehrere erweiterte Sicherheitsfeatures im Einsatz, Datenverschlüsselung vorhanden	Umfassende Sicherheitsfeatures inklusive Datenverschlüsselung, regelmäßige Audits und Compliance-Überprüfungen
Support und Wartung	10%	Kein Support vorhanden	Sehr begrenzter Support, Reaktionszeit über einer Woche	Begrenzter Support, Reaktionszeit über drei Tage	Guter Support, Reaktionszeit von 1-2 Tagen	Direkter Ansprechpartner beim Hersteller oder Partner mit 24/7 Verfügbarkeit und proaktiver Unterstützung	

Tabelle 12: Bewertung der Kriterien

VMware Horizon

Kriterium	Punkte	Begründung
Kosten	1	Nach der Übernahme durch Broadcom, wurde die Partnerschaften zu KMUs beendet. Die Lizenzkosten für Partnerschaften sind nun auf einem Vielfach gestiegen ⁵
Anforderungen	5	Durch die breite Produktpalette von VMware können alle Anforderungen mit dem benötigten Know-how gelöst werden
Komplexität	2	Für die Implementierung und Verwaltung dieser Lösung benötigt es Fachwissen
Kompatibilität	4	Diese Lösung kann, ohne den Betrieb zu stören implementiert werden. Dabei verfügt es über alle benötigten Betriebssysteme. Probleme könnten auftauchen bei Kompatibilität mit CAD oder Rendering-Software
Benutzerfreundlichkeit	4	Der VMware Horizon Client hat eine übersichtliche und intuitive Benutzeroberfläche. VMware besitzt ausgereifte und moderne Management-Tools. Einige Einstellungen können jedoch verschachtelt und somit schwierig zu finden sein
Leistung	4	VMware Blast ermöglicht eine stabile VDI-Verbindung mit 30 FPS
Skalierbarkeit	4	Instant Clones ermöglichen es, VMs bei Bedarf schnell einzurichten und vorzubereiten. Cluster und Ressourcenpools erleichtern die Verwaltung der Ressourcen
Nachhaltigkeit	5	Durch den bedarfsorientierten Ressourcenverbrauch und Energiesparoptionen für inaktive VMs kann VMware erheblich Energie einsparen
Sicherheit	5	VMware bietet eine breite Palette an Sicherheitsprodukten und -einstellungen, die zur Verbesserung der Sicherheit beitragen können
Support und Wartung	3	Aufgrund der Beendigung mehrerer Partnerschaften nach der Übernahme durch Broadcom ist es schwieriger geworden, einen VMware-Partner für Support und Wartung zu finden oder direkt auf den Hersteller Support zuzugreifen

Tabelle 13: Variantenbewertung VMware

⁵ <https://www.netzwoche.ch/news/2024-01-22/broadcom-verkleinert-das-vmware-angebot-stark>

Citrix

Kriterium	Punkte	Begründung
Kosten	3	Das Pricing von Citrix ohne Partnerschaft ist immer noch preiswerter als das von VMware
Anforderungen	5	Citrix erfüllt umfassend alle Anforderungen, unterstützt durch eine breite Palette an Funktionen und hohe Anpassungsfähigkeit ihrer Produkte
Komplexität	2	Citrix-Produkte können komplex in der Implementierung und Verwaltung sein und erfordern in der Regel Fachkenntnisse
Kompatibilität	4	Ähnlich wie VMware Horizon, kann es zu Kompatibilitätsproblemen kommen bei CAD und Rendering-Software
Benutzerfreundlichkeit	4	Der Citrix Workspace lässt sich ähnlich wie VMware Horizon bedienen. Die Management-Tools von Citrix sind zwar almodischer, jedoch fast übersichtlicher
Leistung	5	Mit ihrem langentwickelten HDX-Protokoll bietet Citrix eine hervorragende Performance, die in der Lage ist, bis zu 120 FPS zu bieten, auch wenn dies durch die Internetleistung nicht immer realistisch ist
Skalierbarkeit	5	Wie bei VMware, können durch Instant Clones VMs auf Anfrage aufgebaut und vorbereitet werden. Durch Delivery Groups und Machine Catalogs können Ressourcen einfach verwaltet werden. Durch verbesserte Integration mit dem Speicher, kann Citrix ein Image um ein Vielfaches schneller freigeben
Nachhaltigkeit	5	Ähnlich wie bei VMware, kann Citrix Energie sparen, indem Ressourcen nur zur Verfügung gestellt werden, wenn ein Bedarf besteht. Außerdem können zu Peak- und Off-Peak-Zeiten verschiedene Einstellungen angewendet werden
Sicherheit	5	Citrix bietet robuste Sicherheitsfunktionen und Compliance-Optionen, um den Schutz sensibler Daten und Anwendungen zu gewährleisten und modernsten Sicherheitsanforderungen zu entsprechen
Support und Wartung	4	Es besteht eine Basis von Citrix-Partnern in der Schweiz. Öffentliche Support-Rufnummern und Live-Chats sind verfügbar

Tabelle 14: Variantenbewertung Citrix

Azure

Kriterium	Punkte	Begründung
Kosten	1	Die Anforderungen und Ansprüche an unsere Leistung und Sicherheit können bei Azure die Preise deutlich erhöhen
Anforderungen	5	Azure VDI erfüllt durch seine tiefe Integration in das Microsoft-Ökosystem und die breite Palette an unterstützten Diensten alle Anforderungen
Komplexität	3	Azure ist eine umfangreiche Cloud-Plattform mit vielen Diensten. Die Einrichtung und Verwaltung von AVD ist eher einfach gestaltet
Kompatibilität	4	Azure VDI bietet eine hohe Kompatibilität mit der Microsoft-Umgebung und deren Anwendungen, könnte jedoch bei speziellen Nischenanwendungen auf Kompatibilitätsprobleme stossen
Benutzerfreundlichkeit	4	Azure VDI ist bekannt für seine benutzerfreundliche Oberfläche und die einfache Integration in andere Microsoft-Produkte
Leistung	4	Azure VDI gewährleistet eine stabile Leistung, abhängig von der Auswahl der Maschinen, und kann eine breite Palette von Anwendungen effizient ausführen
Skalierbarkeit	5	Dank der Cloud-Infrastruktur von Azure lassen sich Ressourcen dynamisch anpassen, um Skalierungsanforderungen zu erfüllen. Dies ermöglicht eine schnelle Anpassung an benötigte Maschinenkapazitäten. Zudem unterstützt Azure VDI neuerdings Multisession-Funktionen, wodurch einzelne VMs von mehreren Benutzern gemeinsam genutzt werden können
Nachhaltigkeit	5	Microsoft hat sich zum Ziel gesetzt, nachhaltige Praktiken voranzutreiben, und arbeitet daran, den Energieverbrauch zu optimieren und den Einsatz erneuerbarer Energiequellen zu erhöhen, was die Nachhaltigkeit von Azure VDI unterstützt
Sicherheit	4	Azure VDI profitiert von Microsoft umfangreichen Sicherheitsprotokollen und Compliance-Massnahmen, einschliesslich regelmässige Sicherheitsupdates und strikter Datenschutzstandards. Ein Nachteil ist jedoch, dass die Server nicht vor Ort sind, was bedeutet, dass sensible Daten potenziell an ungewollte Orte gelangen oder eingesehen werden können
Support und Wartung	4	Abhängig vom gewählten Support-Plan kann direkter Support vom Hersteller in Anspruch genommen werden. Zudem bestehen verschiedene Partner in der Schweiz die Azure VDI anbieten

Tabelle 15: Variantenbewertung Azure

Ergebnisse der Nutzwertanalyse

In der Analyse wurden VMware, Citrix und Azure Virtual Desktop umfassend untersucht und anhand von zehn Schlüsselkriterien bewertet, die von Kosten und Anforderungserfüllung bis hin zu Nachhaltigkeit und Support reichen. Die resultierenden Daten ermöglichen es, eine fundierte Entscheidung zu treffen.

Kriterien	Erläuterung	Gewichtung (G)	VMware		Citrix		Azure	
			Note (W)	G*W	Note (W)	G*W	Note (W)	G*W
Kosten	günstig: 5 / teuer: 0	15	1	15	3	45	1	15
Anforderungen	alle: 5 / keine 0	15	5	75	5	75	5	75
Komplexität	einfach: 5 / komplex 0	10	2	20	2	20	3	30
Kompatibilität	kompatibel: 5 / nicht kompatibel 0	10	4	40	4	40	4	40
Benutzerfreundlichkeit	Intuitiv: 5 / Komplex 0	5	4	20	4	20	4	20
Leistung	Schnell: 5 / langsam 0	10	4	40	5	50	4	40
Skalierbarkeit	Skalierbar: 5 / nicht skalierbar 0	10	4	40	5	50	5	50
Nachhaltigkeit	Nachhaltig: 5 / nicht nachhaltig 0	5	5	25	5	25	5	25
Sicherheit	Compliance: 5 / Sicherheitslücken 0	10	5	50	5	50	4	40
Support und Wartung	innert 24h 5 / mehr als 72h 0	10	3	30	4	40	4	40
Total		100		355		415		375

Tabelle 16: Ergebnisse der Nutzwertanalyse

5 Variantenentscheid

Nach sorgfältiger Abwägung der verschiedenen Lösungsoptionen und Durchführung einer detaillierten Nutzwertanalyse wurde Citrix Virtual Apps and Desktops als die bevorzugte Lösung entschieden. Die Entscheidung für Citrix wurde durch mehrere ausschlaggebenden Faktoren bestimmt, die im Folgenden erläutert werden:

Kosten: Ein entscheidender Faktor in der Entscheidung für Citrix ist eine bestehende Partnerschaft mit einer vertrauenswürdigen Person, der bereits ein etablierter Citrix-Partner ist. Diese Beziehung ermöglicht es, Citrix-Lizenzen zu vorteilhaften Konditionen zu beziehen, was die Gesamtkosten der Lösung signifikant reduziert. Zudem sind die Standardpreise von Citrix schon sehr wettbewerbsfähig.

Leistung: In der Kategorie Leistung hat Citrix eine Spitzenbewertung erhalten. Insbesondere die Geschwindigkeit der Bereitstellung von Desktops, die für einen dynamischen Betrieb entscheidend ist. Mit Citrix sind wir in der Lage, auch leistungsintensive Anwendungen wie CAD-Tools ohne grosse Latenz oder Performance Einbussen bereitzustellen.

Skalierbarkeit: Die Skalierbarkeit ist für unser Unternehmen von entscheidender Bedeutung, da wir schnell auf Veränderungen in der Arbeitslast reagieren müssen. Citrix ermöglicht eine dynamische Skalierung unserer Ressourcen, was es uns erlaubt, effizient und Energie schonend zu operieren.

Sicherheit: Da alle unserer Projekte unter strengen Vertraulichkeitsvereinbarungen stehen, ist es von entscheidender Bedeutung, eine Lösung zu wählen, die die sichere Handhabung sensibler Daten gewährleisten kann. Citrix ermöglicht nicht nur umfassende Sicherheitsfeatures, sondern bietet auch die Möglichkeit, es als eine komplette On-Premise Lösung zu implementieren. Diese Option ist für uns besonders wichtig, da sie es uns erlaubt, die volle Kontrolle über unsere Daten zu behalten und den Zugriff streng zu regulieren. Durch die Wahl einer On-Premise Konfiguration mit Citrix können wir sicherstellen, dass unsere geheimhaltungsbedürftigen Projekte in einer hochgesicherten Umgebung bearbeitet werden, was ein Schlüsselement unserer IT-Sicherheitsstrategie darstellt.

Support: Durch einen langjährigen Partner besteht eine direkte Ansprechperson für Support und Implementierungsunterstützung. Diese Kontakterson dient als Anlaufstelle für technische Herausforderungen oder Fragen.

In Anbetracht dieser Schlüsselfaktoren und der Tatsache, dass Citrix in der Gesamtbewertung die höchste Punktzahl erreicht hat, wurde es zu dem Schluss gekommen, dass Citrix Virtual Apps and Desktops die ideale Lösung für das Unternehmen ist. Es bietet das beste Gleichgewicht zwischen Kosten, Funktionalität und strategischer Ausrichtung für unsere zukünftigen Ziele.

6 Wirtschaftlichkeit

In diesem Abschnitt wird der Total Cost of Ownership (TCO) der verschiedenen Varianten analysiert. Dies Spielt eine zentrale Rolle, um die langfristigen finanziellen Auswirkungen zu verstehen. Diese Analyse zielt darauf ab, nicht nur die direkten Kosten wie Anschaffungs- und Implementierungskosten zu erfassen, sondern auch indirekte Ausgaben, die über die Lebensdauer der Lösung anfallen, wie Betriebskosten und Supportleistungen.

Personalaufwand

Phase	Start	Ende	Ressourcen SOLL			
			Shipinyuan Su	Sirak Yosef	Thomas Staub	Tenzin Langdun
Initialisierung	11.12.2023	14.03.2024	51,5h	51,5h	2h	2h
Konzept	18.03.2024	12.04.2024	44h	44h	0h	0h
Realisierung	15.04.2024	24.05.2024	84h	84h	0h	0h
Einführung	27.05.2024	07.06.2024	8h	8h	0h	0h
Abschluss	11.12.2023	07.06.2024	62h	62h	4h	4h
		Total	249.5h	249.5h	6h	6h
		Kosten	8'732,50 CHF	8'732,50 CHF		

Tabelle 17: Wirtschaftlichkeit - Personalaufwand

Sachmittel

Hardware-Komponente	Beschreibung	Kosten (CHF)
Server VDI	Von SuperMicro zusammengestellt	
Gehäuse	SYS-220U-MTNR	
CPUs	2x Intel Xeon Gold 5317 CPU at 3.00 GHz / 12 Cores pro CPU	
RAM	1 TB	
GPUs	2x NVIDIA A16	
SSDs	2x 2 TB SSD	
RAID-Controller	1x	
Netzwerkkarte 10Gbps	1x	
Gesamt Hardware-Kosten		~20'000

Tabelle 18: Wirtschaftlichkeit - Anschaffung Server1

Hardware-Komponente	Beschreibung	Kosten (CHF)
Server Mgmt	Hardware von SuperMicro, viel selbst umgebaut	
Gehäuse		2'800
CPUs	2x Intel Xeon Silver 2.4GHz 10 Cores	1'000
RAM	768GB	1'800
GPUs	NVIDIA A16	3'200
SSDs	2x 2TB	360
RAID-Controller	1x	550
Netzwerkkarte 10Gbps	1x	350
Gesamt Hardware-Kosten		~9'160

Tabelle 19: Wirtschaftlichkeit - Anschaffung Server2

Hardware-Komponente	Beschreibung	Kosten (CHF)
Synology Nas FS6400	Eine modifizierte Version mit aufgerüsteter Hardware	~15'000
RAM	128 GB	
CPUs	Intel Xeon Silver 4110 2.1GHz 16 Cores	
SSDs	24x	~14'000
Gesamt Hardware-Kosten		~29'000

Tabelle 20: Wirtschaftlichkeit - Anschaffung Synology NAS

6.1 TCO der verschiedenen Varianten

Investitionskosten	VMware	Citrix	Azure
Anschaffungskosten	58'160.-	58'160.-	29'000.- (Speicher)
Implementierungskosten	17'465.-	17'465.-	17'465.-
Schulungskosten	11'000.- ⁶	9'000.- ⁷	5'100.- ⁸
Totalle Kosten	86'625.-	84'625.-	51'565.-

Tabelle 21: Investitionskosten

Die Anschaffungskosten umfassen die Sachmittel, die für die Umsetzung des Projektes erforderlich sind. Diese Kosten fallen zu Projektbeginn einmalig an. Die Implementierungskosten beziehen sich auf den internen Aufwand für die Realisierung des Projektes, entsprechend dem Personaleinsatz. Die Schulungskosten decken interne Schulungen der Ingenieure ab und sind auf zwei Personen kalkuliert.

Laufende Kosten	VMware	Citrix	Azure
Lizenzierung / Monatliche Abrechnungen	~28\$ Pro Benutzer (Partner)	~28\$ Pro Benutzer	~5'000.-
Betriebskosten	200.-	200.-	200.-
Externe Supportkosten	240.-	240.-	240.-
Wartungskosten	240.-	240.-	0
Totalle Kosten (Lizenzen auf 15 Personen gerechnet)	1'455.-	1'455.-	5'840.-

Tabelle 22: Laufende Kosten

Diese Lizenzpreise sind ohne Währungsschwankungen und Mehrwertsteuer preisgegeben. Für die Berechnung des Azure Virtual Desktop wurde ein virtueller Server ausgewählt, der eine ähnliche Leistung wie eines der aktuellen Sachmittel aufweist. Bei der Ermittlung der Betriebskosten wurden die aktuellen internen Support-Tickets analysiert, die sich auf durchschnittlich etwa 30 Tickets pro Monat belaufen, welche der Kategorie VDI zugeordnet sind. Da die Kundenbasis in der produktiven Umgebung wesentlich grösser sein wird, wurde lediglich einen Bruchteil dieser Basis für diese Berechnungen herangezogen und die Zeit mit einem Stundensatz von 40 CHF veranschlagt. Für externen Support wurden zwei Stunden pro Monat eingeplant, basierend auf einem Stundensatz von 120 CHF. Die Wartungskosten wurden mit einem Aufwand von 2,7 Stunden pro Monat kalkuliert, ebenfalls zu einem internen Stundensatz von 40 CHF.

⁶ <https://www.digicomp.ch/weiterbildung-it-provider/vmware/end-user-computing/kurs-vmware-horizon-deploy-and-manage-v8-8>

⁷ <https://www.digicomp.ch/weiterbildung-it-provider/citrix/kurs-citrix-virtual-apps-and-desktops-7-administration-on-premises-and-in-citrix-cloud-cws-215>

⁸ <https://www.digicomp.ch/weiterbildung-microsoft-technology/microsoft-azure/kurs-configuring-and-operating-microsoft-azure-virtual-desktop-intensive-training-az-140>

Microsoft Azure Estimate

Ihre Schätzung

Service category	Service type	Custom name	Region	Description	Estimated monthly cost	Estimated upfront cost
Compute	Virtual Machines		Switzerland North	1 NC24rs v3 (24 vCPUs, 448 GB RAM) (3 Jahre reserviert), Windows (AHB), Nur Betriebssystem; 0 verwaltete Datenträger – S4; Regionsübergreifender Übertragungstyp, Ausgehende Datenübertragung (5 GB) von Schweiz, Norden zu Ostasien	\$5'116.53	\$0.00
Support		Support			\$100.00	\$0.00
		Licensing Program		Microsoft Customer Agreement (MCA)		
		Billing Account				
		Billing Profile				
		Total			\$5'216.53	\$0.00

Disclaimer

All prices shown are in United States – Dollar (\$) USD. This is a summary estimate, not a quote. For up to date pricing information please visit <https://azure.microsoft.com/pricing/calculator/>

This estimate was created at 3/25/2024 2:16:16 AM UTC.

Tabelle 23: Microsoft Azure Estimate

Es ist zu beachten, dass derzeit lediglich **ein** Azure Virtual Desktop ausgewählt wurde. Für einen direkten Vergleich wäre es erforderlich, einen zusätzlichen virtuellen Server hinzuzufügen. Allerdings wurde bewusst darauf verzichtet, den zusätzlichen Server bereits in die Berechnung einzubeziehen, um die Grundlage des Vergleichs zu vereinfachen und die Ergebnisse zunächst isoliert zu betrachten. Auf diese Weise können wir klarer erkennen, wie sich die Leistung und Kosten des Azure Virtual Desktops allein verhalten, bevor weitere Variablen hinzugefügt werden.

Nutzungsdauer	VMware	Citrix	Azure
Jahr 1	88'080.-	84'625.-	57'405.-
Jahr 2	89'535.-	86'080.-	63'245.-
Jahr 3	90'990.-	87'535.-	69'085.-
Jahr 4	92'445.-	88'990.-	74'925.-
Jahr 5	93'900.-	90'445.-	80'765.-

Tabelle 24: Nutzungsdauer auf 5 Jahren

7 Glossar

Abkürzung / Fachbegriff	Erklärung / Bedeutung
NAS	Network Attached Storage
KMU	Kleine und mittlere Unternehmen
CAD	Computer-Aided Design
FPS	Frames per second
VM	Virtuelle Maschine
Images	Eine Softwarekopie eines physischen Computers, die in einer Datei gespeichert ist. Diese Datei beinhaltet das gesamte System, einschliesslich des Betriebssystems, der installierten Software, der Konfigurationen und der gespeicherten Daten
AVD	Azure Virtual Desktop
VDI	Virtual Desktop Infrastructur
Tenant	Dedizierte und isolierte Instanz innerhalb einer Cloud-Plattform
Peak- und Off-Peak-Zeiten	Höchste Benutzeranmeldung und niedrigste Benutzeranmeldung

Tabelle 25: Glossar

8 Quellenverzeichnis

- Cowley, S. (06. 06 2005). Abgerufen am 17. 03 2024 von
<https://www.networkworld.com/article/865742/software-gaining-speed-citrix-buys-netscaler.html>
- Digicomp. (25. 03 2024). *Digicomp*. Abgerufen am 25. 03 2024 von
<https://www.digicomp.ch/weiterbildung-it-provider/citrix/kurs-citrix-virtual-apps-and-desktops-7-administration-on-premises-and-in-citrix-cloud-cws-215>
- Digicomp. (25. 03 2024). *Digicomp*. Abgerufen am 25. 03 2024 von
<https://www.digicomp.ch/weiterbildung-microsoft-technology/microsoft-azure/kurs-configuring-and-operating-microsoft-azure-virtual-desktop-intensive-training-az-140>
- Digicomp. (25. 03 2024). *Digicomp*. Abgerufen am 25. 03 2024 von
<https://www.digicomp.ch/weiterbildung-it-provider/vmware/end-user-computing/kurs-vmware-horizon-deploy-and-manage-v8-8>
- Mechanics, M. (06. 12 2022). Abgerufen am 17. 03 2024 von
https://www.youtube.com/watch?v=aPEibGMvxZw&ab_channel=MicrosoftMechanics
- Meier, S. (22. 01 2024). *Netzwoche*. Abgerufen am 26. 03 2024 von
<https://www.netzwoche.ch/news/2024-01-22/broadcom-verkleinert-das-vmware-angebot-stark>
- Rao, K. (11. 08 2020). Abgerufen am 17. 03 2024 von
<https://blogs.vmware.com/euc/2020/08/vmware-horizon-8-generally-available.html>
- Tan, H. (22. 11 2023). Abgerufen am 17. 03 2024 von <https://www.broadcom.com/blog/broadcom-announces-successful-acquisition-of-vmware>

Abbildungsverzeichnis

Abbildung 1: NAS von Lugano.....	4
Abbildung 2: Arbeitsmaterial Lugano	5
Abbildung 3: Arbeitsplatz Lugano	5
Abbildung 4: VMware Lösung grafisch.....	13
Abbildung 5: Citrix Lösung grafisch.....	14
Abbildung 6: MS AVD Lösung grafisch	15
Abbildung 7: MS AVD Multisession.....	17

Tabellenverzeichnis

Tabelle 1: Änderungsverzeichnis.....	1
Tabelle 2: Inventar Lugano.....	4
Tabelle 3: Zur Verfügung gestellte Sachmittel	6
Tabelle 4: User Stories.....	8
Tabelle 5: Funktionale Anforderungen	10
Tabelle 6: Nicht-funktionale Anforderungen.....	11
Tabelle 7: Eigenschaften der Lösungsvarianten	13
Tabelle 8: Anforderungsabdeckung	19
Tabelle 9: SWOT-Analyse.....	20
Tabelle 10: Kriterien der Nutzwertanalyse.....	21
Tabelle 11: Gewichtung der Kriterien.....	22
Tabelle 12: Bewertung der Kriterien.....	24
Tabelle 13: Variantenbewertung VMware.....	25
Tabelle 14: Variantenbewertung Citrix	26
Tabelle 15: Variantenbewertung Azure	27
Tabelle 16: Ergebnisse der Nutzwertanalyse.....	28
Tabelle 17: Wirtschaftlichkeit - Personalaufwand.....	30
Tabelle 18: Wirtschaftlichkeit - Anschaffung Server1	30
Tabelle 19: Wirtschaftlichkeit - Anschaffung Server2	31
Tabelle 20: Wirtschaftlichkeit - Anschaffung Synology NAS	31
Tabelle 21: Investitionskosten	32
Tabelle 22: Laufende Kosten.....	32
Tabelle 23: Microsoft Azure Estimate.....	33
Tabelle 24: Nutzungsdauer auf 5 Jahren.....	34
Tabelle 25: Glossar.....	35

Anhang C



Projektauftrag

VDI as a Service

Auftraggeber	Micha Bucher
Projektleiter	Shipinyuan Su, Sirak Yosef
Autor	Shipinyuan Su, Sirak Yosef
Klassifizierung	Intern
Status	Abgesegnet

Änderungsverzeichnis

Datum	Version	Änderung	Autor
03.02.2024	0.1	Dokument erstellt	Shipinyuan Su, Sirak Yosef
17.03.2024	1.1	IST/SOLL Analyse	Shipinyuan Su, Sirak Yosef
22.03.2024	1.2	Projektziele und Lieferobjekte	Shipinyuan Su, Sirak Yosef
24.03.2024	1.3	Abschluss Projektauftrag – Vorgehensweise, Projektplan, Kosten	Shipinyuan Su, Sirak Yosef

Tabelle 1: Änderungsverzeichnis

Inhaltsverzeichnis

1	Ausgangslage	3
2	IST/SOLL Analyse.....	4
3	Projektziele	5
4	Lieferobjekte	6
5	Vorgehensweise & Methodik.....	7
6	Ressourcen	8
7	Projektplan.....	9
8	Freigabe	10

1 Ausgangslage

Dieses Projekt konzentriert sich auf einen speziellen Anwendungsfall: die Verwaltung sensibler Projekte mit strengen Geheimhaltungsanforderungen. Unser Ziel ist es, eine innovative Lösung zu entwickeln, die nicht nur den hohen Sicherheitsstandards gerecht wird, sondern auch die Vorteile der Virtual Desktop Infrastructure (VDI) optimal nutzt. Die Lösung soll eine sichere und isolierte Arbeitsumgebung für vertrauliche Projekte bereitstellen, dabei jedoch die Flexibilität und Standortunabhängigkeit des modernen Arbeitens beibehalten. Auf Basis einer umfassenden Studie, in der verschiedene Virtual Desktop Infrastructure (VDI)-Lösungen evaluiert wurden, wurde die Implementierung der Citrix VDI-Lösung ausgewählt.

2 IST/SOLL Analyse

IST-Zustand

Wie bereits in der Ausgangslage beschrieben, konzentriert sich diese Diplomarbeit auf einen speziellen Anwendungsfall. Im Folgenden wird der IST-Zustand dazu dargelegt.

- **Arbeitsumgebung:** Kunden der Finitia AG, die an streng geheimen Projekten arbeiten, sind an stationäre Arbeitsplätze innerhalb bestimmter Einrichtungen gebunden. Nach gebraucht der Geräte (Notebook & NAS) werden diese wieder in einem Schrank versorgt und eingeschlossen. Diese Arbeitsweise gewährleistet zwar die Sicherheit der sensiblen Daten, schränkt jedoch die Flexibilität der Nutzer erheblich ein.
- **Zugriff auf Daten und Applikationen:** Der Zugang zu Projektdaten und Anwendungen ist ausschliesslich lokal an den zugewiesenen Arbeitsplätzen möglich und sind in einem eigenen Netz.
- **Internetzugang:** Die Arbeitsplätze verfügen über keinen Internetzugang, um die Sicherheit der Daten zu gewährleisten und potenzielle Risiken durch externe Bedrohungen zu minimieren.
- **Flexibilität und Agilität:** Die derzeitige Lösung unterstützt keine flexible oder agile Arbeitsweise. Mitarbeiter können ihre Arbeit nicht von verschiedenen Standorten aus erledigen, was insbesondere in Anbetracht der wachsenden Nachfrage nach flexiblen Arbeitsmodellen als Nachteil wahrgenommen wird.

SOLL-Zustand

Im Rahmen dieses Projekts soll eine neue Citrix VDI-Lösung entwickelt werden, die präzise auf die Bedürfnisse der Kunden von Finitia AG zugeschnitten ist, die an Geheimhaltungsprojekte arbeiten. Sie vereint Modernität mit umfassender Sicherheit und entspricht dabei den strengen Sicherheitsrichtlinien der Finitia AG. Um dies zu erreichen, sollen neue Konzepte entworfen und in einem nächsten Schritt mit bestehenden Lösungen verglichen werden. Das Ziel ist es, eine VDI-Lösung zu schaffen, die nicht nur die aktuellen Anforderungen erfüllt, sondern auch zukunftssicher ist und einen echten Mehrwert für die Nutzern darstellt.

- **Erhöhte Flexibilität und Mobilität:** Durch die Einführung einer sicheren VDI-Lösung von Citrix können die Mitarbeiter der Finitia AG unabhängig von ihrem physischen Standort auf Daten und Applikationen zugreifen. Dies ermöglicht eine flexible Arbeitsweise und unterstützt das Arbeiten von verschiedenen Standorten aus, einschliesslich Homeoffice.
- **Sicherer Fernzugriff:** Die Citrix VDI-Lösung bietet einen sicheren Zugang zu Unternehmensressourcen, selbst wenn Mitarbeiter von ausserhalb der Unternehmensinfrastruktur darauf zugreifen. Sicherheitsrichtlinien und -protokolle sorgen dafür, dass die Integrität und Vertraulichkeit der Daten auch im mobilen Einsatz gewahrt bleibt.
- **Kontinuierlicher Zugriff auf Ressourcen:** Die VDI-Lösung ermöglicht einen konstanten Zugriff auf notwendige Daten und Applikationen, unabhängig von lokalen Einschränkungen. Dies trägt zu einer kontinuierlichen und effizienten Arbeitsweise bei.
- **Anpassung an moderne Arbeitsumgebungen:** Die Implementierung der VDI-Lösung entspricht dem Bedarf an modernen, flexiblen und agilen Arbeitsumgebungen. Sie ermöglicht es der Finitia AG und ihren Kunden, mit den aktuellen Trends der Arbeitswelt Schritt zu halten und die Zufriedenheit und Produktivität der Mitarbeiter zu steigern.

3 Projektziele

Folgende Ziele müssen mit dem ausgewählter Lösungsvariante Citrix VDI erreicht werden.

Nr.	Kategorie	Beschreibung	Messgrösse	Priorität
1	Lieferobjekt	Implementierung einer Citrix VDI (Virtual Desktop Infrastructure) -Lösung als PoC, um flexibles Arbeiten zu ermöglichen	Externes verbinden auf die VDI ist möglich	M
2	Betriebliches Ziel	Gewährleistung der kontinuierlichen Verfügbarkeit der VDI-Lösung, durch strategische Lösungen wie Instant Clones oder Redundanz	Uptime der VDI-Lösung in Prozent in Vergleich zur üblichen Lösung	1
3	Technisches Ziel	Implementierung einer Citrix VDI-Umgebung, die plattformübergreifend kompatibel ist und die Nutzung auf verschiedenen Geräten, einschliesslich auch Smartphones und Tablets, ermöglicht	Prüfung des Abnahmeprotokolls	1
4	Technisches Ziel	Durch den Einsatz von Citrix VDI soll ermöglicht werden, dass auch auf weniger leistungsfähigen Geräten mit hoher Rechenleistung gearbeitet werden kann. Mit der Voraussetzung einer stabilen Internetverbindung.	Zugriffszeiten auf CAD-Programmen: Zeitmessen vom aufstarten von Programmen und öffnen von Dateien sowie das Bearbeiten von Elementen Nutzererfahrung und Reaktionszeit: Feedback von Testusern	1
5	Leistungsziel	Effiziente und Qualitative Leistung von überall	Kein Defizit der Arbeitseffizienz und -qualität, solange eine stabile Internetverbindung vorhanden ist, im Vergleich zu einem PC	1
6	Betriebliches Ziel	Implementierung einer Lösung, die während der Einführungsphase minimale Auswirkungen auf den IT-Betrieb hat	Anzahl Ausfällen und Wartungsarbeiten, die passieren oder gemacht werden müssen während der Implementierung	2
7	Betriebliches Ziel	Reduzierung der Dauer und Erhöhung der Effizienz von Wartungsarbeiten und Änderungsprozesse im IT-Betrieb	Reduzierung der Anzahl Stunden die benötigt werden für einen Change. Analyse der Wiederherstellungszeit des Service	2
8	Technisches Ziel	Projektdaten sind für aussenstehende nicht erreichbar	Daten können nur von bestimmten Personen zugegriffen werden. Es werden mehr als zwei verschiedene Sicherheitsstandards verwendet	M

Priorität: M = Muss / 1 = hoch, 2 = mittel, 3 = tief

Tabelle 2: Projektziele

4 Lieferobjekte

In diesem Kapitel sind die Lieferobjekte für die noch anstehenden Projektphasen definiert und beschrieben.

Konzeptphase:

- **Detailkonzept:** Erarbeitung umfassender technischer Spezifikationen und Designprinzipien für die Citrix VDI-Lösung, inklusive einer klaren Definition der technischen Anforderungen und architektonischen Struktur. Jedes Element des Detailkonzepts sollte mit Erfolgskriterien versehen werden, um die Übereinstimmung mit den Projektzielen messbar zu machen.
- **Testkonzept:** Ausarbeitung einer detaillierten Teststrategie, die spezifische Testfälle, Erfolgskriterien für jeden Testfall und die Methodik zur Bewertung der Testergebnisse umfasst.
- **Migrationskonzept:** Detaillierte Planung des Übergangs von der aktuellen Infrastruktur zur neuen VDI-Umgebung, mit klar definierten Schritten und messbaren Erfolgskriterien für jeden wichtigen Schritt der Phase Migration.
- **Betriebskonzept:** Definition der Betriebsprozesse und -richtlinien mit klaren Leistungsindikatoren (KPIs), die den Erfolg des laufenden Betriebs messbar machen.

Realisierungs- und Einführungsphase

- **Arbeitsprotokoll:** Dokumentation des Projektfortschritts, einschließlich Zeitstempel und Verantwortlichkeiten für jede durchgeführte Aktivität, um die Nachvollziehbarkeit zu gewährleisten.
- **Testbericht:** Darstellung der Testergebnisse mit einer klaren Zuordnung zu den im Testkonzept definierten Testfällen und Erfolgskriterien.
- **Auswertung des Nutzerfeedbacks:** Systematische Zusammenfassung des Feedbacks von Pilotbenutzern mit Nutzerzufriedenheit und Verbesserungsvorschlägen, basierend auf vordefinierte Bewertungskriterien.
- **Schulungsunterlagen/Anleitung:** Entwicklung von Schulungsmaterialien mit klar definierten Lernzielen, die den Benutzern nicht nur die Nutzung, sondern auch das Verständnis der VDI-Lösung erleichtern, inklusive Bewertungsmethoden zur Überprüfung des Lernerfolgs.
- **Endabnahmebericht:** Erstellung eines formalen Dokuments zur offiziellen Projektübergabe, inklusive einer detaillierten Überprüfung, ob und wie die definierten Projektziele erreicht wurden.

Abschluss der Diplomarbeit

- **Kostenberechnung:** Aufstellung aller Projektkosten, mit einem Vergleich der geplanten zu den tatsächlich entstandenen Kosten.
- **Abschlussbericht:** Vollständige Dokumentation der Diplomarbeit und Abgabe
Präsentation: Erstellung einer abschließenden Präsentation, die die Kernergebnisse der Diplomarbeit zusammenfasst.

5 Vorgehensweise & Methodik

Um die VDI-Lösung für die Kunden der Finitia AG zu entwickeln, wird folgende Vorgehensweise verfolgt.

1. **Entwicklung der Konzepte:** In der Konzeptphase wird zunächst eine kurze Analyse der bestehenden Infrastruktur durchgeführt, um ein noch tieferes Verständnis der aktuellen Arbeitsprozesse und Technologien zu erlangen. Darauf aufbauend werden vier Konzepte für die neue VDI-Lösung entwickelt, um den spezifischen Anforderungen der Finitia AG Kunden gerecht zu werden.
2. **Umsetzung der VDI-Lösung:** Nach der Konzeptionsphase folgt die Implementierung der geplanten VDI-Lösung. In dieser Phase wird die technische Realisierung der zuvor entwickelten Konzepte vorgenommen.
3. **Testen der VDI-Lösung:** Die implementierte VDI-Lösung wird anschliessend umfassenden Tests unterzogen, um Funktionalität, Sicherheit und Benutzerfreundlichkeit sicherzustellen. Diese Tests sind entscheidend, um zu gewährleisten, dass die Lösung den festgelegten Anforderungen entspricht.
4. **Auswertung und Anpassung:** Die Ergebnisse aus der Testphase sowie das Feedback der Endnutzer werden sorgfältig dokumentiert und analysiert. Dieser Schritt dient dazu, die Effektivität der VDI-Lösung zu evaluieren und festzustellen, ob sie den definierten Anforderungen gerecht wird. Basierend auf dieser Auswertung werden gegebenenfalls Anpassungen vorgenommen, um die Lösung zu optimieren.

Im folgenden Kapitel ist der Projektplan ersichtlich. Dieser zeigt alle Aktivitäten mit der jeweiligen Deadline genau auf.

6 Ressourcen

Personenaufwand

Person	Stunden insgesamt	Kosten insgesamt
Shipinyuan Su	249.5h	8'732,50 CHF
Sirak Yosef	249.5h	8'732,50 CHF
Thomas Staub	6h	
Tenzin Langdun	6h	

Tabelle 3: Personalaufwand

Kosten

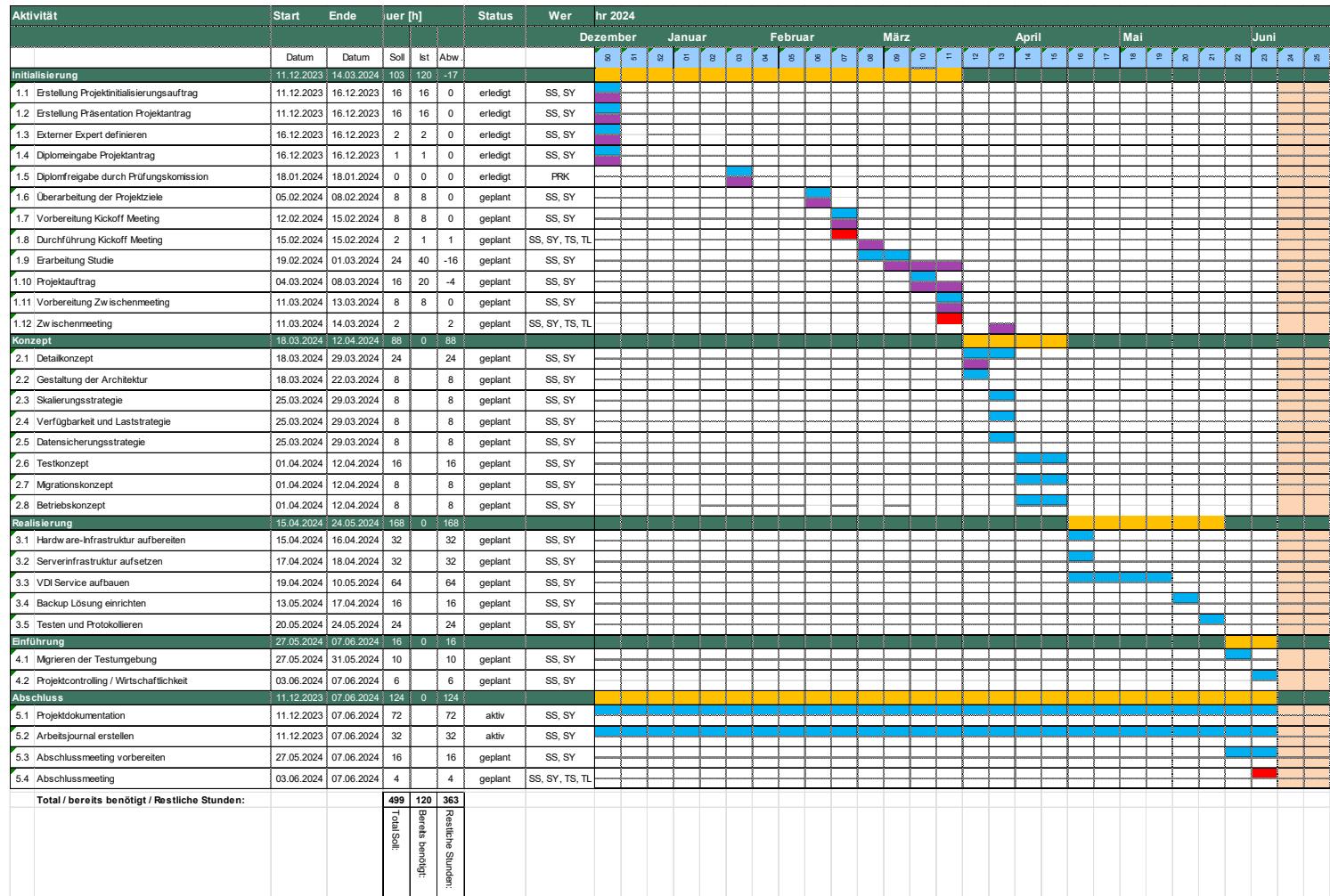
Im Rahmen der Studie wurde eine Analyse der Wirtschaftlichkeit durchgeführt. Dies zielte darauf ab, die finanzielle Auswirkung der Implementierung jeder Lösung über einen Zeitraum von fünf Jahren zu verstehen und miteinander zu vergleichen. Für weitere Details siehe die Studie.

Nutzungsdauer	VMware	Citrix	Azure
Jahr 1	88'080.-	77'089.-	57'405.-
Jahr 2	89'535.-	78'544.-	63'245.-
Jahr 3	90'990.-	79'999	69'085.-
Jahr 4	92'445.-	81'454	74'925.-
Jahr 5	93'900.-	82'909	80'765.-

Tabelle 4: Kosten

7 Projektplan

Das ist der Projektplan von der Diplomarbeit VDI as a Service.



Legende

Name	Abteilung	Abk.
Micha Bucher	Auftraggeber	MB
Thomas Staub	Dozent, Experte	TS
Tenzin Langdun	Experte	TL
Shipinyuan Su	Projektmitarbeiter	SS
Sirak Yosef	Projektmitarbeiter	SY
Marc Aeby, Stefan Krähenbühl	Prüfungskommision	PRK

█ SOLL
█ IST
█ Meilenstein

Abbildung 1: Projektplan

8 Freigabe

Mit der Unterschrift erklären die Experten die Freigabe für den Start der Konzipierung und Umsetzung der Diplomarbeit VDI as a Service für die Firma Finita AG.

Ort / Datum

Unterschrift

Thomas Staub

Ort / Datum

Unterschrift

Tenzin Langdun

Abbildungsverzeichnis

Abbildung 1: Projektplan	9
--------------------------------	---

Tabellenverzeichnis

Tabelle 1: Änderungsverzeichnis.....	1
Tabelle 2: Projektziele.....	5
Tabelle 3: Personalaufwand.....	8
Tabelle 4: Kosten.....	8

Anhang D

Projektplan: VDI as a Service

Aktivität	Start	Ende	Dauer [h]			Status	Wer	Jahr 2023/24																												
			Datum	Datum	Soll	Ist	Abw.	Dezember			Januar			Februar			März			April			Mai			Juni										
								50	51	52	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Initialisierung																																				
1.1 Erstellung Projektinitialisierungsauftrag	11.12.2023	14.03.2024	103	122	-19																															
1.2 Erstellung Präsentation Projektantrag	11.12.2023	16.12.2023	16	16	0	erledigt	SS, SY																													
1.3 Externer Expert definieren	16.12.2023	16.12.2023	2	2	0	erledigt	SS, SY																													
1.4 Diplomeingabe Projektantrag	16.12.2023	16.12.2023	1	1	0	erledigt	SS, SY																													
1.5 Diplomfreigabe durch Prüfungskommission	18.01.2024	18.01.2024	0	0	0	erledigt	PRK																													
1.6 Überarbeitung der Projektziele	05.02.2024	08.02.2024	8	8	0	geplant	SS, SY																													
1.7 Vorbereitung Kickoff Meeting	12.02.2024	15.02.2024	8	8	0	geplant	SS, SY																													
1.8 Durchführung Kickoff Meeting	15.02.2024	15.02.2024	2	1	1	geplant	SS, SY, TS, TL																													
1.9 Erarbeitung Studie	19.02.2024	01.03.2024	24	40	-16	geplant	SS, SY																													
1.10 Projektauftrag	04.03.2024	08.03.2024	16	20	-4	geplant	SS, SY																													
1.11 Vorbereitung Zwischenmeeting	11.03.2024	13.03.2024	8	8	0	geplant	SS, SY																													
1.12 Zwischenmeeting	11.03.2024	14.03.2024	2	2	0	geplant	SS, SY, TS, TL																													
Konzept	18.03.2024	12.04.2024	88	112	-24																															
2.1 Detailkonzept	18.03.2024	29.03.2024	24	34	-10	geplant	SS, SY																													
2.2 Gestaltung der Architektur	18.03.2024	22.03.2024	8	6	2	geplant	SS, SY																													
2.3 Skalierungsstrategie	25.03.2024	29.03.2024	8	4	4	geplant	SS, SY																													
2.4 Verfügbarkeit und Laststrategie	25.03.2024	29.03.2024	8	4	4	geplant	SS, SY																													
2.5 Datensicherungsstrategie	25.03.2024	29.03.2024	8	8	0	geplant	SS, SY																													
2.6 Testkonzept	01.04.2024	12.04.2024	16	24	-8	geplant	SS, SY																													
2.7 Migrationskonzept	01.04.2024	12.04.2024	8	16	-8	geplant	SS, SY																													
2.8 Betriebskonzept	01.04.2024	12.04.2024	8	16	-8	geplant	SS, SY																													
Realisierung	15.04.2024	24.05.2024	168	128	40																															
3.1 Hardware-Infrastruktur aufbereiten	15.04.2024	16.04.2024	32	32	0	geplant	SS, SY																													
3.2 Serverinfrastruktur aufsetzen	17.04.2024	18.04.2024	32	16	16	geplant	SS, SY																													
3.3 VDI Service aufbauen	19.04.2024	10.05.2024	64	40	24	geplant	SS, SY																													
3.4 Backup Lösung einrichten	13.05.2024	17.05.2024	16	16	0	geplant	SS, SY																													
3.5 Testen und Protokollieren	20.05.2024	24.05.2024	24	24	0	geplant	SS, SY																													
Einführung	27.05.2024	07.06.2024	16	16	0																															
4.1 Migrieren der Testumgebung	27.05.2024	31.05.2024	10	8	2	geplant	SS, SY																													
4.2 Projektcontrolling / Wirtschaftlichkeit	03.06.2024	07.06.2024	6	8	-2	geplant	SS, SY																													
Abschluss	11.12.2023	07.06.2024	124	148	-24																															
5.1 Projektdokumentation	11.12.2023	07.06.2024	72	96	-24	aktiv																														

Anhang E1



Detailkonzept

VDI as a Service

Auftraggeber	Micha Bucher
Projektleiter	Shipinyuan Su, Sirak Yosef
Autor	Shipinyuan Su, Sirak Yosef
Klassifizierung	Intern
Status	Von AG abgesegnet

Änderungsverzeichnis

Datum	Version	Änderung	Autor
06.04.2024	0.1	Dokument erstellt	Shipinyuan Su, Sirak Yosef
21.04.2024	1.0	Abschluss Detailkonzept	Shipinyuan Su, Sirak Yosef
25.04.2024	1.1	Erweiterung Architektur und Design, Portzuweisung	Shipinyuan Su, Sirak Yosef
27.04.2024	1.2	Erweiterung Kommunikationsgrafik	Shipinyuan Su, Sirak Yosef

Tabelle 1: Änderungsverzeichnis

Inhaltsverzeichnis

1	Detailkonzept	3
2	Systemübersicht	3
2.1	Voraussetzungen der Umgebung	3
2.2	Architektur und Design	5
2.3	Schnittstellen	7
3	Komponentenbeschreibung	11
3.1	Firewall.....	11
3.2	Switches.....	11
3.3	XenServer Management Server	12
3.4	XenServer Management Server 2	14
3.5	XenServer VDI Server.....	15
3.6	Hauptspeicher	16
3.7	Backupspeicher.....	17
4	Netzwerkkonzept.....	18
4.1	Namenskonzept	18
4.2	VLAN-Segmentierung mit Richtlinien.....	20
4.3	IP-Adressierung.....	21
4.4	Portzuweisungen.....	24
5	Serverrollen & Netzwerk Dienste.....	25
5.1	Domain.....	25
5.2	Active Directory Struktur.....	26
5.3	DNS	28
5.4	DHCP	28
5.5	NTFS.....	29
6	Backup.....	30
6.1	Systemübersicht.....	30
6.2	Ziel system	31
6.3	Strategie.....	31
6.3.1	Aufgabenliste.....	32
6.3.2	Sicherheit und Integrität.....	35

1 Detailkonzept

In diesem Dokument werden Einzelheiten der geplanten VDI-Umgebung definiert. Dies dient als Anhaltspunkt und Leitfaden für die Realisierungsphase. Ziel ist es, zu definieren welche Anforderungen der bestehenden Infrastruktur bestehen, welche Parameter beachtet werden müssen für die Erfüllung der Anforderungen und die allgemeine Dokumentation für die Vollständigkeit. Dabei können potenzielle Herausforderungen und Risiken frühzeitig identifiziert und adressiert werden.

Betriebliche Aspekte wie Wartung, Backupkontrolle, Monitoring, Wirtschaftlichkeit und Support werden separat im Betriebskonzept behandelt.

2 Systemübersicht

In diesem Kapitel erfolgt die konzeptionelle Ausarbeitung des Systems. Zunächst werden die erforderlichen Anforderungen der vorhandenen Umgebung erfasst, die für die Realisierung der geplanten Lösung notwendig sind. Im weiteren Verlauf wird die Gesamtarchitektur des Systems detailliert dargelegt. Dabei werden die Schnittstellen der einzelnen Komponenten dokumentiert. Diese umfangreiche Darstellung ermöglicht es die Interaktionen zwischen den Komponenten zu verstehen und bildet die Grundlage für eine effiziente Implementation des Systems.

2.1 Voraussetzungen der Umgebung

Damit die geplante Infrastruktur aufgebaut werden kann braucht es einige Voraussetzungen der vorhandenen Umgebung.

Anforderung	Erfüllung	Zustand	Massnahmen
Hardwarekomponenten	Die benötigte Hardware ist für die Implementierung der Lösung bereitgestellt	Die erforderlichen Komponenten sind derzeit über verschiedene Standorte verteilt. Die meisten Komponenten sind inaktiv und für die Implementierung bereit. Ein Server wird noch produktiv genutzt	Die Komponenten am vorgesehenen Standort bereitstellen. Den aktuell noch genutzten Server freigeben, damit dieser in der geplanten Umgebung implementiert werden kann
Netzwerkkonfiguration	Alle benötigten VLANs sind auf der Firewall eingerichtet. Es stehen genügend Ports zur Verfügung. Die Ports sind mit den richtigen VLANs konfiguriert	Gewünschte Konfigurationen und Regeln wurden an Dritte weitergeleitet für die Anpassung. Switches und Ports stehen bereit	Definition der genauen Ports und deren Konfigurationen

Anforderung	Erfüllung	Zustand	Massnahmen
Sicherheit	<p>Die Komponenten werden an einem sicheren Ort betrieben.</p> <p>Die Verwendung eines Antivirusprogramms ist vorgesehen.</p> <p>Das Netzwerk ist sicher segmentiert und isoliert.</p>	<p>Die Server werden in einem Tier-4-Rechenzentrum betrieben.¹</p> <p>Auf den Management-Server kann durch die Internetverbindung ein Endpoint Security-Programm installiert werden. Für die VMs ist der Windows Defender ausreichend.</p> <p>Das Netzwerk wird über VLANs segmentiert und isoliert.</p>	Keine spezifischen Massnahmen erforderlich
Lizenzen und Software	<p>Lizenzen für den Betrieb der VDI-Umgebung muss bereitgestellt sein</p> <p>Lizenzen für gewünschte CAD-Programme stehen zur Verfügung</p>	<p>Citrix Lizenzen stehen der Firma zur Verfügung</p> <p>Lizenzen für CAD-Programme müssen von den Kunden selbst organisiert werden. Die Einrichtung wird vom Engineering Team übernommen</p>	Definition der gewünschten CAD-Programme und Einrichtung der Lizenzserver
Ressourcen	<p>Das Engineering Team ist einsatzbereit für die Realisation</p> <p>Drittpartner sind bei Anfragen oder Fragen erreichbar</p>	<p>Das Engineering Team ist einsatzbereit</p> <p>Drittpartner sind bei Anfragen oder Fragen erreichbar</p>	Keine spezifischen Massnahmen erforderlich

Tabelle 2: Voraussetzungen der Umgebung

¹ <https://www.datacenter-insider.de/von-tier1-bis-tier-4-die-vier-qualitaetsstufen-eines-rechenzentrums-a-341120/>

2.2 Architektur und Design

In der nachfolgenden Grafik sieht man die oberflächliche Architektur der VDI-Umgebung.

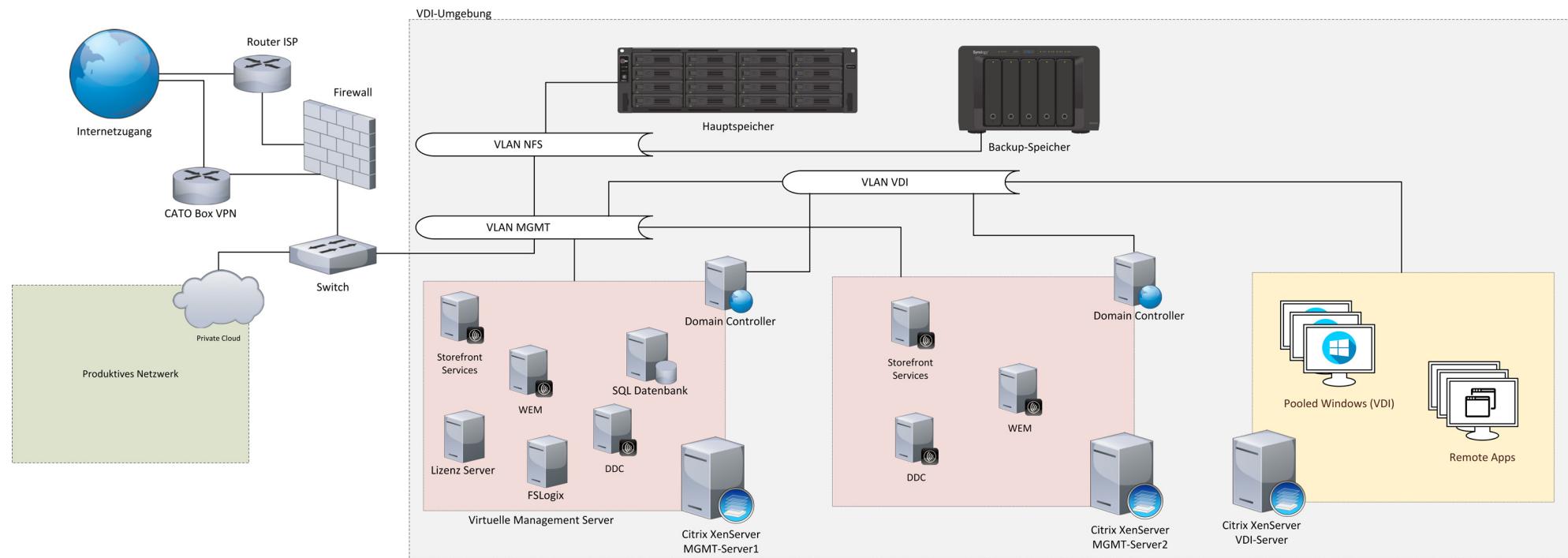


Abbildung 1: Oberflächliche Architektur Grafik

Diese Grafik dient als Orientierungspunkt für die Konzeptionierung der Infrastruktur. Als Grundlage werden drei VLANs verwendet: MGMT (Management), NFS (Network File System) und VDI (Virtual Desktop Infrastructure). Diese stellen sicher, dass die einzelnen Komponenten korrekt segmentiert sind und durch Regeln die korrekten Kommunikationswege geschaffen werden. Diese Umgebung wird zur vorhandenen Umgebung ergänzt.

Für die ausgewählte Lösung, Citrix, werden verschiedene Servicekomponenten benötigt, damit das Ganze reibungslos funktioniert.²

Desktop Delivery Controller (DDC): Ist die zentrale Verwaltungskomponente und muss mindestens auf einem Server pro Standort installiert sein. Man kann den DDC redundant aufbauen, indem man den Kontroller auf verschiedene Server installiert. Mit einem Management Server wird es in dieser Umgebung nicht möglich sein, eine Hardwareredundanz aufzubauen. Der DDC ist zuständig für:

- Verteilung von Desktops und Anwendungen
- Authentifizierung und Verwaltung des Benutzerzugriffs
- Vermittlung von Verbindungen zwischen Benutzern und ihren Desktops und Anwendungen
- Optimierung von Benutzerverbindungen
- Lastausgleich der Verbindungen

Datenbank: Für jeden Standort ist eine Microsoft SQL Datenbank erforderlich, welche die Konfigurations- und Sitzungsinformationen speichert. Die Kontroller müssen eine konsistente Verbindung auf diese Datenbanken haben, da hier die Daten gespeichert sind, die von den Diensten der Kontroller erfasst und verwaltet werden. Diese Datenbank wird standardmäßig auch als Logdatenbank verwendet.

StoreFront: Ist zuständig für die Authentifizierung der Benutzer und verwaltet die Zugriffe von Desktops und Anwendungen, auf denen die Benutzer Zugriff haben. Mit diesem Service haben Benutzer die Möglichkeit auf eine Selbstbedienungszugriff auf Ihre Desktops und Anwendungen. Dies bietet dem Benutzer eine einheitliche Benutzererfahrung über verschiedene Geräte hinweg.

Lizenz Server: Zuständig für die Verwaltung der Citrix-Produktlizenzen. Kommuniziert mit dem Kontroller, um die Lizenzierung für die Sitzungen der einzelnen Benutzer zu verwalten. Auch hier braucht es mindestens einen Lizenz Server pro Standort.

Workspace Environment Management (WEM): Service für die Profilbereitstellung von Ressourcen wie: Anwendungen, Drucker, Netzlaufwerke, Registrierungsschlüssel und mehr.

FSLogix: Ein Microsoft Produkt für das managen von Windows-Benutzerprofile in virtuellen Desktop-Computing-Umgebungen.

² <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/technical-overview.html>

2.3 Schnittstellen

Durch die Verwendung von mehreren Komponenten gibt es viele verschiedene Schnittstellen die zu beachten sind und dokumentiert werden müssen.

Netzwerkinfrastruktur: Die vorhandene Netzwerk Infrastruktur wird von einem Drittpartner verwaltet. Die Internetverbindung wird durch den Internet Service Provider (ISP) Sunrise über eine Business Leitung bereitgestellt. Hierbei kommen CAT6A Kupferkabel als auch Glasfaserkabel für die Verbindung zum Einsatz.

Zur Verwaltung des Netzwerkes werden die vom Hersteller bereitgestellten Management Tools genutzt. Um die Konfigurationen der Switches anzupassen, müssen Änderungsaufträge an den Dritt-partner gesendet werden.

Schnittstelle	Typ	Protokoll / Standard	Verwendung	Bemerkung
RJ45	Hardware	CAT6A Kupfer-kabel	Verbindung zwi-schen Geräten im Netzwerk	Optimal für kurze Strecken. Unter-stützt eine Daten-übertragung bis zu 10Gb/s
SFP-Ports	Hardware	Glasfaser	Verbindung zwi-schen Standorten	Optimal für längere Strecken
Netzwerk-Ma-nagement	Software	OSI-Schichten 2-3 (z.B. IP, TCP, UDP)	Netzwerkkommuni-kation und -manage-ment	Unterstützt eine Viel-zahl von Netzwerk-protokollen
Webzugänge	Software	HTTP/HTTPS	Management über Webbrowser	Wird meist als Haupt Verwaltungstool ver-wendet
CLI	Software	SSH	Fernsteuerung von Netzwerkgeräten und Server	Befehlsausführung über Commando Zeilen
VPN	Software	SSL, TCP	Sichere Verbindung über öffentliches Netz ins interne	Wichtig für die Si-cherstellung des ex-ternen Zugangs
NAS	Hardware	NFS, iSCSI	Netzwerkspeicher	Wird als Hauptspei-cher der Umgebung verwenden
Router	Hardware	Ethernet	Netzwerkgerät für den Verkehr zwi-schen dem Internet und dem internen Netzwerk	Wird vom ISP zur Verfügung gestellt

Schnittstelle	Typ	Protokoll / Standard	Verwendung	Bemerkung
Switch	Hardware	Ethernet	Netzwerkgerät für den Verkehr zwischen verschiedenen Netzwerkkomponenten	Wird vom Dritt-partner verwaltet
Firewall	Hardware	Ethernet	Überwacht und steuert den ein- und ausgehenden Datenverkehr	Schutz durch Sicherheitsregeln, die weiter unten im Netzwerkkonzept definiert werden
VLAN	Software	VLAN-Tagging	Segmentiert ein physisches Netzwerk in mehrere logischen Netzwerke	Trennung des Datenverkehrs, gemäss Anforderungen

Tabelle 3: Schnittstellen Netzwerk Infrastruktur

Citrix Umgebung: In der neu implementierten VDI-Lösung führt es zu viele neue Schnittstellen, die sowohl während der Implementierung als auch im laufenden Betrieb berücksichtigt werden müssen. Es ist entscheidend, das Zusammenspiel der verschiedenen Komponenten zu dokumentieren, um einen effizienten und sicheren Betrieb der Lösung zu gewährleisten. Die Arten der Verbindungen und die Methoden für die Fernverwaltung, die bereits in der bestehenden Netzwerkinfrastruktur Anwendung finden, werden auch hier verwendet und bedürfen daher keiner erneuten Erörterung.

Schnittstelle	Typ	Protokoll / Standard	Verwendung	Bemerkung
Virtual Delivery Agent (VDA)	Software	TCP	Stellt die Verbindung zwischen der VM und dem Benutzerendgerät her	Muss auf jede VM installiert sein, damit eine Sitzung aufgebaut werden kann
Citrix Workspace App	Software	TCP, HTML5	Bietet Zugriff auf die zugewiesenen Desktops und Anwendungen	Wird auf den Endgeräten installiert oder kann über einen HTML5 kompatiblen Webbrowser direkt eine Sitzung gestartet werden
Citrix Studio	Software	TCP	Ist die Verwaltungskonsole für die Bereitstellung von Citrix Virtual Apps und Desktops. Verwaltung von Lizenzien	Kommuniziert mit dem DDC und wird auch auf dem Server betrieben

Schnittstelle	Typ	Protokoll / Standard	Verwendung	Bemerkung
Citrix Director	Software	OData, HTTPS, SQL	Ermöglicht die Überwachung der Umgebung	Kann mehrere Citrix Virtual Apps und Virtual Desktops Standorte verbinden und diese überwachen, sei es Echtzeit oder über Datenbanken
Domain Controller	Software	DNS, DHCP, LDAP, Kerberos	Benutzeroauthentifizierungsstelle, IP-Verteilung und Namesauflösung	Zentral für die Verwaltung der Domäne
VDI-Maschinen	Software	ICA /HDX	Ressource der virtuellen Desktops	Zentrale Komponente der VDI-Lösung
Lizenz Server	Software	TCP	Verwaltung von Citrix Lizzenzen	Mindestens ein Lizenzserver pro Standort erforderlich
FSLogix	Software	SMB	Profilmanagement in VDI-Umgebungen	Verbessert die Benutzererfahrung
WEM	Software	TCP, UDP	Profil- und Umgebungsmanagement	Verbessert die Benutzererfahrung und stellt die korrekten Ressourcen zur Verfügung
SQL-Datenbank	Software	TCP/IP	Speichern von Konfigurations- und Sitzungsinformationen	Zentral für die Datenhaltung und Reporting
DDC	Software	LDAP, Kerberos, HTTPS, XML	Zuständig für die Zuweisung und Verwaltung von VDIs	Ist das Zentrale Verwaltungssystem für die VDIs
StoreFront	Software	HTTPS/SSL	Dient als Zugangspunkt für Benutzer und verwaltet die Authentifizierung	Bietet eine personalisierbare Benutzeroberfläche

Tabelle 4: Schnittstellen Citrix Umgebung

Kommunikationsgrafik

Diese Grafik zeigt, wie die einzelnen Komponenten miteinander kommunizieren. Dabei werden die wichtigsten Ports dargestellt, die für den Service notwendig sind. Die durchgehenden Pfeile stellen physische Verbindungen dar, während die gestrichelten Pfeile logische Kommunikation anzeigen.

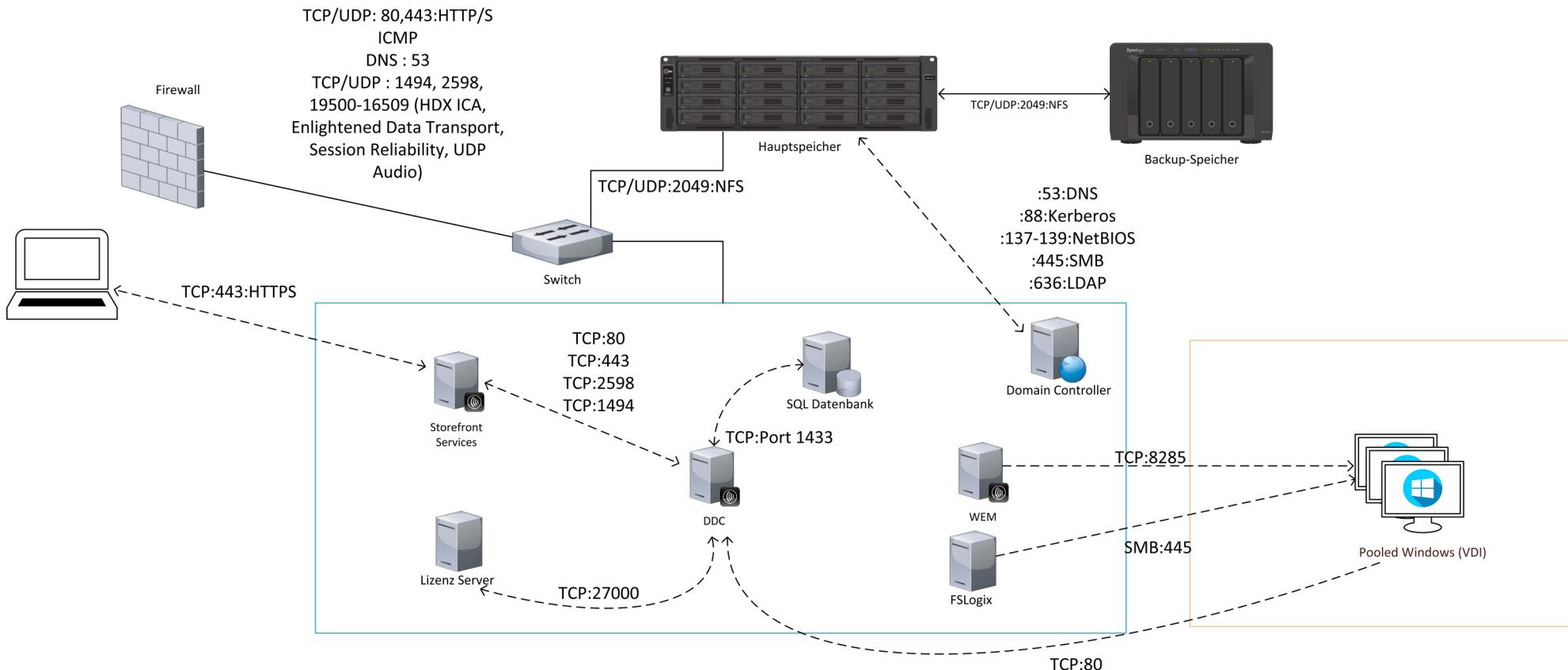


Abbildung 2: Kommunikationsgrafik

3 Komponentenbeschreibung

Alle Komponenten werden vollständig von der Firma Finitia AG zur Verfügung gestellt. In diesem Kapitel werden alle Komponenten aufgelistet und beschrieben.

3.1 Firewall

Neben der Rolle, den Datenverkehr zu kontrollieren und zu überwachen, hat es auch noch andere Funktionen, wie VLAN-Regelungen oder E-Mail-Filterung.

Komponente	Funktion	Konfiguration	Wartung und Support	Hersteller
Sophos X430	Überwacht und steuert den ein- und ausgehenden Datenverkehr	High Availability (HA) ist eingerichtet (Active-Passive)	Wird vom Dritt-partner verwaltet	Sophos

Tabelle 5: Firewall Beschreibung

3.2 Switches

Switches übernehmen eine Kernfunktion im Netzwerk bei der Segmentierung von Netzwerken. Sie sind ein unverzichtbarer Bestandteil des Netzwerks, nicht nur für die Weiterleitung des Datenverkehrs, sondern auch für dessen Steuerung und Sicherheit.

Komponente	Funktion	Anzahl Ports	Spezifikation	Wartung und Support	Hersteller
Core switch	Netzwerkgerät für den Verkehr zwischen verschiedenen Netzwerk-komponenten	96 Ports	Netgear M4300-96X Modular Managed Switch Module APM408C Module für Glas APM408F	werden vom Drittpartner verwaltet	Netgear
Core Switch		96 Ports	Netgear M4300-96X Modular Managed Switch	werden vom Drittpartner verwaltet	Netgear
Core Switch		48 Ports	Netgear M4300-48X ProSAFE	werden vom Drittpartner verwaltet	Netgear

Tabelle 6: Switches Beschreibung

3.3 XenServer Management Server

Der Management Server ist ein Kernstück der VDI-Umgebung und hostet mehrere virtuelle Maschinen, die wichtige Funktionen für die Umgebung bereitstellen.

Komponente	Funktion	Spezifikationen ³	Betriebs-system	Wartung und Sup-port	Hersteller
Rack Server	Dient als Hypervisor für alle Management VMs, die für die Umgebung benötigt werden	2x Intel Xeon Silver 2.4 GHz, 10 Cores 768GB RAM 1x NVIDIA A16 2x 2TB SSD 10Gbp/s Netzwerkarte	XenServer Version 8	5 Jahre On-Site Garantie vom Hersteller	Super-Micro
StoreFront	Dient als Zugangspunkt für Benutzer und bietet eine personalisierbare Benutzeroberfläche	2 CPU-Cores 4GB RAM 100GB Speicher	Microsoft Windows Server 2022 21H2	Support von Citrix Cloud Service Provider, Wartung durch Engineering Team	Citrix Microsoft
SQL-Datenbank	Speichern von Konfigurations- und Sitzungsinformationen	4 CPU-Cores 4 GB RAM 200GB Speicher	Microsoft Windows Server 2022 21H2	Wie im oberen Feld	Microsoft
Lizenzserver	Verwaltung von Citrix Lizenzen	2 CPU-Cores 4 GB RAM 100 GB Speicher	Microsoft Windows Server 2022 21H2	Wie im oberen Feld	Citrix Microsoft
WEM	Profil- und Umgebungsmanagement	2 CPU-Cores 4 GB RAM 100 GB Speicher	Microsoft Windows Server 2022 21H2	Wie im oberen Feld	Citrix Microsoft

³ <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/1912-ltsr/system-requirements.html>

Komponente	Funktion	Spezifikationen ³	Betriebs-system	Wartung und Sup-port	Hersteller
DDC	Zuständig für die Zuweisung und Verwaltung von VDIs	4 CPU-Cores 8 GB RAM 100 GB Speicher	Microsoft Windows Server 2022 21H2	Wie im oberen Feld	Citrix Microsoft
FSLogix	Profilmanagement in VDI-Umgebungen	6 CPU-Cores 32 GB RAM 500 GB Speicher	Microsoft Windows Server 2022	Wie im oberen Feld	Microsoft
VDI-Klone	Kopie des Golden Images. Steht zur Verfügung für eine Individuelle Benutzerinstanz Durch Verfügbare Grafikkarte des Servers ist es auch hier möglich VDI-Klone zu Verfügung zu stellen	Identisch zur ausgewähltem Golden Image	Windows Pro 22H2	Wie im oberen Feld	Microsoft
DC	Benutzeroauthentifizierungsstelle, IP-Verteilung und Namesauflösung	2 CPU-Cores 4 GB RAM 100 GB Speicher	Microsoft Windows Server 2022 21H2	Engineering Team und Dritt-partner	Microsoft

Tabelle 7: XenServer Management Server

3.4 XenServer Management Server 2

Komponente	Funktion	Spezifikationen ⁴	Betriebs-system	Wartung und Sup-port	Hersteller
Desktop PC	Dient als Hypervisor für alle Management VMs, die für die Umgebung benötigt werden	2x Intel Xeon Silver 2.4 GHz, 10 Cores 768GB RAM 1x NVIDIA A16 2x 2TB SSD 10Gbp/s Netzwerkkarte	XenServer Version 8	5 Jahre On-Site Garantie vom Hersteller	Super-Micro
StoreFront	Dient als Zugangspunkt für Benutzer und bietet eine personalisierbare Benutzeroberfläche	2 CPU-Cores 4GB RAM 100GB Speicher	Microsoft Windows Server 2022 21H2	Wie im oberen Feld	Citrix Microsoft
WEM	Profil- und Umgebungsmanagement	2 CPU-Cores 4 GB RAM 100 GB Speicher	Microsoft Windows Server 2022 21H2	Wie im oberen Feld	Citrix Microsoft
DDC	Zuständig für die Zuweisung und Verwaltung von VDIs	4 CPU-Cores 8 GB RAM 100 GB Speicher	Microsoft Windows Server 2022 21H2	Wie im oberen Feld	Citrix Microsoft
DC	Benutzerauthentifizierungsstelle, IP-Verteilung und Namesauflösung	2 CPU-Cores 4 GB RAM 100 GB Speicher	Microsoft Windows Server 2022 21H2	Engineering Team und Dritt-partner	Microsoft

Tabelle 8: XenServer Management Server 2

⁴ <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/1912-ltsr/system-requirements.html>

3.5 XenServer VDI Server

Der VDI-Server ist ein zentraler Bestandteil der Umgebung und verantwortet die Bereitstellung und Verwaltung der virtuellen Desktops, die den Benutzern in der Umgebung zur Verfügung gestellt werden.

Komponente	Funktion	Spezifikationen	Betriebs-system	Wartung und Sup-port	Hersteller
Rack Server	Dient als Hypervisor für alle VDIs, die für die Benutzern zur Verfügung gestellt werden	2x Intel Xeon Gold 5317 CPU at 3.00 GHz / 12 Cores pro CPU 1TB RAM 2x NVIDIA A16 2x 2TB SSD 1x RAID-Controller 10Gbp/s Netzwerkkarte	XenServer Version 8	5 Jahre On-Site Garantie vom Hersteller	Super-Micro
Golden Image grosse Profil	Dient als Vorlage für das Windows Image, für das grössere Profil	10 CPU-Cores 64 GB RAM 500 GB Speicher 8 GB VRAM	Windows 10 Pro 22H2	Monatliche Updates, Helpdesk Support gemäss SLA	Microsoft
Golden Image kleine Profil	Dient als Vorlage für das Windows Image, für das kleinere Profil	8 CPU-Cores 32 GB RAM 500 GB Speicher 4 GB VRAM	Windows 10 Pro 22H2	Monatliche Updates, Helpdesk Support gemäss SLA	Microsoft
VDI-Klone vom grossen Profil	Kopie des Golden Images. Steht zur Verfügung für eine Individuelle Benutzerinstanz	10 CPU-Cores 64GB RAM 500 GB Speicher 8 GB VRAM	Windows 10 Pro 22H2	Monatliche Updates, Helpdesk Support gemäss SLA	Microsoft

Komponente	Funktion	Spezifikationen	Betriebs-system	Wartung und Sup-port	Hersteller
VDI-Klone vom kleinen Profil	Kopie des Golden Images. Steht zur Verfügung für eine Individuelle Benutzerinstanz	8 CPU-Cores 32 GB RAM 500 GB Speicher 4 GB VRAM	Windows 10 Pro 22H2	Monatliche Updates, Helpdesk Support gemäss SLA	Microsoft

Tabelle 9: XenServer VDI Server

3.6 Hauptspeicher

Komponente	Funktion	Spezifikationen	Betriebs-system	Wartung und Sup-port	Hersteller
Synology FS6400	Hauptspeicher für die Datenablage	INTEL Xeon Silver 4110 at 2.1 GHz / 16 Cores 128 GB RAM 24x 3.5 TB SSD 2x 10Gbp/s Netzwerkkarte	DSM 7.2-64570 Update 1	5 Jahre On-Site Garantie vom Hersteller	Synology

Tabelle 10: Hauptspeicher Synology FS6400

3.7 Backupspeicher

Komponente	Funktion	Spezifikationen	Betriebs-system	Wartung und Sup-port	Hersteller
Synology DS1823xs+	Dient als Backup-Speicher für alle Server	AMD Ryzen V1780B at 3.35 GHz / 4 Cores 24 GB RAM 5x 9.1 TB HDD	DSM 7.2-64570 Update 1	5 Jahre On-Site Garantie vom Hersteller	Synology

Tabelle 11: Backupspeicher

4 Netzwerkkonzept

Dieses Kapitel vermittelt klare Einblicke in die Struktur und das Design des Netzwerks. Es beginnt mit dem Namenskonzept, das die Bezeichnung von den Ressourcen erläutert. Die VLAN-Segmentierung wird beschrieben, also wie das Netzwerk unterteilt ist. Im Teil IP-Adressierung wird die Vergabe der IP-Adressen für eine nahtlose Konnektivität besprochen. Zum Schluss zeigt das Unterkapitel Portzuweisung, den physischen Anschluss im Netzwerk dar.

4.1 Namenskonzept

Das Namenskonzept für die Citrix VDI-Poc-Umgebung bringt Klarheit und Struktur in die IT-Infrastruktur und erleichtert die Navigation durch virtuelle Architektur. Zudem wurde ausser bei den physischen und virtuellen Servern, entscheiden das noch "poc" im Namen steht, um sie noch besser von der produktiven Umgebung zu unterscheiden.

Namensaufbau

Für physische XenServer beginnt der Namensaufbau mit "xen", gefolgt von der Funktion des Servers und schliesst mit einer numerischen Sequenz ab.

- Beispiel: "xen-mgmt-01" für den ersten Management-Server.

Bei anderen Servern beginnt der Name mit "srv", gefolgt von der Abkürzung der Funktion des Servers und endet ebenfalls mit einer numerischen Sequenz, um zusätzliche Server des gleichen Typs kenntlich zu machen.

- Beispiel: "srv-dc-01" für den ersten Domain Controller und "srv-dc-02" für den zweiten.

Für die VLANs beginnt der Name mit der Abkürzung des Netzwerks, gefolgt von "poc".

- Beispiel: "vdi-poc" für das Virtual-Desktop-Infrastrukturnetzwerk oder "mgmt-poc" für das Managementnetzwerk.

Die Namen der verschiedenen VDI-Gruppen beginnen mit dem Typ, wie "MC". Danach folgt "VDI" zusammen mit der entsprechenden Abstufe. Am Ende werden bei Bedarf die Sprache und eine numerische Sequenz hinzugefügt.

- Beispiel: "MC/DG_VDI-Basic-DE"
- Beispiel: "AG_VDI-Premium-DE" (Zugriffsgruppe/Access Group)

In diesem Projekt gibt es zwei Profiltypen: Basic mit normaler Leistung und Premium mit erhöhter Leistung. Die Namenskonvention dieser Profiltypen ist wie folgt aufgebaut: Sie beginnt mit "vdi", was den Typ beschreibt, gefolgt von "basic" oder "premium", die Sprache und schliesst mit einer numerischen Sequenz ab.

- Beispiel: "vdi-basic-de-01"

Wie folgt sind noch alle Server, VLANs, VDI-Ressourcen und Profile mit der Namenskonvention ersichtlich.

Physische Server:

- XenServer Management-Server: xen-mgmt-01
- XenServer VDI-Server: xen-vdi-01

Virtuelle Server:

- **Domain Controller:**
 - Erster Domain Controller: srv-dc-01
 - Zweiter Domain Controller: srv-dc-02
- **Zugang und Services:**
 - Access Gateway: srv-gw-01
 - Storefront Services: srv-sfs-01
 - Workspace Environment Management (WEM): srv-wem-01
 - Desktop Delivery Controller (DDC): srv-ddc-01
- **Datenbank und Lizenzen:**
 - SQL-Datenbankserver: srv-dc-01
 - Lizenzserver: srv-lic-01
 - FSLogix: srv-fslx-01

Virtuelle Netzwerke:

- NFS-Netzwerk: nfs-poc
- Management-Netzwerk: mgmt-poc
- VDI-Netzwerk: vdi-poc

VDI-Ressourcen:

- Machine Catalog und Delivery Group: MC/DG_VDI-Basic-de

VDI-Desktop:

- Windows VDI Desktop: GP-Basic-VDI-DE

VDI-Gruppen:

- Active Directory Gruppen für VDI: AG_VDI-Basic-DE
- Active Directory Gruppen für WEM: AG_WEM-Projekt0001-DE

Profile:

- Basisprofil (normale Leistung): vdi-basic-de-01
- Premiumprofil (fortgeschrittene Leistung): vdi-prem-de-01

4.2 VLAN-Segmentierung mit Richtlinien

Um die Netzwerksicherheit zu erhöhen und ein flaches Netzwerk zu vermeiden, in dem alle Geräte sich im gleichen Netzwerksegment befinden, wurde entschieden, drei VLANs zu etablieren, die virtuell voneinander getrennt sind.

Hier sind die drei neu definierten VLANs mit ihren spezifischen IDs:

- ID 210: Netzwerk für Network File System (NFS)
- ID 220: Management-Netzwerk (MGMT)
- ID 230: Virtual Desktop Infrastructure-Netzwerk (VDI)

Darüber hinaus existiert das VLAN 301, welches Teil des Produktionsnetzwerks ist. Über dieses VLAN kann auf das MGMT-Netzwerk zugegriffen werden. Die Netzwerksegmentierung ermöglicht es, Zugriffsrechte durch Netzwerkrichtlinien präzise zu definieren und zu steuern. Die beigegebene Abbildung veranschaulicht die Segmentierung und die definierten Netzwerkrichtlinien, repräsentiert durch die eingezeichneten Verbindungen und Pfeile. In der grafischen Darstellung erscheint der zentrale Speicher doppelt, was darauf hinweist, dass er eine Schnittstelle sowohl zum MGMT-Netzwerk als auch zum NFS-Netzwerk besitzt.

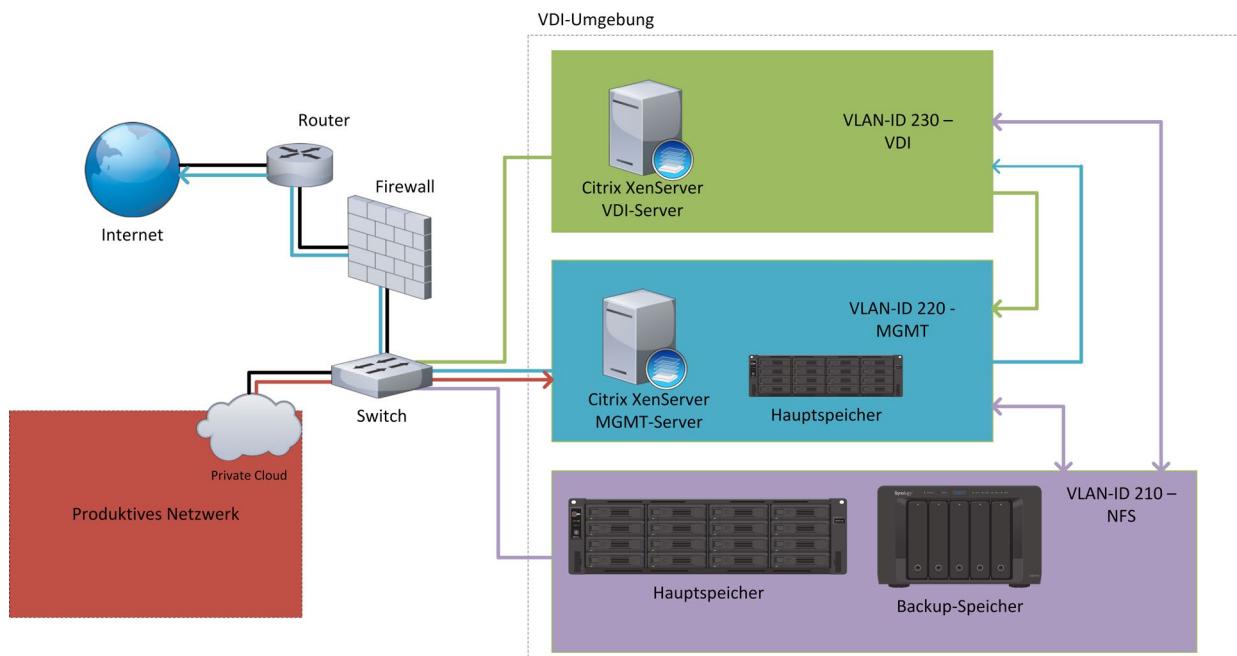


Abbildung 3: Netzwerksegmentierung

Es wurden folgende Netzwerkrichtlinien festgelegt:

- Das NFS-Netzwerk ist ein abgeschlossenes Segment, das speziell für den Datentransfer zwischen den virtuellen Servern und für Backup-Prozesse zuständig ist. Dies wird in der Abbildung durch violette Pfeile dargestellt
- Das MGMT-Netzwerk ist mit dem Internet verbunden und ermöglicht Zugriff auf das VDI-Netzwerk. Außerdem ist es vom produktiven Netzwerk über VLAN 301 zugänglich, allerdings ist keine gegenseitige Verbindung möglich. Diese Verbindungen sind in der Abbildung mit blauen Pfeilen markiert.
- Das VDI-Netzwerk ist ein isoliertes Segment ohne direkten Internetzugang. Es hat lediglich Zugriff auf den Hauptspeicher, der sich im MGMT-Netzwerk befindet, da dieser die Datenablage bereitstellt. Diese Verbindung ist in der Abbildung mit einem grünen Pfeil gekennzeichnet. Nur das MGMT-Netzwerk hat Zugriff, während alle anderen Netze keinen Zugriff haben auf das VDI-Netzwerk haben.

4.3 IP-Adressierung

Die IP-Adressierung bietet eine klare und detaillierte Darstellung der Adressvergabe innerhalb der PoC-Umgebung. Sie legt die Adresszuweisungen innerhalb der VLAN-Struktur fest. Um die Klarheit des IP-Konzepts zu gewährleisten und gleichzeitig eine deutliche Abgrenzung zur Produktivumgebung zu schaffen, wurde entschieden, die VLAN-ID im dritten Oktett zu platzieren. Somit ergibt 192.168.[VLAN-ID].0/24 für das entsprechende Netz.

Hier werden alle drei VLANs sowie die zugehörigen Gateways dargestellt.

Subnetz	VLAN-ID	Gateway	Beschreibung
192.168.210.0/24	210	keiner	Nur auf Switch Layer-2
192.168.220.0/24	220	192.168.220.1	Sophos Firewall
192.168.230.0/24	230	192.168.230.1	Sophos Firewall

Tabelle 12: VLANs & Gateways

Hier sind die XenServer, Backup-Server und der Hauptspeicher ersichtlich, die über die NFS-Verbindung kommunizieren. Da es sich um physische Geräte mit festen Anschlüssen handelt, beginnt deren IP-Adressierung bei ".10."

Typ	Hostname	IP-Adresse	Beschreibung
XenServer	xen-mgmt-01	192.168.210.10	MGMT / NFS-Leitung
XenServer	xen-mgmt-02	192.168.210.11	MGMT / NFS-Leitung
XenServer	xen-vdi-01	192.168.210.13	VDI / NFS-Leitung 1
XenServer	xen-vdi-01	192.168.210.14	VDI / Backup NFS-Leitung 2
Storage	srv-backup-01	192.168.210.15	Backup / NFS-Leitung
Storage	srv-data-01	192.168.210.16	Hauptspeicher / NFS-Leitung 1
Storage	srv-data-01	192.168.210.17	Hauptspeicher / Backup NFS-Leitung 2

Tabelle 13: NFS-Leitung

Hier sind die beiden XenServer mit ihren jeweiligen IP-Adressen aufgeführt, sowie der Hauptserver, der über eine zweite Netzwerkschnittstelle Zugang zu diesem Netzwerksegment besitzt. Da es sich bei diesen Komponenten um physische Geräte handelt, beginnt die IP-Addressierung auch in diesem Fall bei ".10."

Typ	Hostname	IP-Adresse	Beschreibung
XenServer	xen-mgmt-01	192.168.220.10	Physischer MGMT-Server 1
XenServer	xen-mgmt-02	192.168.220.11	Physischer MGMT-Server 2
XenServer	xen-vdi-01	192.168.220.13	Physischer VDI-Server
XenServer	xen-vdi-01	192.168.220.14	Physischer VDI-Server
Storage	srv-data-01	192.168.220.15	Hauptspeicher / MGMT-Leitung

Tabelle 14: XenServer & Storage

Hier sind alle virtuellen Server aufgeführt. Es wurde entschieden, bei den virtuellen Servern mit der IP-Adressvergabe innerhalb des jeweiligen Netzwerks bei .20 zu beginnen.

Typ	Hostname	IP-Adresse	Beschreibung
Virtueller Windows Server	srv-sfs-01	192.168.220.21	Storefront Services
Virtueller Windows Server	srv-sfs-02	192.168.220.31	Storefront Services
Virtueller Windows Server	srv-wem-01	192.168.220.22	Workspace Environment Management
Virtueller Windows Server	srv-wem-02	192.168.220.32	Workspace Environment Management
Virtueller Windows Server	srv-ddc-01	192.168.220.23	Desktop Delivery Controller
Virtueller Windows Server	srv-ddc-02	192.168.220.33	Desktop Delivery Controller
Virtueller Windows Server	srv-db-01	192.168.220.24	SQL-Datenbankserver
Virtueller Windows Server	srv-lic-01	192.168.220.25	Lizenzserver
Virtueller Windows Server	srv-fslx-01	192.168.220.26	FSLogix

Tabelle 15: Virtuelle Server

Hier sind die beiden Domain Controller, der Windows VDI-Pool sowie der DHCP-Bereich dargestellt. Der DHCP-Bereich erstreckt sich von .30 bis .200.

Typ	Hostname	IP-Adresse	Beschreibung
Virtueller Windows Server	srv-dc-01	192.168.230.20	DC / DHCP / DNS
Virtueller Windows Server	srv-dc-02	192.168.230.21	DC / DHCP / DNS
DHCP-Range	vdi-range	192.168.230.30 – 192.168.230.200	DHCP => srv-dc-01/02

Tabelle 16: Domain Controller & DHCP Range

4.4 Portzuweisungen

In dieser Grafik wird gezeigt, wie die verschiedenen Komponenten über die jeweiligen Ports verbunden sind.

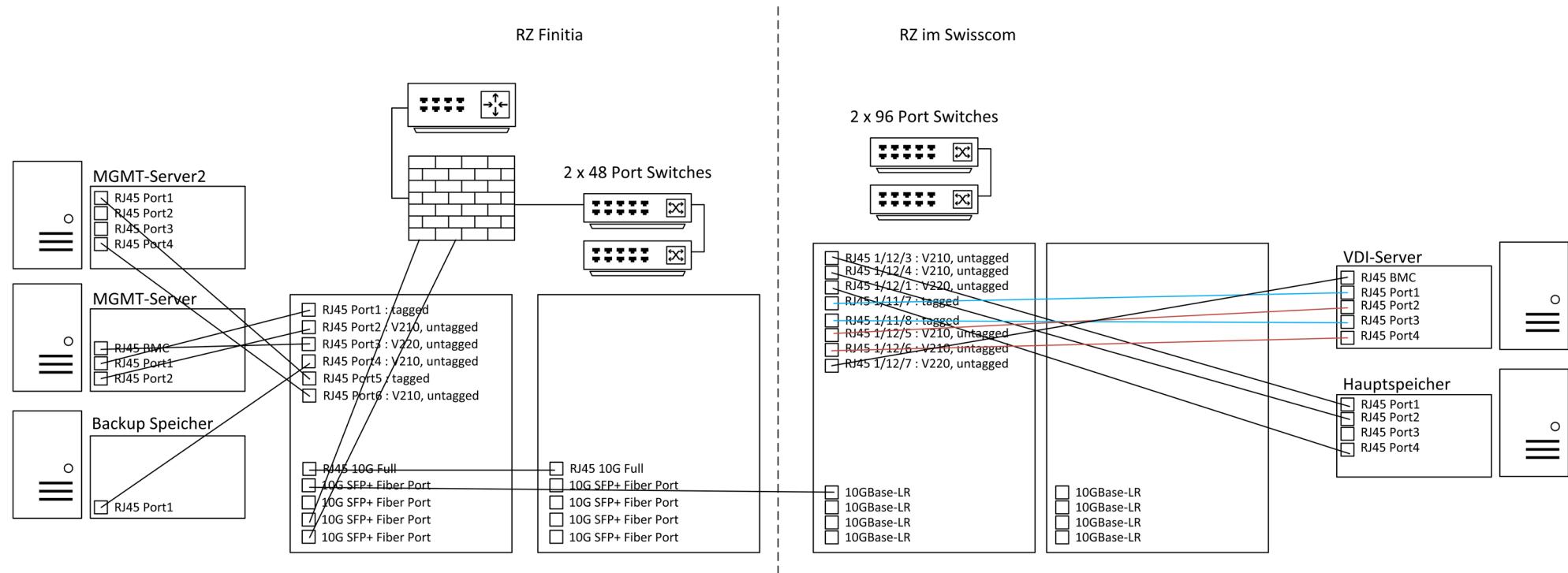


Abbildung 4: Portzuweisungen

5 Serverrollen & Netzwerk Dienste

Das Kapitel bietet einen Überblick über die entscheidenden Serverrollen & Netzwerkdienste. Jeder Dienst wurde gezielt ausgewählt. Im Zentrum steht die Active Directory Struktur, die eine robuste Nutzerverwaltung und präzise Zugriffskontrollen ermöglicht. Durch eine klare Organisation in OUs wird eine strukturierte Verwaltung erreicht. Die NTFS-Berechtigungen sind entscheidend, um den Zugriff innerhalb des Netzwerks zu regulieren. Durch den DNS-Server wird eine korrekte Namensauflösung, die sowohl für interne Kommunikationswege als auch für die Verbindung ins Internet unerlässlich ist. Schliesslich stellt der DHCP-Server die Verwaltung der IP-Adressen im VLAN 230 sicher. In den folgenden Unterkapitel wird genauer auf die Rollen/Dienste eingegangen.

5.1 Domain

Für das Proof of Concept des Projekts "VDI as a Service" wird eine neue Domäne erstellt, unter dem Namen "dom-poc.local". Diese Domäne ist speziell für die Testumgebung konzipiert und beinhaltet sämtliche erforderlichen Server, Benutzerkonten und Gruppen. Um eine klare Trennung zur Produktionsumgebung zu gewährleisten, wird diese Domäne von Grund auf neu aufgebaut und operiert vollständig isoliert.

5.2 Active Directory Struktur

Die Active Directory Struktur ist geplant, um eine klare Trennung der Ressourcen und eine effiziente Verwaltung zu gewährleisten. Die Struktur ist in verschiedene Organisationseinheiten (OUs) unterteilt, die spezifischen Komponenten und Zugriffsrechte in der Domäne "dom-poc.local" repräsentieren. Diese sind in der folgenden Abbildung als Ordner ersichtlich.

Die OU "Access-Groups" bildet die Grundlage der Zugriffsverwaltung. Hier werden die Berechtigungen für die Datenablage festgelegt, um zu steuern, wer Zugriff auf welche Ordner hat mittels Gruppen. Innerhalb der OU "Access" gibt es eine weitere OU namens "VDI-Profile". Dort gibt es zwei Gruppen die unterschieden werden unter zwei Arten von VDI-Profilen: das Basic Profil für Standardnutzungen mit normaler Leistung und das Premium Profil für anspruchsvollere Anwendungen, das erhöhte Leistungskapazitäten bietet.

Unter der OU "Service Accounts" werden spezielle Konten für die Systemadministration verwaltet. Diese Konten, wie der Local Admin oder Domain Admin, sind für Aufgaben vorgesehen, die umfassende Berechtigungen im Netzwerk erfordern.

Die OU "Servers" ist in zwei Bereiche untergliedert: die physischen XenServers und die Member Servers. Diese Struktur erlaubt es Serverressourcen geordnet und effizient zu verwalten.

Die OU "Users" beinhaltet alle Benutzerkonten der Domäne. Hier werden die individuellen Benutzerprofile und -einstellungen hinterlegt. Die folgende Abbildung illustriert das Ganze.

Zuletzt umfasst die OU "VDI-Machines" alle Computerobjekte der VDI-Maschinen.

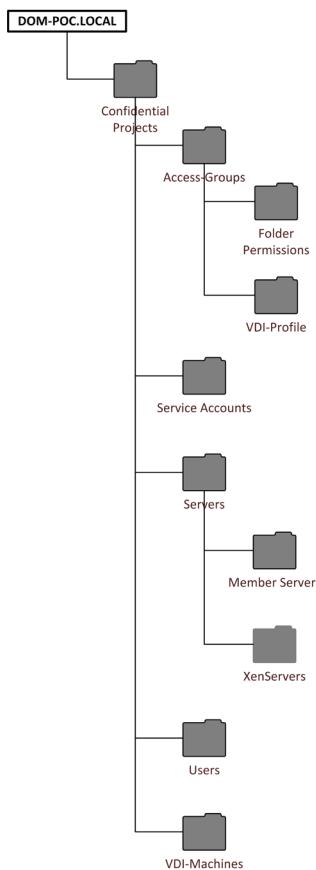


Abbildung 5: AD Struktur

Namenskonvention Benutzer-Accounts

Die Benutzer, die in der OU "Users" erfasst sind, folgen speziellen Namenskonventionen, um sie auf den ersten Blick von anderen regulären Nutzern zu unterscheiden, selbst wenn diese in einer speziell eingerichteten, separaten Domäne sind. Die Namenskonvention ist wie folgt strukturiert:

Nachname: Mustermann

Vorname: Max

Benutzername: gp-mmu

Das Präfix "gp" im Benutzernamen steht für "Geheimhaltungsprojekt" und wird durch einen Bindestrich mit den initialen Benutzerdaten verbunden: dem ersten Buchstaben des Vornamens und den ersten zwei Buchstaben des Nachnamens. Diese Konvention erleichtert die Identifikation und Verwaltung der Benutzerkonten, insbesondere in Projekten mit erhöhten Sicherheitsanforderungen.

5.3 DNS

Die Domain Controller haben eine zusätzliche Rolle als DNS-Server. Diese Rolle wird dementsprechend auf beide DCs installiert und eingerichtet. Ziel ist es, eine effiziente Namensauflösung innerhalb und ausserhalb des eigenen Netzwerks zu gewährleisten.

Es werden sowohl Forward-Lookup- als auch Reverse-Lookup-Zonen eingerichtet. Diese Zonen sind verantwortlich, für das Umwandeln von Hostnamen in IP-Adressen (Forward-Lookup) und IP-Adressen in Hostnamen (Reverse-Lookup). Um die Hochverfügbarkeit des DNS-Dienstes sicherzustellen, werden diese Zonen zwischen beiden DCs repliziert, so dass der andere übernimmt, wenn der andere ausfallen sollte.

Innerhalb des VLAN 230, welches für die VDI-Desktops gedacht ist, erfüllen die DNS-Server primär die Aufgabe, die Auflösung interner Adressen. Da dieses Netzwerk keinen direkten Internetzugang hat, beschränkt sich die Funktionalität auf interne Anfragen, wie beispielsweise die Auflösung des Hostnamens `srv-data-01` in die zugehörige IP-Adresse und umgekehrt.

Im Gegensatz dazu wird im Management-Netzwerk (MGMT-Netz) der DNS-Dienst auch für die Auflösung von Internetadressen konfiguriert. Da dieses Netzwerk einen Internetzugang hat.

Darüber hinaus ist der DNS-Dienst essenziell für das Joinen der Server in die neu erstellte Domäne. Die Konfiguration des DNS ist eine der ersten Schritte, die nach der Erstellung der Domäne gemacht werden muss.

5.4 DHCP

Für diese Infrastruktur wird nur ein DHCP-Scope konfiguriert, der einen IP-Adressbereich von 192.168.230.30 – 200 umfasst. Dieser Bereich ist ausschliesslich für die VDI-Desktops vorgesehen. Für die Server ist kein Scope vorgesehen da die IPs dort statisch konfiguriert werden auf der Netzwerkkarte.

Das konfigurierte Gateway für dieses VLAN ist die Adresse 192.168.230.1, welche die VDI-Clients für die Ausgangsnetzwerkkommunikation nutzen. Für die Namensauflösung sind zwei Domain Controller definiert, einerseits `srv-dc-01` mit der IP-Adresse 192.168.230.20 als primärer und `srv-dc-02` mit der IP-Adresse 192.168.230.21 als sekundärer definiert. Die standardmässige Lease-Dauer für zugewiesene IP-Adressen dauert 8 Tage.

Des Weiteren ist der `srv-dc-02` als Failover für den DHCP-Dienst eingerichtet. Dieses Failover ist als Load-Balance Konfiguration wird mit einer 50/50 Aufteilung eingerichtet sein, was bedeutet, dass `srv-dc-01` und `srv-dc-02` die DHCP-Anfragen gleichmässig untereinander aufteilen. Dies erhöht die Verfügbarkeit und Zuverlässigkeit des DHCP-Diensts, indem sichergestellt wird, dass im Falle eines Serverausfalls der andere Server die Adresszuweisung übernimmt.

5.5 NTFS

Die Speicherung und Verwaltung der Daten erfolgen auf dem Server srv-data-01, wobei die Daten lokal über Netzwerkfreigaben (Shares) zugänglich gemacht werden. Die Zugriffskontrolle auf diese Netzlaufwerke basiert auf der NTFS-Technologie.

Um eine strukturierte und sichere Zugriffssteuerung zu gewährleisten, werden Active Directory Gruppen verwendet, die speziell für diesen Zweck unter der OU "Folder Permissions" angelegt wurden. Jeder Benutzer wird entsprechend seiner Rolle einer bestimmten Gruppe hinzugefügt. Diese Gruppenzugehörigkeit definiert, auf welche Teile des Netzlaufwerks ein Benutzer zugreifen darf.

Die Integration der Netzlaufwerke in die Benutzerumgebung erfolgt mithilfe von WEM (Workspace Environment Management). Dadurch wird sichergestellt, dass bei jedem Benutzer die korrekten Netzlaufwerke entsprechend seiner Gruppenzugehörigkeit eingebunden sind. Dieser Prozess minimiert erheblich den administrativen Aufwand.

Die NTFS-Berechtigungen sind so konfiguriert, dass sie eine genaue Steuerung ermöglichen, von Lesezugriffen bis hin zu vollständigen Schreib- und Bearbeitungsrechten. Das heisst, dass der Zugriff nicht nur auf Datei- oder Ordner gesteuert wird, sondern auch, dass bestimmte Aktionen wie das Erstellen, Ändern oder Löschen von Dateien kontrolliert und angepasst werden können.

6 Backup

Um die Integrität und Verfügbarkeit von wichtigen und sensiblen Daten zu gewährleisten, ist eine Backup-Strategie unausweichlich. Dieses Kapitel umfasst das Backupkonzept, um den Schutz unserer kritischen Daten sicherzustellen. Es werden Aspekte behandelt, wie Definition der Ziele für die Datensicherung, Auswahl der Backup-Technologie und Definition der Strategie, wie Zeitpläne. Betriebliche Prozesse wie Wiederherstellungsverfahren werden im Betriebskonzept festgelegt.

6.1 Systemübersicht

In einer VDI-Umgebung gibt es zahlreiche Potentielle Datenquellen, die regelmässig gesichert werden sollten. Folgend eine Liste der schützenswerte Datenquellen.

Datentyp	Beschreibung
Benutzerprofile	Persönliche Einstellungen, Desktop-Layouts und benutzerspezifische Daten
Benutzerdaten	Dokumente, Bilder, Videos, Browserfavoriten und andere Dateien der Benutzer
Golden Images	Images von Betriebssystemen und Anwendungen für die Bereitstellung von Desktops
Projektdateien	Dateien, welche auf dem Projektvolumen gespeichert werden
Anwendungskonfigurationen	Einstellungen und Konfigurationsdateien für installierte Anwendungen, inklusive Lizenzdateien
Datenbanken	Zentrale Datenbanken mit Konfigurationsdaten, Benutzerinformationen und Managementdaten
Management- und Konfigurationsdaten	Daten für das Management der VDI-Umgebung, wie Infrastrukturkonfigurationen und Sicherheitsrichtlinien
Logs und Überwachungsdaten	Sicherheitslogs, Audit-Logs und Performance-Daten für Monitoring und Troubleshooting
Snapshot-Daten	Momentaufnahmen von virtuellen Maschinen, die zur schnellen Wiederherstellung verwendet werden können.
Lizenzerierung	Informationen über Software-Lizenzerierung
Backup-Software und Konfigurationsdateien	Sicherung der Backup-Lösungen selbst, einschliesslich ihrer Konfigurationsdateien

Tabelle 17: Sicherungsquellen

6.2 Zielsystem

In der PoC-Umgebung ist es essenziell, strategisch beim Backup vorzugehen, um die Ressourcen optimal zu nutzen. Dabei ist es wichtig, sich auf die Sicherung der kritischsten und unentbehrlichsten Daten zu konzentrieren. Folgend wird die Auswahl der Ziele für das Backup vorgestellt:

Ziel-ID	Sicherungsziel	Sicherungsdateien	Priorität	Notwendigkeit
1	Golden Images	Hauptdateien und Snapshots Dateien der Virtuellen Maschinen	Hoch	Hoch
2	FSLogix	Benutzerprofile und -daten	Hoch	Kritisch
3	Netzlaufwerk	Projektdateien	Hoch	Kritisch
4	Alle anderen Management Server	Hauptdateien und Snapshots Dateien der Virtuellen Maschinen	Mittel	Moderat

Tabelle 18: Sicherungsziele Backup

Es ist zu beachten, dass es sich hierbei ausschliesslich um die dedizierte Backup-Lösung handelt. Snapshots wurden in dieser Betrachtung nicht berücksichtigt.

6.3 Strategie

Der Hauptspeicher beinhaltet fast alle Dateien, von der Verwaltung der virtuellen Maschinen bis hin zu den Netzlaufwerken. Daher ist es notwendig, diese Dateien von dem Hauptspeicher auf ein externes Medium zu sichern. Optimalerweise sollte dieses externe Speichermedium an einem anderen Standort betrieben werden.

Mit der fortschrittlichen Synology FlashStation FS6400 ist es möglich, eine selbst gehostete Backup-Lösung von Synology zu nutzen. Allerdings unterstützt dieses System in einer virtuellen Umgebung nur VMware vSphere und Microsoft Hyper-V. Für den Einsatz in Citrix-Umgebungen ist daher ein spezieller Agent von Synology erforderlich.

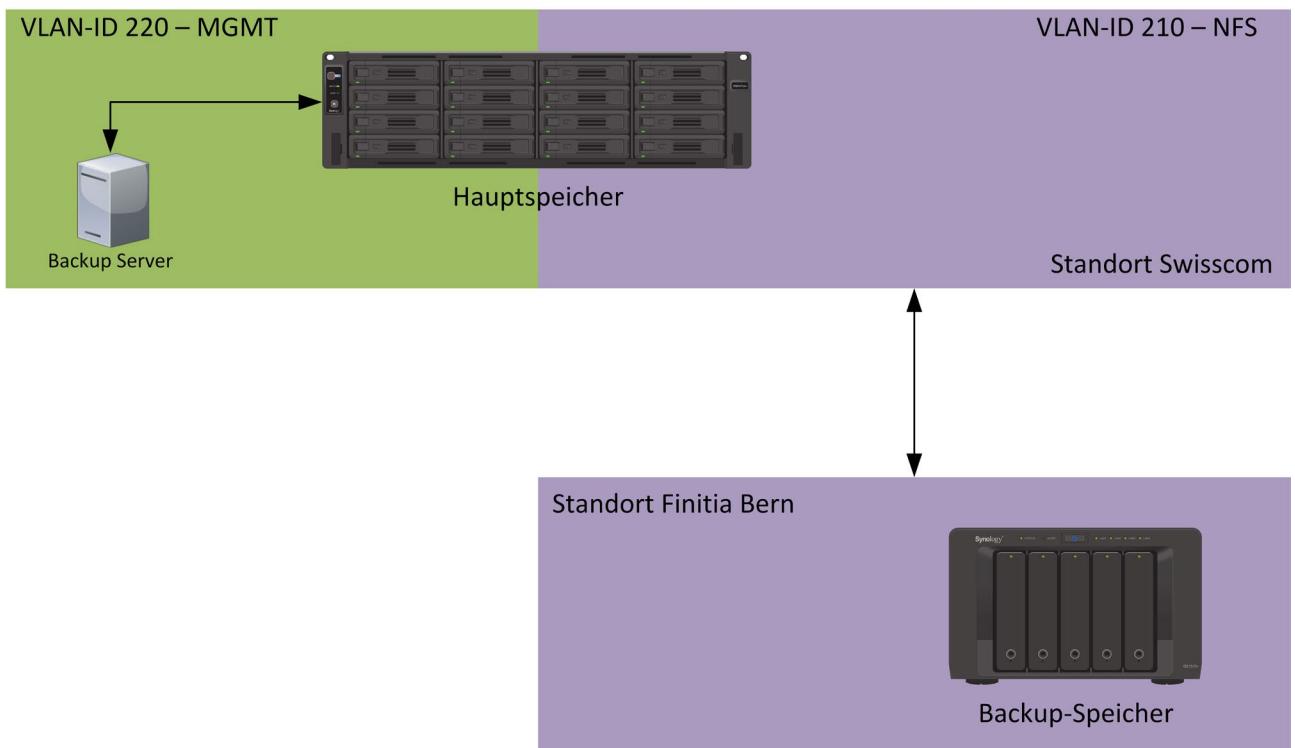


Abbildung 6: Backupinfrastruktur

Der Backupspeicher befindet sich im internen Rechenzentrum. Beide Synology-Speicher sind über ein geschlossenes VLAN miteinander verbunden. Die intern gehostete Backup-Lösung vom Hauptspeicher nutzt den Backupspeicher als angebundener NFS-Speicher. Die erstellten Backups können somit vom Hauptspeicher auf den Backupspeicher übertragen werden.

6.3.1 Aufgabenliste

In diesem Abschnitt werden die Regelmässigkeiten und Aufbewahrungsrichtlinien der Backups definiert.

Stündlich

Ziel-ID	Art	Bezeichnung	Ausführung	Aufbewahrungszeit
3	Snapshot	Hourly-Data	Jede Stunde von 6 – 20 Uhr	7 Tage

Tabelle 19: Stündliche Backups

Täglich

Ziel-ID	Art	Bezeichnung	Ausführung	Aufbewahrungszeit
1	Full Backups / inkrementell	Daily-Golden	Mo-Fr um 22 Uhr	31 Tage
2	Full Backups / inkrementell	Daily-Profile	Jeden Tag um 21 Uhr	31 Tage
3	Snapshot Replikation	Daily-Rep-Data	Jeden Tag um 21 Uhr	31 Tage
4	Full Backups / inkrementell	Daily-Server	Jeden Tag um 23	7 Tage

Tabelle 20: Tägliche Backups

Wöchentlich

Ziel-ID	Art	Bezeichnung	Ausführung	Aufbewahrungszeit
1	Full Backups / inkrementell	Weekly-Golden	Jeden Sonntag um 01:00 Uhr	4 Wochen
2	Full Backups / inkrementell	Weekly-Profile	Jeden Samstag um 01:00 Uhr	10 Wochen
3	Snapshot Replikation	Weekly-Rep-Data	Jeden Samstag um 02:00 Uhr	26 Wochen
4	Full Backups / inkrementell	weekly-Server	Jeden Sonntag um 02:00 Uhr	4 Wochen

Tabelle 21: Wöchentliche Backups

Monatliche

Ziel-ID	Art	Bezeichnung	Ausführung	Aufbewahrungszeit
1	Full Backups / inkrementell	Monthly-Golden	Ende Monat	3 Monate
2	Full Backups / inkrementell	Monthly-Profile	Ende Monat	6 Monate
3	Snapshot Replikation	Monthly -Rep-Data	Ende Monat	6 Monate
4	Full Backups / inkrementell	Monthly -Server	Ende Monat	3 Monate

Tabelle 22: Monatliche Backups

Jährlich

Ziel-ID	Art	Bezeichnung	Ausführung	Aufbewahrungszeit
1	Full Backups / inkrementell	Yearly-Golden	Anfangs Januar	3 Jahre
2	Full Backups / inkrementell	Yearly-Profile	Anfangs Januar	5 Jahre
3	Snapshot Replikation	Yearly-Rep-Data	Anfangs Januar	5 Jahre
4	Full Backups / inkrementell	Yearly-Server	Anfangs Januar	3 Jahre

Tabelle 23: Jährliche Backups

6.3.2 Sicherheit und Integrität

Um die fortwährende Sicherheit und Integrität der Backups zu gewährleisten, werden mehrere spezielle Prozesse implementiert. Alle freigegebenen Ordner sind verschlüsselt und ihre Integrität wird regelmässig überprüft. Durch die Verschlüsselung sind die Snapshots nicht für die Benutzer durchsuchbar. Zudem sind alle Snapshots für vier Tage gegen Löschung geschützt, um zusätzliche Sicherheit zu bieten und die Integrität weiter zu sichern. Der Zugang ist strikt über AD-Authentifizierung mit definierten Benutzergruppen geregelt. Zugriff auf das zentrale Dateisystem ist ausschliesslich autorisierten Personen erlaubt, die eine Vertraulichkeitsvereinbarung unterschrieben haben. Die Hardware wird in gesicherten Umgebungen betrieben, die nur mit spezieller Autorisierung zugänglich sind. Mitarbeiter werden regelmässig geschult, um ein Bewusstsein für die Bedeutung der Datensicherheit und die korrekte Handhabung von Backup-Prozessen zu schaffen.

Das Backup erfolgt regelmässig gemäss einer detaillierten Aufgabenliste. Es ist erforderlich, dass das Backup täglich von einer zugewiesenen Person überprüft wird, um die Einhaltung der Sicherheitsstandards sicherzustellen. Der Prozess wird im Betriebskonzept weiterführend detailliert beschrieben

Quellenverzeichnis

Ostler, U. (06. 12 2011). *Datacenter-insider*. Abgerufen am 12. 04 2024 von Datacenter-insider:

<https://www.datacenter-insider.de/von-tier1-bis-tier-4-die-vier-qualitaetsstufen-eines-rechenzentrums-a-341120/>

Staff, C. (10. 11 2022). *Citrix Docs*. Abgerufen am 15. 04 2024 von Citrix Docs:

<https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/1912-ltsr/system-requirements.html>

Wang, B. (08. 06 2023). *Citrix Docs*. Abgerufen am 12. 04 2024 von Citrix Docs:

<https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/technical-overview.html>

Abbildungsverzeichnis

Abbildung 1: Oberflächliche Architektur Grafik	5
Abbildung 2: Kommunikationsgrafik	10
Abbildung 3: Netzwerksegmentierung.....	20
Abbildung 4: Portzuweisungen.....	24
Abbildung 5: AD Struktur.....	26
Abbildung 6: Backupinfrastruktur	32

Tabellenverzeichnis

Tabelle 1: Änderungsverzeichnis	1
Tabelle 2: Voraussetzungen der Umgebung	4
Tabelle 3: Schnittstellen Netzwerk Infrastruktur	8
Tabelle 4: Schnittstellen Citrix Umgebung.....	9
Tabelle 5: Firewall Beschreibung	11
Tabelle 6: Switches Beschreibung	11
Tabelle 7: XenServer Management Server	13
Tabelle 8: XenServer Management Server 2	14
Tabelle 9: XenServer VDI Server	16
Tabelle 10: Hauptspeicher Synology FS6400	16
Tabelle 11: Backupspeicher.....	17
Tabelle 12: VLANs & Gateways.....	21
Tabelle 13: NFS-Leitung	21
Tabelle 14: XenServer & Storage.....	22
Tabelle 15: Virtuelle Server.....	23
Tabelle 16: Domain Controller & DHCP Range.....	23
Tabelle 17: Sicherungsquellen	30
Tabelle 18: Sicherungsziele Backup	31
Tabelle 19: Stündliche Backups	32
Tabelle 20: Tägliche Backups	33
Tabelle 21: Wöchentliche Backups	33
Tabelle 22: Monatliche Backups	34
Tabelle 23: Jährliche Backups	34

Anhang E2



Testkonzept

VDI as a Service

Auftraggeber	Micha Bucher
Projektleiter	Shipinyuan Su, Sirak Yosef
Autor	Shipinyuan Su, Sirak Yosef
Klassifizierung	Intern
Status	Von AG abgesegnet

Änderungsverzeichnis

Datum	Version	Änderung	Autor
08.04.2024	0.1	Dokument erstellt	Shipinyuan Su, Sirak Yosef
21.04.2024	1.0	Fertigstellung	Shipinyuan Su, Sirak Yosef

Tabelle 1: Änderungsverzeichnis

Inhaltsverzeichnis

1	Einleitung	3
2	Testziele	3
3	Testorganisation	4
4	Testablauf	5
5	Testrahmen	7
5.1	Testvoraussetzungen	7
5.2	Fehlerklassifizierung	7
5.3	Start- und Abbruchbedingungen	8
6	Testinfrastruktur	9
6.1	Testsystem	9
6.2	Testhilfsmittel	9
7	Testplan	10
8	Anforderungen	11
9	Testfälle	28
9.1	Komponententests	28
9.2	Integrationstests	32
9.3	Systemtests	40
9.4	Abnahmetests	44
10	Testausführung	47
10.1	Test erfolgreich	47
10.2	Test nicht erfolgreich	47
10.3	Testauswertung	47

1 Einleitung

Dieses Testkonzept dient als Grundlage für die systematische Überprüfung der VDI-Lösung, nachdem sie implementiert wurde. Es umfasst klare Testziele sowie eine strukturierte Übersicht über die Organisation, Planung und Durchführung der Tests. Des Weiteren wurde ein Testrahmen definiert und eine Testinfrastruktur. Ziel ist es, durch diese methodische Herangehensweise alle Anforderungen zu validieren.

2 Testziele

Die Testziele dieses Konzept sind darauf ausgelegt, die funktionalen und nicht funktionalen Anforderungen der VDI-Lösung zu überprüfen. Die Ziele umfassen:

- IT-Infrastruktur: Überprüfung der gesamten Infrastruktur, einschliesslich Server und Netzwerk, um sicherzustellen, dass sie funktionsfähig sind und ihre Aufgaben erledigen
- Leistung: Sicherstellung, dass die VDI die erforderliche Leistung für kritische Anwendungen, insbesondere CAD-Programme bereitstellt
- Anpassungsfähigkeit: Bewertung der Flexibilität der VDI, Anpassungen wie Ressourcen Verteilung und VDI-Images ohne Beeinträchtigung des laufenden Betriebs
- Datensicherheit: Überprüfung der täglichen Backups, um den Schutz vor Datenverlust zu garantieren
- Sicherheitsrichtlinien: Gewährleistung der Sicherheit durch spezifische Massnahmen, wie die Verhinderung des Internetzugangs über die VDI

All diese Ziele werden durch spezifisch erstellte Testfälle adressiert, die sicherstellen sollen, dass die VDI-Lösung den Anforderungen entspricht.

3 Testorganisation

In der folgenden Grafik wird die hierarchische Struktur der Testorganisation mit den entsprechenden Rollen innerhalb dieser Testphase dargestellt.

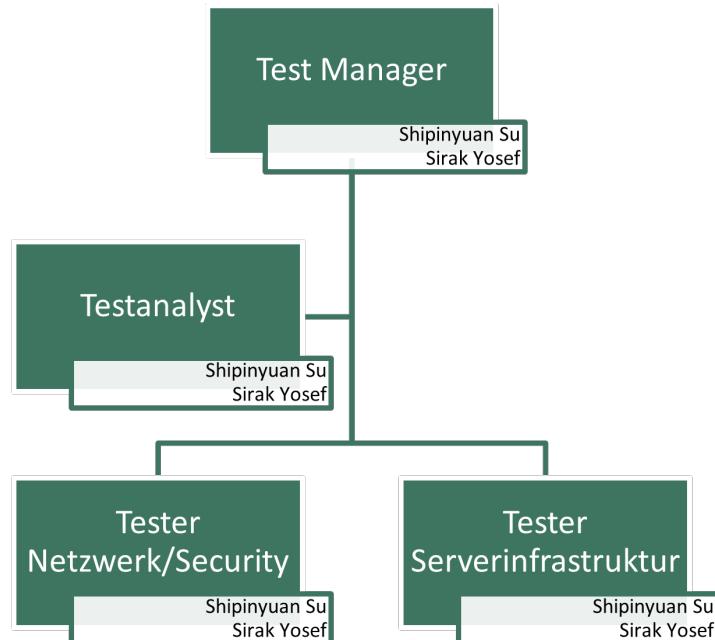


Abbildung 1: Testorganisation

Die Rollen wurden wie folgt definiert:

Test-Manager:

- Planung und Definition der Testziele
- Strukturierung der Testfälle
- Abdeckung der Anforderungen

Testanalyst:

- Erstellung der Testfälle
- Definieren der Abnahmekriterien

Tester Netzwerk/Security:

- Durchführung der Tests mit Fokus Netzwerk & Security
- Dokumentation der Fehler

Tester Serverinfrastruktur:

- Durchführung der Tests mit Fokus Serverinfrastruktur – Citrix VDI
- Dokumentation der Fehler

4 Testablauf

Folgende Test-Etappen wird die VDI-Lösung durchlaufen.



Abbildung 2: Testablauf

Komponententest

Ziel	Verifizierung, dass jede Komponente der VDI-Lösung funktioniert.
Tester	Shipinyuan Su, Sirak Yosef
Vorbedingungen	Konfiguration der Komponente abgeschlossen
Bedingung für nächste Phase	Komponente erreichen definierte Testkriterien
Inputs für die Tests	Dokumentation der Komponenten

Tabelle 2: Komponententest

Integrationstest

Ziel	Sicherstellung, dass die Komponenten zusammen als integriertes System arbeiten und richtig untereinander kommunizieren.
Tester	Shipinyuan Su, Sirak Yosef
Vorbedingungen	Alle Komponententests sind erfolgreich abgeschlossen
Bedingung für nächste Phase	Integration und korrektes Zusammenarbeiten der Komponente
Inputs für die Tests	Schnittstellenbeschreibung

Tabelle 3: Integrationstest

Systemtest

Ziel	Bewertung des Gesamtsystems, um sicherzustellen das die Anforderungen erfüllt sind.
Tester	Shipinyuan Su, Sirak Yosef
Vorbedingungen	Integrationstest wurden abgeschlossen
Bedingung für nächste Phase	Das System erfüllt die Anforderungen und funktioniert
Inputs für die Tests	Vollständige Systemdokumentation

Tabelle 4: Systemtest

Abnahmetest

Ziel	Endgültige Validierung der Citrix VDI-Lösung.
Tester	Shipinyuan Su, Sirak Yosef, Micha Bucher (Auftraggeber)
Vorbedingungen	Systemtests wurden erfolgreich durchgeführt
Inputs für die Tests	Abnahmekriterien, Feedback von Pilotbenutzer

Tabelle 5: Abnahmetest

5 Testrahmen

In diesem Kapitel wird der Rahmen für die Durchführung der Tests der VDI-Lösung definiert. Es beschreibt die notwendigen Voraussetzungen, unter denen die Tests durchgeführt werden können, sowie die Klassifizierung von Fehlern, die während der Tests auftreten können. Darüber hinaus werden die Bedingungen erläutert, unter denen Tests gestartet oder abgebrochen werden müssen, um sicherzustellen, dass die Tests effektiv und unter den richtigen Bedingungen ablaufen.

5.1 Testvoraussetzungen

Um alle Tests erfolgreich durchführen zu können, sind sowohl physischer Zugriff zum Serverraum/Verteiler als auch virtueller Zugang notwendig. Der virtuelle Zugang kann über XenCenter oder per RDP auf den Host erfolgen. Zusätzlich müssen alle relevanten Systeme und Netzwerkkonfigurationen betriebsbereit und korrekt eingerichtet sein, um eine reibungslose Durchführung der Tests zu gewährleisten.

5.2 Fehlerklassifizierung

Die Fehlerklassifizierung ist ein wichtiger Bestandteil des Testrahmens und dient dazu, die gefundenen Fehler nach ihrer Schwere und Auswirkung auf das System zu bewerten. Die folgende Tabelle zeigt die unterschiedlichen Fehlerklassen und deren Beschreibungen, die in den Testfällen verwendet werden.

Nr.	Fehlerklassen	Beschreibung
0	Fehlerfrei	Erfüllt die Anforderungen
1	Belangloser Mangel	Erfüllt die Anforderungen, Mängel sollten nicht vorkommen
2	Leichter Mangel	Erfüllt die Anforderungen nicht komplett, es gibt nur kleine Betriebsbehinderungen
3	Schwerer Mangel	Erfüllt die Anforderungen nicht, grössere Betriebsbehinderungen
4	Kritischer Mangel	Erfüllt die Erwartungen nicht, Betrieb nicht möglich

Tabelle 6: Fehlerklassifizierung

5.3 Start- und Abbruchbedingungen

Hier werden die Bedingungen definiert, unter denen die noch anstehenden Tests gestartet oder abgebrochen werden. Diese Start- und Abbruchbedingungen sind wichtig, um sicherzustellen, dass die Tests unter den richtigen Voraussetzungen durchgeführt werden und dass klare Kriterien für den Abbruch definiert sind, für den Fall von unvorhergesehenen Problemen.

Startbedingungen

Die Startbedingungen beschreiben Voraussetzungen, die erfüllt sein müssen, bevor der Test gestartet werden kann:

- Die gesamte VDI-Lösung muss implementiert und betriebsbereit sein.
- Alle Testpersonen müssen den erforderlichen Zugang sowie Berechtigungen zu physischen und virtuellen Ressourcen haben.
- Alle relevanten Dokumentationen wie Anforderungen und Testfälle müssen vollständig vorliegen.

Abbruchbedingungen

Die Abbruchbedingungen legen fest, wann ein Test nicht mehr fortgesetzt werden darf:

- Kritische Fehler auf Fehlerklasse 4, die das Betreiben der VDI-Lösung nicht ermöglichen.
- Testabweichungen, die eine erfolgreiche Durchführung der Tests verhindern.
- Wenn die Ressourcen überlastet werden oder technische Probleme auftreten, die den Test beeinflussen könnten.

6 Testinfrastruktur

Die Testinfrastruktur bildet die Grundlage für die Durchführung aller notwendigen Tests für die VDI-Lösung. Sie umfasst sowohl die physischen als auch die virtuellen Komponenten, die zur Durchführung der Tests notwendig sind.

6.1 Testsystem

Testsysteme umfassen alle Komponenten, die für die Bereitstellung und den Betrieb der Lösung notwendig sind. Dazu gehören:

- Netzkomponenten: Dazu zählen Firewalls und Switches, die für die Netzwerksicherheit und Verwaltung erforderlich sind.
- Physische Server: Dies umfasst die XenServer, welche die Virtualisierung der VDI-Umgebung ermöglichen.
- Speicherlösungen: Hauptspeicher und Backup-Speicher, die für die Datenspeicherung und -sicherung wichtig sind.
- Virtuelle Server: Notwendig für die Durchführung von Tests auf verschiedenen virtuellen Servern, um die Funktionsfähigkeit der VDI-Lösung zu sicherzustellen.
- Test-Notebook: Ein Reservegerät der Finitia AG, das keine zusätzlichen Kosten verursacht und für allgemeine Tests an der VDI-Umgebung verwendet wird.

6.2 Testhilfsmittel

Für die Durchführung der Tests werden verschiedene Hilfsmittel innerhalb der VDI-Infrastruktur verwendet. Diese Hilfsmittel umfassen:

- Erstellung von Testusern: Testuser werden erstellt, um mit ihnen verschiedene Tests innerhalb der VDI-Umgebung durchzuführen.
- Überwachungstools: Integrierte Überwachungstools von Citrix werden genutzt, um die Citrix Infrastruktur zu überwachen.
- Remote-Zugriff: XenCenter, RDP und SSH-Tools wie Putty werden verwendet, um auf die XenServer, virtuellen Server oder Netzwerkgeräte zuzugreifen.

7 Testplan

Im folgenden Testplan sind die Hauptaktivitäten beschrieben. Die Aktivitäten werden strukturiert und termingerecht durchgeführt.

Nr.	Aktivität	Verantwortlich	Termin
1	Überprüfung der Testinfrastruktur	Test-Manager	KW21
2	Durchführung der Komponententests	Test-Manager	KW21
3	Durchführung der Integrationstests	Test-Manager	KW21
4	Durchführung der Systemtests	Test-Manager	KW21
5	Durchführung der Abnahmetests	Test-Manager	KW21
6	Dokumentation der Testergebnisse	Test-Manager	KW21

Tabelle 7: Testplan

8 Anforderungen

In diesem Kapitel sind alle Anforderungen definiert, die als Grundlage für die Testfälle im nächsten Kapitel dienen. Jede Anforderung ist mit einer eindeutigen Nummer versehen, beginnend mit «ANF» für Anforderung, um eine klare Identifikation und Referenzierung zu ermöglichen. Diese Anforderungen decken die spezifischen Funktionalitäten und Sicherheitsaspekte ab, die in den verschiedenen Komponenten der IT-Infrastruktur implementiert und validiert werden müssen.

ANF-01: Funktionalität der Sophos Firewall

Die Funktionalität der eingesetzten Sophos Firewall muss gewährleistet werden, damit die erforderlichen Netzwerkkonfiguration, die für den Service notwendig sind, problemlos implementiert werden können.

Name	Funktionalität der Sophos Firewall
Kurzbeschreibung	Sicherstellung, dass die Sophos Firewall die Netzwerksicherheit durch Kontrolle und Überwachung des Datenverkehrs, einschliesslich der Funktion VLAN effektiv unterstützt.
Akteure	Tester Netzwerk/Security
Vorbedingungen	Die Firewall wurde vom Drittanbieter, der Firma Finita AG, vorbereitet und konfiguriert.
Hauptszenario	Die Firewall unterstützt spezifische Netzwerkanforderungen, einschliesslich VLAN-Konfigurationen und Richtlinien.
Nachbedingungen	Die Firewall bleibt stabil und behält die Konfigurationseinstellungen bei, nachdem diese gespeichert wurden.

Tabelle 8: ANF-Funktionalität der Sophos Firewall

ANF-02: Funktionalität der Netzwerk-Switches

Wie bei der Sophos Firewall, muss auch hier die Funktionalität der Netzwerk-Switches geprüft werden, um die erforderlichen Konfigurationen erfolgreich implementieren zu können.

Name	Funktionalität der Netzwerk-Switches
Kurzbeschreibung	Gewährleistung, dass die Switches ihre zentrale Rolle im Netzwerkmanagement erfüllen, indem sie effektiv die Netzwerksegmentierung unterstützen.
Akteure	Tester Netzwerk/Security
Vorbedingungen	Die Switches wurden vom Drittanbieter, der Firma Fintia AG vorbereitet und konfiguriert.
Hauptszenario	Die Switches verarbeiten den Netzwerkverkehr der segmentierten Netzwerke problemlos.
Nachbedingungen	Die Switches bleiben stabil und behalten die Konfigurationseinstellungen bei, nachdem diese gespeichert wurden.

Tabelle 9: ANF-Funktionalität der Netzwerk-Switches

ANF-03: XenServer Management 1

Auf dem Management XenServer werden hauptsächlich alle virtuellen Server, die für den Betrieb der VDI-Lösung benötigt werden, eingerichtet. Der Server muss mit den erforderlichen Ressourcen ausgestattet sein und die neueste XenServer Version verwenden.

Name	XenServer Management 1
Kurzbeschreibung	Der Management Server ist das Kernstück der VDI-Lösung und ist mit den notwendigen Ressourcen ausgestattet.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	XenServer und alle Komponenten wurden geliefert und sind einsatzbereit.
Hauptszenario	Installation und Konfiguration von CPU, RAM, Grafikkarte, SSD, RAID-Controller und einer zweiten Netzwerkkarte. Der Server wird mit XenServer Version 8.0 eingerichtet.
Nachbedingungen	Der Server startet problemlos und alle Komponenten arbeiten fehlerfrei.

Tabelle 10: ANF-XenServer Management 1

ANF-04: XenServer Management 2

Der zweite Management-Server hat die gleiche Funktionalität wie der erste Management-Server und dient als zusätzlicher Server, sodass die virtuellen Server über zwei physische Server verteilt laufen. Es ist daher wichtig, die Ressourcen des Servers auch hier zu überprüfen.

Name	XenServer Management 2
Kurzbeschreibung	Überprüfung der Ressourcen des zweiten Management-Servers für VM- und Lastverteilung.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	Management-Server 2 ist einsatzbereit
Hauptszenario	CPU, RAM, Grafikkarte, SSD, RAID-Controller und Netzwerkkarten laufen auf dem Server. Der Server läuft zudem mit XenServer Version 8.0
Nachbedingungen	Der Server startet problemlos und alle Komponenten arbeiten fehlerfrei.

Tabelle 11: ANF-XenServer Management 2

ANF-05: XenServer VDI

Auf dem VDI XenServer werden alle VDI-Maschinen laufen. Anders als beim Management Server handelt es sich hier um einen bestehenden Server, der aktuell im Einsatz ist. Es ist wichtig zu überprüfen, ob der Server richtig ausgestattet ist.

Name	XenServer VDI
Kurzbeschreibung	Bestehender XenServer, der noch im Einsatz ist, und dessen Ressourcen überprüft werden müssen.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	Server wird nicht mehr in der produktiven Umgebung gebraucht.
Hauptszenario	CPU, RAM, Grafikkarte, SSD, RAID-Controller und Netzwerkkarten laufen auf dem Server. Der Server läuft zudem mit XenServer Version 8.0.
Nachbedingungen	Der Server startet problemlos und alle Komponenten arbeiten fehlerfrei.

Tabelle 12: ANF-XenServer VDI

ANF-06: Hauptspeicher Synology NAS

Das Synology NAS wird als zentrale Datenablage eingerichtet. Es ist wichtig, dass die Festplatten korrekt eingerichtet sind, das NAS auf dem neuesten Update-Stand ist und über das Netzwerk erreichbar ist.

Name	Hauptspeicher Synology NAS
Kurzbeschreibung	Das NAS dient als Datenablage und muss über das Netzwerk erreichbar sein. Zudem müssen die Festplatten und der Update-Stand geprüft werden.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	Synology NAS ist einsatzbereit
Hauptszenario	NAS ist über das Netzwerk erreichbar, Festplatten sind eingerichtet und das NAS ist auf dem aktuellsten Stand.
Nachbedingungen	NAS funktioniert einwandfrei.

Tabelle 13: ANF-Hauptspeicher Synology NAS

ANF-07: Backupspeicher Synology NAS

Damit die Backups auf das Backup-NAS übertragen werden können, muss das NAS einwandfrei laufen. Es ist wichtig, dass die Festplatten korrekt eingerichtet sind und das NAS auf dem neuesten Update-Stand ist.

Name	Backupspeicher Synology NAS
Kurzbeschreibung	Backup-Speicher für Server im geschlossenen NFS-Netz. Es muss sichergestellt werden, dass die Festplatten korrekt eingerichtet wurden und das NAS auf dem aktuellsten Update-Stand ist.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	Synology NAS ist einsatzbereit
Hauptszenario	Festplatten sind eingerichtet und NAS ist auf dem aktuellsten Update-Stand.
Nachbedingungen	NAS funktioniert einwandfrei.

Tabelle 14: Backupspeicher Synology NAS

ANF-08: Netzwerk VLAN 210 NFS

Das Netzwerk VLAN 210 NFS ist speziell für den Datentransfer zwischen virtuellen Servern und Backup-Prozessen konzipiert. Als Layer 2 Netzwerksegment bietet es eine wichtige Komponente, die hohe Datenintegrität und schnelle Übertragungsraten gewährleisten muss, ohne von externen Netzwerken beeinflusst zu werden.

Name	Netzwerk VLAN 210 NFS
Kurzbeschreibung	Ein Layer 2 Netzwerk, das als abgeschlossenes Segment für den Datentransfer zwischen virtuellen Servern und Backup-Prozessen dient.
Akteure	Tester Netzwerk/Security
Vorbedingungen	VLANs und Firewall-Regeln sind erstellt und physische sowie virtuelle Server sind eingerichtet.
Hauptszenario	Das NFS-Netzwerk unterstützt den Datentransfer und die Backup-Prozesse ohne Zugriff von oder zu anderen Netzwerken.
Nachbedingungen	Die Integrität und Isolation des NFS-Netzes bleibt nach der Implementierung erhalten.

Tabelle 15: ANF-Netzwerk VLAN 210 NFS

ANF-09: Netzwerk VLAN 220 MGMT

Das Netzwerk VLAN 220 MGMT spielt eine zentrale Rolle in der Netzwerkverwaltung. Es verfügt über Internetzugang und gewährt einen kontrollierten Zugriff auf das VDI-Netzwerk. Die Anforderungen müssen gewährleisten, dass die Netzwerkkommunikationen stets korrekt funktionieren.

Name	Netzwerk VLAN 220 MGMT
Kurzbeschreibung	Ein Netzwerk, das mit dem Internet verbunden ist und sowohl das Management als auch den Zugriff auf das VDI-Netzwerk ermöglicht.
Akteure	Tester Netzwerk/Security
Vorbedingungen	VLANs und Firewall-Regeln sind erstellt und physische sowie virtuelle Server sind eingerichtet.
Hauptszenario	Das MGMT-Netzwerk ermöglicht die Administration und Überwachung von Netzwerkressourcen und bietet Zugriff auf das isolierte VDI-Netzwerk.
Nachbedingungen	Das MGMT-Netzwerk bleibt mit kontrollierten Zugriffsrichtlinien sicher.

Tabelle 16: ANF-Netzwerk VLAN 220 MGMT

ANF-10: Netzwerk VLAN 230 VDI

Das Netzwerk VLAN 230 VDI ist für die Bereitstellung eines isolierten und sicheren Umfelds für virtuelle Desktop-Infrastrukturen konzipiert. Es hat keinen direkten Internetzugang, was die Sicherheit erhöht, erfordert jedoch spezielle Konfigurationen, um dennoch Zugriff auf notwendige Ressourcen wie den Hauptspeicher im MGMT-Netzwerk zu ermöglichen. Die Anforderungen für dieses Netzwerk müssen eine strikte Isolation gewährleisten, während sie dennoch notwendige Verbindungen für den Betrieb und die Verwaltung ermöglichen.

Name	Netzwerk VLAN 230 VDI
Kurzbeschreibung	VLAN 230 VDI ist ein isoliertes Netzwerk für virtuelle Desktops ohne Internetzugang, dass dennoch Zugriff auf notwendige Ressourcen im MGMT-Netzwerk erlaubt.
Akteure	Tester Netzwerk/Security
Vorbedingungen	VLANs und Firewall-Regeln sind erstellt.
Hauptszenario	Das VDI-Netzwerk ermöglicht sicheren und isolierten Zugriff auf Speicherressourcen im MGMT-Netzwerk, während es von anderen Netzwerken abgeschottet bleibt.
Nachbedingungen	Das VDI-Netzwerk bleibt so weit wie möglich isoliert.

Tabelle 17: ANF-Netzwerk VLAN 230 VDI

ANF-11: Erstellung der Domäne

Die Einrichtung einer neuen Domäne mit einem eigenen Domain Controller ermöglicht eine klare Trennung von der produktiven Umgebung, was wichtig für die Sicherheit und Verwaltung ist. Diese Einrichtung wird getestet, um sicherzustellen, dass die Domäne dom-poc.local unabhängig funktioniert und die Active Directory-Dienste korrekt implementiert wurden.

Name	Erstellung der Domäne
Kurzbeschreibung	Einrichtung einer isolierten Domäne dom-poc.local mit eigenem Domain Controller für verbesserte Sicherheit und unabhängige Verwaltung.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	<ul style="list-style-type: none">- Netzwerkkonfiguriert- XenServer zusammengebaut und aufgesetzt
Hauptszenario	Die Domäne dom-poc.local verfügt über einen dedizierten Domain Controller, der als primärer Authentifizierungsserver dient. Auf diesem Domain Controller sind die Active Directory-Domänen Dienste installiert und konfiguriert, die eine effiziente Verwaltung von Objekten und Gruppen ermöglichen.
Nachbedingungen	Die neue Domäne ist vollständig von der produktiven Umgebung isoliert.

Tabelle 18: ANF-Erstellung der Domäne

ANF-12: Konfiguration DNS Server

Die korrekte Konfiguration des DNS-Servers ist entscheidend für die Netzwerkfunktionalität. Die Anforderung zielt darauf ab zu überprüfen, ob der DNS-Server im VDI-Netzwerk ausschliesslich interne Namensauflösungen durchführt, während er im MGMT-Netzwerk sowohl interne als auch externe Auflösungen ermöglicht.

Name	Konfiguration DNS Server
Kurzbeschreibung	Einrichtung und Konfiguration des Domain Name Systems (DNS) zur Gewährleistung einer korrekten Namensauflösung innerhalb verschiedener Netzwerksegmente.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	<ul style="list-style-type: none">- Netzwerkconfiguriert- XenServer zusammengebaut und aufgesetzt- Domäne und Domain Controller sind eingerichtet
Hauptszenario	Im VDI-Netz löst der DNS-Server ausschliesslich interne Namen und IP-Adressen auf. Im MGMT-Netz dagegen ermöglicht er die Auflösung von sowohl internen als auch externen Namen und IP-Adressen.
Nachbedingungen	Die Namensauflösung funktioniert für das VDI- und MGMT-Netz einwandfrei.

Tabelle 19: ANF-Konfiguration DNS Server

ANF-13: Konfiguration DHCP Server

Die korrekte Konfiguration des DHCP-Servers ist von entscheidender Bedeutung, um eine effiziente Netzwerkverfügbarkeit innerhalb des VDI-Netzes sicherzustellen. Diese Anforderung bezieht sich auf die automatische Vergabe von IP-Adressen, Gateway und DNS durch den DHCP-Server.

Name	Konfiguration DHCP Server
Kurzbeschreibung	Automatische IP-Adressen Vergabe des DHCP-Servers im VDI-Netz.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	<ul style="list-style-type: none">- Netzwerkconfiguriert- XenServer zusammengebaut und aufgesetzt- Domäne und Domain Controller sind eingerichtet- DNS ist eingerichtet auf Domain Controller
Hauptszenario	Der DHCP-Server vergibt automatisch IP-Adressen, Gateway und DNS im VDI ausschliesslich für das VDI-Netz, vom definierten IP-Bereich.
Nachbedingungen	Alle VDI-Maschinen erhalten die korrekten Netzwerkconfigurationn vom DHCP-Server, um eine stabile und sichere Netzwerkverbindung ohne IP-Konflikte und Fehlkonfigurationen zu gewährleisten.

Tabelle 20: ANF-Konfiguration DHCP Server

ANF-14: Replikation auf zweiten Domain Controller

Die Replikation zwischen zwei Domain Controllern sichert die Betriebskontinuität durch regelmässige und vollständige Synchronisation aller Domänendaten. Dies gewährleistet die Datenintegrität und ständige Verfügbarkeit, auch beim Ausfall eines Domain Controllers.

Name	Replikation auf zweiten Domain Controller
Kurzbeschreibung	Sicherstellung der Konsistenz und Verfügbarkeit der Domänendaten durch die Replikation aller relevanten Konfigurationen und Daten auf einen zweiten Domain Controller.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	<ul style="list-style-type: none">- Netzwerkconfiguriert- XenServer zusammengebaut und aufgesetzt- Domäne und Domain Controller sind eingerichtet- DNS ist eingerichtet auf Domain Controller- DHCP ist eingerichtet auf Domain Controller- Active Directory Organizational Unit (OU) Struktur ist eingerichtet
Hauptszenario	Alle Domänendaten, einschliesslich der Active Directory-Objekte, werden regelmässig und vollständig zwischen den beiden Domain Controllern synchronisiert.
Nachbedingungen	Der zweite Domain Controller ist voll funktionsfähig und kann im Falle eines Ausfalls des ersten Domain Controllers die vollständige Kontrolle übernehmen.

Tabelle 21: ANF-Replikation auf zweiten DC

ANF-15: Backup erfolgt automatisch täglich

Die Anforderung legt fest, dass die tägliche Datensicherung automatisch durchgeführt wird, um die Verlässlichkeit und Sicherheit sensibler Daten innerhalb der VDI-Lösung zu gewährleisten.

Name	Backup erfolgt automatisch täglich
Kurzbeschreibung	Automatische Sicherung sensibler Daten mindestens einmal täglich, um die Integrität und Verfügbarkeit der Daten zu gewährleisten.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	VDI-Lösung ist bereit und funktioniert einwandfrei.
Hauptszenario	Das Backup wird täglich automatisch um 2 Uhr morgens durchgeführt.
Nachbedingungen	Durch die Durchführung des Backups während Zeiten geringer Aktivität wird sichergestellt, dass der Betrieb ungestört bleibt.

Tabelle 22: ANF-Backup erfolgt automatisch täglich

ANF-16: Auf VDI läuft ein Antivirus

Die Nutzung von Windows Defender auf VDI-Clients ist essenziell, um durchgehenden Schutz gegen Malware zu gewährleisten.

Name	Auf VDI läuft ein Antivirus
Kurzbeschreibung	Windows Defender wird auf VDI-Clients genutzt, um kontinuierlichen Schutz gegen Malware und andere sicherheitsrelevante Bedrohungen zu bieten.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	VDI-Lösung ist bereit und funktioniert einwandfrei.
Hauptszenario	Auf dem VDI-Client ist Windows Defender mit Echtzeitschutz aktiviert, was eine ununterbrochene Überwachung aller Dateiaktivitäten ermöglicht.
Nachbedingungen	Der Antivirus sorgt dafür, dass alle VDI-Maschinen laufend überwacht und Malware-Bedrohungen effektiv abgewehrt werden.

Tabelle 23: ANF-Auf VDI läuft ein Antivirus

ANF-17: Anmeldung auf die isolierte Umgebung

Die Sicherstellung einer isolierten Anmeldung und eines unabhängigen Betriebs in der VDI-Umgebung ist entscheidend, um die Sicherheit und Integrität der Systeme zu wahren.

Name	Anmeldung auf die isolierte Umgebung
Kurzbeschreibung	Gewährleistung, dass die Anmeldung und der Betrieb innerhalb der isolierten VDI-Umgebung ausschliesslich über eine separate Domäne erfolgen.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	<ul style="list-style-type: none">- Neue Domäne ist erstellt separat zu produktiven- Alle Projektmitarbeiter sind in der neuen Domäne erfasst- Netzwerkrichtlinien wurden erstellt und umgesetzt- Citrix VDI-Lösung ist auch bereit und funktioniert
Hauptszenario	Benutzer melden sich mit ihren Zugangsdaten über die neue Domäne an der VDI-Umgebung an.
Nachbedingungen	Die Anmeldung und Netzwerkverbindung innerhalb der VDI-Umgebung sind vollständig isoliert von der produktiven Umgebung.

Tabelle 24: ANF-Anmeldung auf die isolierte Umgebung

ANF-18: Schutz gegen Geräteverlust oder Diebstahl

Es ist von zentraler Bedeutung, präventive Massnahmen zu ergreifen, um die Kontrolle und den Schutz sensibler Daten zu gewährleisten, insbesondere bei Ereignissen wie Verlust oder Diebstahl.

Name	Schutz gegen Geräteverlust oder Diebstahl
Kurzbeschreibung	Sicherstellen, dass bei Verlust oder Diebstahl meines Arbeitsgerätes keine signifikanten Sicherheitsrisiken entstehen.
Akteure	Tester Netzwerk/Security
Vorbedingungen	<ul style="list-style-type: none">- Notebook ist vollständig eingerichtet mit Antivirus und VPN- Zugriffsberechtigungen nur für autorisierte Benutzer
Hauptszenario	Wenn das Arbeitsnotebook im schlimmsten Fall gestohlen wird, kann der IT-Administrator die gesamte VPN-Verbindung unterbrechen, wodurch auch die aktive VDI-Verbindung getrennt wird.
Nachbedingungen	Verbindung auf Infrastruktur über Citrix VDI nicht möglich.

Tabelle 25: ANF-Schutz gegen Geräteverlust oder Diebstahl

ANF-19: Durchführung von Benutzermutationen

Effiziente Verwaltung von Benutzerkonten ist entscheidend für die Aufrechterhaltung einer reibungslos funktionierenden VDI-Umgebung. Diese Anforderung definiert die Fähigkeit des IT-Supports, Benutzerkonten hinzuzufügen, zu bearbeiten und zu löschen, um die Anpassungsfähigkeit und Sicherheit des Systems zu gewährleisten.

Name	Durchführung von Benutzermutationen
Kurzbeschreibung	Der IT-Support kann Benutzerkonten in der VDI-Infrastruktur hinzufügen, bearbeiten und löschen
Akteure	Tester Serverinfrastruktur
Vorbedingungen	VDI-Lösung ist bereit und funktioniert einwandfrei.
Hauptszenario	Neue Benutzer können erstellt, Eigenschaften angepasst oder gelöscht werden.
Nachbedingungen	Verwaltung durch den IT-Support ist möglich.

Tabelle 26: ANF-Durchführung von Benutzermutationen

ANF-20: Performance und Verfügbarkeit

Um die konstant hohe Leistung und Verfügbarkeit der VDI-Infrastruktur zu gewährleisten, erfolgt eine kontinuierliche Überwachung mittels Citrix-Überwachungstools. Diese sorgfältige Überwachung ist entscheidend, um die Effizienz und Stabilität des Systems sicherzustellen und eine optimale Nutzererfahrung zu bieten.

Name	Performance und Verfügbarkeit
Kurzbeschreibung	Die VDI-Infrastruktur wird kontinuierlich überwacht, um eine leistungsfähige und effiziente Umgebung sicherzustellen.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	VDI-Lösung ist bereit und funktioniert einwandfrei.
Hauptszenario	Die Performance und Verfügbarkeit der VDI-Systeme werden durch den Einsatz von Citrix-Überwachungstools regelmässig überprüft.
Nachbedingungen	Proaktive Massnahmen zur Performance-Optimierung und Verfügbarkeitssicherung können basierend auf den Überwachungsergebnissen getroffen werden.

Tabelle 27: ANF-Performance und Verfügbarkeit

ANF-21: Skalierung während dem laufenden Betrieb

Die flexible und störungsfreie Skalierung der VDI-Infrastruktur während des laufenden Betriebs ist essenziell, um auf veränderte Anforderungen reagieren zu können. Diese Anforderung beschreibt, wie der IT-Administrator die Systemkapazitäten nahtlos anpasst, um die kontinuierliche Produktivität und Benutzerzufriedenheit sicherzustellen.

Name	Skalierung während dem laufenden Betrieb
Kurzbeschreibung	Der IT-Administrator kann die Infrastruktur skalieren, ohne den laufenden Betrieb zu stören.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	VDI-Lösung ist bereit und funktioniert einwandfrei.
Hauptszenario	Bei steigender Anzahl gleichzeitig angemeldeter Benutzer und zunehmendem Ressourcenbedarf kann der IT-Administrator die Kapazitäten der Benutzer individuell anpassen, ohne Unterbrechungen der gesamten Infrastruktur.
Nachbedingungen	Die Skalierung der Infrastruktur erfolgt nahtlos und ohne Unterbrechungen der gesamten VDI-Infrastruktur.

Tabelle 28: ANF-Skalierung während dem laufenden Betrieb

ANF-22: Redundanz der Dienste

Damit die VDI-Lösung ausfallsicherer ist, muss die Redundanz einiger wichtiger Dienste geprüft werden. Zu diesen Diensten gehören der StoreFront-Server, der Desktop Delivery Controller (DDC) und der Workspace Environment Management (WEM) Server.

Name	Redundanz der Dienste
Kurzbeschreibung	Redundanz der StoreFront-Server, DDC und WEM-Server prüfen für den Fall eines Serverausfalls.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	VDI-Lösung ist bereit und funktioniert einwandfrei.
Hauptszenario	Bei einem Ausfall eines dieser Server übernimmt der zweite Server die Aufgaben des ersten.
Nachbedingungen	Die Benutzer merken keinen Unterschied und können sich weiterhin mit ihrer VDI-Umgebung verbinden.

Tabelle 29: ANF-Redundanz der Dienste

ANF-23: Benutzeranpassungen der VDI-Umgebung

Die Anpassungsfähigkeit der VDI-Umgebung ist entscheidend, um Benutzerbedürfnisse effektiv zu erfüllen, während gleichzeitig Sicherheitsstandards eingehalten werden.

Name	Benutzeranpassungen der VDI-Umgebung
Kurzbeschreibung	Benutzeranpassung der VDI-Umgebung werden unterstützt, sofern sie die Sicherheitsrichtlinie nicht verletzen.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	VDI-Lösung ist bereit und funktioniert einwandfrei.
Hauptszenario	Standard VDI-Image kann angepasst werden wie Programm Konfigurationen oder Installationen.
Nachbedingungen	So kann man auf Wunsch vom Kunden noch weitere Anpassungen durchführen.

Tabelle 30: ANF-Benutzeranpassungen der VDI-Umgebung

ANF-24: Fernzugriff

Kunden haben die Möglichkeit, von beliebigen Standorten, einschliesslich des Homeoffice, eine sichere Verbindung zu ihrer VDI-Umgebung herzustellen. Diese Remoteverbindung wird durch die Implementierung einer Zwei-Faktor-Authentifizierung zusätzlich abgesichert.

Name	Fernzugriff
Kurzbeschreibung	Kunden können sich sicher von jedem Ort, einschliesslich des Homeoffice, auf ihre VDI verbinden.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	VDI-Lösung ist bereit und funktioniert einwandfrei.
Hauptszenario	Sobald der Benutzer eine Verbindung zum Firmennetzwerk hat und sich über Citrix Storefront einloggen kann, kann auf die berechtigte Umgebung gearbeitet werden.
Nachbedingungen	Erfolgreiche Anmeldung auf Citrix VDI-Umgebung.

Tabelle 31: ANF-Fernzugriff

ANF-25: Kollaboration mit Projektmitarbeitern

Die Anforderung fokussiert auf die Unterstützung von Kollaboration innerhalb der Citrix VDI-Umgebung, um sicherzustellen, dass Projektmitarbeiter effizient und ohne gegenseitige Störungen zusammenarbeiten können.

Name	Echtzeit Kollaboration mit Projektmitarbeitern
Kurzbeschreibung	Gewährleistung einer nahtlosen und effizienten Kollaboration zwischen Projektmitarbeitern innerhalb der Citrix VDI-Umgebung.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	VDI-Lösung ist bereit und funktioniert einwandfrei.
Hauptszenario	Mehrere Benutzer melden sich gleichzeitig an der Citrix VDI an und arbeiten gemeinsam an Projekten, ohne dass es zu Verzögerungen oder Interferenzen kommt.
Nachbedingungen	Die Kollaboration führt zu einer messbaren Steigerung der Effizienz und Produktivität.

Tabelle 32: ANF-Kollaboration mit Projektmitarbeitern

ANF-26: VDI hat kein Internetzugang

Diese Anforderung spezifiziert die Konfiguration der VDI-Umgebung, um direkten Internetzugang zu verhindern und die Sicherheit zu erhöhen. Durch die Beschränkung auf interne Ressourcen wird sichergestellt, dass die VDI-Umgebung die strikten Sicherheitsrichtlinien der Organisation erfüllt.

Name	VDI hat kein Internetzugang
Kurzbeschreibung	Die VDI-Umgebung ermöglicht keinen Internetzugang.
Akteure	Tester Netzwerk/Security
Vorbedingungen	VDI-Lösung ist bereit und funktioniert einwandfrei.
Hauptszenario	In der VDI-Umgebung wird der Internetzugang gesperrt, um zu gewährleisten, dass Benutzer ausschliesslich auf interne Netzwerkressourcen zugreifen können.
Nachbedingungen	Die Sicherheitsrichtlinien des Kunden werden eingehalten.

Tabelle 33: ANF-VDI hat kein Internetzugang

ANF-27: Vordefinierte Programme sind auf der VDI installiert

Diese Anforderung definiert die Installation und Funktionalität spezifischer, vorab festgelegter Programme innerhalb der VDI-Umgebung, um sicherzustellen, dass alle notwendigen Arbeitswerkzeuge für die Benutzer verfügbar und betriebsbereit sind.

Name	Vordefinierte Programme sind auf der VDI installiert
Kurzbeschreibung	Sicherstellung, dass spezifische, für die Arbeit notwendige Programme vorab auf der VDI installiert und funktionsfähig sind.
Akteure	Tester Serverinfrastruktur
Vorbedingungen	VDI-Lösung ist bis auf diesen Punkt eingerichtet.
Hauptszenario	Projektmitarbeiter können die vordefinierten Applikationen auf der VDI-Umgebung ohne technische Hindernisse starten und nutzen.
Nachbedingungen	Die Benutzer können dieselben Programme in der VDI-Umgebung nutzen.

Tabelle 34: ANF-Vordefinierte Programme sind auf der VDI installiert

ANF-28: Sicherheitsfunktionen

Diese Anforderung spezifiziert die Implementierung von Sicherheitsmechanismen innerhalb der VDI-Umgebung, um sicherzustellen, dass vertrauliche Informationen geschützt bleiben.

Name	Sicherheitsfunktionen
Kurzbeschreibung	Einführung spezieller Sicherheitsfunktionen zur Verhinderung von Screenshots und Videoaufnahmen in der VDI-Umgebung, um die Sicherheit sensibler Daten zu verstärken.
Akteure	Tester Netzwerk/Security
Vorbedingungen	VDI-Lösung ist bereit und funktioniert einwandfrei
Hauptszenario	Die VDI-Umgebung ist so konfiguriert, dass Screenshots oder Bildschirmaufnahmen nicht möglich sind.
Nachbedingungen	Die Sicherheitsmaßnahmen sind effektiv implementiert und aktiviert, wodurch die Vertraulichkeit und Integrität der Informationen in der VDI-Umgebung sichergestellt wird.

Tabelle 35: ANF-Sicherheitsfunktionen

9 Testfälle

In diesem Kapitel werden die verschiedenen Testfälle zur Sicherstellung der Qualität und Funktionalität der VDI-Lösung beschrieben. Die Testfälle sind in vier Hauptkategorien unterteilt: Komponententests, Integrationstests, Systemtests und Abnahmetests. Diese Kategorien decken alle Aspekte des Testprozesses ab. Wie bei den Anforderungen sind die Testfälle ebenfalls nummeriert, wobei «TF» für Testfall steht.

9.1 Komponententests

In diesem Unterkapitel werden die Testfälle aller Komponenten aufgezeigt und beschrieben. Der Komponententests dient dazu, zu überprüfen, ob die Komponenten ordnungsgemäss funktionieren, um die Integration erfolgreich durchzuführen.

TF-01: Funktionalität der Sophos Firewall

ANF-01: Funktionalität der Sophos Firewall

Ziele des Tests:

- Sicherstellen, dass die Sophos Firewall korrekt konfiguriert ist, um den Netzwerkverkehr effektiv zu kontrollieren und zu überwachen, insbesondere hinsichtlich der Unterstützung für VLANs und Sicherheitsrichtlinien

Schritt	Beschreibung	Erwartetes Ergebnis
1	Erreichbarkeit der Firewall über das produktive Netzwerk mit dem folgenden Befehl. - PING (IP von Firewall)	Die Firewall ist erreichbar.
2	Zugriff auf das Webinterface der Firewall über das produktive Netzwerk mit einem Browser.	Man kann sich auf der Firewall mit den Zugangsdaten anmelden.
3	Überprüfung, ob VLANs und Richtlinien auf der Firewall erstellt werden können.	Neue VLANs und Richtlinien können auf der Firewall eingerichtet werden.

Tabelle 36: TF-Funktionalität der Sophos Firewall

TF-02: Funktionalität der Netzwerk-Switches

ANF-02: Funktionalität der Netzwerk-Switches

Ziele des Tests:

- Sicherstellen, dass die Netzwerk-Switches korrekt Grundkonfiguriert sind, um die Erstellung von VLANs zu ermöglichen und ihre zentrale Rolle im Netzwerkmanagement effektiv zu erfüllen

Schritt	Beschreibung	Erwartetes Ergebnis
1	Erreichbarkeit der Switches über das produktive Netzwerk mit dem folgenden Befehl. - PING (IP von Switch)	Die Switches sind erreichbar.
2	Zugriff auf das Webinterface der Switches über das produktive Netzwerk mit einem Browser.	Man kann sich auf die Switches mit den Zugangsdaten anmelden.
3	Überprüfung, ob VLANs auf die Switches erstellt werden können.	Neue VLANs können auf die Switches eingerichtet werden.

Tabelle 37: TF-Funktionalität der Netzwerk-Switches

TF-03: XenServer Management 1

ANF-03: XenServer Management 1

Ziele des Tests:

- Überprüfung der Funktionalität aller eingebauten Komponenten des XenServer Management Servers

Schritt	Beschreibung	Erwartetes Ergebnis
1	Verfügbarkeit des Servers über das Netzwerk prüfen mit dem Befehl: PING 192.168.220.10	Server ist über das Netzwerk erreichbar.
2	Verbindung zum Server über XenCenter herstellen.	Verbindung über XenCenter ist erfolgreich.
3	Ressourcen im XenCenter überprüfen.	Alle Komponenten sind ersichtlich und laufen einwandfrei.
4	Version des Servers im XenCenter überprüfen.	XenServer Version 8.0 wird angezeigt.

Tabelle 38: TF-XenServer Management 1

TF-04: XenServer Management 2

ANF-04: XenServer Management 2

Ziele des Tests:

- Überprüfung der Funktionalität aller Komponenten vom XenServer MGMT-2

Schritt	Beschreibung	Erwartetes Ergebnis
1	Verfügbarkeit des Servers über das Netzwerk prüfen mit dem Befehl: PING 192.168.220.11	Server ist über das Netzwerk erreichbar.
2	Verbindung zum Server über XenCenter herstellen.	Verbindung über XenCenter ist erfolgreich.
3	Ressourcen im XenCenter überprüfen.	Alle Komponenten sind ersichtlich und laufen einwandfrei.
4	Version des Servers im XenCenter überprüfen.	XenServer Version 8.0 wird angezeigt.

Tabelle 39: XenServer Management 2

TF-05: XenServer VDI

ANF-05: XenServer VDI

Ziele des Tests:

- Überprüfung der Funktionalität aller Komponenten des XenServer VDI Servers

Schritt	Beschreibung	Erwartetes Ergebnis
1	Verfügbarkeit des Servers über das Netzwerk prüfen mit dem Befehl: PING 192.168.220.13	Server ist über das Netzwerk erreichbar.
2	Verbindung zum Server über XenCenter herstellen.	Verbindung über XenCenter ist erfolgreich.
3	Ressourcen im XenCenter überprüfen.	Alle Komponenten sind ersichtlich und laufen einwandfrei.
4	Version des Servers im XenCenter überprüfen.	XenServer Version 8.0 wird angezeigt.

Tabelle 40: TF-XenServer VDI

TF-06: Hauptspeicher Synology NAS

ANF-06: Hauptspeicher Synology NAS

Ziele des Tests:

- Überprüfung der Festplattenkonfiguration und des Updatestands des Hauptspeichers

Schritt	Beschreibung	Erwartetes Ergebnis
1	Verbindung über das Webinterface auf Synology NAS mit der folgenden URL: https://192.168.220.15	Verbindung ist über das Netzwerkinterface möglich.
2	Überprüfung, ob ein RAID auf dem NAS eingerichtet wurde.	Ein RAID wurde eingerichtet, um Ausfallsicherheit bei einem Festplattenausfall zu gewährleisten.
3	Überprüfung des Updatestands des Synology NAS.	Das NAS ist auf dem neuesten Stand.

Tabelle 41: TF-Hauptspeicher Synology NAS

TF-07: Backupspeicher Synology NAS

ANF-07: Backupspeicher Synology NAS

Ziele des Tests:

- Überprüfung der Festplattenkonfiguration und des Updatestands des Backup-Speichers

Schritt	Beschreibung	Erwartetes Ergebnis
1	NAS mit Monitor, Tastatur und Maus verbinden, um darauf zuzugreifen, da es sich im geschlossenen NFS-Netz befindet.	Anmeldung auf dem NAS ist erfolgreich.
2	Überprüfung, ob ein RAID auf dem NAS eingerichtet wurde.	Ein RAID wurde eingerichtet, um Ausfallsicherheit bei einem Festplattenausfall zu gewährleisten.
3	Überprüfung des Updatestands des Synology NAS.	Das NAS ist auf dem neuesten Stand.

Tabelle 42: TF-Backupspeicher Synology NAS

9.2 Integrationstests

Hier werden alle Integrationstests durchgeführt, um zu überprüfen, ob die Komponenten miteinander ordnungsgemäss funktionieren. Dies ist notwendig, um anschliessend die Systemtests durchzuführen.

TF-08: Netzwerk VLAN 210 NFS

ANF-08: Netzwerk VLAN 210 NFS

Ziele des Tests:

- Überprüfung, ob die Zugriffsrichtlinien vom VLAN 210 ordnungsgemäss funktionieren

Schritt	Beschreibung	Erwartetes Ergebnis
1	Von srv-dc-01 (VDI-Netz) und srv-ddc-01 (MGMT-Netz) den Backup-Server srv-backup-01 (NFS-Netz) mit folgenden Befehlen anpingen: - PING 192.168.210.15 - PING srv-backup-01	Der Backup-Server ist über diese IP nicht erreichbar, da sowohl das VDI- als auch das MGMT-Netz keinen Zugriff auf das NFS-Netz haben.
2	Von srv-backup-01 den srv-dc-01 und srv-ddc-01 mit folgenden Befehlen anpingen: - PING 192.168.230.20 - PING srv-dc-01 - PING 192.168.220.23 - PING srv-ddc-01	Die DC- und DDC-Server sind vom NFS-Netz nicht erreichbar, da das Netz keinen Zugriff auf das VDI- und MGMT-Netz hat.
3	Von srv-backup-01 den srv-data-01 (NFS-Leitung) mit folgenden Befehlen anpingen: - PING 192.168.210.17 - PING srv-data-01	Der Data-Server ist über diese IP erreichbar, da er sich im gleichen Netz wie der Backup-Server befindet.

Tabelle 43: Netzwerk VLAN 210 NFS

TF-09: Netzwerk VLAN 220 MGMT

ANF-09: Netzwerk VLAN 220 MGMT

Ziele des Tests:

- Überprüfung, ob die Zugriffsrichtlinien vom VLAN 220 ordnungsgemäss funktionieren

Schritt	Beschreibung	Erwartetes Ergebnis
1	Von produktivem Netzwerk den MGMT-XenServer anpingen mit folgendem Befehl: - PING 192.168.220.10	XenServer ist mit dieser IP erreichbar.
2	Von MGMT-XenServer einen Client im produktiven Netzwerk anpingen.	Client ist nicht erreichbar, da das MGMT-Netzwerk keinen Zugriff auf das produktive Netz hat.
3	Internetzugang überprüfen von srv-ddc-01 mit dem folgenden Befehl: - PING 8.8.8.8	Da sich srv-ddc-01 im MGMT-Netz befindet und dieser Internetzugang hat, sollte der PING erfolgreich ausgeführt werden.
5	Vom srv-ddc-01 den srv-dc-01 anpingen mit dem folgenden Befehl: - PING 192.168.230.20 - PING srv-dc-01	DC ist vom MGMT-Netz erreichbar.

Tabelle 44: TF-Netzwerk VLAN 220 MGMT

TF-10: Netzwerk VLAN 230 VDI

ANF-10: Netzwerk VLAN 230 VDI

Ziele des Tests:

- Überprüfung, ob die Zugriffsrichtlinien vom VLAN 220 ordnungsgemäss funktionieren

Schritt	Beschreibung	Erwartetes Ergebnis
1	Von einer VDI-Maschine die folgende URL abrufen: - www.google.com	Die URL kann nicht aufgelöst werden, da es keinen Internetzugang vom VDI-Netzwerk gibt.
2	Vom srv-dc-01 den srv-ddc-01 anpingen mit dem folgenden Befehl: - PING 192.168.220.23 - PING srv-ddc-01	Der DDC-Server ist vom VDI-Netz nicht erreichbar.

Tabelle 45: TF-Netzwerk VLAN 230 VDI

TF-11: Erstellung der Domäne

ANF-11: Erstellung der Domäne

Ziele des Tests:

- Überprüfen der erfolgreichen Einrichtung der Domäne «dom-poc.local» gemäss den definierten Anforderungen
- Sicherstellen, dass der dedizierte Domain Controller ordnungsgemäss funktioniert und als primärer Authentifizierungsserver fungiert
- Überprüfung der Active Directory Struktur

Schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung, ob der Domain Controller (DC) im Netzwerk erreichbar ist, indem die statische IP-Adresse der VM angepingt wird.	Die DC ist erreichbar.
2	Anmeldung auf DC über Remote Desktop (RDP) mit Domain-Admin und Überprüfung, ob die Active Directory-Domänen Dienste installiert sind.	Erfolgreiche Anmeldung und die Active Directory-Domänen Dienste sind installiert.
3	Überprüfung, ob die Domäne «dom-poc.local» in der Active Directory angezeigt wird.	Die Domäne «dom-poc.local» wird in der Active Directory angezeigt
4	Überprüfung der Active Directory (AD) Struktur gemäss Detailkonzept.	Die AD-Struktur ist wie im Detailkonzept beschrieben erstellt.

Tabelle 46: TF-Erstellung der Domäne

TF-12: Konfiguration DNS Server

ANF-12: Konfiguration DNS Server

Ziele des Tests:

- Bestätigung der erfolgreichen Einrichtung und Konfiguration des DNS-Servers gemäss den spezifizierten Anforderungen
- Gewährleistung, dass der DNS-Server im VDI-Netz nur interne Namen und IP-Adressen auflöst, während er im MGMT-Netz sowohl interne als auch externe Namen und IP-Adressen auflöst
- Überprüfung der korrekten Funktionsweise der Namensauflösung für sowohl das VDI- als auch das MGMT-Netz, um sicherzustellen, dass alle Netzwerksegmente ordnungsgemäss arbeiten

Schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung der DNS-Server-Konfiguration auf dem Domain Controller, um sicherzustellen, dass er sowohl das MGMT- als auch das VDI-Netz auflöst.	Die DNS-Server-Konfiguration zeigt, dass der Domain Controller korrekt konfiguriert ist und Anfragen für das MGMT-Netz (192.168.220.0) und das VDI-Netz (192.168.230.0) auflösen kann.
2	Überprüfung der Namensauflösung im MGMT-Netz durch Anfragen an den DNS-Server für sowohl interne als auch externe Adressen durch folgende Befehle: - NSLOOKUP srv-lic-01 - NSLOOKUP 192.168.220.25 - NSLOOKUP www.google.com - NSLOOKUP 8.8.8.8	Die DNS-Anfragen für interne und externe Adressen werden korrekt aufgelöst.
3	Überprüfung der Namensauflösung im VDI-Netz durch Anfragen an den DNS-Server für interne Adressen mit dem folgenden Befehl: - NSLOOKUP srv-dc-02 - NSLOOKUP 192.168.230.21	Die DNS-Anfragen für interne Adressen im VDI-Netz werden korrekt aufgelöst, während Anfragen für externe Adressen fehlgeschlagen.

Tabelle 47: TF-Konfiguration DNS Server

TF-13: Konfiguration DHCP Server

ANF-13: Konfiguration DHCP Server

Ziele des Tests:

- Überprüfung der erfolgreichen Einrichtung und Konfiguration des DHCP-Servers gemäss den spezifizierten Anforderungen
- Sicherstellung, dass der DHCP-Server im VDI-Netz automatisch IP-Adressen, Gateway und DNS-Server vergibt

Schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung der DHCP-Server-Konfiguration, um sicherzustellen, dass der IP-Adressbereich (192.168.230.30 - 192.168.230.200), der Gateway (192.168.230.1) und die DNS-Server (192.168.230.20 und 192.168.230.21) korrekt eingetragen sind.	Die DHCP-Server-Konfiguration zeigt, dass der IP-Adressbereich, der Gateway und die DNS-Server korrekt konfiguriert sind.
2	Verbindung auf einer VDI-Maschine und Überprüfung, ob die IP-Adresse automatisch vom DHCP-Server bezogen wird.	Die VDI-Maschine erhält automatisch eine IP-Adresse im Bereich von 192.168.230.30 bis 192.168.230.200.
3	Überprüfung, ob die VDI-Maschine den richtigen Gateway (192.168.230.1) und die richtigen DNS-Server (192.168.230.20 und 192.168.230.21) erhalten hat mit dem folgenden Befehl: - IPCONFIG /ALL	Die VDI-Maschine hat das Gateway 192.168.230.1 und die DNS-Server 192.168.230.20 und 192.168.230.21 zugewiesen bekommen.
4	Überprüfung der Lease-Dauer auf der VDI-Maschine, um sicherzustellen, dass sie auf 8 Tage eingestellt ist.	Die Lease-Dauer der IP-Adresse auf der VDI-Maschine zeigt 8 Tage an.

Tabelle 48: TF-Konfiguration DHCP Server

TF-14: Replikation auf zweiten Domain Controller

ANF-14: Replikation auf zweiten Domain Controller

Ziele des Tests:

- Sicherstellung, dass alle Domänendaten regelmässig und vollständig zwischen den beiden Domain Controllern synchronisiert werden
- Überprüfung der vollständigen Funktionsfähigkeit des zweiten Domain Controllers, einschliesslich seiner Fähigkeit, im Falle eines Ausfalls des ersten Domain Controllers die volle Kontrolle über die Domäne zu übernehmen

Schritt	Beschreibung	Erwartetes Ergebnis
1	Erstellen eines neuen Objekts im Active Directory auf dem ersten Domain Controller (srv-dc-01).	Das neue Objekt erscheint automatisch im Active Directory auf dem zweiten Domain Controller (srv-dc-02).
2	Erstellen einer Datei im SYSVOL-Ordner auf dem ersten Domain Controller (srv-dc-01).	Die Datei erscheint automatisch im SYSVOL-Ordner auf dem zweiten Domain Controller (srv-dc-02).
3	Erstellen eines neuen DNS-Eintrags auf dem ersten Domain Controller (srv-dc-01).	Der neue DNS-Eintrag erscheint automatisch im DNS-Manager auf dem zweiten Domain Controller (srv-dc-02).
4	Erstellen einer Test-GPO (Gruppenrichtlinie) auf dem ersten Domain Controller (srv-dc-01).	Die Test-GPO erscheint automatisch im Gruppenrichtlinien-Manager auf dem zweiten Domain Controller (srv-dc-02).
5	Erstellung einer DHCP-Failover-Konfiguration vom ersten Domain Controller (srv-dc-01) auf dem zweiten.	Die DHCP-Failover-Konfiguration ist auf dem zweiten Domain Controller (srv-dc-02) im DHCP-Manager eingerichtet.
6	Herunterfahren des ersten Domain Controllers (srv-dc-01) und Überprüfung, ob der zweite Domain Controller (srv-dc-02) alle Aufgaben übernimmt.	Der zweite Domain Controller (srv-dc-02) übernimmt erfolgreich alle Aufgaben und die Domäne funktioniert weiterhin ordnungsgemäss.

Tabelle 49: TF-Replikation auf zweiten DC

TF-15: Backup erfolgt automatisch täglich

ANF-15: Backup erfolgt automatisch täglich

Ziele des Tests:

- Überprüfung, dass das Backup täglich um 2 Uhr morgens automatisch durchgeführt wird, um die Integrität und Verfügbarkeit der Daten zu gewährleisten

Schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung der Backup-Konfiguration, um sicherzustellen, dass ein tägliches Backup um 2 Uhr morgens geplant ist.	Die Backup-Konfiguration zeigt, dass ein tägliches Backup um 2 Uhr morgens korrekt geplant ist.
2	Überwachung der Backup-Protokolle am nächsten Tag, um zu bestätigen, dass das Backup erfolgreich durchgeführt wurde.	Die Backup-Protokolle bestätigen, dass das tägliche Backup um 2 Uhr morgens erfolgreich durchgeführt wurde.

Tabelle 50: TF-Backup erfolgt automatisch täglich

TF-16: Auf VDI läuft ein Antivirus

ANF-16: Auf VDI läuft ein Antivirus

Ziele des Tests:

- Sicherstellung, dass der Echtzeitschutz von Windows Defender aktiviert ist, um eine kontinuierliche Überwachung aller Dateiaktivitäten auf den VDI-Clients zu ermöglichen
- Überprüfung, ob der Antivirus sicherstellt, dass alle VDI-Maschinen laufend überwacht werden und effektiv vor Malware-Bedrohungen geschützt sind

Schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung, ob Windows Defender mit Echtzeitschutz den VDI-Maschinen aktiviert ist.	Windows Defender mit Echtzeitschutz ist aktiviert.
2	Durchführung eines vollständigen Systemscans auf einer VDI-Maschine	Der vollständige Systemscan zeigt keine Malware-Bedrohungen an und bestätigt, dass das System überwacht wird.

Tabelle 51: TF-Auf VDI läuft ein Antivirus

9.3 Systemtests

Hier werden alle Systemtests durchgeführt. Das System wird als Ganzes getestet, um zu überprüfen, ob die VDI-Lösung betrieben werden kann.

TF-17: Anmeldung auf die isolierte Umgebung

ANF-17: Anmeldung auf die isolierte Umgebung

Ziele des Tests:

- Sicherstellen, dass Benutzer sich erfolgreich mit ihren Zugangsdaten über die neue Domäne an der VDI-Umgebung anmelden können

Schritt	Beschreibung	Erwartetes Ergebnis
1	Anmeldung über die neue Domäne auf der eigenen VDI-Umgebung.	Die Anmeldung war erfolgreich.
2	Nach der Anmeldung überprüfen, mit welchem Benutzer man angemeldet ist, durch den Befehl: - WHOAMI	Als Ausgabe erscheint der eigene Benutzername.

Tabelle 52: TF-Anmeldung auf die isolierte Umgebung

TF-18: Schutz gegen Geräteverlust oder Diebstahl

ANF-18: Schutz gegen Geräteverlust oder Diebstahl

Ziele des Tests:

- Gewährleistung, dass im Falle von Verlust oder Diebstahl des Arbeitsnotebooks der IT-Administrator in der Lage ist, die gesamte VPN-Verbindung zu unterbrechen, was auch die aktive VDI-Verbindung trennt

Schritt	Beschreibung	Erwartetes Ergebnis
1	Trennung der VPN-Verbindung eines Notebooks, um den Verlust oder Diebstahl zu simulieren.	Das Notebook kann keine Verbindung mehr zum Firmennetzwerk herstellen, und die aktive VDI-Verbindung wird sofort getrennt.

Tabelle 53: TF-Schutz gegen Geräteverlust oder Diebstahl

TF-19: Durchführung von Benutzermutationen

ANF-19: Durchführung von Benutzermutationen

Ziele des Tests:

- Gewährleistung, dass die Verwaltung von Benutzerkonten in der VDI-Infrastruktur durch den IT-Support effizient und fehlerfrei erfolgen kann

Schritt	Beschreibung	Erwartetes Ergebnis
1	Ein Testbenutzerkonto wird im Active Directory erstellt und der Benutzer wird der neuen VDI-Umgebung zugewiesen.	Das Testbenutzerkonto wird erfolgreich erstellt und zugewiesen.
2	Anmeldung des Testbenutzers an der VDI-Umgebung, um die Funktionsfähigkeit des Kontos zu überprüfen.	Der Testbenutzer kann sich erfolgreich an der VDI-Umgebung anmelden.
3	Überprüfung, ob der Testbenutzer Zugriff auf die notwendigen Ressourcen und Anwendungen hat, die für seine Rolle vorgesehen sind.	Der Testbenutzer hat Zugriff auf alle zugewiesenen Ressourcen und Anwendungen.
4	Löschen des Testbenutzerkontos und Überprüfung, ob alle zugehörigen Daten und Zugriffe korrekt entfernt wurden.	Das Testbenutzerkonto und alle zugehörigen Daten und Zugriffe werden vollständig entfernt.

Tabelle 54: TF-Durchführung von Benutzermutationen

TF-20: Performance und Verfügbarkeit

ANF-20: Intuitiv Performance und Verfügbarkeit

Ziele des Tests:

- Bestätigung, dass die Performance der VDI-Systeme regelmässig überwacht wird, um eine leistungsfähige und effiziente Umgebung sicherzustellen

Schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung der Performance und Verfügbarkeit der VDI-Umgebung über das Citrix Dashboard.	Die Performance- und Verfügbarkeitsdaten sind im Citrix Dashboard sichtbar und zeigen keine Auffälligkeiten.
2	Durchführung eines Lasttests auf einer Test-VDI-Umgebung, um die Systemleistung unter hoher Auslastung zu überprüfen.	Das System bleibt auch unter hoher Last stabil und die Performance-Daten werden korrekt im Dashboard angezeigt.

Tabelle 55: TF-Performance und Verfügbarkeit

TF-21: Skalierung während dem laufenden Betrieb

ANF-21: Skalierung während dem laufenden Betrieb

Ziele des Tests:

- Bestätigung, dass die VDI-Infrastruktur während des laufenden Betriebs skalierbar ist, um den steigenden Anforderungen gerecht zu werden
- Sicherstellung, dass die Nutzer während des Skalierungsvorgangs weiterhin uneingeschränkt auf die VDI-Infrastruktur zugreifen können und ihre Arbeitsabläufe nicht beeinträchtigt werden

Schritt	Beschreibung	Erwartetes Ergebnis
1	Mehrere Testbenutzer melden sich an und führen einen Lasttest aus.	Im Citrix Dashboard wird angezeigt, dass die Ressourcen ausgelastet sind.
2	Die Testbenutzer, die am meisten Leistung benötigen, erhalten eine VDI-Maschine mit mehr Ressourcen.	Alle anderen Testbenutzer können weiterarbeiten, ohne unterbrochen zu werden.
3	Überprüfung nach Skalierung	Die Ressourcen liegen innerhalb der akzeptablen Grenzwerte.

Tabelle 56: TF-Skalierung während dem laufenden Betrieb

TF-22: Redundanz der Dienste

ANF-22: Redundanz der Dienste

Ziele des Tests:

- Überprüfung der Ausfallsicherheit der Dienste Storefront Server, Desktop Delivery Controller und Workspace Environment Management

Schritt	Beschreibung	Erwartetes Ergebnis
1	Verbindung auf XenServer über den XenCenter herstellen.	Verbindung zu XenServer kann erfolgreich hergestellt werden.
2	Um einen Ausfall zu simulieren, werden alle drei Server über XenCenter heruntergefahren: - srv-sfs-01 - srv-ddc-01 - srv-wem-01	VMs werden im XenCenter als heruntergefahren angezeigt.
3	Überprüfen, ob die redundanten Server die Aufgaben übernommen haben, indem eine Testanmeldung auf die VDI-Umgebung durchgeführt wird.	Die Testanmeldung ist erfolgreich, und die redundanten Server haben die Aufgaben übernommen: - srv-sfs-02 - srv-ddc-02 - srv-wem-02

Tabelle 57: Redundanz der Dienste

TF-23: Benutzeranpassungen der VDI-Umgebung

ANF-23: Benutzeranpassungen der VDI-Umgebung

Ziele des Tests:

- Sicherstellung, dass zusätzliche Anpassungen am Standard-Image auf Wunsch des Kunden durchgeführt werden können

Schritt	Beschreibung	Erwartetes Ergebnis
1	Installation des Programms PDF24 auf dem Standard-VDI-Image.	Die Installation ist für alle VDI-Maschinen verfügbar und bleibt nach einer erneuten Anmeldung des Benutzers erhalten.
2	Der Testbenutzer meldet sich erneut an der VDI-Umgebung an und überprüft, ob die vorgenommenen Anpassungen vorhanden sind.	Das installierte Programm ist nach der erneuten Anmeldung weiterhin vorhanden.
3	Testen der Funktionalität des installierten Programms, um sicherzustellen, dass es ordnungsgemäß funktioniert.	Das Programm funktioniert einwandfrei.

Tabelle 58: TF-Benutzeranpassungen der VDI-Umgebung

9.4 Abnahmetests

Im Abnahmetest werden alle wichtigen Funktionen getestet, die für den Auftraggeber von Bedeutung sind und das gesamte Projekt ausmachen.

TF-24: Fernzugriff

ANF-24: Fernzugriff

Ziele des Tests:

- Sicherstellung, dass Kunden sicher von jedem Ort auf ihre VDI-Umgebung zugreifen können

Schritt	Beschreibung	Erwartetes Ergebnis
1	Das eingerichtete VPN auf dem Firmen-notebook starten.	Verbindung zum Firmennetzwerk ist möglich und es erscheint die Citrix Storefront-Anmeldemaske.
2	Anmeldung auf Citrix VDI.	Die Eingabe war erfolgreich.
3	VDI-Umgebung starten und Überprüfung der Verbindung und Funktionalität.	Die VDI-Umgebung startet erfolgreich.

Tabelle 59: TF-Fernzugriff

TF-25: Kollaboration mit Projektmitarbeitern

ANF-25: Kollaboration mit Projektmitarbeitern

Ziele des Tests:

- Überprüfung, ob mehrere Benutzer gleichzeitig auf die Citrix VDI-Umgebung zugreifen und gemeinsam an Projekten arbeiten können

Schritt	Beschreibung	Erwartetes Ergebnis
1	Mehrere Testbenutzer melden sich gleichzeitig an der VDI-Umgebung an.	Die Anmeldung ist erfolgreich und die Mitarbeiter blockieren sich nicht gegenseitig.
2	Jeder Projektmitarbeiter hat Zugriff auf die für ihn freigegebenen Daten und Ressourcen.	Die Mitarbeiter können auf die freigegebenen Daten zugreifen und diese nach Absprache gemeinsam bearbeiten.

Tabelle 60: TF-Kollaboration mit Projektmitarbeitern

TF-26: VDI hat kein Internetzugang

ANF-26: VDI hat kein Internetzugang

Ziele des Tests:

- Bestätigung, dass die VDI-Umgebung keinen Internetzugang ermöglicht, wie spezifiziert
- Sicherstellen, dass Benutzer ausschliesslich auf interne Netzwerkressourcen zugreifen können

Schritt	Beschreibung	Erwartetes Ergebnis
1	Einen Webbrowser in der VDI-Umgebung öffnen und die folgende Webseite aufrufen: - www.gibb.ch	Der Zugriff auf externe Webseiten ist nicht möglich und es wird eine Fehlermeldung angezeigt.

Tabelle 61: TF-VDI hat kein Internetzugang

TF-27: Vordefinierte Programme sind auf der VDI installiert

ANF-27: Vordefinierte Programme sind auf der VDI installiert

Ziele des Tests:

- Sicherstellung, dass die spezifischen Programme, die für die Arbeit notwendig sind, vorab auf der VDI installiert wurden
- Überprüfung, ob die vordefinierten Anwendungen auf der VDI-Umgebung funktionsfähig sind

Schritt	Beschreibung	Erwartetes Ergebnis
1	Die vorinstallierten Anwendungen in der VDI-Umgebung starten und ihre Funktionalität überprüfen.	Die Anwendungen starten ohne Probleme und funktionieren einwandfrei.
2	Eine Testaufgabe mit jeder der vorinstallierten Anwendungen durchführen, um ihre Leistungsfähigkeit und Stabilität zu prüfen.	Jede Anwendung führt die Testaufgabe erfolgreich aus, ohne Abstürze oder Fehlermeldungen.

Tabelle 62: TF-Vordefinierte Programme sind auf der VDI installiert

TF-28: Sicherheitsfunktionen

ANF-28: Sicherheitsfunktionen

Ziele des Tests:

- Gewährleistung, dass die implementierten Sicherheitsmaßnahmen effektiv aktiviert wurden

Schritt	Beschreibung	Erwartetes Ergebnis
1	Versuchen, Daten von der VDI-Umgebung auf das lokale Notebook zu kopieren und umgekehrt.	Die Kopierfunktion ist blockiert und es können keine Daten vom lokalen Notebook in die VDI-Umgebung oder aus der VDI-Umgebung auf das lokale Notebook kopiert werden.
2	Überprüfung, ob Screenshots oder Videoaufnahmen vom lokalen Notebook aus von der VDI-Umgebung gemacht werden können.	Screenshots und Videoaufnahmen können vom lokalen Notebook aus nicht gemacht werden.
3	Beim Anmeldeprozess in die VDI-Umgebung muss mindestens einmal eine Zwei-Faktor-Authentifizierung (2FA) durchgeführt werden.	Die Multi-Faktor-Authentifizierung ist erfolgreich implementiert und funktioniert einwandfrei.

Tabelle 63: TF-Sicherheitsfunktionen

10 Testausführung

Die Testergebnisse werden in die Kategorien «erfolgreich» und «nicht erfolgreich» eingeteilt und bewertet. In diesem Kapitel wird erläutert, welche Bedingungen zur Einordnung in diese Kategorien führen und wie die Testauswertung erfolgt.

10.1 Test erfolgreich

Ein Test gilt als erfolgreich, wenn alle vordefinierten Testziele und Anforderungen erfüllt sind. Die folgenden Punkte beschreiben einen erfolgreichen Test.

- Alle Testfälle werden ohne Fehler abgeschlossen.
- Die VDI-Lösung funktioniert wie erwartet und erfüllt die festgelegten Spezifikationen.
- Es gibt keine kritischen oder schweren Mängel in der Fehlerklasse 3 und 4.

10.2 Test nicht erfolgreich

Ein Test wird als nicht erfolgreich eingestuft, wenn eine oder mehrere der folgenden Bedingungen zutreffen sind.

- Es treten kritische oder schwere Mängel auf, die den Betrieb der VDI-Lösung beeinträchtigen oder unmöglich machen.
- Die definierten Testziele und Anforderungen werden nicht erreicht.
- Es gibt signifikante Abweichungen vom erwarteten Ergebnis.

10.3 Testauswertung

Nach der Durchführung der Tests wird eine Auswertung vorgenommen. Die Auswertung umfasst:

- Eine Zusammenfassung der erfolgreichen und nicht erfolgreichen Tests.
- Eine Analyse der aufgetretenen Fehler und Mängel.
- Eine Bewertung der Gesamttests und der erreichten Testziele.

Abbildungsverzeichnis

Abbildung 1: Testorganisation	4
Abbildung 2: Testablauf	5

Tabellenverzeichnis

Tabelle 1: Änderungsverzeichnis	1
Tabelle 2: Komponententest	5
Tabelle 3: Integrationstest	5
Tabelle 4: Systemtest	6
Tabelle 5: Abnahmetest	6
Tabelle 6: Fehlerklassifizierung	7
Tabelle 7: Testplan	10
Tabelle 8: ANF-Funktionalität der Sophos Firewall	11
Tabelle 9: ANF-Funktionalität der Netzwerk-Switches	12
Tabelle 10: ANF-XenServer Management 1	12
Tabelle 11: ANF-XenServer Management 2	13
Tabelle 12: ANF-XenServer VDI	13
Tabelle 13: ANF-Hauptspeicher Synology NAS	14
Tabelle 14: Backupspeicher Synology NAS	14
Tabelle 15: ANF-Netzwerk VLAN 210 NFS	15
Tabelle 16: ANF-Netzwerk VLAN 220 MGMT	15
Tabelle 17: ANF-Netzwerk VLAN 230 VDI	16
Tabelle 18: ANF-Erstellung der Domäne	16
Tabelle 19: ANF-Konfiguration DNS Server	17
Tabelle 20: ANF-Konfiguration DHCP Server	18
Tabelle 21: ANF-Replikation auf zweiten DC	19
Tabelle 22: ANF-Backup erfolgt automatisch täglich	20
Tabelle 23: ANF-Auf VDI läuft ein Antivirus	20
Tabelle 24: ANF-Anmeldung auf die isolierte Umgebung	21
Tabelle 25: ANF-Schutz gegen Geräteverlust oder Diebstahl	21
Tabelle 26: ANF-Durchführung von Benutzermutationen	22
Tabelle 27: ANF-Performance und Verfügbarkeit	23
Tabelle 28: ANF-Skalierung während dem laufenden Betrieb	24
Tabelle 29: ANF-Redundanz der Dienste	24
Tabelle 30: ANF-Benutzeranpassungen der VDI-Umgebung	25
Tabelle 31: ANF-Fernzugriff	25
Tabelle 32: ANF-Kollaboration mit Projektmitarbeitern	26
Tabelle 33: ANF-VDI hat kein Internetzugang	26
Tabelle 34: ANF-Vordefinierte Programme sind auf der VDI installiert	27
Tabelle 35: ANF-Sicherheitsfunktionen	27
Tabelle 36: TF-Funktionalität der Sophos Firewall	28
Tabelle 37: TF-Funktionalität der Netzwerk-Switches	29
Tabelle 38: TF-XenServer Management 1	29
Tabelle 39: XenServer Management 2	30
Tabelle 40: TF-XenServer VDI	30
Tabelle 41: TF-Hauptspeicher Synology NAS	31
Tabelle 42: TF-Backupspeicher Synology NAS	31
Tabelle 43: Netzwerk VLAN 210 NFS	32
Tabelle 44: TF-Netzwerk VLAN 220 MGMT	33

Tabelle 45: TF-Netzwerk VLAN 230 VDI.....	34
Tabelle 46: TF-Erstellung der Domäne	35
Tabelle 47: TF-Konfiguration DNS Server	36
Tabelle 48: TF-Konfiguration DHCP Server	37
Tabelle 49: TF-Replikation auf zweiten DC	38
Tabelle 50: TF-Backup erfolgt automatisch täglich.....	39
Tabelle 51: TF-Auf VDI läuft ein Antivirus	39
Tabelle 52: TF-Anmeldung auf die isolierte Umgebung.....	40
Tabelle 53: TF-Schutz gegen Geräteverlust oder Diebstahl	40
Tabelle 54: TF-Durchführung von Benutzermutationen	41
Tabelle 55: TF-Performance und Verfügbarkeit	41
Tabelle 56: TF-Skalierung während dem laufenden Betrieb.....	42
Tabelle 57: Redundanz der Dienste	42
Tabelle 58: TF-Benutzeranpassungen der VDI-Umgebung.....	43
Tabelle 59: TF-Fernzugriff.....	44
Tabelle 60: TF-Kollaboration mit Projektmitarbeitern.....	45
Tabelle 61: TF-VDI hat kein Internetzugang.....	45
Tabelle 62: TF-Vordefinierte Programme sind auf der VDI installiert.....	46
Tabelle 63: TF-Sicherheitsfunktionen.....	46

Anhang E3



Migrationskonzept

VDI as a Service

Auftraggeber Micha Bucher

Projektleiter Shipinyuan Su, Sirak Yosef

Autor Shipinyuan Su, Sirak Yosef

Klassifizierung Intern

Status Von AG abgesegnet

Änderungsverzeichnis

Datum	Version	Änderung	Autor
15.04.2024	0.1	Dokument erstellt, Einleitung, Ziele definiert, Migrationsobjekte	Shipinyuan Su, Sirak Yosef
16.04.2024	0.2	Migrationsverfahren	Shipinyuan Su, Sirak Yosef
17.04.2024	1.0	Risiken, Fertigstellung	Shipinyuan Su, Sirak Yosef

Tabelle 1: Änderungsverzeichnis

Inhaltsverzeichnis

1	Migrationskonzept.....	3
2	Ziele der Migration	3
3	Migrationsobjekte	3
4	Migrationsverfahren	4
4.1	Migrationsplan	5
5	Risiken	6
5.1	Machbarkeit.....	7

1 Migrationskonzept

Da es einige Komponenten gibt, die derzeit in Gebrauch sind, wie der VDI-Server, sowie Komponenten, die neu hinzukommen, wie der MGMT-Server, ist ein durchdachtes Migrationskonzept notwendig. Dieses Konzept stellt die Ziele der Migration, die betroffenen Objekte und das geplante Verfahren dar. Es beschreibt detailliert, wie die Migration durchgeführt werden soll. Zudem werden mögliche Risiken identifiziert und bewertet.

2 Ziele der Migration

Das Hauptziel ist eine reibungslose Migration während der Realisierung und dass alle Migrationsobjekte miteinander arbeiten ohne ungeplante Betriebsunterbrechungen zu gewährleisten. Dies umfasst mehrere spezifische Zielsetzungen:

- Identifizierung aller zu migrierende Elemente
- Ermitteln und Einschätzen von Risiken
- Entwicklung eines präzisen Migrationsverfahren
- Umsetzung gemäss dem vorbereiten Verfahren

3 Migrationsobjekte

Die folgende Auflistung präsentiert eine Übersicht der Migrationsobjekte und Ressourcen, die eine zentrale Rollen im Migrationsprozess spielen werden:

- VDI-Server: Ein bereits bestehender und bis voraussichtlich Ende April in der Produktivumgebung eingesetzter Server
- MGMT-Server: Dieser ist ein neuer Server, der von Grund aus zusammengebaut und eingerichtet wird
- Hauptspeicher: Ist vorhanden aber ist im Gegensatz zum VDI-Server nicht in der produktiven Umgebung im Einsatz
- Backup NAS: Das NAS ist aktuell nicht produktiv in Verwendung und enthält Daten, die Überprüft werden müssen
- Core-Switche: Es werden die beiden Core Switche von Finita AG gebraut die produktiv im Einsatz sind
- Firewall: Es wird der gleiche Firewall benutzt der produktiv auch gebraucht wird
- Router: Es wird der gleiche Router gebraucht der produktiv auch gebraucht wird
- VPN-Verbindung: Es wird die gleiche VPN-Verbindung gebraucht die produktiv auch gebraucht wird
- Domäne: Es wird eine komplett neue Domäne unabhängig von der produktiven erstellt und eingerichtet
- DCs: Es werden zwei neue DC mit den nötigen Diensten unabhängig von der produktiven erstellt
- Notebook: Es werden bestehende Notebook werden verwendet und unter anderem für die Einrichtung der VPN-Verbindung konfiguriert

4 Migrationsverfahren

Dieses Kapitel stellt die Migrationsobjekte dar und beschreibt deren Abhängigkeiten sowie die jeweiligen Migrationsverfahren. Es wird ausserdem das methodische Vorgehen für den gesamten Migrationsprozess aufgezeigt.

Migrationsobjekt	Anforderung	Abhängigkeit	Migrationsverfahren
VDI-Server	Minimale Downtime	Hauptspeicher, Netzwerkkonfiguration	Übernahme und neu Konfiguration
MGMT-Server	Konfiguration vor Produktivsetzung	Hauptspeicher, Netzwerkkonfiguration	Neuaufbau und Konfiguration
Hauptspeicher	Reibungslose Datenübertragung	VDI-Server, Backup NAS	Datenübertragung und -synchronisation
Backup NAS	Datensicherung	Hauptspeicher	Datenmigration und -bereinigung
Core-Switche	VLANs und Switch-Konfiguration	Firewall, Router	Einrichtung der VLANs auf den Switches vor der Serverkonfiguration
Firewall	Netzwerksicherheit und Richtlinien	Core-Switche, Router	Konfiguration der VLANs und Sicherheitsrichtlinien
Router	WAN-Konnektivität	WAN-Anschluss, Firewall, Core-Switche	Sicherstellung der reibungslosen WAN-Verbindung
VPN-Verbindung	Sichere Remote-Zugänge	Firewall, Router	Einrichtung des VPNs auf den lokalen Notebooks
Domäne	Unabhängige Betriebsumgebung	DCs	Einrichtung einer neuen unabhängigen Domäne
DCs	Verzeichnisdienste	MGMT-Server, Netzwerkinfrastruktur	Aufbau neuer DCs mit DNS und DHCP
Notebook / PC	Windows 10 Pro OS	Domäne, DCs, VPN-Verbindung	Einrichtung benötigter Software wie Citrix Workspace und VPN

Tabelle 2: Migrationsobjekte

4.1 Migrationsplan

Um die Migration erfolgreich durchzuführen, müssen die einzelnen Aufgaben in einer sinnvollen Reihenfolge abgewickelt werden. Die Realisierung Phase erstreckt sich von KW16 – KW21, wobei die letzte Woche für das Testen und Protokollieren reserviert ist. Während der vorangehenden Wochen wird die Lösung implementiert und dort findet die Migration der Objekte statt. Aus der folgenden Abbildung wird ersichtlich, in welcher Reihenfolge die einzelnen Aufgaben durchgeführt werden und die Abhängigkeit, wie dass zuerst das Netzwerk eingerichtet werden muss und dann die Server. Besonders hervorzuheben ist, dass die Konfiguration des VDI-Servers erst in KW19 startet, wenn dieser nicht mehr in der Produktivumgebung genutzt wird, um Betriebsunterbrechungen zu vermeiden.

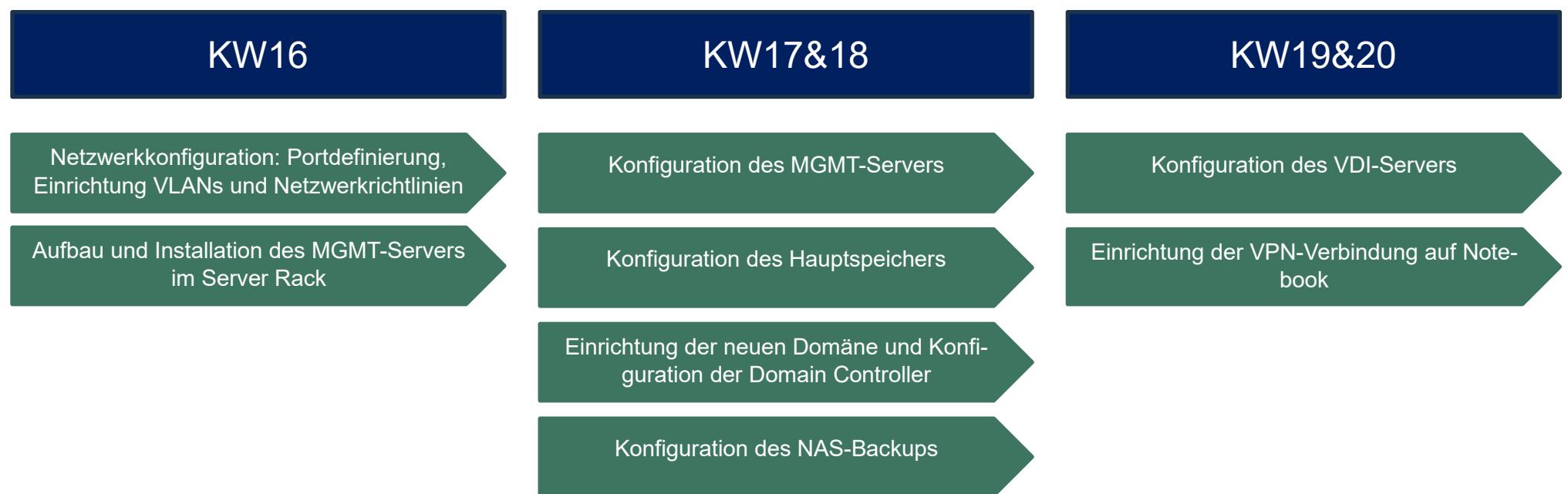


Abbildung 1: Migrationsplan

5 Risiken

Eine Risikoanalyse wurde durchgeführt, um potenzielle Risiken während der Migrationsphase zu identifizieren. Es wurden vier primäre Risiken, definiert als R1 bis R4 und innerhalb der folgenden Risikomatrix dargestellt. Diese Matrix ordnet die Risiken in drei Kategorien ein. Grün symbolisiert ein niedriges Risiko, Gelb ein mittleres Risiko und Rot ein hohes Risiko.

Die beiden grössten Risiken sind R1 und R4, mit Risikozahlen von 4 und 6. R1 betrifft den VDI-Server: Sollte dieser über Ende April hinaus immer noch in der Produktivumgebung benötigt werden, wäre eine Einrichtung des VDI-Services auf dem MGMT-Server erforderlich. Dies würde kein unlösbares Problem darstellen, jedoch zusätzliche Zeit beanspruchen. R4 adressiert den Zeitfaktor des umfangreichen Projekts und das Risiko, dass die zur Verfügung stehende Zeit möglicherweise nicht ausreicht, um alle Aufgaben zu erfüllen.

Nr.1	Risiko	Eintrittswahrscheinlichkeit	Auswirkungsgrad	Risikozahl
R1	VDI-Server wird über den ganzen Zeitraum produktiv gebraucht	2	2	4
R2	Defekte Komponente	1	3	3
R3	Personalausfall	2	1	2
R4	Zeitverlust	2	3	6

Tabelle 3: Risikobewertung Migration

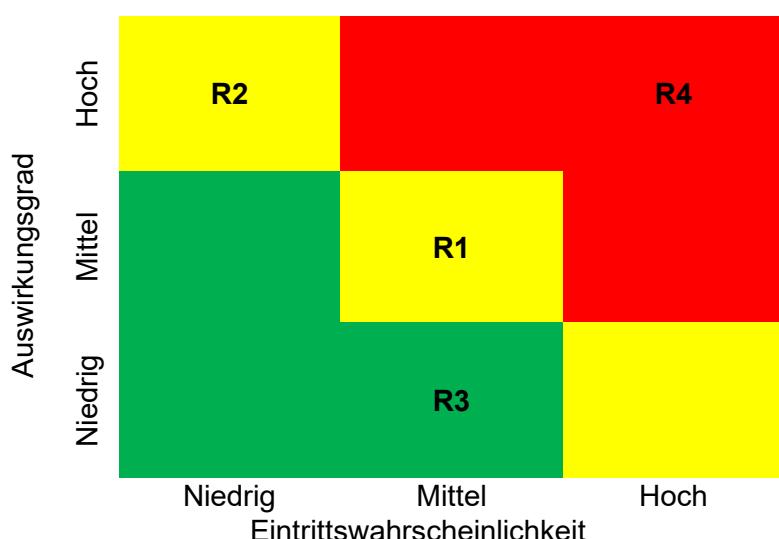


Tabelle 4: Risikomatrix Migration

5.1 Machbarkeit

Die Durchführung des Projekts wird für den Zeitraum von Kalenderwoche 16 bis 21 angesetzt und die benötigten Ressourcen sind vorhanden. Die Installation und Konfiguration neuer Systeme wie der MGMT-Server und die Domäne, die Integration bestehender Ressourcen wie VDI- und Backup-Server sowie die Anpassung der Netzwerkinfrastruktur sind machbar und im vorgegebenen Zeitrahmen umsetzbar.

Abbildungsverzeichnis

Abbildung 1: Migrationsplan	5
-----------------------------------	---

Tabellenverzeichnis

Tabelle 1: Änderungsverzeichnis	1
Tabelle 2: Migrationsobjekte	4
Tabelle 3: Risikobewertung Migration	6
Tabelle 4: Risikomatrix Migration	6

Anhang E4



Betriebskonzept

VDI as a Service

Auftraggeber Micha Bucher

Projektleiter Shipinyuan Su, Sirak Yosef

Autor Shipinyuan Su, Sirak Yosef

Klassifizierung Intern

Status Von AG abgesegnet

Änderungsverzeichnis

Datum	Version	Änderung	Autor
15.04.2024	0.1	Dokument erstellt	Shipinyuan Su, Sirak Yosef
21.04.2024	1.0	Dokument fertiggestellt	Shipinyuan Su, Sirak Yosef

Tabelle 1: Änderungsverzeichnis

Inhaltsverzeichnis

1	Betriebskonzept	4
2	Organisationsstruktur	4
2.1	Rollen und Verantwortlichkeiten	5
2.2	Kommunikation.....	5
2.3	Systemberechtigung.....	5
3	Betriebsprozesse	6
3.1	Management Golden Images	6
3.2	Benutzerverwaltung.....	7
3.3	Sicherheit	8
3.4	Support.....	9
3.5	Projektnotebook	10
3.6	Wartung.....	12
3.7	Backup	13
3.8	Monitoring	14
4	Wirtschaftlichkeit	16
4.1	Projektkosten.....	16
4.2	Kundenschätzung.....	17
4.3	Materialkosten	18
4.4	Betriebskosten.....	20
4.5	Erlös	21
4.6	Break-Even	22
4.6.1	Break-Even (Jahre)	23
5	SLA.....	28
5.1	Generelle Vereinbarung	28
5.1.1	Vertragsparteien.....	28
5.1.2	Ansprechpartner.....	28
5.1.3	Beginn SLA	28
5.1.4	Laufzeit SLA.....	28
5.1.5	Kündigungsfrist.....	28
5.1.6	Vertragsrücktritt bei Nichterfüllung.....	28
5.2	Allgemeiner IT-Support.....	29
5.2.1	Zeiten Servicebereitschaft	29
5.2.2	Kontakt bei Service-Bedarf	29
5.2.3	Servicelevel und Reaktionszeiten	29
5.3	Dienstleistungen: Abonnementen	30
5.3.1	Abonnement Basic	30
5.3.2	Abonnement Premium.....	30
5.4	Detaillierte Leistungsbeschreibung	31
5.4.1	Support Projektnotebooks	31
5.4.2	Support VDI.....	31
5.5	Bestellung / Modifikation / Laufzeit	32
5.6	Leistungsvergütung	32
5.6.1	Abonnement Basic	32
5.6.2	Abonnement Premium.....	32
5.6.3	Supportleistungen	32

5.7	Ergänzende Anmerkungen.....	33
5.7.1	Endgeräte.....	33
5.7.2	Abrechnungsformalitäten.....	33
5.7.3	Vertraulichkeit.....	33
5.7.4	Haftung.....	33
5.7.5	Mitwirkung Auftraggeber.....	34
5.7.6	Verschiedenes.....	34

1 Betriebskonzept

Dieses Dokument dient als Leitfaden für die Struktur, Prozesse und Richtlinien, die den täglichen Betrieb steuern. Das Dokument sollte dabei helfen eine konsistente Ausführung der Geschäftsstrategie zu gewährleisten und stellt sicher, dass alle Beteiligten denselben Kenntnisstand haben.

Neben den Beschreibungen der Prozesse und organisatorischen Strukturen werden auch wirtschaftliche Aspekte hervorgehoben. Behandelt werden Themen wie die Darstellung und Berechnung des Break-Even, die Definierung des Service Level Agreements (SLA) und die Präsentation eines Factsheets. Dies spiegelt die Leistungsfähigkeit des Services wider und sind entscheidend für das Verständnis der finanziellen und betrieblichen Leistungsfähigkeit des Services.

2 Organisationsstruktur

Die Finitia AG verfügt über mehrere Abteilungen, wobei in diesem Dokument der Fokus ausschliesslich auf die IT-Abteilung gelegt wird. Diese besteht aus einem kleinen Team von weniger als zehn Personen und zeichnet sich durch eine flache Hierarchiestruktur aus.

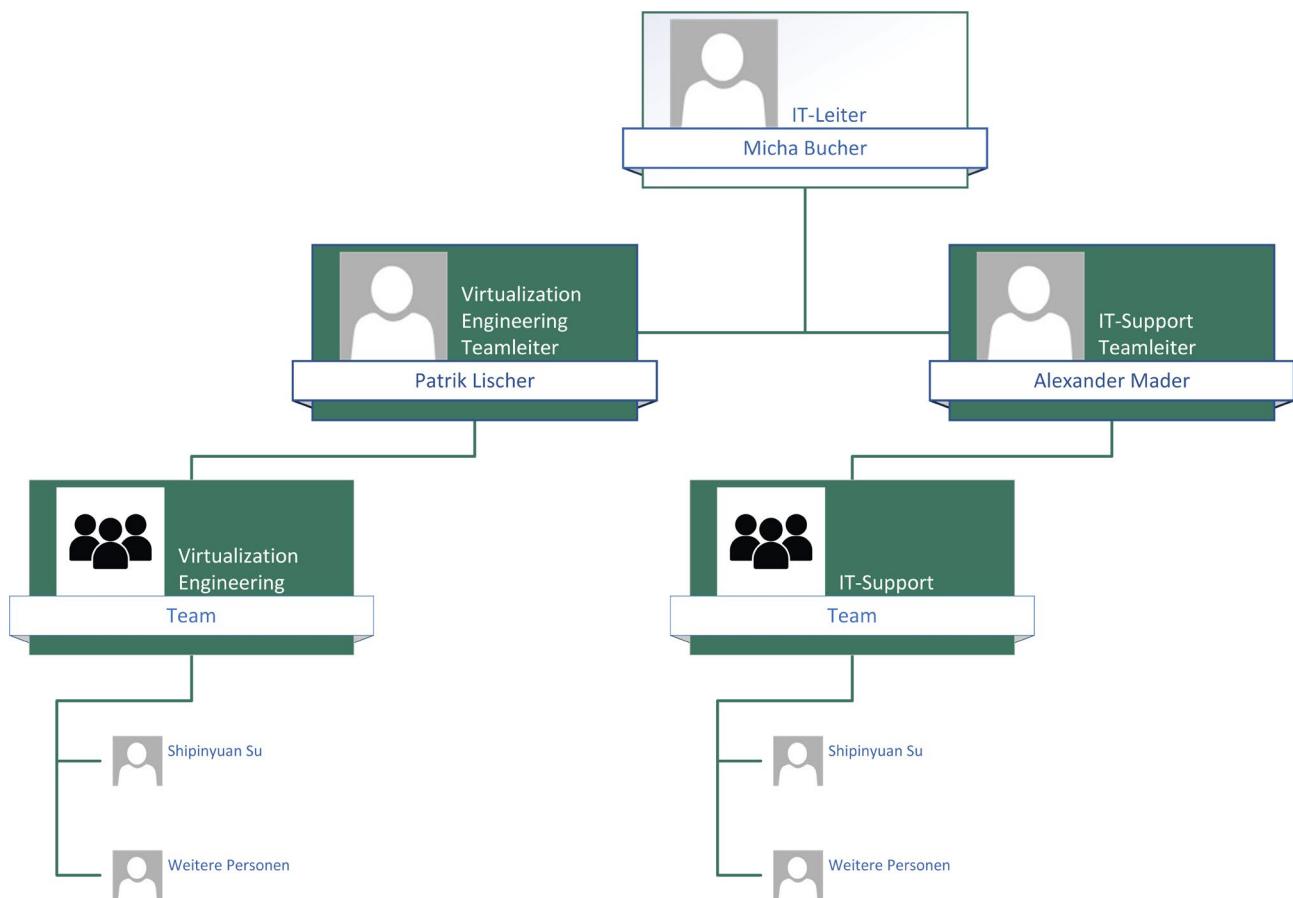


Abbildung 1: Organigramm

2.1 Rollen und Verantwortlichkeiten

In dem kleinen Team werden keine festen Rollen zugewiesen. Jede Person übernimmt Verantwortung in verschiedenen Fachgebieten, wie Drucker, Netzwerk, Virtualisierung und Programmierung. Das Ziel ist es, dass sich jede Person mit jedem Fachgebiet vertraut macht und entsprechend Auskunft geben kann. In jedem Bereich gibt es mehrere Zuständige oder Stellvertreter. Die Verantwortlichkeiten werden nach Fähigkeiten und Interessen vergeben. Neues Wissen oder Änderungen werden bei Bedarf wöchentlich in Teammeetings vermittelt.

2.2 Kommunikation

Durch die flache Hierarchie sind sowohl die vertikalen als auch die horizontalen Kommunikationswege sehr kurz und effizient. Teammitglieder jeder Stufe verfügen über eine eigenständige Entscheidungsbefugnis und können Bestellungen über kleinere Beträge eigenmächtig tätigen. Bei grösseren Beträgen ist jedoch die Zustimmung eines Vorgesetzten erforderlich, wobei eine mündliche Genehmigung meist ausreichend ist. Für betriebsrelevante Änderungen oder grössere Anschaffungen muss ein Antrag an die Geschäftsleitung gestellt werden, in solchen Fällen fungiert der IT-Leiter oder ein Teamleiter üblicherweise als Schnittstelle. Die Kommunikation mit externen Schnittstellen wie anderen Abteilungen oder externen Partnern kann von jeder Person initiiert werden, wobei die Verantwortung für den Aufbau und die Pflege von Beziehungen meist bei den zuständigen Personen des Fachgebietes liegt.

2.3 Systemberechtigung

Als vollwertiges Mitglied des IT-Teams hat man grundsätzlich Zugriffsberechtigung auf alle Systeme, sofern die Probezeit erfolgreich abgeschlossen wurde. Aufgrund der flachen Hierarchie und der geringen Teamgrösse ist eine Unterteilung der Abteilung in einzelne Teams nicht möglich, da sonst ein Mangel an Personalressourcen entstehen würde. Daher wurde kein Role-Based Access Control (RBAC) implementiert. Es gibt jedoch Systeme, auf die nur Personen Zugriff haben, die explizit dafür verantwortlich sind, wie beispielsweise auf den Speicher der produktiven VDI-Umgebung. Falls Zugriff durch nicht zuständige Personen benötigt wird, kann dieser entsprechend eingerichtet werden.

Dies gilt ebenfalls für diese Umgebung. Für den Support der Umgebung ist es erforderlich, dass alle Supportmitarbeiter Zugriff auf die notwendigen Systeme haben. Aufgrund des Umgangs mit sensiblen Daten kann es notwendig sein, dass das Support-Team eine Geheimhaltungsvereinbarung unterschreiben muss.

3 Betriebsprozesse

Klar definierte Betriebsprozesse sind von zentraler Bedeutung für den reibungslosen Ablauf des Services. In diesem Abschnitt werden Schlüsselprozesse dargelegt, um eine kontinuierliche, sichere und effiziente Operation des Services gewährleisten zu können.

3.1 Management Golden Images

Die Golden Images spielen eine zentrale Rolle für diesen Service. Sie bilden die Grundlage für alle bereitgestellten Desktops. Diese Images werden als normale VMs erstellt und gemäss den spezifischen Anforderungen konfiguriert. Mit der Snapshot-Technologie können mehrere Versionen eines Images erstellt werden. Dies ermöglicht es, bei Problemen auf einen früheren Snapshot zurückzugreifen. Als zentrale Komponente müssen diese Golden Images regelmässig gesichert werden.

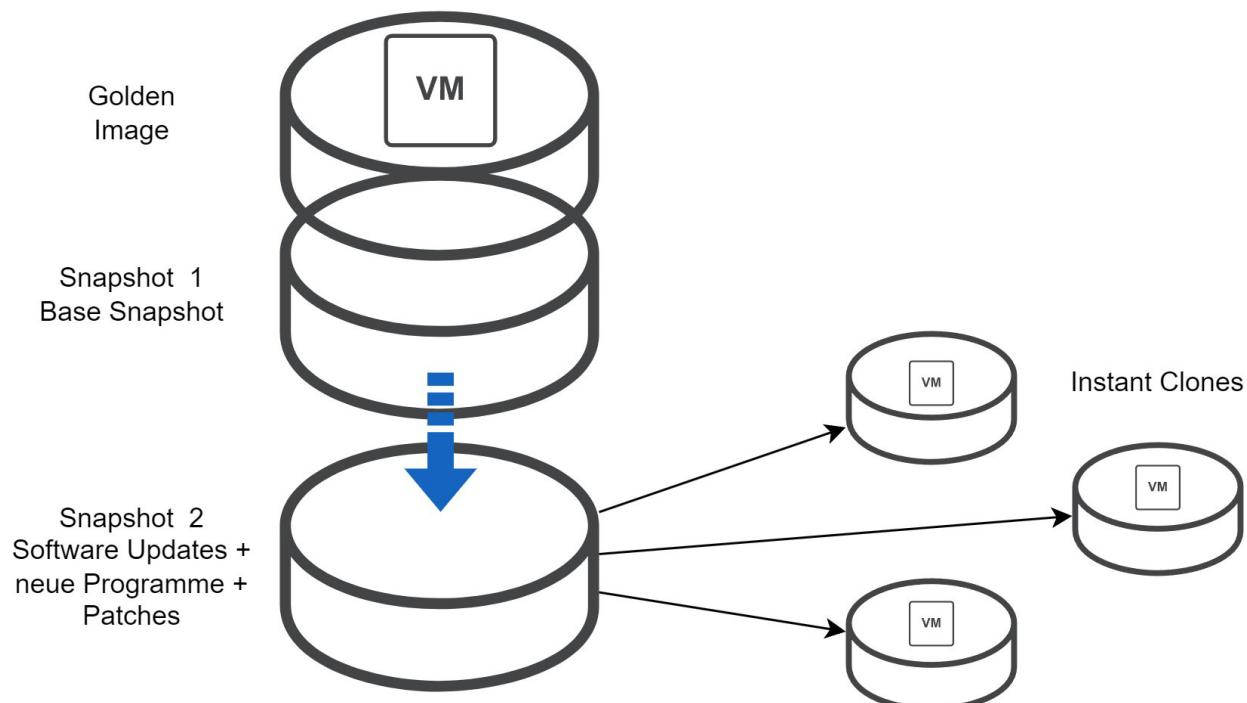


Abbildung 2: Golden Image

Ein neues Golden Image kann je nach Bedarf und speziellen Anforderungen erstellt werden. Es ist wichtig, dass jede neue Version des Images zunächst von Pilotnutzern getestet wird. Erst nach einer positiven Rückmeldung kann die Version für die breite Nutzung freigegeben werden. Ein Golden Image kann für mehrere Projekte verwendet werden. Sobald jedoch grössere Unterschiede zwischen den Anforderungen der Projekte bestehen, müssen separate Images erstellt werden.

Durch den Einsatz von FSLogix und Dynamic Environment Manager (DEM) können benutzerspezifische Anpassungen vorgenommen werden und müssen somit nicht manuell in den Golden Images implementiert werden. Neu erstellte Snapshots müssen detailliert dokumentiert werden, um die vorgenommenen Änderungen klar festzuhalten. Dies ist entscheidend, um bei auftretenden Problemen nachvollziehen zu können, wo mögliche Fehlerquellen liegen.

3.2 Benutzerverwaltung

Dieser Service kann zusätzlich zur produktiven VDI-Umgebung angeboten werden. Die Abrechnung dieses Dienstes erfolgt separat und kann je nach Situation entweder direkt den Projektkosten zugeordnet oder der Firma in Rechnung gestellt werden. Dank der unabhängigen Infrastruktur können beide Systeme parallel existieren, ohne sich gegenseitig zu beeinträchtigen, beispielsweise durch das Überschreiben von Benutzerprofilen.

Nachdem der Einführungsprozess für einen neuen Mitarbeiter in das geheime Projekt abgeschlossen ist und alle erforderlichen Geheimhaltungsvereinbarungen unterzeichnet wurden, kann eine autorisierte Person z.B. die Vorgesetzte (Projektleitung oder eine höherrangige Instanz) eine VDI für den Neuzugang bestellen. Der Neuzugang wird im System mit allen erforderlichen Berechtigungen erfasst. Jegliche Mutationen an Benutzerkonten, wie die Erstellung, Löschung oder Anpassung, werden über das Ticketing-Tool abgewickelt. Dabei liegt die Verantwortung für die Bearbeitung der Anfragen bei der zuständigen Person im Ticketing, unabhängig davon, ob die Anfrage selbst bearbeitet oder an einen Engineer eskaliert wird. Die Übergabe der VDI zusammen mit dem vorbereiteten Projektnotebook muss von einem IT-Mitarbeiter begleitet werden. Diese Unterstützung kann sowohl vor Ort als auch remote erfolgen und wird durch detaillierte Anleitungen ergänzt. Es ist wichtig, dass der Prozess nicht nur die technische Einrichtung umfasst, sondern auch eine umfassende Einführung in die Nutzung der VDI-Umgebung bietet. Hierbei sollten folgende Punkte berücksichtigt werden:

- **Ersteinrichtung:** Sicherstellen, dass alle relevanten Anwendungen und Tools auf dem Notebook vorinstalliert und funktionsfähig sind.
- **Verwendung:** Durchführung einer kurzen Schulungssession, um die Prozesse zu erklären, wie man sich mit der VDI verbindet und worauf man für eine erfolgreiche Authentifizierung achten muss. Bei Bedarf auch Vermittlung der Grundlagen der VDI-Benutzung.
- **Richtlinien:** Vermittlung der angewandten Richtlinien und Erläuterung der unterschriebenen Geheimhaltungsvereinbarungen.
- **Support und Dokumentation:** Information über den Kontakt zum IT-Support und den Prozess für die Meldung von technischen Problemen. Bereitstellung von schriftlichen Anleitungen.

Alle Berechtigungen für das VDI-System müssen in Active Directory über Gruppen geregelt werden. Zusätzlich ist es wichtig, dass regelmässige Überprüfungen und Aktualisierungen der Berechtigungen stattfinden, um die Sicherheit und Effizienz des Systems zu gewährleisten.

3.3 Sicherheit

Durch eine separate Authentifizierungsstelle nur für diese Umgebung, kann die Authentifizierung mit höheren Sicherheitsmaßnahmen ausgestattet und überwacht werden. Durch kleinere Benutzeranzahl besteht ein besserer Überblick über die Zugriffskontrolle. Mit Implementierung von Mehrfaktor-Authentifizierung über mehrere Anmeldung Instanzen, ist die Authentifikation auf ein hohes Mass gesichert. Durch die Verwendung von Benutzergruppen können Zugriffrechte einfach und übersichtlich verwaltet werden.

Für optimale Sicherheit sind spezifische Prozesse und Verhaltensregeln für die Nutzung dieser Umgebung definiert. Diese Prozesse können je nach Projektanforderungen variieren, doch einige grundlegende Regeln gelten stets:

- Die Nutzung dieses Service ist ausschliesslich mit Projektnotebooks gestattet
- Jegliche Aufnahmen der VDI-Sitzung sind strikt untersagt
- Das Arbeiten in öffentlichen Räumen wie Kaffees, Bibliotheken oder Parks ist verboten
- Das Kopieren von Projektdaten auf externe Medien ist in jeglicher Form untersagt
- Eine private Nutzung der Projektnotebooks ist nicht gestattet

Diese Regeln müssen von allen Nutzern eingehalten werden, um die Sicherheit der Daten und Systeme zu gewährleisten. Neben diesen Verhaltensregeln wird die Sicherheit durch mehrere technischen Maßnahmen verstärkt:

- Die Verwendung einer VPN-Verbindung ist erforderlich, da die VDI-Umgebung nur über das interne Netzwerk zugänglich ist. Nutzer müssen sich daher über einen sicheren Tunnel verbinden
- Alle Projektnotebooks werden mit einem Sicherheitszertifikat ausgestattet. Dies stellt sicher, dass nur zertifizierte Geräte eine Verbindung zur VDI-Umgebung herstellen können
- Bei Bedarf können zusätzliche Sicherheitsmaßnahmen implementiert werden, wie zum Beispiel USB-Authentifizierungsschlüssel, die eine weitere Ebene der Identitätsprüfung bieten

Diese umfassenden Sicherheitsmaßnahmen sind entscheidend, um die Integrität und Vertraulichkeit der in der VDI-Umgebung verarbeiteten Informationen zu schützen und Risiken wie Datenlecks oder unautorisierte Zugriffe effektiv zu minimieren.

3.4 Support

Der Support gliedert sich in drei Stufen: 1st Level, 2nd Level und 3rd Level Support. Diese Kategorisierung basiert auf den jeweiligen Aufgabenbereichen. Anfragen im Bereich des 1st Level Supports werden von den dafür von der Standortleitung bestimmten Mitarbeitenden am Standort direkt bearbeitet oder nach Absprache an den 2nd Level Support weitergeleitet. Anfragen, die den 2nd Level Support betreffen, können ebenfalls direkt dorthin gerichtet werden. Der 2nd Level Support kümmert sich um die Bearbeitung dieser Anfragen und zieht bei komplexeren Problemen den 3rd Level Support, bestehend aus Fachexperten und Herstellern, hinzu.

Die nachfolgende Tabelle zeigt Beispiele von 1st Level und 2nd Level Support Anfragen.

1st Level Support	2nd Level Support
<ul style="list-style-type: none"> - Kein Bild auf Bildschirm - Keine Netzwerkverbindung - Notebook startet nicht - Umzug des Arbeitsplatzes 	<ul style="list-style-type: none"> - Datenwiederherstellung - Anpassung der Berechtigung - Anfrage von Programmen oder Updates - Lizenzierungen - Probleme mit der VDI - Hardwaredefekt - Probleme Zugriff VPN - Probleme des Netzwerkes

Tabelle 2: Beispiele 1st- und 2nd Level Support

Die Kontaktaufnahme mit dem 2nd Level Support ist auf zwei Wegen möglich:

- Per E-Mail an helpdesk@finitia.net
- Telefonisch über die Hotline-Nummer +41 31 340 83 00

Bei einer Supportanfrage per E-Mail wird automatisch ein Ticket erstellt. Wird die Anfrage telefonisch gestellt, hängt die Eröffnung eines Support-Tickets von der Komplexität der Anfrage ab.

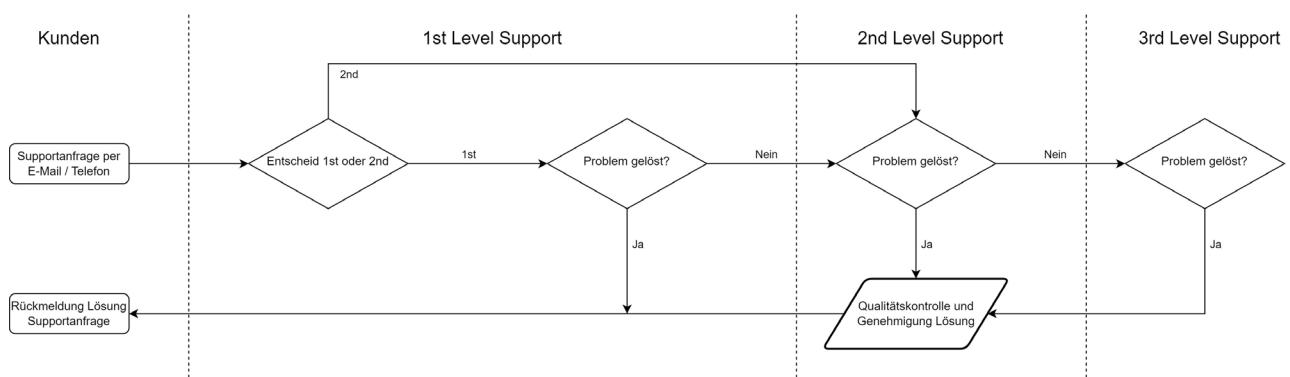


Abbildung 3: Support Ablaufdiagramm

3.5 Projektnotebook

Obwohl das Einrichten der Notebooks mit Sicherheitsfunktionen in der Realisierung nicht thematisiert wird, wurde hier dennoch ein möglicher Ablauf für die Notebook Einrichtung definiert. Es wird der Standardprozess für die Einrichtung von Notebooks beschrieben, die speziell für diese VDI-Lösung vorgesehen sind. Diese Notebooks sind für interne Mitarbeiter gedacht, die an den geheimen Projekten arbeiten. Sie sollten gemäss spezifischer Sicherheits- und Funktionalitätsanforderungen konfiguriert werden, um eine optimale und sichere Nutzung zu gewährleisten. Der Fokus liegt darauf, sicherzustellen, dass die Benutzer über Citrix arbeiten und keine Daten auf den lokalen Notebooks gespeichert werden. Nachfolgend wird der Einrichtungsablauf detailliert dargestellt:

1. Installation von Windows 10 Pro:

Als Erstes wird auf jedem Notebook das Betriebssystem Windows 10 Pro installiert. Diese Version bietet erweiterte Management- und Sicherheitsfunktionen, die entscheidend sind, um alle Anforderungen abzudecken.

2. BIOS-Verschlüsselung & Aktivierung von TPM:

Nach der Installation des Betriebssystems wird das BIOS verschlüsselt. Dies stellt eine zusätzliche Sicherheitsebene dar, um den physischen Zugriff auf das Notebook zu sichern und den Schutz zu erhöhen. TPM muss ebenfalls im BIOS aktiviert werden, um die Verwendung von BitLocker zu ermöglichen.

3. Aktivierung von BitLocker:

BitLocker wird anschliessend aktiviert, um die Daten auf der Festplatte zu schützen. Diese Funktion verschlüsselt die Festplatte und schützt sie vor unbefugtem Zugriff, auch wenn das Notebook gestohlen werden sollte.

4. Installation eines Endpoint Detection and Response (EDR) Programm:

Ein EDR-Programm wird lokal installiert, um das Notebook vor Malware zu schützen. Dies ist wichtig, da das Notebook Internetzugriff hat und potenziell durch heruntergeladene Dateien ein Virus mit holen könnte.

5. Installation von Citrix Workspace:

Citrix Workspace wird installiert, damit die Benutzer auf ihren VDI-Desktop zugreifen können. Diese Software fungiert wie ein Treiber; ohne sie kann der VDI-Desktop nicht dargestellt werden.

6. VPN-Einrichtung:

Ein VPN wird eingerichtet, um eine sichere Verbindung zum Firmennetzwerk herzustellen. Dies ist entscheidend für den sicheren Datenaustausch zwischen den Endpunkten und ist essenziell für die Verbindung auf die VDI-Infrastruktur.

7. Zertifikat:

Alle Projektnotebooks werden mit einem Zertifikat ausgestattet, welcher für die Verbindung zur VDI-Infrastruktur notwendig ist.

8. USB-Authentifizierungsschlüssel (Optional):

Optional kann ein USB-Authentifizierungsschlüssel für mehreren Authentifizierungsinstanzen eingerichtet werden.

9. Einrichtung von Deep Freeze:

Abschliessend wird Deep Freeze eingerichtet. Diese Software stellt sicher, dass keine lokalen Benutzerdaten auf dem Notebook gespeichert werden, da das lokale Konto bei jedem Neustart auf die vordefinierte Konfiguration zurückgesetzt wird. Dies erhöht die Sicherheit erheblich, sollte das Notebook auch in diesem Fall gestohlen werden.

3.6 Wartung

Für die Aufrechterhaltung der Betriebssicherheit, Leistung und Verfügbarkeit ist es entscheidend, regelmässig Wartungen durchzuführen. Diese umfassen nicht nur softwareseitige Updates und Sicherheitspatches, sondern auch Netzwerkanpassungen und möglicherweise notwendige physische Änderungen an der Hardware. Durch proaktive Wartungsmassnahmen können die Systemstabilität gesichert und potenzielle Risiken frühzeitig identifiziert werden.

Wartungsziele

Was durch regelmässige Wartungstätigkeiten erreicht werden sollte:

- Systemverfügbarkeit: Minimierung der Ausfallzeiten durch proaktive Wartungen
- Performance-Optimierung: Optimierung durch regelmässige Updates und Hardwareerweiterungen
- Sicherheit: Implementierung der neusten stabilen Sicherheitsupdate und Patches

Ein Wartungsfenster ermöglicht es grössere Änderungen am laufenden System vorzunehmen, ohne die Downtime zu beeinträchtigen.

Wartungsplan

Aufgrund der speziellen Anforderungen der Umgebung, die eine sichere und isolierte Umgebung darstellt, sind weniger häufig kleine Anpassungen notwendig, die Umgebung bleibt daher eher statisch. Es wurden zwei grosse Wartungsfenster pro Jahr für umfangreichere Wartungsarbeiten eingeplant. An diesen nehmen das gesamte Engineering-Team sowie externe Dienstleister teil, falls erforderlich. Der Arbeitsaufwand wird auf mindestens zwei volle Tage pro Jahr geschätzt.

Monatlich wird überprüft, ob neue kritische Updates vorliegen. Sollten solche vorhanden sein, wird geprüft, ob sie über Nacht eingespielt werden können oder ob ein Wartungsfenster erforderlich ist. Falls ein Wartungsfenster notwendig wird, sammelt das Team Anpassungen und Updates, die bei den nächsten Wartungsarbeiten umgesetzt werden sollen. Kunden werden einen Monat im Voraus über geplante Wartungsarbeiten informiert. Änderungen an systemkritischen Komponenten müssen in irgendeiner Form für die Notfallwiederherstellung gesichert sein.

Das Engineering-Team ist verantwortlich für den gesamten Zyklus der Wartungsarbeiten und wird vom Supportteam unterstützt.

Wartungsverfahren

Alle geplanten Anpassungen werden dokumentiert und während des Wartungstermins als Checkliste abgearbeitet. Automatische Prozesse werden zu Beginn der Wartungsarbeiten gestartet. Die Dokumentation dient als Grundlage, um Änderungen am System festzuhalten, damit das Supportteam einschätzen kann, was geändert wurde und bei Supportanfragen Probleme auf die Wartung zurückführen kann. Nach der Wartung wird das gesamte System überwacht und es wird ein Bericht über den Status der Wartungsarbeiten erstellt.

3.7 Backup

Das Ziel dieses Kapitels ist die Definition der Backupprozesse, die im operativen Betrieb Anwendung finden. Es dient als fundamentale Grundlage und Richtlinie für den Umgang mit Backups innerhalb der VDI-Umgebung. Das Konzept legt fest, wie Backups verwaltet und überprüft werden sollen, um die Betriebskontinuität zu gewährleisten und Risiken zu minimieren. Es umfasst klare Anweisungen und Best Practices, die sicherstellen, dass alle Mitarbeiter, die mit der Durchführung und Überwachung von Backups betraut sind, ein einheitliches Verständnis der Prozesse haben und wissen, welche Aspekte zu beachten sind.

Zugang

Ähnlich wie in den anderen Bereichen hat das komplette IT-Team Zugriff auf das System, solange keine Geheimhaltung verlangt wird, sonst wird das System nur für betroffene freigegeben. Das System wird mit einem zentralen Administratorkonto verwaltet. Bei Bedarf kann man auf Benutzerbezogene Accounts umsteigen.

Überprüfung

Es ist zwingend täglich das Backupverfahren zu kontrollieren, um sicherzustellen, dass die Backups wie geplant durchgeführt werden. Neben der Kontrolle der Durchführung sollten auch Aspekte wie die Einhaltung der Sicherheitsstandards und die Angemessenheit der Speicherorte überprüft werden. Die Überprüfung sollte auch eine Bewertung der Effektivität der Backup-Strategie beinhalten, um sicherzustellen, dass sie weiterhin alle Anforderungen erfüllt. Um die Integrität zu überprüfen, müssen die Backups regelmässig getestet werden, einschliesslich der Wiederherstellungsprozesse.

Tests

Ausgeführte Backups heisst lange noch nicht, dass sie auch funktionieren. Somit müssen Backups regelmässig getestet werden. Diese Tests sollten die Wiederherstellung von Daten aus Backups unter verschiedenen Szenarien umfassen, um die tatsächliche Wiederherstellungszeit und die Integrität der Daten zu validieren. Diese Tests müssen mindestes zweimal im Jahr durchgeführt werden. Dafür können produktive oder auch Testdaten oder VMs verwendet werden.

Verantwortlichkeiten

Die Hauptverantwortlichkeit der Arbeit- und Verantwortungsverteilung liegt beim Teamleiter oder beim IT-Leiter. Nach direkter Verteilung hat jede Person seine eigene Verantwortung im Bereich seiner Aufgaben. Schlussendlich sind der Teamleiter und IT-Leiter zuständig für die Kontrolle der Erledigung.

3.8 Monitoring

Die Überwachung des Systems ist ein entscheidendes Element für den Betrieb der IT-Infrastruktur. Sie bestimmt, ob die Stabilität, Sicherheit und Leistungsfähigkeit des Services gewährleistet sind.

Ziele

Mit einem zentralen Monitoring-Tool können zahlreiche Metriken erfasst und weiterverarbeitet werden. Diese Metriken zeigen an, ob gesetzte Ziele erreicht werden oder ob Verbesserungen erforderlich sind. In dieser Umgebung ist es wichtig, folgende Werte zu überwachen: die Verfügbarkeit von Systemen, die Sicherheitsüberwachung verdächtiger Aktivitäten sowie das Kapazitätsmanagement von Ressourcen wie CPU, Speicher und Netzwerk. Durch die Analyse dieser Daten können Probleme frühzeitig erkannt und proaktiv behoben werden. Zudem ermöglichen die erfassten Metriken die Erstellung detaillierter Berichte für Kunden, die als Nachweis der erbrachten Leistungen dienen.

Überwachung

Mit dem schon intern verwendeten Tool PRTG können an viel Zahl von Sensoren verwendet werden, um verschiedene Komponente auf Werte zu überwachen. Optimal ist eine komplette Überwachung über alle Server und deren Werten, sowie die Überwachung der Funktionalität von wichtigen Services. Für die Effektivität der Sensoren und die frühzeitige Alarmierung sollen die Sensoren eine Intervallzeiten von ein paar Sekunden haben.

Alarmierung und Benachrichtigungen

PRTG ermöglicht die Definition von Schwellenwerten, deren Überschreitung eine automatische Benachrichtigung auslöst. Dies ist ein wesentlicher Bestandteil des proaktiven Managements einer IT-Umgebung, da es den Administratoren erlaubt, potenzielle Probleme frühzeitig zu erkennen und zu adressieren, bevor diese schwerwiegenderen Auswirkungen haben können. Darüber hinaus bietet PRTG eine visuelle Darstellung der überwachten Daten durch umfassende Dashboards. Diese Dashboards ermöglichen eine intuitive Analyse und erleichtern das schnelle Erkennen von Trends oder Anomalien.

Bei einer Alarmierung oder der Erkennung von Problemen ist das Engineering-Team gefordert, schnell und effizient zu reagieren. PRTG unterstützt dabei nicht nur mit Echtzeitdaten, sondern auch durch die Integration mit anderen Systemen, wie Ticketing- oder E-Mail-Systemen, um sicherzustellen, dass alle relevanten Stakeholder sofort informiert werden. Zusätzlich lassen sich die Benachrichtigungen nach Priorität, Art des Problems oder betroffenem System anpassen, um eine zielgerichtete Kommunikation zu gewährleisten.

Berichte und Analyse

Mit PRTG ist es möglich, die gesammelten Daten ausführlich auszuwerten, um detaillierte Analysen zur Performance verschiedener Services zu erstellen. Diese Analysen sind für alle Stakeholder interessant, da sie tiefgreifende Einblicke in die Effizienz und Zuverlässigkeit der IT-Infrastruktur bieten. PRTG ermöglicht die direkte Erstellung von detaillierten Berichten, die speziell auf die Bedürfnisse der Nutzer zugeschnitten sind. Diese Berichte können automatisch generiert und an vordefinierte Empfängergruppen gesendet werden, was die Kommunikation und Entscheidungsfindung innerhalb des Unternehmens verbessert.

Verantwortlichkeiten

Die Überwachung der IT-Systeme ist eine Aufgabe, die auf mehrere Instanzen innerhalb der Organisation verteilt ist, um eine kontinuierliche und effektive Überwachung sicherzustellen. Eine der zentralen Rollen in diesem Prozess spielt der Tagessupport. Dieses Team ist verantwortlich für die regelmässige Überprüfung des Dashboards, welches alle kritischen Systemdaten und Performance-Indikatoren in Echtzeit anzeigt. Bei der Identifizierung von Unregelmässigkeiten oder potenziellen Problemen ist der Tagessupport dafür zuständig, entsprechende Eskalationsprozesse einzuleiten, um schnell und effektiv auf mögliche Störungen zu reagieren.

Darüber hinaus wird das gesamte Engineering-Team durch automatisierte Benachrichtigungssysteme informiert. Im Falle von Alarmierungen, die kritische Schwellenwerte überschreiten, erhalten die Teammitglieder sowohl E-Mail-Benachrichtigungen als auch Desktop-Popups. Diese Massnahmen stellen sicher, dass alle relevanten Personen sofort informiert werden und schnell reagieren können, unabhängig davon, ob sie gerade aktiv das Dashboard überwachen oder nicht.

Die Einrichtung von Multi-Channel-Benachrichtigungen und die Verteilung der Überwachungsaufgaben auf verschiedene Teams tragen dazu bei, dass die IT-Infrastruktur jederzeit optimal funktioniert und mögliche Probleme minimiert werden.

4 Wirtschaftlichkeit

Nach der Analyse der Wirtschaftlichkeit und der Total Cost of Ownership verschiedener Varianten in der Studie, fokussiert dieses Kapitel auf die detaillierte Untersuchung der ausgewählten Lösung. Es werden zentrale ökonomische Faktoren beleuchtet, wie Projektkosten, Materialkosten, Kundenschätzungen, Erlöse und Betriebskosten. Zudem wird der Break-Even-Punkt berechnet, um die finanzielle Machbarkeit zu verdeutlichen. Abschliessend werden ein SLA und ein Factsheet erstellt, die als Grundlage für die weiterführende Implementierung und das Management der Lösung dienen.

4.1 Projektkosten

Das Projekt umfasst einen Gesamtaufwand von etwa 500 Stunden, der von zwei Projektmitarbeitern bewältigt wird. Der Aufwand wird zu einem internen Stundensatz von 55 CHF berechnet. Alle Materialkosten, die nicht bereits durch die bestehende Infrastruktur abgedeckt sind, wie Firewall und Switches, wurden berücksichtigt. Während des Projekts wurden verschiedene Dienstleistungen von Drittanbietern in Anspruch genommen. Diese Dienste wurden auf 10 Stunden zu einem Stundensatz von 150 CHF geschätzt.

Tätigkeiten Projekt	Stunden [h]	Ansatz [CHF]	Kostenprojekt
Initialisierung	103	55	5665
Konzept	88	55	4840
Realisierung	168	55	9240
Einführung	16	55	880
Abschluss	124	55	6820
Totalle Stunden	499	Total Aufwand	27445
Material HW/SW etc.			61000
Externe Dienstleistungen	10	150	1500
		Total Projektkosten	89945

Tabelle 3: Projektkosten

4.2 Kundenschätzung

Die Kundenakquise könnte aufgrund der speziellen Anforderungen dieser Lösung eine bedeutende Herausforderung darstellen, da die Bedürfnisse stark von den jeweiligen Projekten abhängen können. Diese Projekte dauern jedoch oft mehrere Jahre und bieten hinsichtlich der Langfristigkeit eine größere Sicherheit. Aufgrund der Natur von VDI-Systemen wäre eine Überprovisionierung der VDIs grundsätzlich möglich. Allerdings wird dies durch die Nutzung von Grafikleistung einer Drittkomponente verhindert, da das System diese Komponente nicht direkt ansprechen und steuern kann. Eine Überprovisionierung der VDIs ist somit nicht möglich, was jedoch nicht bedeutet, dass eine Überbuchung der Kundenanzahl ausgeschlossen ist. Bei der Überbuchung wird davon ausgegangen, dass nicht alle Kunden gleichzeitig ihre gebuchten Ressourcen in Anspruch nehmen. Dies ermöglicht es, diesen Service an mehr Kunden zu verkaufen, als gleichzeitig bedient werden könnten. Dies hat den Vorteil, dass die vorhandenen Ressourcen besser genutzt und die Einnahmen maximiert werden können. Eine Überbuchung birgt jedoch auch Risiken wie Leistungsprobleme bei hoher Nutzerauslastung oder Kundenunzufriedenheit, falls die Leistung und Verfügbarkeit der Systeme nicht gewährleistet werden können.

In der folgenden Tabelle wird die geschätzte Anzahl der Kunden über die nächsten fünf Jahre dargestellt. Weiter unten findet man die maximale Anzahl an möglichen Kunden, die je nach Leistungsbedarf der VDI variieren kann. Diese maximale Anzahl basiert auf der vorhandenen Kapazität des VRAMs der Grafikkarten. Dabei verfügt der VDI-Server über 128 GB VRAM und der MGMT-Server über 64 GB VRAM. Für das Jahr 2028 wird eine Überbuchung von 25% erwartet. Das Ziel ist es, den Service unter Berücksichtigung dieser Überbuchungsrate weitgehend zu betreiben.

Anzahl Kunden	2024	2025	2026	2027	2028
Premium	5	8	10	12	15
Basic	10	14	18	24	30
Gesamt	15	22	28	36	45
Neu	15	7	6	8	9

Maximale mögliche Anzahl Kunden

Insgesamte Kapazität VRAM 128+64

	Total	Verteilt 50/50%
Premium	24	12
Basic	48	24

Tabelle 4: Kundenschätzung

4.3 Materialkosten

Eines der grössten Investitionselemente des Projekts betrifft die Beschaffung der Hardware. Die Materialbeschaffung erfolgt einmalig und ist nicht direkt von der Anzahl der Kunden abhängig, mit Ausnahme der Anschaffung von Projekt-Laptops. Aus der folgenden Tabelle geht hervor, dass die Materialkosten über einen Zeitraum von drei Jahren amortisiert werden. Dies bietet den Vorteil, dass ab dem dritten Jahr mit einem Gewinn gerechnet werden kann. Eine Amortisationsdauer von mehr als drei Jahren wäre risikoreich, da nach diesem Zeitraum möglicherweise ein Bedarf an Erweiterung oder Upgrade der bestehenden Infrastruktur entstehen könnte.

Neben den fixen Materialkosten fallen auch variable Kosten an, wie etwa für die Projekt-Laptops. Diese werden basierend auf der aktuellen Kundenzahl bestellt, wobei jährlich mindestens drei Reserve-Laptops eingeplant werden. Es wird davon ausgegangen, dass Geräte innerhalb des Jahres ausfallen können. Trotz der On-Site-Garantie kann es oft sinnvoller sein, ein defektes Gerät auszutauschen und beim Standort der IT reparieren zu lassen, um Zeit zu sparen. Es kann auch vorkommen, dass plötzlich neue Mitarbeiter hinzukommen, die Arbeitsgeräte benötigen, oder dass Geräte ausfallen, die nicht durch die Garantieregel abgedeckt sind. Diese variablen Kosten werden ebenfalls über drei Jahre amortisiert, geregelt durch eine dreijährige Abschreibung, die auf der nächsten Seite dargestellt wird. In der Tabelle weiter unten werden die gesamten Materialkosten pro Kunde und Monat aufgeführt. Diese werden basierend auf der jährlichen Kundenanzahl berechnet und sind für die Break-Even-Analyse relevant.

Materialkosten	Anzahl	Einkaufspreise in CHF	Total Materialkosten	Amortisation in Monat	Kosten pro Jahr
VDI-Server	1	20000	20000	36	6667
MGMT-Server	1	9000	9000	36	3000
Synology FS6400 Hauptspeicher	1	29000	29000	36	9667
Synology DS1823xs+ Backup	1	3000	3000	36	1000
Projekt Laptop (variabel)	1	1000	1000	36	333.33

Total fixe Materialkosten pro Jahr 20333

(Fixe Materialkosten pro Jahr + variable Materialkosten pro Jahr) \ 12 \ Anzahl Kunden	Jahr			
	2024	2025	2026	2027
146	112	97	82	
2028				
89				

Tabelle 5: Materialkosten

Abschreibung

Die Kosten der Laptops müssen durch jährliche Abschreibungen ermittelt werden, da es von Jahr zu Jahr unterschiedliche Anschaffungen gibt und die Geräte nach einer dreijährigen Amortisationszeit keinen Restwert mehr aufweisen. In den nachfolgenden Tabellen wird die Berechnung detailliert dargestellt. Die Anzahl der Laptop-Anschaffungen basiert auf die Schätzung der Kundenzahl. Jährlich werden Laptops für neue Benutzer angeschafft. Hinzu kommen Geräte, die vollständig abgeschrieben wurden, sowie drei Reservegeräte. Am Ende ergibt sich aus diesen Angaben die Gesamtsumme der Abschreibungskosten für das Jahr, die zu den Materialkosten des Jahres hinzugefügt werden kann.

Jahr	Gesamtzahl Notebooks	Kosten pro Notebook	Gesamtkosten	Abschreibung pro Jahr	Bemerkung
2024	18	1000	18000	6000	
2025	10	1000	10000	3333	
2026	9	1000	9000	3000	
2027	26	1000	26000	8667	Neue Geräte für 2024
2028	19	1000	19000	6333	Neue Geräte für 2025

Anzahl neue Kunden + 3 als Reserve

Jahr	Abschreibung 2024	Abschreibung 2025	Abschreibung 2026	Abschreibung 2027	Abschreibung 2028
2024	6000	6000	6000	0	0
2025	0	3333	3333	3333	0
2026	0	0	3000	3000	3000
2027	0	0	0	8667	8667
2028	0	0	0	0	6333

Jahr	Gesamtabschreibung
2024	6000
2025	9333
2026	12333
2027	15000
2028	18000

Tabelle 6: Abschreibungskosten

4.4 Betriebskosten

Die Betriebskosten wurden nicht pro Kunde berechnet, da die Probleme häufig miteinander zusammenhängen und trotz einer Zunahme der Kundenzahl gemeinsam zusammengefasst und vereinfacht berechnet werden können. Es wurde ein grosszügiger Wert von 8 Stunden Supportaufwand pro Monat angesetzt, da das System wenig Anpassungen bezüglich Updates und Änderungen benötigt und dementsprechend weniger unvorhergesehene Probleme oder Anpassungsaufwände auftreten. Geplant sind halbjährliche umfangreiche Wartungen und Updates der Infrastruktur und Golden Images, die auf insgesamt zwei ganze Tage geschätzt werden und von zwei Mitgliedern des Engineering-Teams an einem Wochenende durchgeführt werden.

Neben diesen Wartungstätigkeiten fallen laufende Lizenzkosten an, die pro Person berechnet werden müssen. Diese Kosten werden den Kunden jedoch nicht direkt in Rechnung gestellt, sondern sind in den Abonnementgebühren enthalten. Lizenzen für spezielle Programme wie CAD-Software müssen allerdings von den Kunden selbst beschafft werden. In diesen Fällen ist die IT-Abteilung für die Einrichtung der Software und die Verwaltung des Lizenzservers zuständig, sofern dies erforderlich ist.

Tätigkeiten	Häufigkeit	Zuständigkeit	Arbeitsumfang (Stunden/Jahr)	
Support Anfragen	8h/Monat	Service Desk	96	
Log und Backup Kontrolle	1.5h/Monat	Engineering	18	
Wartungsarbeit	34h/Jahr	Engineering	34	
			148	
Laufende Kosten				CHF pro Person
Citrix Lizenzen	1x/Monat	Engineering	30	

	Jahr			
Aufwand im Jahr	2024	2025	2026	2027
Total Aufwand für alle Kunden	8140	8140	8140	8140
	2028			
	8140			
Interner Ansatz in CHF	55			
Laufende Kosten Im Jahr	2024	2025	2026	2027
Citrix Lizenzen	450	660	840	1080
	2028			
	1350			

Tabelle 7: Betriebskosten

4.5 Erlös

Der Service wird durch zwei unterschiedliche Abonnements angeboten, die sich lediglich in der Leistung der VDI unterscheiden. Der Preis jedes Abonnements wurde auf Basis der Break-Even festgelegt. Dabei sollte der Preis möglichst fair gestaltet sein, könnte jedoch aufgrund der Unique Selling Proposition (USP) auch höher angesetzt werden. Da es sich um eine spezielle Infrastruktur handelt, können diese Kosten direkt dem Projekt zugeordnet und somit die Preise höher angesetzt werden. Das Ziel dieser Berechnung war es, ab dem dritten Jahr einen Profit zu erzielen, wobei die bestehende Infrastruktur nach drei Jahren amortisiert sein sollte. Für die Break-Even-Berechnung wurde der durchschnittliche Erlös über fünf Jahre herangezogen, der basierend auf der Anzahl der Kunden, die entweder ein Premium- oder ein Basic-Abonnement haben, ermittelt wurde.

Kunden	2024	2025	2026	2027	2028
Premium	24000	38400	48000	57600	72000
Basic	43200	60480	77760	103680	129600

Erlös Premium	400	pro Monat
Erlös Basic	360	pro Monat

Durchschnittserlöse	2024	2025	2026	2027	2028
	373.33	374.55	374.29	373.33	373.33
Durchschnitt	374				

Tabelle 8: Erlös

4.6 Break-Even

Diese Break-Even-Analyse basiert auf vorliegenden Daten und bestimmt, ab welcher Kundenanzahl pro Jahr ein Gewinn erzielt werden kann. Es lässt sich ableiten, dass zwischen dem zweiten und dritten Jahr mit einem Profit gerechnet werden kann. Da für den Zeitraum zwischen 2026 und 2027 eine Kundenbasis von 30 bis 35 Personen prognostiziert wurde, war das Ziel, den Erlös so zu gestalten, dass ab dieser Anzahl ein Gewinn erzielt wird. Die Analyse zeigt, dass der Service mit mehr als 30 Kunden sehr profitabel sein kann. Allerdings könnten die Preise nach einiger Zeit steigen, wenn ein Mehrbedarf an Kapazität sowie eine Erhöhung der Verfügbarkeit und Sicherheit erforderlich werden. Da sich diese Analyse hauptsächlich auf die Anzahl der Kunden konzentriert, wurde auch eine separate Analyse für Jahre mit einer geringeren Kundenzahl durchgeführt, die auf der folgenden Seite näher erläutert wird.

Kun-den	Projektkosten	Betriebskosten	Materialkos-ten	GK15%	Kosten Total	Erlös	Gewinn
15	89945	8590	26333	5239	130107	67278	-62829
20	89945	8740	26970	5356	131011	89704	-41307
25	89945	8890	43889	7917	150641	112130	-38511
30	89945	9040	40455	7424	146864	134556	-12308
35	89945	9190	40833	7504	147472	156982	9510
40	89945	9340	42593	7790	149667	179408	29740
45	89945	9490	47917	8611	155963	201834	45871

Gemeinkostenzuschlag 15% von Betriebskosten + Materialkosten (Kosten für Management und Support Organisationen)

Tabelle 9: Break-Even Kundenanzahl

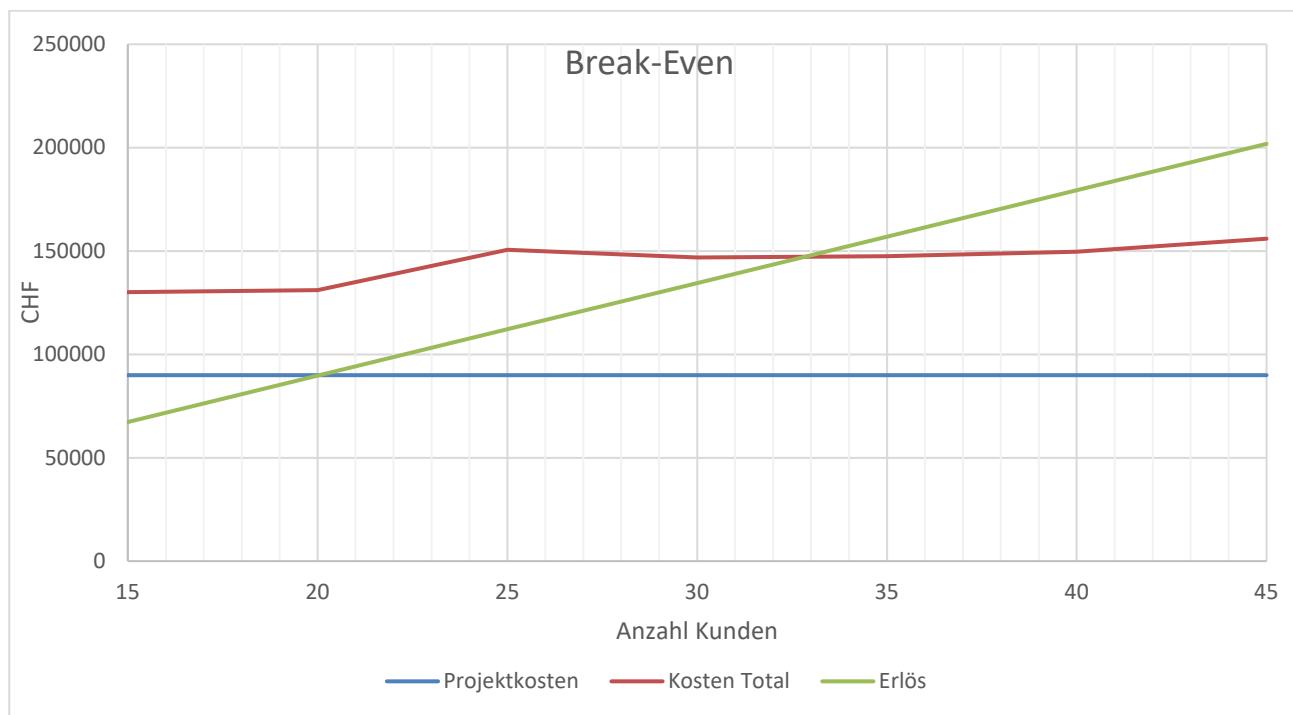


Abbildung 4: Break-Even Kundenanzahl

4.6.1 Break-Even (Jahre)

Diese Break-Even-Analyse dient dazu, die Rentabilität des Services über einen mehrjährigen Zeitraum auch bei einer kleineren Kundenbasis aufzuzeigen. Das angestrebte Ziel ist es, innerhalb von drei Jahren eine vollständige Amortisation zu erreichen und anschliessend profitabel zu arbeiten. Wie in der folgenden Tabelle entnommen werden kann, übersteigt die Kundenzahl zu keinem Zeitpunkt 30. Selbst mit einer geringeren Anzahl an Kunden kann dieser Service langfristig Gewinne erwirtschaften. Es ist jedoch zu beachten, dass in dieser Analyse keine zukünftigen Investitionen in die Infrastruktur berücksichtigt wurden. Wie auch bei der anderen Break-Even-Analyse, müssen wir anerkennen, dass sich Preise sowie die Bedürfnisse der Kunden dynamisch verändern können. Es ist daher entscheidend, eine flexible Preisgestaltung und die Bereitschaft für kontinuierliche Anpassungen der Serviceangebote zu planen, um auf Marktveränderungen und Kundenanforderungen reagieren zu können.

Kunden	Projektkosten	Betriebskosten	Materialkosten	GK15%	Kosten Total	Erlös	Gewinn	Jahr	Bilanz
15	89945	8590	26333	5239	130107	67279	-62828	2024	-62828
15	0	8590	27333	5389	41312	67279	25967	2025	-36861
15	0	8590	28333	5539	42462	67279	24817	2026	-12044
20	0	8740	8000	2511	19251	89705	70454	2027	58410
20	0	8740	9667	2761	21168	89705	68537	2028	126948
20	0	8740	9667	2761	21168	89705	68537	2029	195485
25	0	8890	11333	3034	23257	112131	88875	2030	284360

Gemeinkostenzuschlag 15% von Betriebskosten + Materialkosten (Kosten für Management und Support Organisationen)

Tabelle 10: Break-Even (Jahre)

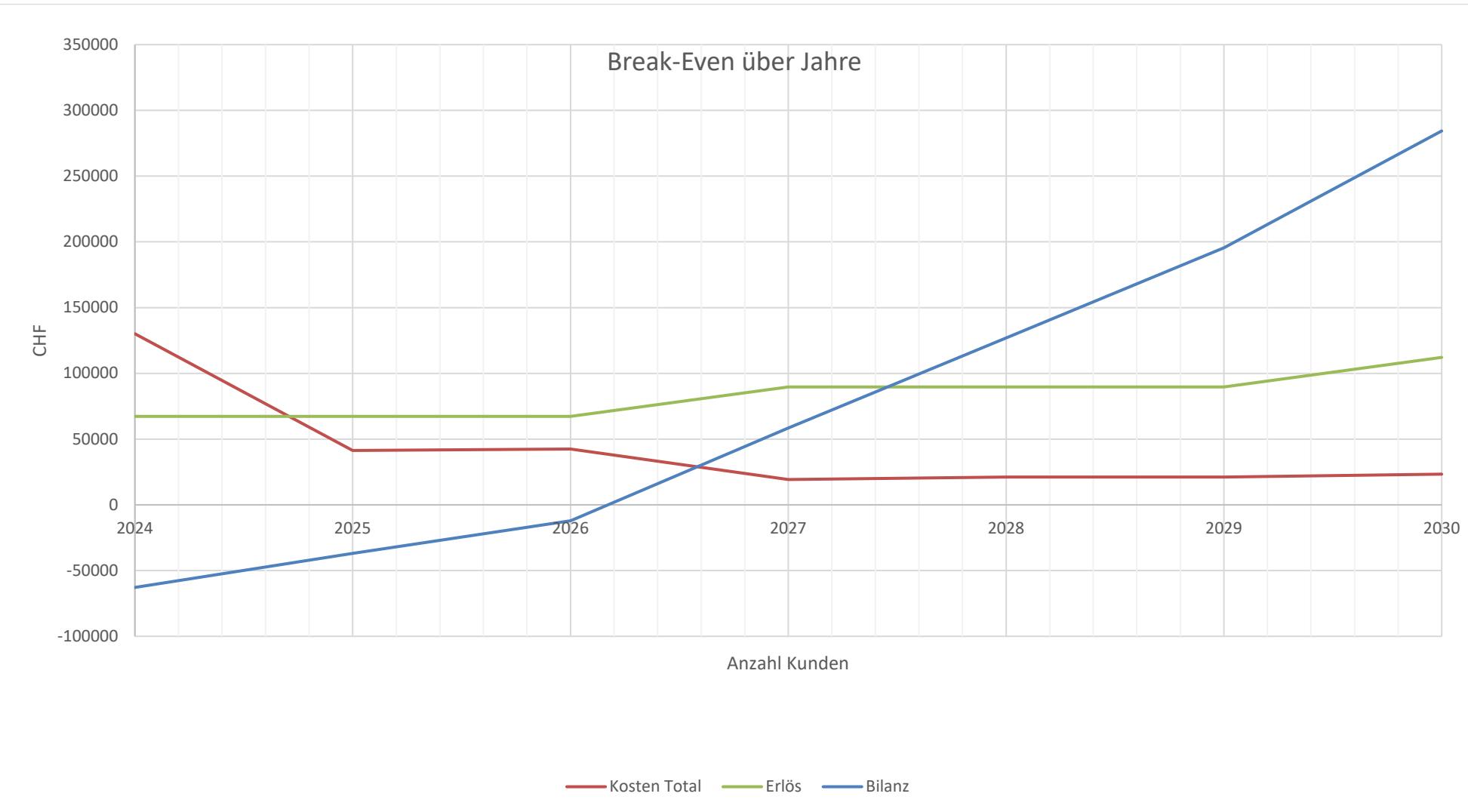


Abbildung 5: Break-Even (Jahre)

Break-Even Daten (Jahre)

Im Folgenden sind die Daten aufgeführt, die als Grundlage für die Break-Even-Analyse über Jahre verwendet wurden.

Tätigkeiten Projekt	Stunden [h]	Ansatz [CHF]	Kostenprojekt
Initialisierung	103	55	5665
Konzept	88	55	4840
Realisierung	168	55	9240
Einführung	16	55	880
Abschluss	124	55	6820
Totale Stunden	499	Total Aufwand	27445
Material HW/SW etc.			61000
Externe Dienstleistungen	10	150	1500
		Total Projektkosten	89945

Tabelle 11: Projektkosten (Jahre)

Anzahl Kunden	2024	2025	2026	2027	2028	2029	2030
Premium	5	5	5	7	7	7	9
Basic	10	10	10	13	13	13	16
Gesamt	15	15	15	20	20	20	25
Neu	15	0	0	5	0	0	5

Tabelle 12: Kundenschätzung (Jahre)

Materialkosten	Anzahl	Einkaufspreise in CHF	Total Materialkosten	Amortisation in Monat	Kosten pro Jahr
VDI-Server	1	20000	20000	36	6667
MGMF-Server	1	9000	9000	36	3000
Synology FS6400 Hauptspeicher	1	29000	29000	36	9667
Synology DS1823xs+ Backup	1	3000	3000	36	1000
Projekt Laptop (variabel)	1	1000	1000	36	333.33

Total fixe Materialkosten pro Jahr 20333

Tabelle 13: Materialkosten (Jahre)

Jahr	Gesamtzahl Notebooks	Kosten pro Notebook	Gesamtkosten	Abschreibung pro Jahr	Bemerkung
2024	18	1000	18000	6000	
2025	3	1000	3000	1000	
2026	3	1000	3000	1000	
2027	23	1000	23000	7667	Neue Geräte für 2024

Jahr	Gesamtzahl Notebooks	Kosten pro Notebook	Gesamtkosten	Abschreibung pro Jahr	Bemerkung
2028	3	1000	3000	1000	
2029	3	1000	3000	1000	
2030	28	1000	28000	9333	Neue Geräte für 2027

Anzahl neue Kunden + 3 als Reserve

Jahr	Abschreibung 2024	Abschreibung 2025	Abschreibung 2026	Abschreibung 2027	Abschreibung 2028
2024	6000	6000	6000	0	0
2025	0	1000	1000	1000	0
2026	0	0	1000	1000	1000
2027	0	0	0	7667	7667
2028	0	0	0	0	1000
2029	0	0	0	0	0
2030	0	0	0	0	0
	Abschreibung 2029	Abschreibung 2030			
	0	0			
	0	0			
	0	0			
	7667	0			
	1000	1000			
	1000	1000			
	0	9333			

Jahr	Gesamtabschreibung
2024	6000
2025	7000
2026	8000
2027	9667
2028	9667
2029	9667
2030	11333

Tabelle 14: Abschreibung (Jahre)

Kunden	2024	2025	2026	2027	2028	2029	2030
Premium	24000	24000	24000	33600	33600	33600	43200
Basic	43200	43200	43200	56160	56160	56160	69120

Erlös Premium	400	pro Monat
Erlös Basic	360	pro Monat

Durchschnittserlöse	2024	2025	2026	2027	2028	2029	2030
	373.33	373.33	373.33	374.00	374.00	374.00	374.40
Durchschnitt	374						

Tabelle 15: Erlös (Jahre)

Tätigkeiten	Häufigkeit	Zuständigkeit	Arbeitsumfang (Stunden/Jahr)	CHF pro Person
Support Anfragen	8h/Monat	Service Desk	96	
Log und Backup Kontrolle	1.5h/Monat	Engineering	18	
Wartungsarbeit	34h/Jahr	Engineering	34	
			148	
Laufende Kosten				
Citrix Lizenzen	1x/Monat	Engineering	30	

	Jahr				
Aufwand im Jahr	2024	2025	2026	2027	2028
Total Aufwand für alle Kunden	8140	8140	8140	8140	8140
	2028	2029	2030		
	8140	8140	8140		
Interner Ansatz in CHF	55				
Laufende Kosten Im Jahr	2024	2025	2026	2027	
Citrix Lizenzen	450	450	450	600	
	2028	2029	2030		
	600	600	750		

Tabelle 16: Betriebskosten (Jahre)

5 SLA

Das Service-Level-Agreement definiert die genauen Erwartungen der angebotenen Dienstleistung zwischen dem Dienstanbieter und den Kunden. Sie legt quantifizierbare und messbare Standards fest, die die Qualität, Verfügbarkeit und die Verantwortlichkeit der Dienstleistung bestimmt. Im Folgenden wird die SLA für den VDI-Service dargelegt.

5.1 Generelle Vereinbarung

5.1.1 Vertragsparteien

Auftraggeber (AG)

Auftragnehmer (AN)

Finitia AG
Nordring 4a
3001

5.1.2 Ansprechpartner

Ansprechpartner des Kunden:

Ansprechpartner Auftragnehmer:

Shipinyuan Su

5.1.3 Beginn SLA

Vertragsbeginn:

01.01.2025

5.1.4 Laufzeit SLA

Die SLA läuft unbefristet, solange keine Anpassungen gemacht werden. Die Laufzeit der Abonnemente sind in Kapitel 5.5 beschrieben.

5.1.5 Kündigungsfrist

Die SLA kann unter Einhaltung einer dreimonatigen Kündigungsfrist per Ende Monat aufgelöst werden. Eine Kündigung des SLAs hat die Kündigung aller Abonnemente als Folge. Die Bedingungen der Kündigungen einzelnen Abonnementen sind im Kapitel 5.5 definiert.

5.1.6 Vertragsrücktritt bei Nichterfüllung

Erfüllt eine Partei diesen SLA nicht, kann die andere Partei eine angemessene Frist zur nachträglichen Erfüllung des jeweiligen Vertrages ansetzen. Erfüllt darauf die Schuldnerpartei nicht innert angesetzter Frist, kann die andere Partei vom entsprechenden Vertrag zurücktreten. Verletzt eine Partei in anderer Weise einen Vertrag, kann die andere Partei von dem entsprechenden Vertrag zurücktreten.

5.2 Allgemeiner IT-Support

5.2.1 Zeiten Servicebereitschaft

Die reguläre Servicebereitschaft zur Erbringung der IT-Dienstleistungen wird wie folgt definiert:

Montag – Freitag jeweils 07:30 – 17:30 Uhr

Ausserhalb dieser Öffnungszeiten wird das Rechenzentrum per Pikettorganisation überwacht. Die Überwachung der zentralen IT-Infrastruktur findet an 365 Tagen 24/7 statt.

5.2.2 Kontakt bei Service-Bedarf

Der AN stellt eine telefonisch und per E-Mail erreichbare Hotline zur Verfügung. Die erhaltenen E-Mails werden direkt in das Ticketingsystem übernommen.

Tel.: +41 31 340 83 00

E-Mail: helpdesk@finitia.net

5.2.3 Servicelevel und Reaktionszeiten

Reaktionszeiten innerhalb der Servicebereitschaft

- | | | |
|------------|--------------------------------|-------------------------|
| • Stufe 1: | kein Arbeiten möglich | 2 Stunden |
| • Stufe 2: | Operation kritisch | halber Arbeitstag |
| • Stufe 3: | Funktion bedingt eingeschränkt | nächster Arbeitstag |
| • Stufe 4: | Schwächen, Optimierungen | nächster Vor-Ort Termin |

Anliegen der Stufen 1 und 2 müssen per E-Mail und per Telefon an den AN gemeldet werden. Anliegen der Stufen 3 und 4 werden vorzugsweise per E-Mail gemeldet.

Reaktionszeiten ausserhalb der Servicebereitschaft (zentrale IT-Infrastruktur)

- | | | |
|------------|-----------------------|--------------|
| • Stufe 1: | kein Arbeiten möglich | 4 Stunden |
| • Stufe 2: | Operation kritisch | nächster Tag |

5.3 Dienstleistungen: Abonnementen

Diese Leistung ist unabhängig von der laufenden WaaS (Workplace as a Service) und wird separat abgerechnet.

5.3.1 Abonnement Basic

Das Basic-Abonnement richtet sich an alle Mitarbeitenden, die ihre Tätigkeiten mit CAD-Anwendungen ausführen. Der Fokus der Basic-Version liegt auf Nutzern, die mit kleineren CAD-Modellen arbeiten und grundlegende Designaufgaben übernehmen. Diese Version bietet eine solide Grundausstattung, die für allgemeine CAD-Arbeiten vollkommen ausreichend ist. Der Service gewährleistet grösstmögliche Mobilität und Flexibilität, gepaart mit optimaler Sicherheit. Die nachfolgend aufgeführten Leistungen sind im Abonnement enthalten:

- 1 Projektnotebook Lenovo E14
- VDI (virtueller Desktop)
- Garantieleistungen der gelieferten Endgeräte (entsprechen der Laufzeit, siehe Kapitel 5.5)
- Problembehebung bei Störungen der Endgeräte
- Systemabhängige Lizenzen wie VPN, Nvidia und Citrix. CAD-Lizenzen gehören nicht dazu

Die Endgerättypen können ändern, entsprechen mindestens der obengenannten Ausführung.

5.3.2 Abonnement Premium

Das Premium-Abonnement ist speziell für Fachkräfte konzipiert, die mit umfangreichen und komplexen CAD-Modellen arbeiten. Diese Version zeichnet sich durch erheblich gesteigerte Leistungsfähigkeit aus, die auch anspruchsvollste Designaufgaben unterstützt. Der Service gewährleistet grösstmögliche Mobilität und Flexibilität, gepaart mit optimaler Sicherheit. Die nachfolgend aufgeführten Leistungen sind im Abonnement enthalten:

- 1 Projektnotebook Lenovo E14
- VDI (virtueller Desktop)
- Garantieleistungen der gelieferten Endgeräte (entsprechen der Laufzeit, siehe Kapitel 5.5)
- Problembehebung bei Störungen der Endgeräte
- Systemabhängige Lizenzen wie VPN, Nvidia und Citrix. CAD-Lizenzen gehören nicht dazu

Die Endgerättypen können ändern, entsprechen mindestens der obengenannten Ausführung.

5.4 Detaillierte Leistungsbeschreibung

5.4.1 Support Projektnotebooks

Der AN erbringt folgende Leistungen im Bereich des Supports der Projektnotebooks:

- Das Aufsetzen der Projektnotebooks
- Update Windows nach Updateplan
 - a. Einspielen der kritischen Windowsupdates
 - b. ausgeschlossen sind die Funktionsupdates
 - c. Garantieabwicklung und Garantieaustausch Hardware
- Organisation des Garantieaustausches
 - a. Bei Bedarf Stellung eines Austauschgerätes
- Einrichtung VDI und VPN
- Abonnement Mutationen (Übergabe an neuen Mitarbeiter bei Kündigung des ehemaligen Mitarbeiters)

5.4.2 Support VDI

Der AN erbringt folgende Leistungen im Bereich des Supports VDI:

- Einrichtung der VDI (anhand Golden-Image)
- Aufschalten neuer Benutzer und Verlinkung mit Endgeräten
- Proaktive Überwachung der VDIs
 - a. Überwachung Performance, Auslastung und Stabilität
 - b. Überwachung Virenschutz
- Update Windows nach Updateplan (Homogenität VDI)
 - a. Einspielen der kritischen Windowsupdates
- Update der Treiber von Citrix und Nvidia
- Update der Standardapplikationen

Nicht enthalten ist die Erarbeitung des Golden-Images. Dieses wird vorab, zusammen mit dem AG in einem Proof of Concept (POC) erarbeitet und freigegeben.

5.5 Bestellung / Modifikation / Laufzeit

Die Bestellung eines Abonnements (Abo) und/oder Ersatz von Endgeräten wird durch den Ansprechpartner des AG schriftlich ausgelöst. Die Laufzeit aller Abos beträgt 48 Monate. Die Laufzeit des Abos startet jeweils neu mit der Auslieferung von Endgeräten an den AG (eine Laufzeit je Abo). Wird nach Ablauf der 48 Monate kein neues Endgerät ausgelöst, kann das Abo jeweils auf Ende Monat gekündigt werden. Wird ein Abo eines Mitarbeiters nicht mehr benötigt kann er einem anderen Mitarbeiter übertragen oder gekündigt werden. Bei einer vorzeitigen Kündigung wird für die ausstehende Restlaufzeit die Kostenanteile Hardware und VDI in Rechnung gestellt.

Bei Eintreten eines speziellen Ereignisses (markante Reduktion des Personals, Auftragsentzug, etc.) wird zwischen AG und AN eine für beide Parteien optimale Lösung gesucht.

5.6 Leistungsvergütung

5.6.1 Abonnement Basic

Für die Erbringung der Leistungen für den Basic Abo wird ein Pauschalbetrag von CHF 360 je Benutzer und Monat verrechnet.

5.6.2 Abonnement Premium

Für die Erbringung der Leistungen für den Basic Abo wird ein Pauschalbetrag von CHF 400 je Benutzer und Monat verrechnet.

5.6.3 Supportleistungen

Für die Leistungserbringung werden die nachfolgend aufgeführten Stundensätze definiert:

Innerhalb der regulären Servicebereitschaft: CHF 120.00

Ausserhalb der regulären Servicebereitschaft: CHF 120.00 + 50%

5.7 Ergänzende Anmerkungen

5.7.1 Endgeräte

Die in Kapitel 5.3 aufgeführten Endgeräte sind zum Zeitpunkt der Unterzeichnung des SLA aktuell. Sollten die aufgeführten Endgeräte nicht mehr lieferbar sein, so wird, wenn immer möglich vergleichbare vom AG zertifizierte Endgeräte eingesetzt.

5.7.2 Abrechnungsformalitäten

Die effektiven Mengen werden Ende Monat erfasst und entsprechend für den gesamten Monat in Rechnung gestellt. Die kleinste verrechnete Einsatzzeit beträgt 0.25 Stunden.

Zuzüglich zu den Pauschal- und Stundensätzen wird die Mehrwertsteuer verrechnet.

Die Kosten von externen Spezialisten werden (nach erfolgter Freigabe durch den AG) an den AG verrechnet. Ferner werden auch Kosten im Zusammenhang mit der Beschaffung von Software durch den AN für den AG an den AG weiterverrechnet.

Reisekosten, Reisezeiten und Spesen innerhalb der Stadt Bern werden dem AG nicht in Rechnung gestellt. Rechnungen sind innerhalb von 30 Tage nach Rechnungslegung zur Zahlung fällig.

5.7.3 Vertraulichkeit

Die gesamten Daten des AG werden vom AN streng vertraulich behandelt. Der AN garantiert die Geheimhaltung dieser Daten und der dazugehörigen Anwendersoftware. Die Vertraulichkeit bleibt auch im Falle der Vertragsauflösung bestehen. Der AG und AN behandeln den SLA und dessen Inhalt vertraulich.

5.7.4 Haftung

Der AN gewährleistet, nach Massgabe dieses Vertrages, einen ordnungsgemässen Betrieb der in dieser Vereinbarung aufgeführten Komponenten und Dienste. Weitergehende Ansprüche des Kunden, insbesondere auf mittelbare Schäden wie entgangenen Gewinn, ausgebliebene Einsparung, Schäden aus Ansprüchen Dritter gegen den Kunden, Verlust von Daten usw. sind in jedem Fall ausgeschlossen.

Die Haftung ist unabhängig vom Rechtsgrund, auf die Leistungsvergütungen beschränkt. Die Haftung für Datenverlust wird auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmässiger und gefahrenentsprechender Anfertigung von Sicherheitskopien gem. gemeinsam definierten Backupplan eingetreten wäre.

Kann der AN einen Reparatur- oder Wartungserfolg deshalb nicht oder lediglich verspätet herbeiführen, weil Ersatzteile, Dokumentationen oder Informationen des Herstellers oder Lieferanten von dieser Seite nicht rechtzeitig zur Verfügung gestellt werden, ist eine Haftung des AN gegenüber dem AG ausgeschlossen, es sei denn der AN handelt grob fahrlässig oder vorsätzlich. Weiter ist auch die Haftung aufgrund externer und nicht durch den AN beeinflussbare Ursachen (z. B. Stromunterbruch oder Ausfall Netzwerk) auszuschliessen.

Für Dateien, welche ausserhalb der im Umfang dieser Vereinbarung definierten Umgebung gespeichert werden (mitgebrachte Datenträger, USB-Sticks, DVDs u.a.) wird jegliche Verantwortung und Haftung ausgeschlossen. Für deren Backup ist der AG verantwortlich.

5.7.5 Mitwirkung Auftraggeber

Die zeitlich und inhaltlich vertragsgemäss Erbringung der Dienstleistung und der Aufwand und folglich die daraus entstehenden Kosten sind massgeblich von der Mitwirkung und Unterstützung durch die Mitarbeitenden vom AG abhängig. Insbesondere stellt der AG folgendes sicher:

- Definition von Ansprechpartnern.
- Rechtzeitige und vollständige Bereitstellung der für die Auftragsdurchführung erforderlichen Unterlagen und Informationen.
- Der AG nennt dem AN die Mitarbeiter, welche die verschiedenen Supportleistungen nutzen dürfen bzw. beauftragen dürfen.

5.7.6 Verschiedenes

Änderungen oder Ergänzungen dieses SLA bedürfen zu ihrer Gültigkeit der Schriftform, der Bezugnahme auf die abzuändernde Bestimmung und der rechtsgültigen Unterzeichnung durch den AG und AN.

Sollte eine Bestimmung dieses SLA ungültig sein oder rechtsunwirksam werden, so gelten die übrigen Bestimmungen weiter. Die ungültige oder rechtsunwirksame Bestimmung soll in diesem Fall durch eine wirksame Bestimmung ersetzt werden, die in ihrer wirtschaftlichen Auswirkung derjenigen der ungültigen oder unwirksamen Bestimmung so nahe wie rechtlich möglich kommt.

Das Vertragsverhältnis zwischen AG und AN untersteht schweizerischem Recht. Ausschliesslicher Gerichtsstand für alle Streitigkeiten zwischen AG und AN ist der jeweilige Sitz vom AN.

Bern, den 01.01.2025

Für den Auftraggeber

Bern, 01. Januar 2025

Für den Auftragnehmer

Bern, 01. Januar 2025

Quellenverzeichnis

Ostler, U. (06. 12 2011). *Datacenter-insider*. Abgerufen am 12. 04 2024 von Datacenter-insider:

<https://www.datacenter-insider.de/von-tier1-bis-tier-4-die-vier-qualitaetsstufen-eines-rechenzentrums-a-341120/>

Staff, C. (10. 11 2022). *Citrix Docs*. Abgerufen am 15. 04 2024 von Citrix Docs:

<https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/1912-ltsr/system-requirements.html>

Wang, B. (08. 06 2023). *Citrix Docs*. Abgerufen am 12. 04 2024 von Citrix Docs:

<https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/technical-overview.html>

Abbildungsverzeichnis

Abbildung 1: Organigramm	4
Abbildung 2: Golden Image.....	6
Abbildung 3: Support Ablaufdiagramm.....	9
Abbildung 4: Break-Even Kundenanzahl.....	22
Abbildung 5: Break-Even (Jahre)	24

Tabellenverzeichnis

Tabelle 1: Änderungsverzeichnis	1
Tabelle 2: Beispiele 1st- und 2nd Level Support	9
Tabelle 3: Projektkosten.....	16
Tabelle 4: Kundenschätzung.....	17
Tabelle 5: Materialkosten	18
Tabelle 6: Abschreibungskosten	19
Tabelle 7: Betriebskosten.....	20
Tabelle 8: Erlös	21
Tabelle 9: Break-Even Kundenanzahl.....	22
Tabelle 10: Break-Even (Jahre)	23
Tabelle 11: Projektkosten (Jahre)	25
Tabelle 12: Kundenschätzung (Jahre).....	25
Tabelle 13: Materialkosten (Jahre).....	25
Tabelle 14: Abschreibung (Jahre)	26
Tabelle 15: Erlös (Jahre).....	27
Tabelle 16: Betriebskosten (Jahre)	27

Anhang E5

VDI as a Service

Übersicht

Um den technologischen Fortschritt und die digitale Transformation zu fördern, ist die Entwicklung neuer Lösungen unerlässlich. Speziell für ein Zielpublikum, das in einer abgeschirmten Umgebung ohne direkten Internetzugang arbeitet, haben wir eine VDI-Lösung auf Basis von Citrix VDI entwickelt. Diese Lösung ermöglicht es Nutzern, sicher und effizient von jedem Ort aus zu arbeiten und gleichzeitig höchste Sicherheitsstandards und optimale Verfügbarkeit zu gewährleisten. Zusätzlich bietet sie erweiterte Funktionalitäten zur Anpassung an spezifische Anforderungen und zur Skalierung entsprechend den Nutzerbedürfnissen, wodurch Unternehmen eine flexible und zukunftssichere Arbeitsumgebung erhalten.

Was macht diesen Service so einzigartig?

Unser Service bietet eine einzigartige Verkaufsposition (USP) und ist speziell auf spezifische Anwendungsfälle zugeschnitten. Unsere Kunden, die diese Lösung implementieren, sind an Geheimhaltungsprojekten beteiligt, die eine hochgesicherte Arbeitsumgebung erfordern. Diesen massgeschneiderten Service bieten wir als exklusiver Dienstleister an. Er ist nicht über grosse Anbieter wie Microsoft verfügbar, da er präzise auf die individuellen Bedürfnisse und Sicherheitsanforderungen unserer Kunden ausgerichtet ist. Darüber hinaus sorgen wir für kontinuierliche Updates und Anpassungen, um den dynamischen Sicherheitsanforderungen gerecht zu werden und eine optimale Leistung zu gewährleisten.



Zielpublikum

Unser Zielpublikum umfasst Organisationen, die höchsten Wert auf Datensicherheit legen und ihre Daten sowie Anwendungen in einer abgeschirmten Umgebung betreiben möchten. Diese Organisationen sind insbesondere auf hohe Rechenleistung angewiesen, um beispielsweise anspruchsvolle CAD-Programme effizient nutzen zu können. Zugleich benötigen sie die Flexibilität, sicher von externen Standorten auf ihre Systeme zugreifen zu können. Unser Service bietet die ideale Lösung für Nutzer, die eine optimale Balance zwischen Sicherheit, Zugänglichkeit und leistungsstarker Rechenkapazität anstreben. Diese Kombination ist entscheidend, um komplexe Design- und Ingenieursaufgaben effektiv zu unterstützen.

VDI as a Service

Technische Spezifikationen

Unser Service bietet technisch fortschrittliche Lösungen für Organisationen, die in ihrer täglichen Arbeit auf maximale Rechenleistung angewiesen sind. Wir stellen leistungsstarke Virtual Desktop Infrastructures (VDIs) bereit, die mit NVIDIA Grafikkarten ausgestattet sind.

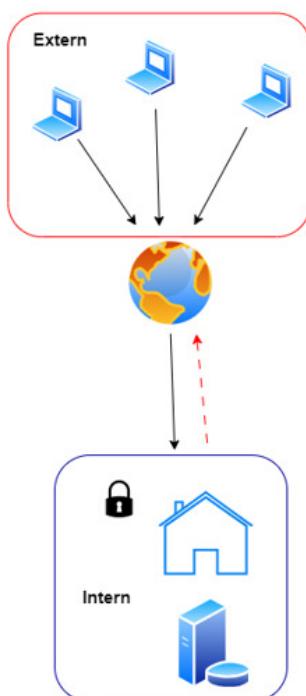
Unsere Infrastruktur umfasst mehrere GPU-Server, die auf einem 2U Dual-Prozessor-System (Intel) mit GPUs von Supermicro basieren. Dank unserer flexibel erweiterbaren Infrastruktur können auf Anfrage zeitnah zusätzliche GPU-Server hinzugefügt werden, um die Leistungsfähigkeit des Systems zu erhöhen und den steigenden Anforderungen gerecht zu werden.

Wir nutzen Citrix als Hypervisor sowie das vollständige Virtual Desktop und Application Toolset, um auf den aktuellen Marktführer im Bereich der Desktop- und Anwendungsvirtualisierung zu setzen. Dies ermöglicht eine effiziente und sichere Verwaltung von Anwendungen und Desktops in unserer hochentwickelten VDI-Umgebung.

Ihr Nutzen

Als Unternehmen können Sie:

- Ständige Erreichbarkeit für Ihre Mitarbeiter sicherstellen
- Flexiblen und sicheren Zugriff auf Anwendungen und Daten von überall
- Skalierung der Leistung der VDI-Umgebung
- Sicherheitsupdates ohne Unterbrechung für die ganze Infrastruktur



Support & Wartung

Unsere Supportzeiten sind von Montag bis Freitag, jeweils von 07:30 bis 17:30 Uhr. Für Infrastrukturstörungen bieten wir außerhalb dieser Öffnungszeiten einen 24/7-Pikettdienst an.

Grosse Server/Infrastruktur Wartungen erfolgen halbjährlich. Zusätzlich überprüfen wir regelmässig, ob wichtige Sicherheitsupdates verfügbar sind, und installieren diese bei Bedarf umgehend.

Anhang F1



Arbeitsbericht

VDI as a Service

Auftraggeber	Micha Bucher
Projektleiter	Shipinyuan Su, Sirak Yosef
Autor	Shipinyuan Su, Sirak Yosef
Klassifizierung	Intern
Status	Von AG abgesegnet

Änderungsverzeichnis

Datum	Version	Änderung	Autor
28.04.2024	0.1	Dokument erstellt	Shipinyuan Su, Sirak Yosef
19.05.2024	1.0	Dokument fertiggestellt	Shipinyuan Su, Sirak Yosef

Tabelle 1: Änderungsverzeichnis

Inhaltsverzeichnis

1	Einleitung	3
2	Netzwerkkonfiguration.....	4
3	Aufbau MGMT-Server	7
4	Konfiguration MGMT-Server	10
5	Konfiguration Hauptspeicher	24
6	Einrichtung Domain Controllers.....	38
7	Konfiguration NAS-Backup.....	41
8	Konfiguration VDI-Server	43
9	Einrichtung Citrix Services	44
10	Einrichtung Citrix Services Redundanz	85
11	Einrichtung WEM und FSLogix.....	91
12	Sonstige Konfigurationen	103

1 Einleitung

Mit der Realisierung ist es wichtig die wichtigsten einzelnen Schritte zu dokumentieren. Dabei werden nicht nur das Wie, sondern auch das Warum dokumentiert. Ziel dieses Berichtes ist es, ein klares Verständnis der durchgeführten Arbeiten und der Entscheidungsprozesse zu vermitteln, die zur erfolgreichen Umsetzung des Projekts beigetragen haben.

Der Bericht ist thematisch strukturiert, wobei jedes Kapitel einem spezifischen Aspekt oder Thema gewidmet ist. Diese Struktur ermöglicht eine fokussierte Darstellung der einzelnen Arbeitsschritte, unabhängig von ihrer tatsächlichen Abfolge während der Projektdurchführung. Diese Vorgehensweise erlaubt es, verwandte Prozesse und deren Auswirkungen detailliert zu beleuchten, ohne durch die chronologische Reihenfolge eingeschränkt zu sein

2 Netzwerkkonfiguration

Als "isolierte" Umgebung, die unabhängig von der produktiven Umgebung operiert, mussten neue Netzwerke erstellt werden. Diese wurden im Detailkonzept definiert und beim externen Drittanbieter angefragt. Nach der Erstellung der segmentierten Netzwerke wurden während der Realisierung immer wieder Anpassungen an den Firewall Regeln vorgenommen.

Firewall Regeln

Es wurde mehrere Firewall Regeln erstellt, welche die Kommunikation zwischen den verschiedenen Netzwerken regelt. (Produktives Netz, VLAN 220 MGMT, VLAN 230 VDI)

VLAN-220-to-WAN: Ermöglicht die Internetverbindung vom MGMT-Netz aus

VLAN-230-to-WAN: Ermöglicht nur die Verbindung zu "*.nvidia.com" Adressen, welches die Lizenzierung der Nvidia Grafikkarten ermöglicht. Sonst gäbe es eine Leistungsreduktion von 75% der Grafikleistung

BernServer-to-VLAN220: Ermöglicht das Verwalten aller Dienste im neuen MGMT-Netz vom produktiven Netzwerk aus

VLAN220-to-VLAN230: Ermöglicht das Verwalten von Geräten und Dienste im VDI-Netz vom MGMT-Netz aus

VLAN230-to-VLAN220: Diese Konfiguration ermöglicht es VDIs, vom VDI-Netzwerk aus auf verschiedene Dienste wie DDC, FSLogix, Dateiablage und WEM zuzugreifen. Ohne diese Kommunikation würden die Dienste nicht funktionieren

Intern-VLAN230: Diese Konfiguration ermöglicht überhaupt erst die Verbindung einer VDI vom internen Netz. Dabei werden die benötigten Ports sowohl vom Source-Netz ins VDI-Netz als auch umgekehrt akzeptiert

Intern-VLAN220-SF: Stellt sicher, dass die HTTP- und HTTPS-Kommunikation vom internen Netzwerk zu VLAN220 sowie umgekehrt akzeptiert wird

1	 VLAN-220-to-WAN in 26.38 GB, out 376.90 MB	TEST_Shipi, TEST-SHIPI WAN, Any host -VLAN-220...	DNS, HTTP, HTTPS, ICM #82 P, NTP_ser...	Accept	IPS AV WEB APP QoS HB LinkedNAT PRX LOG			
2	 VLAN-230-to-WAN in 35.85 MB, out 3.25 MB	TEST_Shipi, TEST-SHIPI WAN, *.nvidia.com -VLAN-230...	Any service	#90	Accept	IPS AV WEB APP QoS HB LinkedNAT PRX LOG		
3	 BernServer-to-VLAN... in 39.15 GB, out 25.07 GB	LAN, CATO, Bern1Client Subnet Bern...	TEST_Shipi, TEST-SHIPI -VLAN-220...	#83	Accept	IPS AV WEB APP QoS HB LinkedNAT PRX LOG		
4	 VLAN220-to-VLAN2... in 291.79 MB, out 218.70 MB	TEST_Shipi, TEST-SHIPI -VLAN-220...	TEST_Shipi, TEST-SHIPI -VLAN-230...	#86	Accept	IPS AV WEB APP QoS HB LinkedNAT PRX LOG		
5	 VLAN230-to-VLAN2... in 12.50 GB, out 2.27 GB	TEST_Shipi, TEST-SHIPI -VLAN-230...	TEST_Shipi, TEST-SHIPI -VLAN-220...	#87	Accept	IPS AV WEB APP QoS HB LinkedNAT PRX LOG		
6	 Intern-VLAN230 in 743.52 MB, out 41.04 MB	CATO, Bern1Clients, TES T_Shipi,...	CATO, Bern1Clients, TES T_Shipi,...	Citrix Session Reliability, #84 Cit...	Accept	IPS AV WEB APP QoS HB LinkedNAT PRX LOG		
7	 Intern-VLAN220-SF in 113 GB, out 112.03 MB	CATO, Bern1Clients, TES T_Shipi,...	CATO, Bern1Clients, TES T_Shipi,...	HTTP, HTTPS	#85	Accept	IPS AV WEB APP QoS HB LinkedNAT PRX LOG	

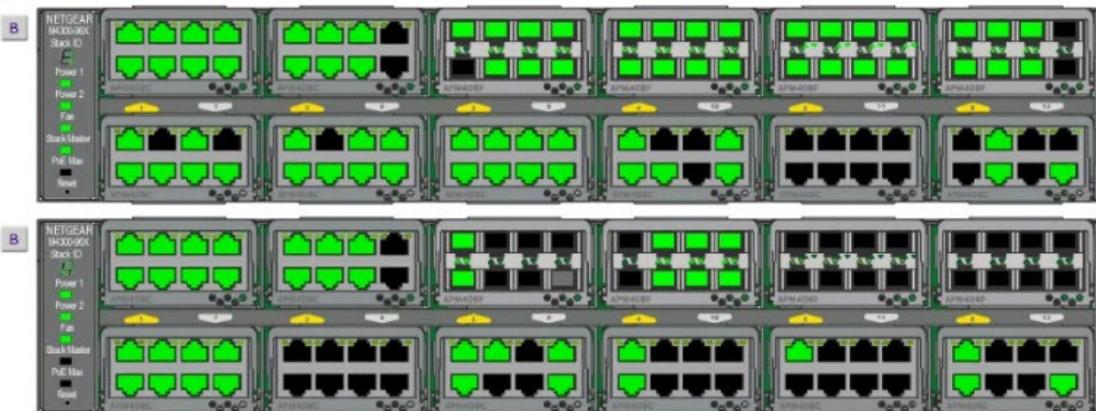
Netzwerk Zones

Bei der erstellen Netzwerk Zonen Ping aktivieren, damit das Troubleshooten der Netzwerkkommunikation einfacher geht.

Interfaces	Zones	WAN link manager	DNS	DHCP	IPv6 router advertisement	Cellular WAN	IP tunnels	Neighbors [ARP-NDP]	Dynamic DNS
Edit zone									
Name *	TEST_Ship1								
Description	Enter description								
Type	LAN								
Members	TEST-MGMT , TEST-VDI								
Device access	Admin services <input type="checkbox"/> HTTPS <input checked="" type="checkbox"/> SSH Authentication services <input type="checkbox"/> Client authentication <input type="checkbox"/> Captive portal <input type="checkbox"/> AD SSO <input type="checkbox"/> RADIUS SSO <input type="checkbox"/> Chromebook SSO Network services <input type="checkbox"/> DNS <input checked="" type="checkbox"/> Ping/ping6 Other services <input type="checkbox"/> Web proxy <input type="checkbox"/> SSL VPN tunnel <input type="checkbox"/> Wireless protection <input type="checkbox"/> User portal <input type="checkbox"/> Dynamic routing <input type="checkbox"/> SNMP <input type="checkbox"/> SMTP relay								

Switch Konfiguration

Bevor die Server und Speichereinheiten an den Switch angeschlossen werden können, müssen zunächst alle Ports definiert und konfiguriert werden. Diese Spezifikationen wurden im Detailkonzept festgelegt und beim Drittanbieter angefragt. Bei der Konfiguration eines Ports ist es wichtig zu bestimmen, ob er als "tagged" mit den entsprechenden VLANs oder als "untagged" mit einem spezifischen VLAN konfiguriert wird.



M4300-48X



Komponenten Patchen

Alle verfügbaren Komponenten wurden gemäss Patchliste gepatcht. Diese Komponenten sind auf zwei Standorte verteilt. Somit mussten man manchmal auswärts ins Rechenzentrum von Swisscom, um etwas umzustecken.

Einige Komponenten waren schon gepatcht und mussten nur umgesteckt werden und andere musste man neu verkabeln.

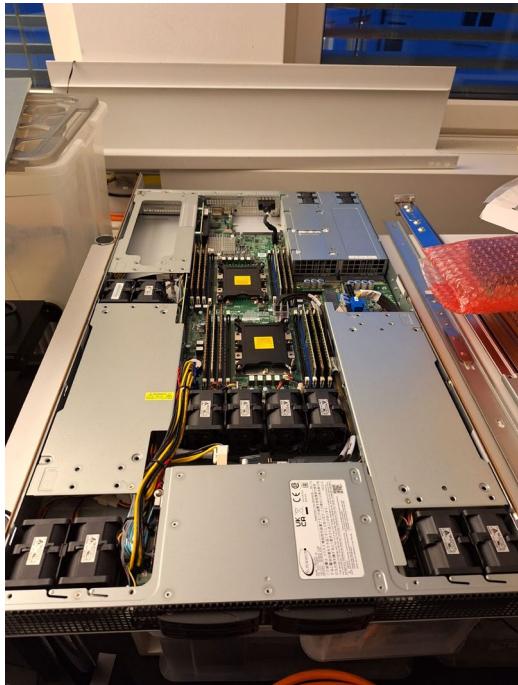


3 Aufbau MGMT-Server

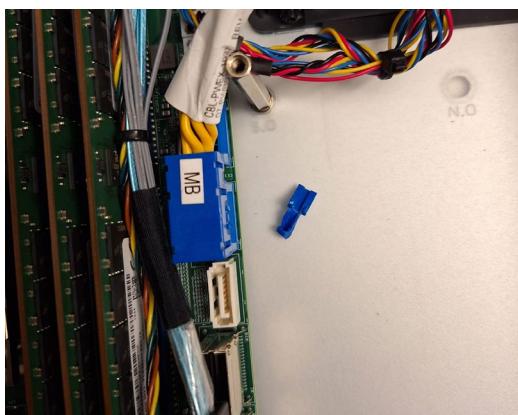
Der Management Server ist eine zentrale Komponente, ohne die der gesamte Service nicht funktionieren würde. Auf ihm laufen alle virtuellen Management-Server, die verschiedene wichtige Dienste verwalten. Aufgrund seiner Bedeutung wurde während der Konzeptphase entschieden, einen zweiten Management-Server zu integrieren, um die wichtigen Dienste redundant betreiben zu können.

Hardwareaufbau

Der Haupt MGMT Server ist ein Mix von Hardware von verschiedenem früherem Nutzen und wurde mit verschiedenen neuen Komponenten aufgerüstet. Beispielsweise besitzt dieser MGMT-Server auch eine Grafikkarte, was normalerweise bei einem MGMT-Server nicht üblich ist.



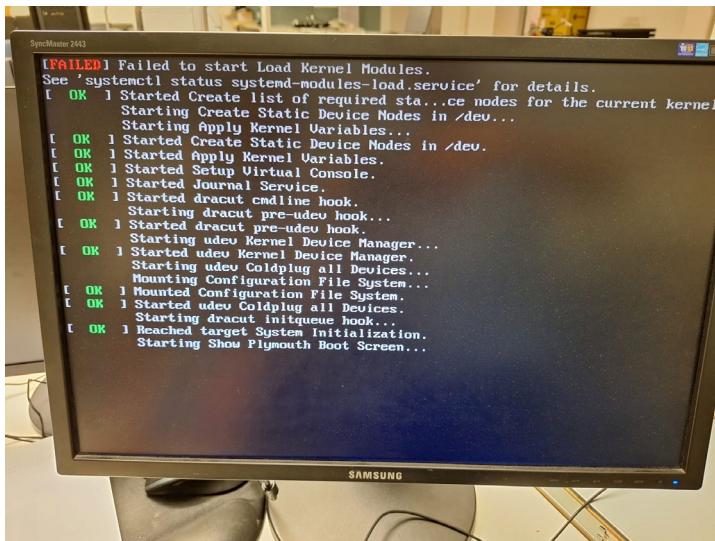
Beim Aufbau verlief das meiste reibungslos. Der Einbau der Grafikkarte gestaltete sich jedoch nicht ganz selbsterklärend, da er nicht einfach durch Einsticken erfolgen konnte. Aufgrund von Abhängigkeiten mit der Reihenfolge des Einbaus der Netzwerkkarte erwies sich dieser Schritt als zeitintensiver als erwartet. Des Weiteren kam es zu Platzproblemen zwischen der Grafikkarte und dem Stromkabel, weshalb letztendlich ein Teil des Stromkabels abgebrochen werden musste.



XenServer Installation

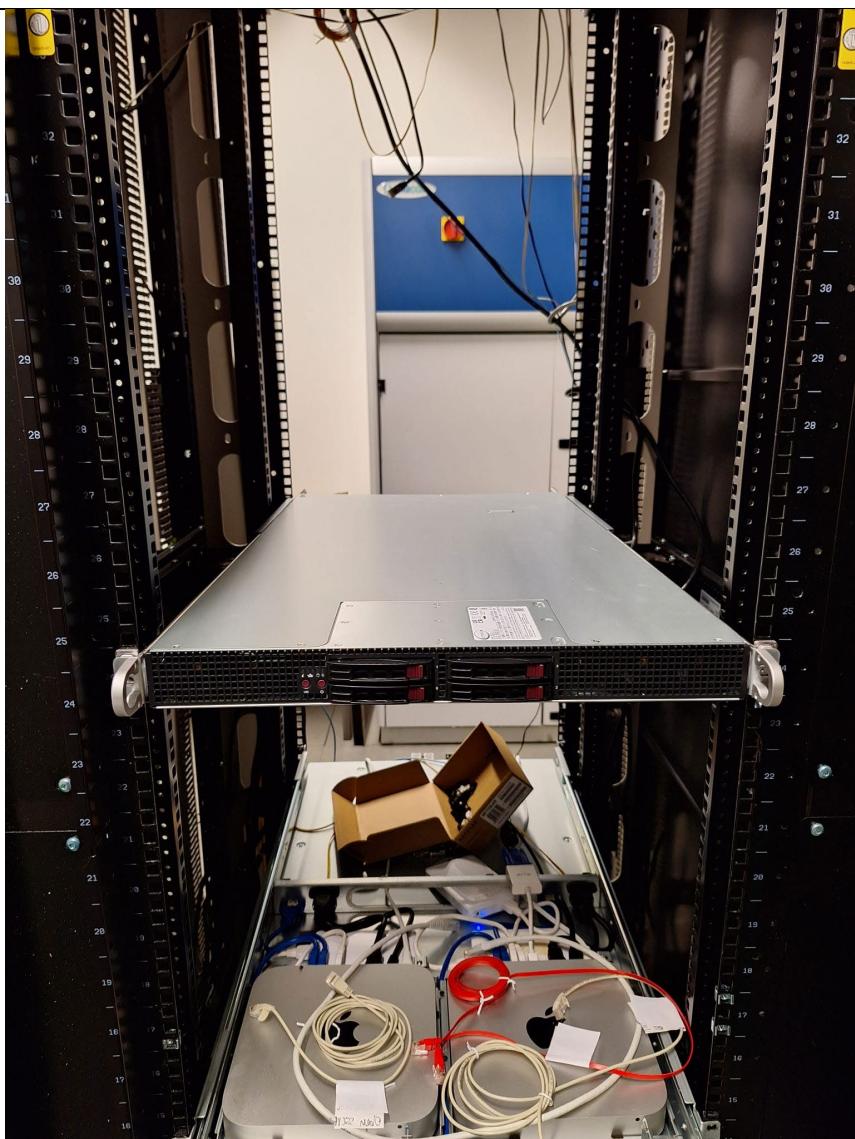
Nach dem erfolgreichen Aufbau des Servers konnte der Hypervisor XenServer installiert werden. Es wurden dabei keine speziellen Einstellungen vorgenommen.

Bei der Fertigstellung kam zwar ein Fehler, jedoch konnte man dies gemäss Experten ignorieren.



Einbau des MGMT-Servers

Nach der fertigen Konfiguration des MGMT-Servers und der Switches konnte man den MGMT-Server im internen Rack einbauen gehen.



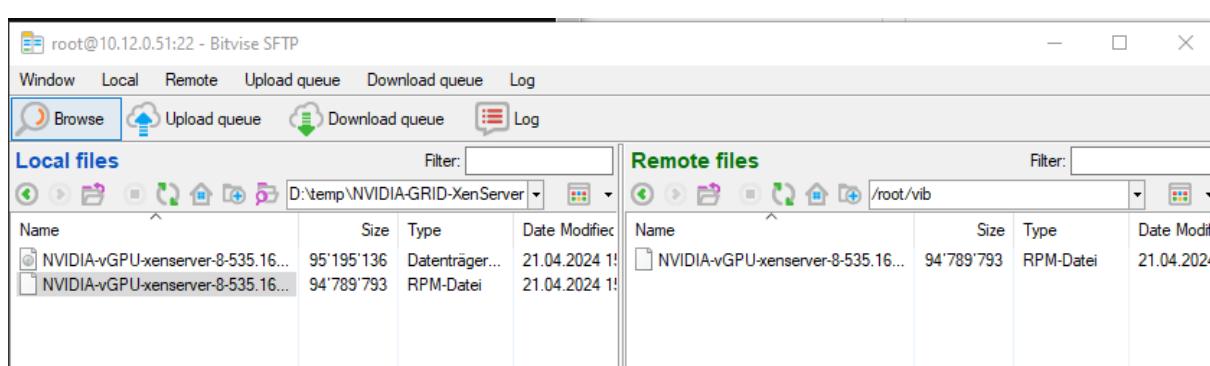
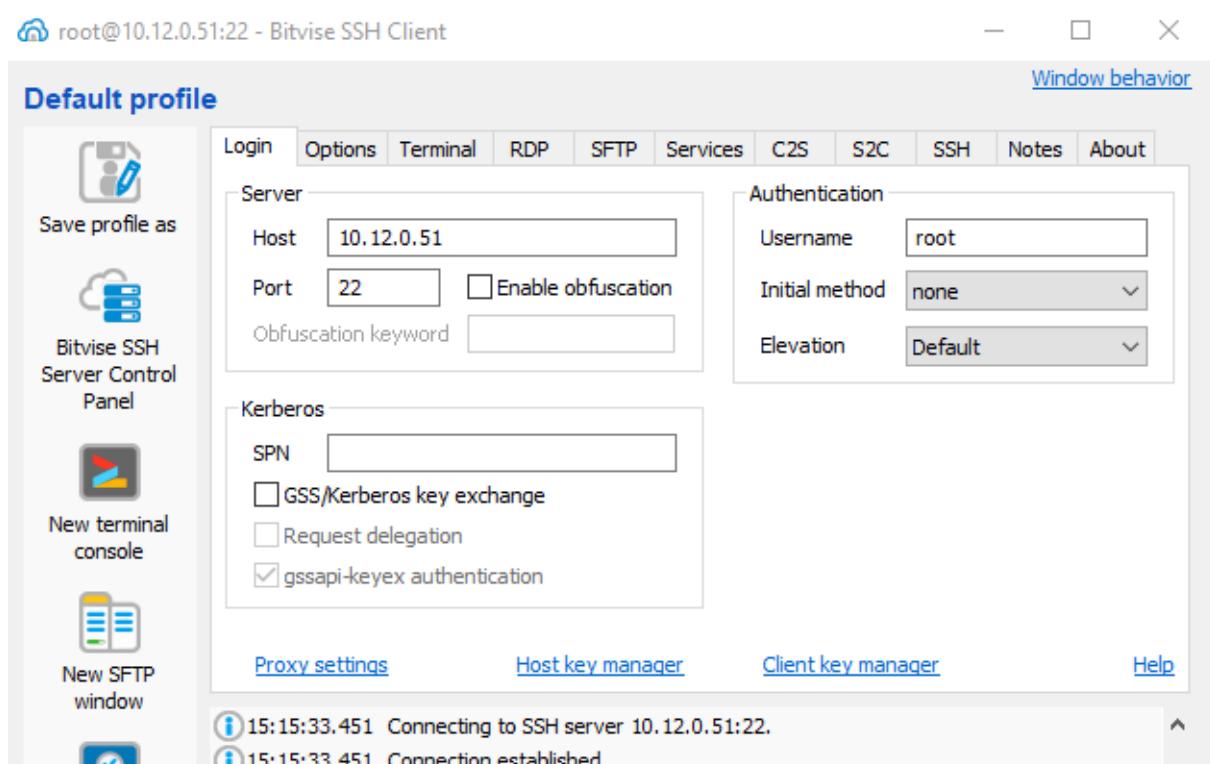
4 Konfiguration MGMT-Server

Nach dem vollständigen Aufbau des MGMT-Servers können die notwendigen Konfigurationen vorgenommen werden. Diese sollten idealerweise abgeschlossen sein, bevor der Server im Rechenzentrum installiert wird.

Konfiguration XenServer

Der XenServer wurde zuerst im internen LAN mit DHCP konfiguriert, bevor er mit den richtigen IP-Adressen konfiguriert wurde.

Mit SSH und SFTP auf den XenServer verbinden, um den Nvidia Treiber zu installieren.



```
root@10.12.0.51:22 - Bitvise xterm - root@localhost:~/vib
Last login: Tue Apr 9 03:06:20 2024
[root@localhost ~]# ls
vib
[root@localhost ~]# cd vib/
[root@localhost vib]# ls
NVIDIA-vGPU-xenserver-8-535.161.05.x86_64.rpm
[root@localhost vib]# rpm -iv NVIDIA-vGPU-xenserver-8-535.161.05.x86_64.rpm
warning: NVIDIA-vGPU-xenserver-8-535.161.05.x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID c10d7
2e3: NOKEY
Preparing packages...
NVIDIA-vGPU-xenserver-1:8-535.161.05.x86_64
[root@localhost vib]#
```

```
root@10.12.0.51:22 - Bitvise xterm - root@localhost:~
Last login: Sun Apr 21 17:15:52 2024 from 10.12.0.80
[root@localhost ~]# nvidia-smi
Sun Apr 21 17:33:45 2024
+-----+
| NVIDIA-SMI 535.161.05      Driver Version: 535.161.05    CUDA Version: N/A |
+-----+
| GPU  Name        Persistence-M | Bus-Id     Disp.A  Volatile Uncorr. ECC | | |
| Fan  Temp  Perf  Pwr:Usage/Cap | Memory-Usage | GPU-Util  Compute M. |
|                               |             |            | MIG M. |
+-----+
|  0  NVIDIA A16      On           00000000:8A:00.0 Off   0 |
|  0%   39C   P8    15W / 62W   0MiB / 15356MiB   0%   Default |
|                               |             |            | N/A |
+-----+
|  1  NVIDIA A16      On           00000000:8B:00.0 Off   0 |
|  0%   41C   P8    15W / 62W   0MiB / 15356MiB   0%   Default |
|                               |             |            | N/A |
+-----+
|  2  NVIDIA A16      On           00000000:8C:00.0 Off   0 |
|  0%   32C   P8    14W / 62W   0MiB / 15356MiB   0%   Default |
|                               |             |            | N/A |
+-----+
|  3  NVIDIA A16      On           00000000:8D:00.0 Off   0 |
|  0%   30C   P8    15W / 62W   0MiB / 15356MiB   0%   Default |
|                               |             |            | N/A |
+-----+
| Processes:          GPU Memory |
|          CI      PID  Type    name                Usage  |
|             ID      ID   |
+-----+
| No running processes found
+-----+
[root@localhost ~]#
```

Netzwerk Konfiguration

Die Netzwerkkonfiguration stellte sich als die grösste Herausforderung bei der Einrichtung des MGMT-Servers dar. Da effektiv nur zwei LAN-Anschlüsse zur Verfügung standen, aber drei VLANs genutzt wurden, musste mit getaggeten Switch-Ports gearbeitet werden. Dabei wurde das VLAN softwareseitig aufgeteilt. Anfangs wurde dies über die Shell versucht, was manchmal funktionierte, jedoch nicht immer stabil war. Nach mehreren Anläufen wurde die Trennung ausschliesslich über den XenCenter durchgeführt, woraufhin die Konfiguration stabil war und funktioniert hat.

Es ist wichtig zu definieren, welches der VLANs als Management-Interface dient. Dadurch ist es nicht nötig, Einstellungen über die Shell oder direkt am XenServer netzwerktechnisch vorzunehmen, sondern dies kann bequem über den XenCenter eingerichtet werden

Server	Interface	Network	NIC	IP Setup	IP Address	Subnet mask	Gateway	DNS
xen-mgmt-01	Management	MGMT-VLAN 220	NIC 1	Static	192.168.220.10	255.255.255.0	192.168.220.1	192.46.181.4
xen-mgmt-01	NFS	Network 0	NIC 0	Static	192.168.210.10	255.255.255.0	192.168.210.1	192.46.181.4

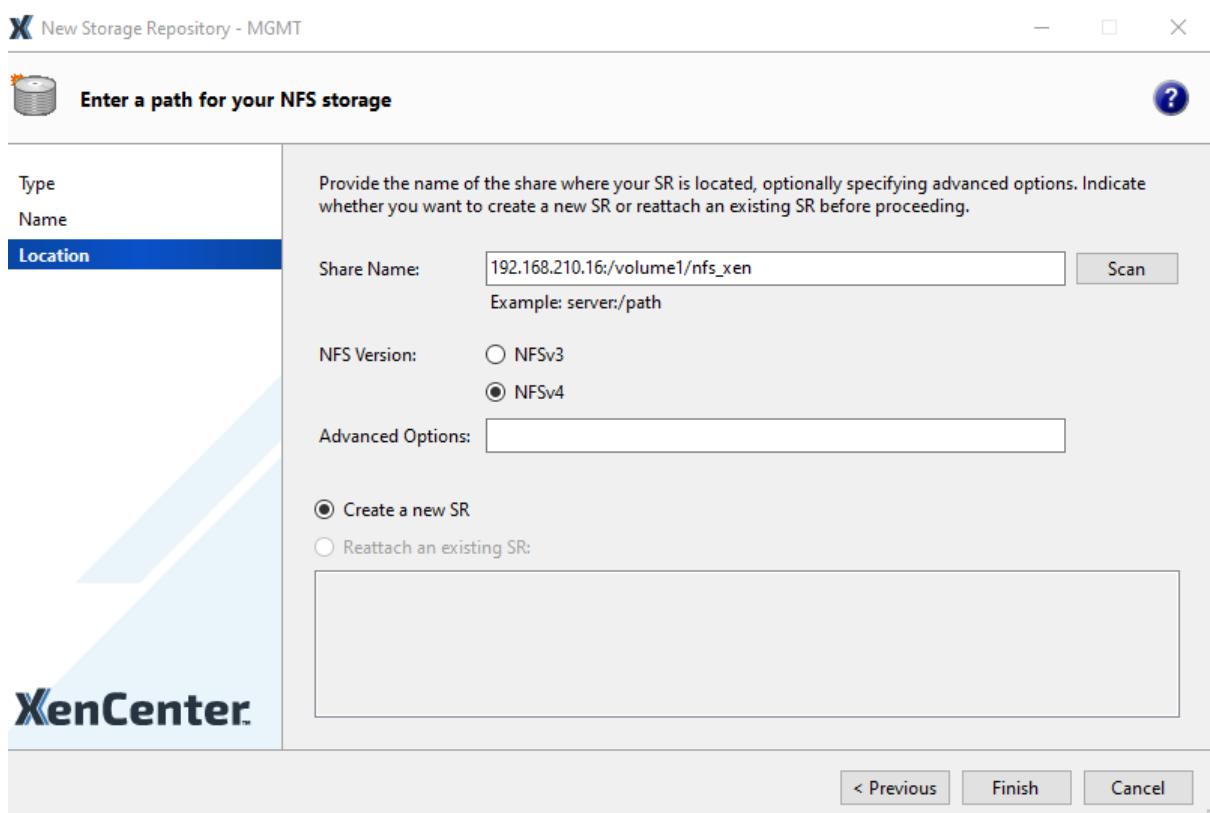
Nach der Netzwerkkonfiguration musste temporär die DNS 8.8.8.8 eingetragen werden, damit der XenServer online Updates ziehen konnte. Da die neuen DCs noch nicht existieren.

Updates available at last synchronization	Update channel	Last synchronized	Last i
xen-mgmt-01	Normal	Apr 30, 2024 12:49:49 PM	Never

NFS einbinden

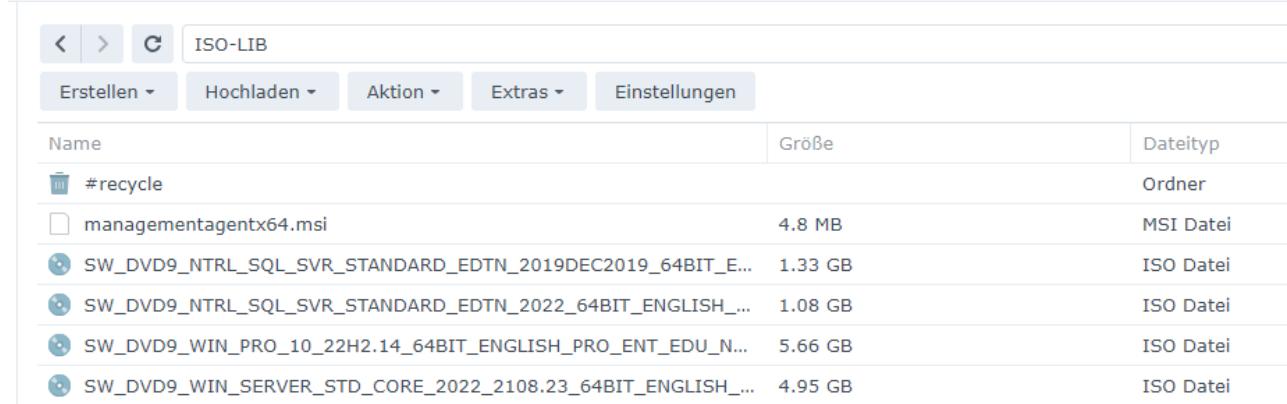
Mit den fertigen Grundkonfigurationen können nun die ersten VMs erstellt werden, die später als virtuelle MGMT-Server für verschiedene Dienste dienen. Dafür sind jedoch einige Vorbereitungen nötig. Dazu gehört das Hinzufügen des Hauptspeichers als Speicherort der VMs sowie das Erstellen einer ISO-Library für die Installationsmedien. Die Schritte der Erstellung werden im nächsten Kapitel „Konfiguration Hauptspeichers“ beschrieben.

Nach der Erstellung der NFS-Shares kann man diese Shares als NFS-Storage anbinden.



The screenshot shows the 'NFS ISO-LIB in 'MGMT'' properties dialog in XenCenter. The 'General' tab is selected. The 'Storage General Properties' section is visible. The 'Properties' button is highlighted. The 'General' table includes the following data:

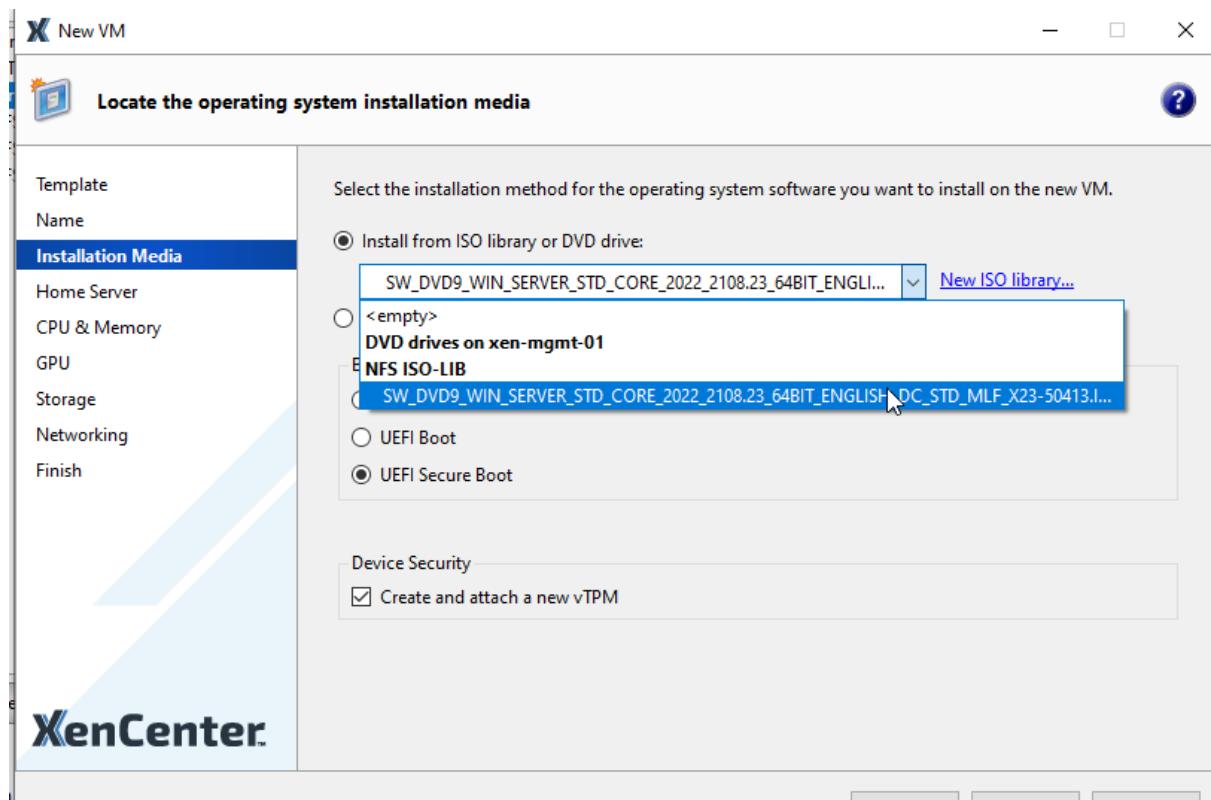
Name:	NFS ISO-LIB
Description:	NFS ISO Library [192.168.210.16:/volume1/ISO-LIB]
Tags:	<None>
Folder:	<None>
Type:	ISO
UUID:	e786d7d9-e98c-8c07-17ec-809ba961d2b1



The screenshot shows a software interface titled "ISO-LIB". At the top, there are navigation buttons: back, forward, and refresh, followed by a dropdown menu labeled "ISO-LIB". Below the menu are five tabs: "Erstellen", "Hochladen", "Aktion", "Extras", and "Einstellungen". The main area is a table with three columns: "Name", "Größe", and "Dateityp". The table lists several ISO files:

Name	Größe	Dateityp
#recycle		Ordner
managementagentx64.msi	4.8 MB	MSI Datei
SW_DVD9_NTRL_SQL_SVR_STANDARD_EDTN_2019DEC2019_64BIT_E...	1.33 GB	ISO Datei
SW_DVD9_NTRL_SQL_SVR_STANDARD_EDTN_2022_64BIT_ENGLISH_...	1.08 GB	ISO Datei
SW_DVD9_WIN_PRO_10_22H2.14_64BIT_ENGLISH_PRO_ENT_EDU_N...	5.66 GB	ISO Datei
SW_DVD9_WIN_SERVER_STD_CORE_2022_2108.23_64BIT_ENGLISH_...	4.95 GB	ISO Datei

Gewünschte ISOs auf den Speicher hochladen, damit sie später im XenCenter zur Verfügung stehen.



Die ersten VMs erstellen

Nun sind alle Voraussetzungen erfüllt, um die ersten VMs zu erstellen. Diese werden gemäss den im Detailkonzept festgelegten Ressourcen konfiguriert. Nachfolgend wird der Prozess zur Erstellung des ersten Domain Controllers dargestellt.

XenCenter

File View Pool Server VM Storage Templates Tools Help

Back Forward Add New Server New Pool New Storage New VM Shut Down Reboot Suspend

xen-mgmt-01 in 'MGMT' (Licensed with XenServer Trial Edition)

General Memory Storage Networking NICs GPU Console Performance Search

New VM

Name the new virtual machine

Template Name

Installation Media

Home Server

CPU & Memory

GPU

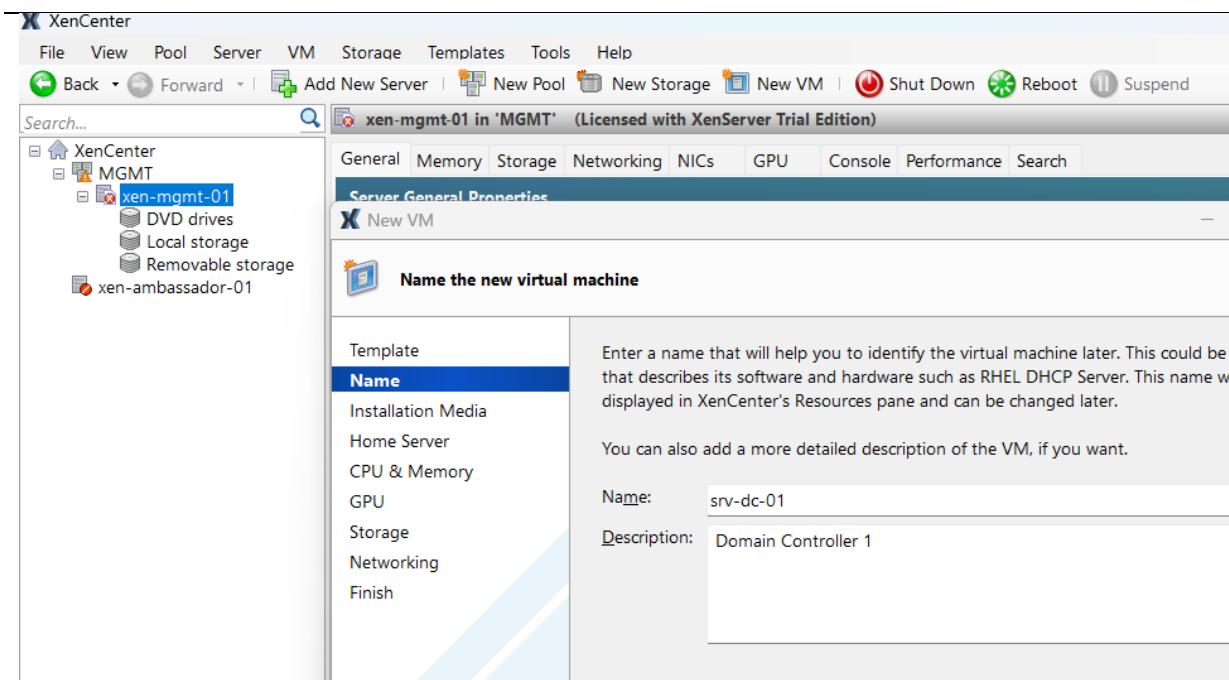
Storage

Networking

Finish

Name: srv-dc-01

Description: Domain Controller 1



New VM

Locate the operating system installation media

Template Name

Installation Media

Home Server

CPU & Memory

GPU

Storage

Networking

Finish

Install from ISO library or DVD drive:

SW_DVD9_WIN_SERVER_STD_CORE_2022_2108.23_64BIT_ENGLI...

<empty>

DVD drives on xen-mgmt-01

NFS ISO-LIB

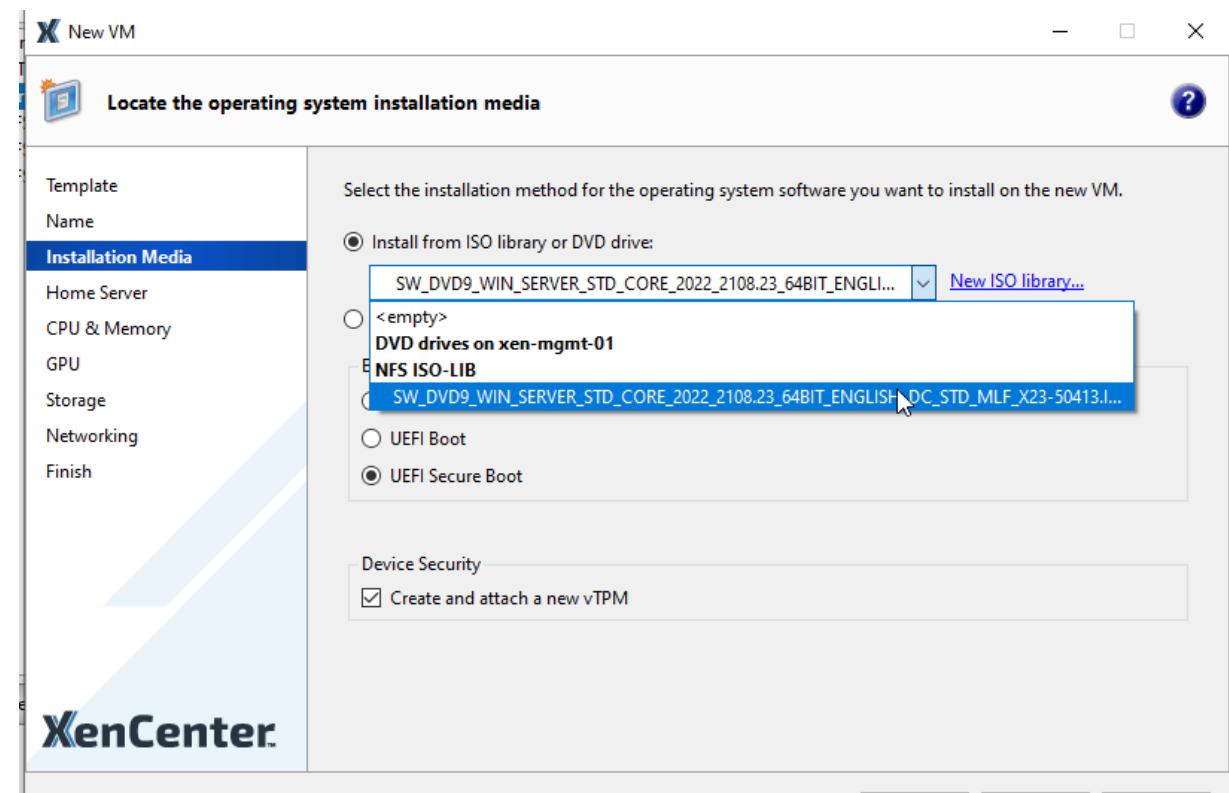
SW_DVD9_WIN_SERVER_STD_CORE_2022_2108.23_64BIT_ENGLISH_DC_STD_MLF_X23-50413.i...

UEFI Boot

UEFI Secure Boot

Device Security

Create and attach a new vTPM

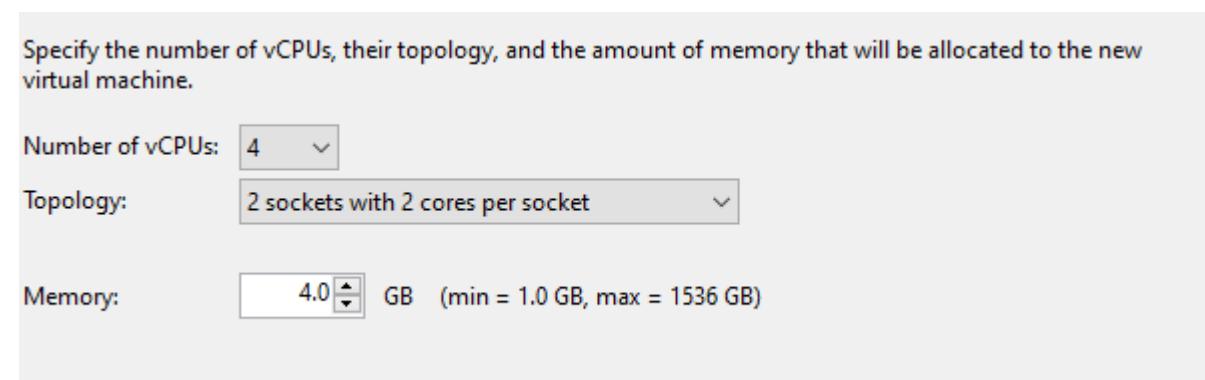


Specify the number of vCPUs, their topology, and the amount of memory that will be allocated to the new virtual machine.

Number of vCPUs: 4

Topology: 2 sockets with 2 cores per socket

Memory: 4.0 GB (min = 1.0 GB, max = 1536 GB)



When you have finished configuring disks for the new virtual machine, click Next to continue to the next step.

Use these virtual disks:

Name	Location	Size	Shared	
srv-dc-01 0	NFS XEN-VDI	100 GB	True	<input type="button" value="Edit..."/>

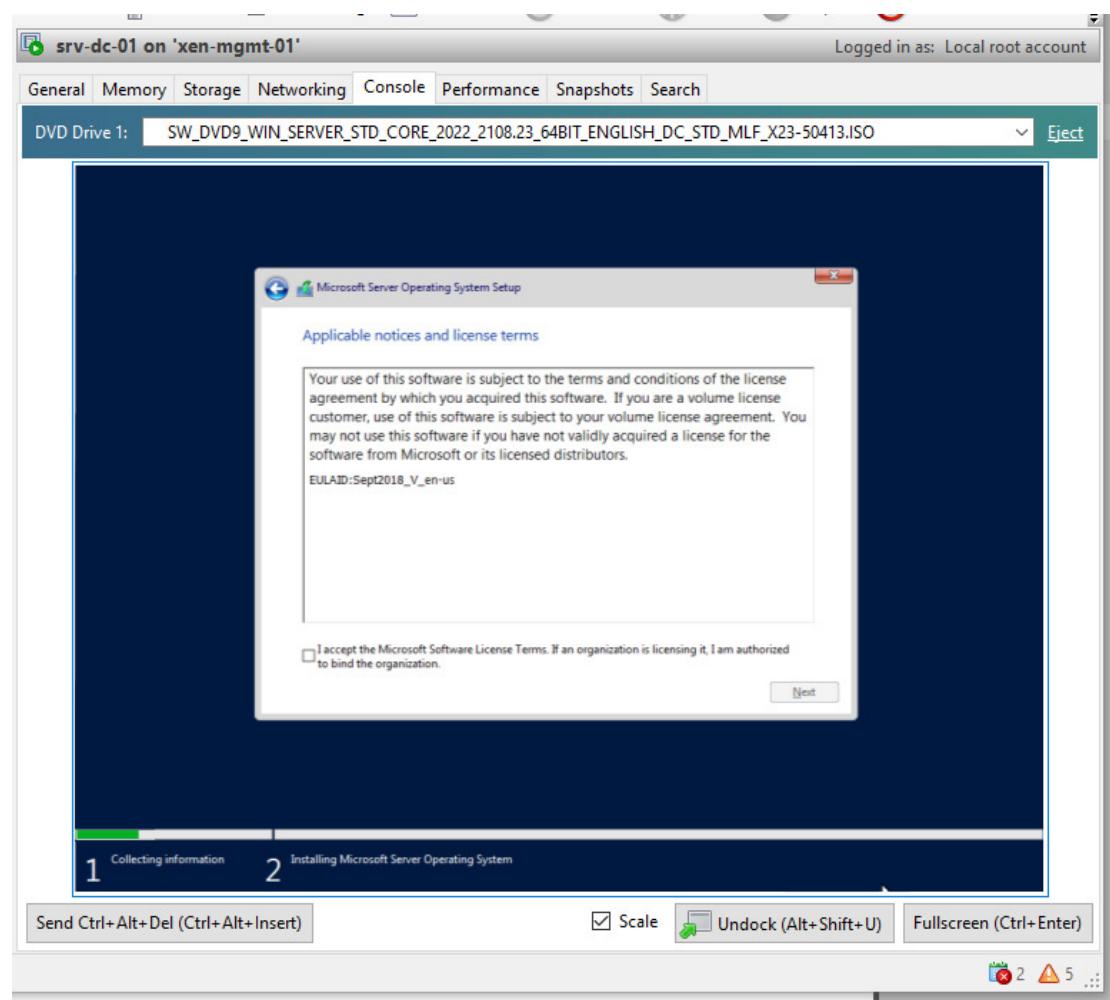
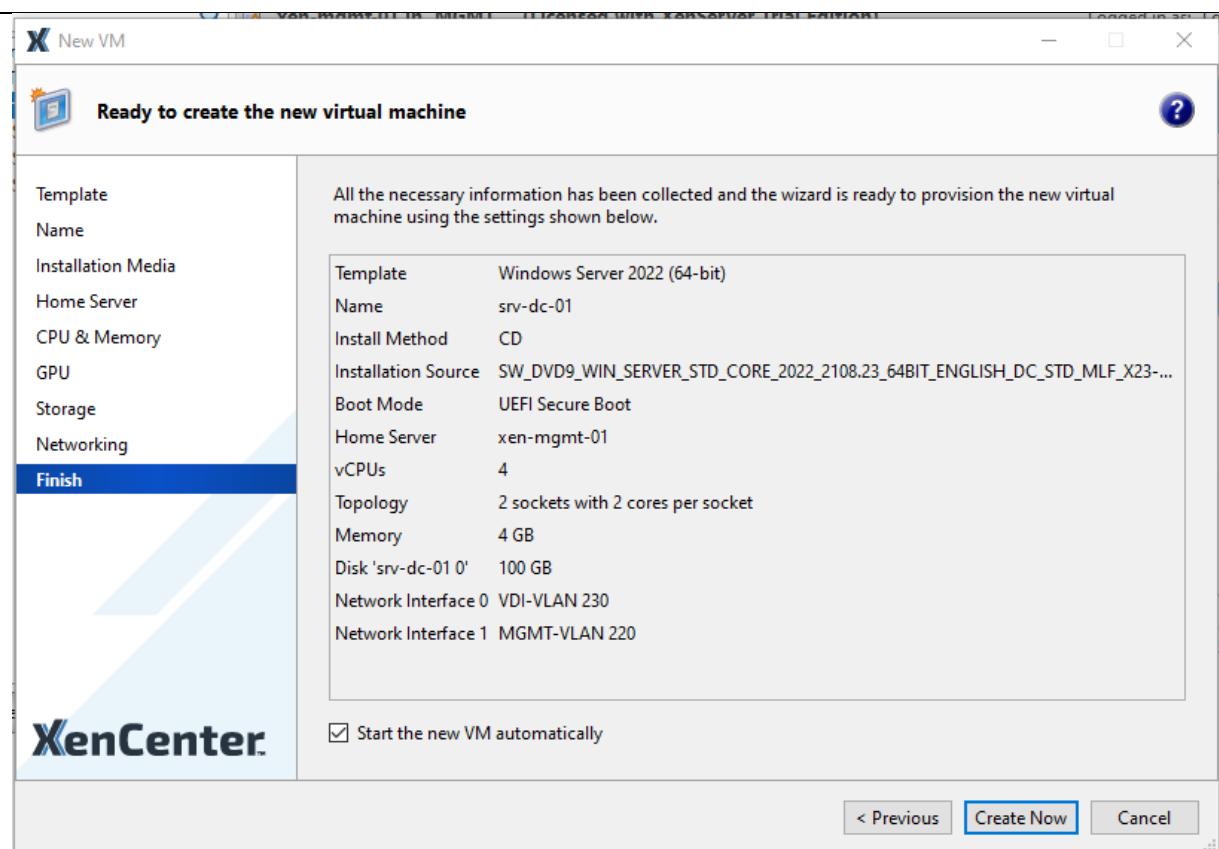
Create a diskless VM that boots from the network

The virtual machine template you have selected provides the virtual network interfaces listed below. You can configure or delete the default virtual network interfaces here, and add more if required.

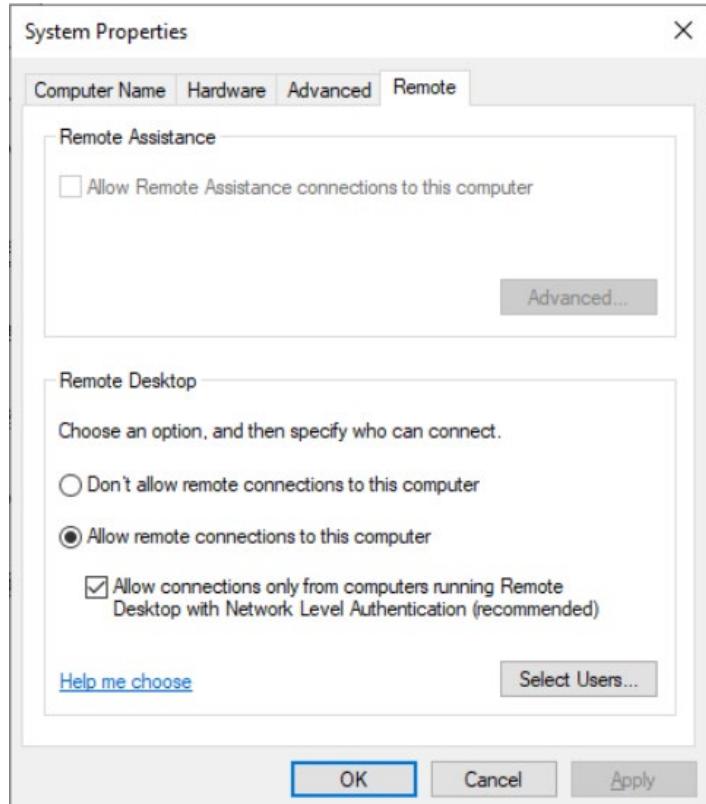
Virtual network interfaces on srv-dc-01

MAC	Network	
 <autogenerated MAC>	VDI-VLAN 230	<input type="button" value="Edit..."/>
 <autogenerated MAC>	MGMT-VLAN 220	<input type="button" value="Delete"/>

- i** Using a Default template, you can configure up to 4 virtual network interfaces during VM creation. To configure more than 4, create a Custom template or add extra virtual network interfaces from the Network tab after creating the new VM.



Sobald die VM bereit ist, kann sie gestartet werden. Durch Drücken einer beliebigen Taste wird der Bootvorgang von der verbundenen DVD-Drive mit dem eingelegten ISO gestartet. Nach Abschluss der Windows-Installation müssen die Netzwerkkonfigurationen eingerichtet werden. Sobald die VM im richtigen Netzwerk konfiguriert ist, kann mit weiteren Einstellungen fortgefahren werden, wie etwa dem Ändern des Hostnamens, dem Beitritt zur Domäne, der Aktivierung von RDP und der Installation der gewünschten Dienste.

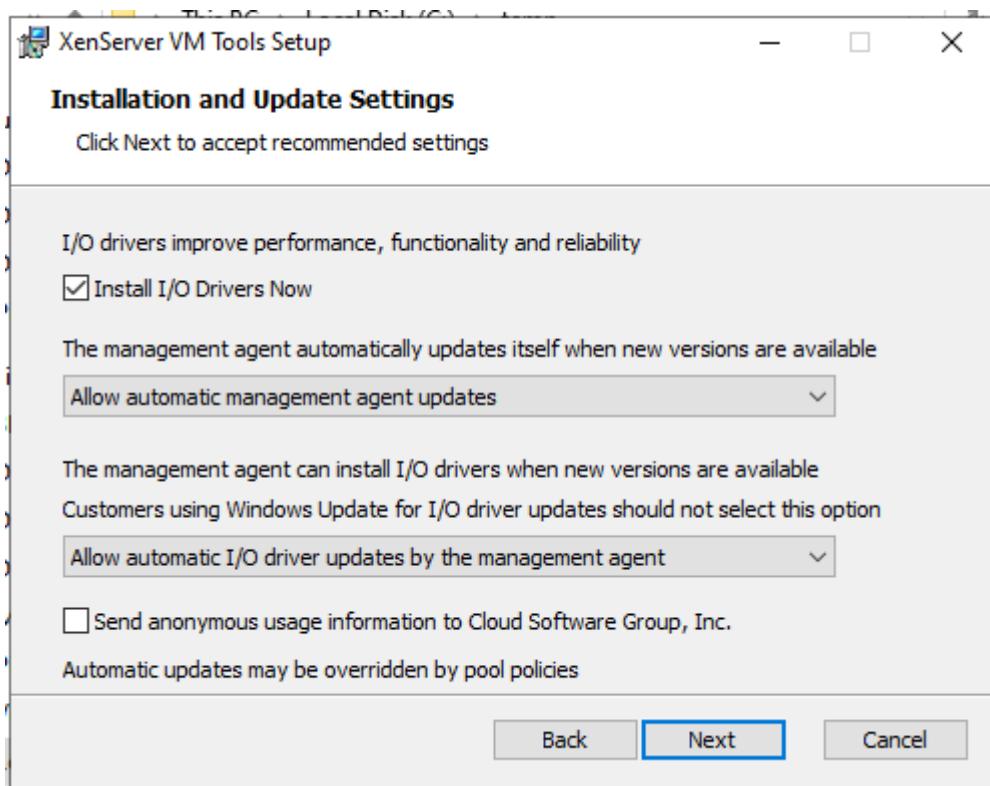


```
Administrator: C:\Windows\system32\cmd.exe
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 2A-45-CB-B7-8E-BF
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8849:9434:242e:ea81%6(Preferred)
IPv4 Address. . . . . : 192.168.220.27(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.220.1
DHCPv6 IAID . . . . . : 103433675
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-C1-B8-1E-2A-45-CB-B7-8E-BF
DNS Servers . . . . . : 192.168.230.20
                                         192.168.230.21
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet 2:

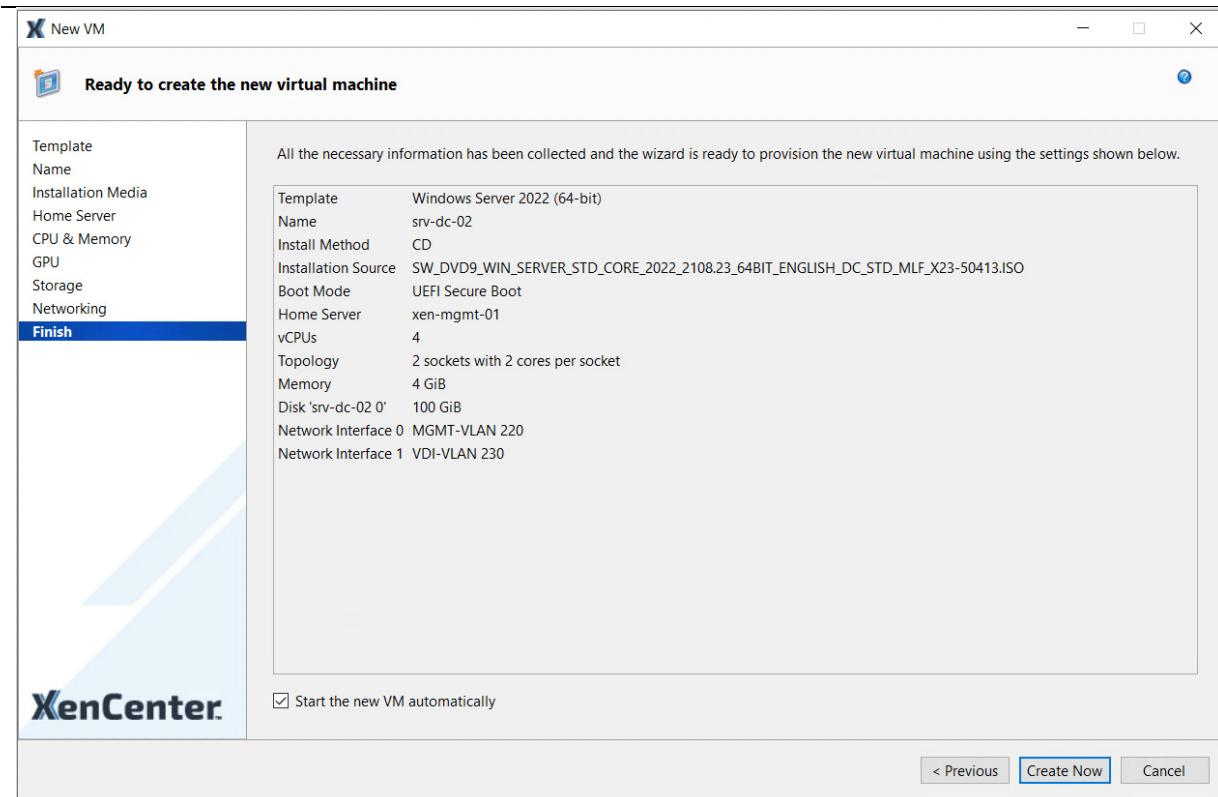
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection #2
Physical Address. . . . . : 66-49-BB-22-78-69
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::101c:790f:cf4c:fd29%3(Preferred)
IPv4 Address. . . . . : 192.168.230.20(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.230.1
DHCPv6 IAID . . . . . : 174475707
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-C1-B8-1E-2A-45-CB-B7-8E-BF
DNS Servers . . . . . : 192.168.230.20
                                         192.168.230.21
```

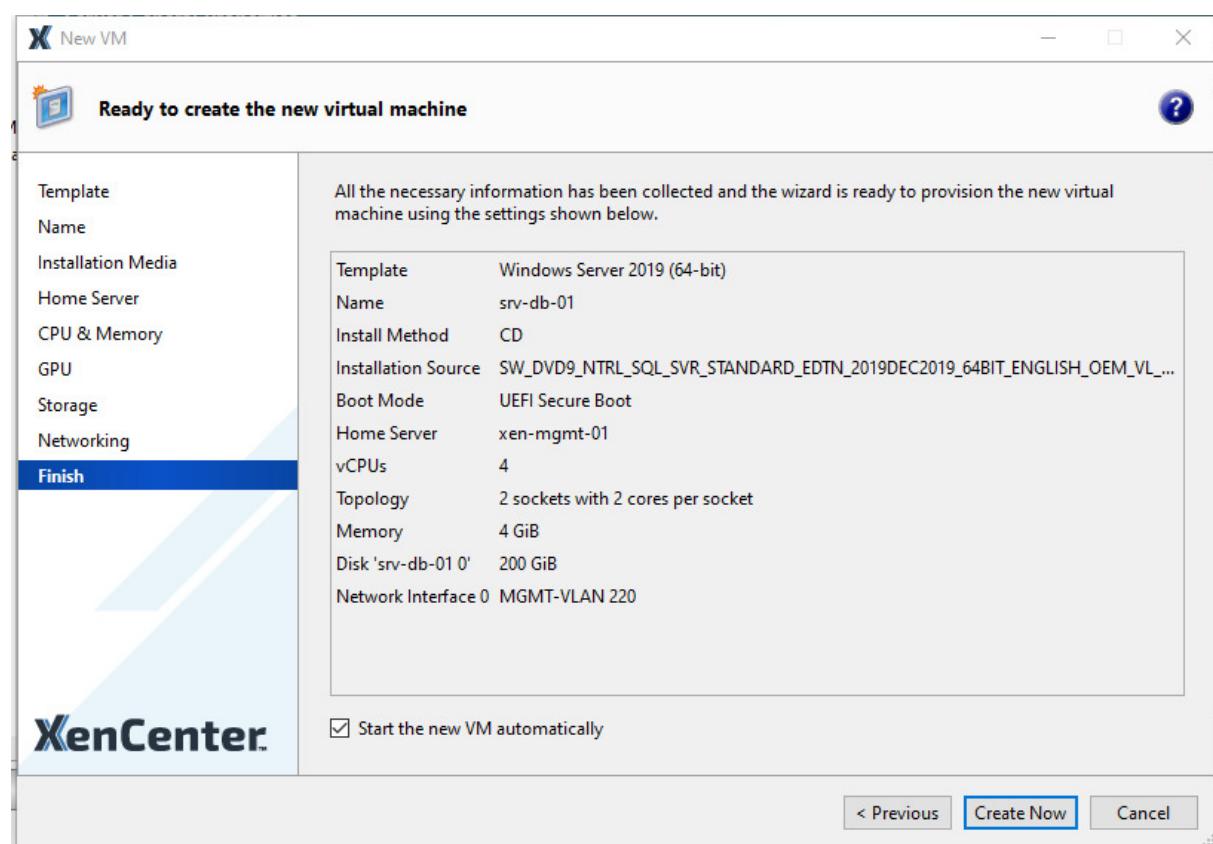
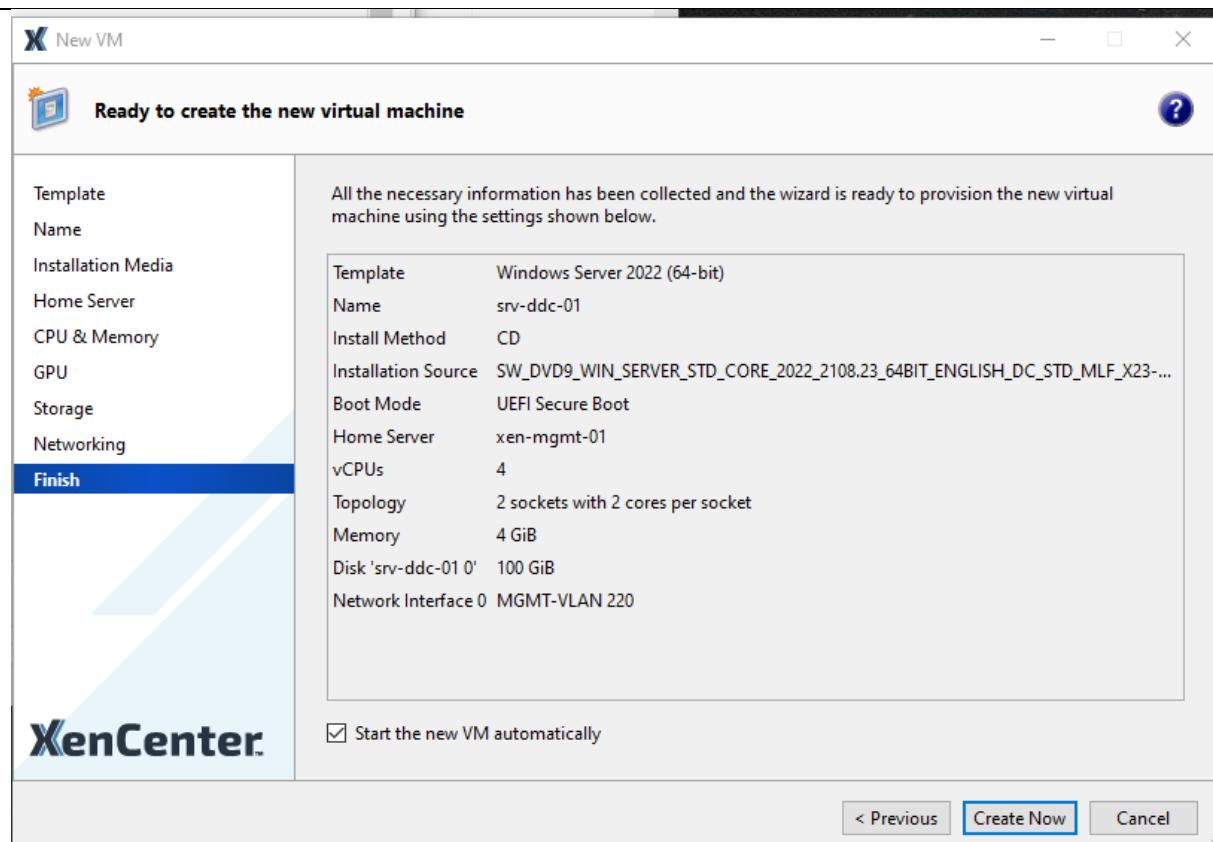
Des Weiteren können Citrix Tools wie VM-Tools installiert werden.

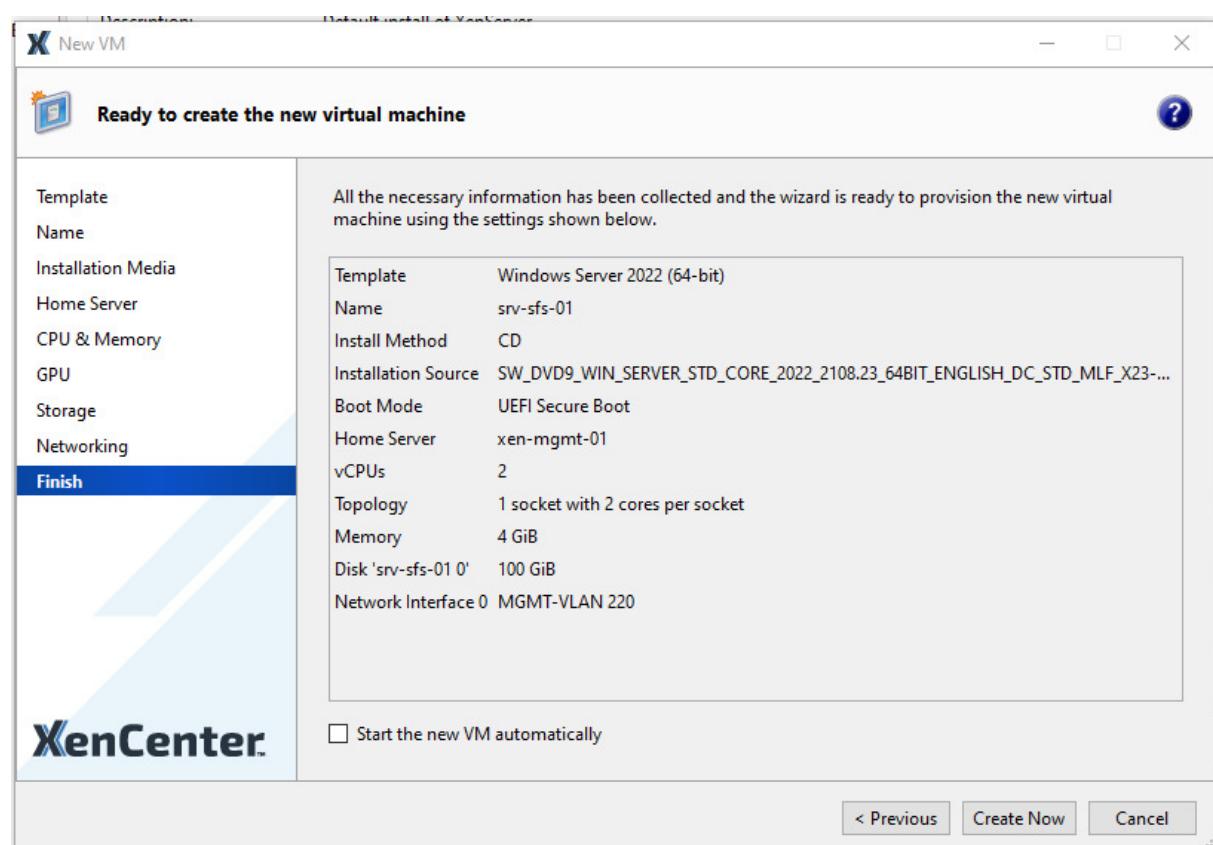
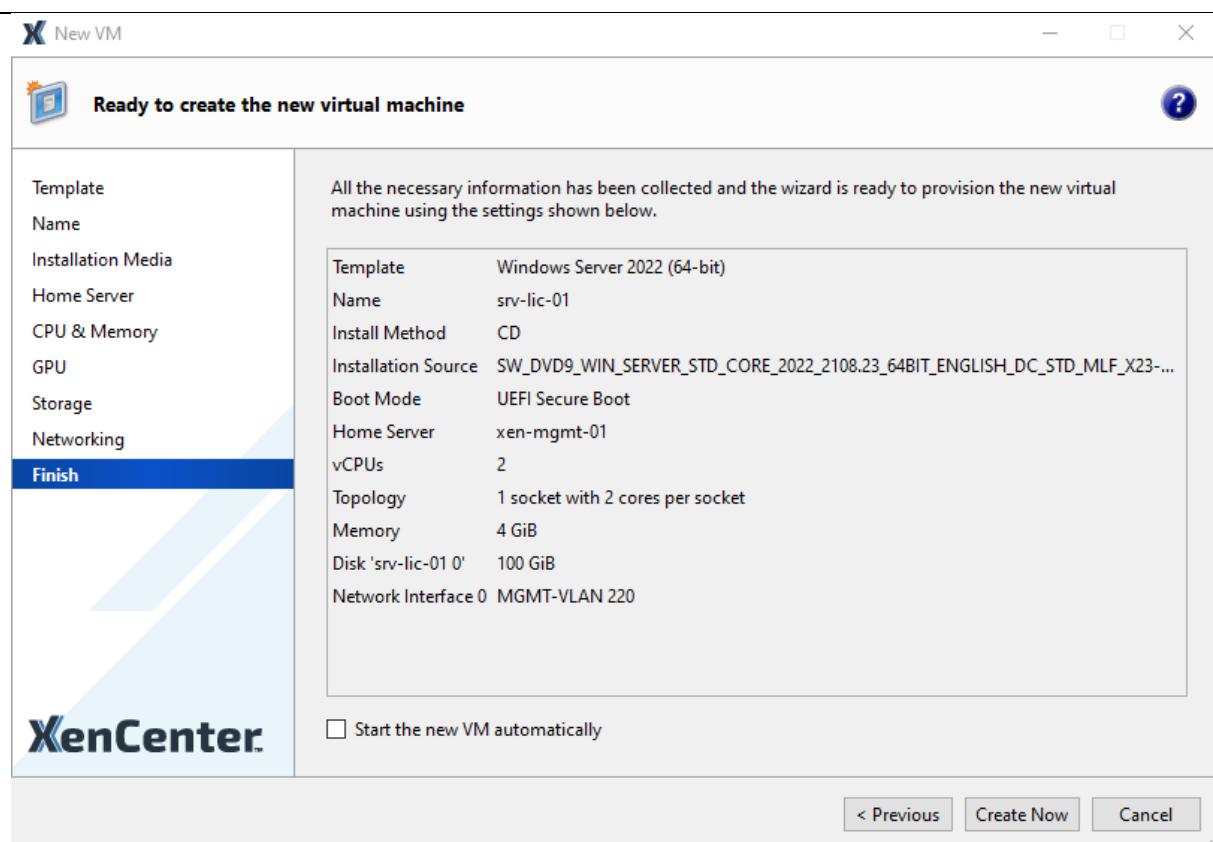


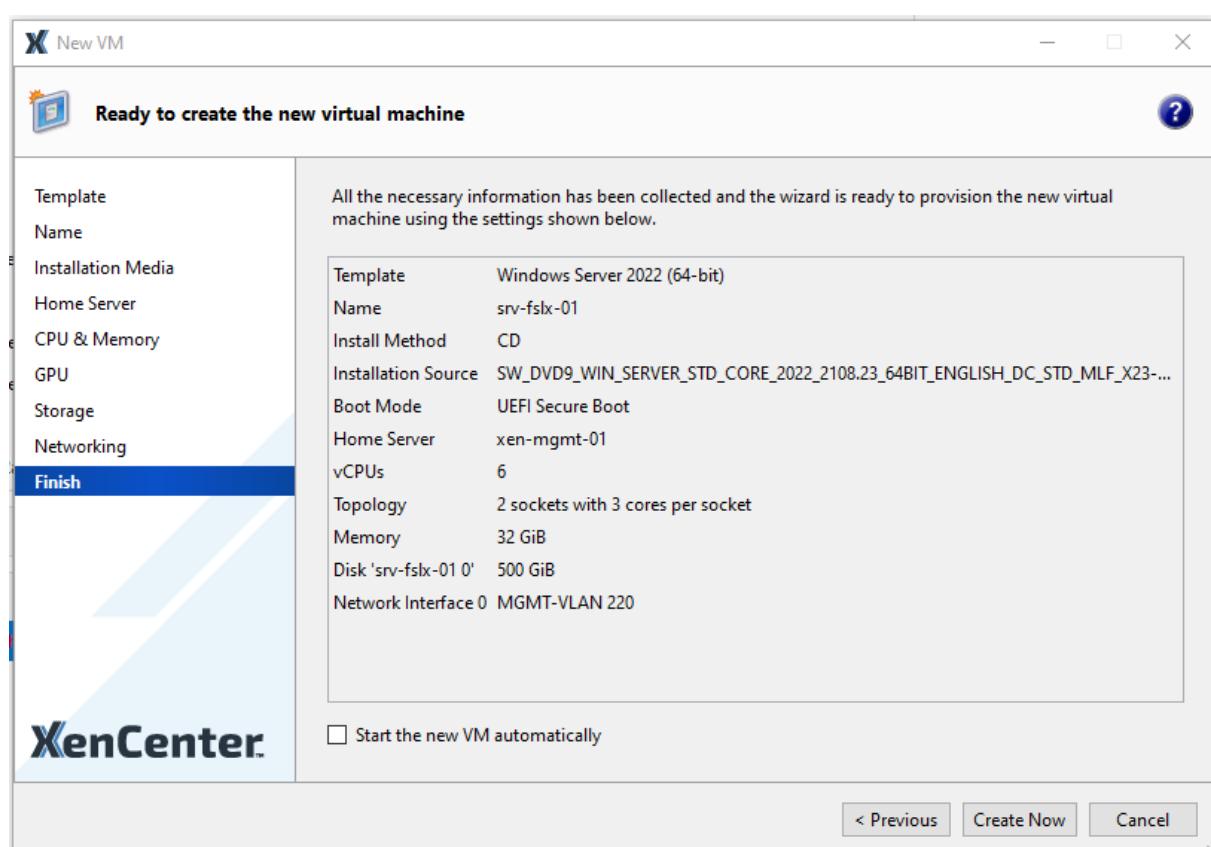
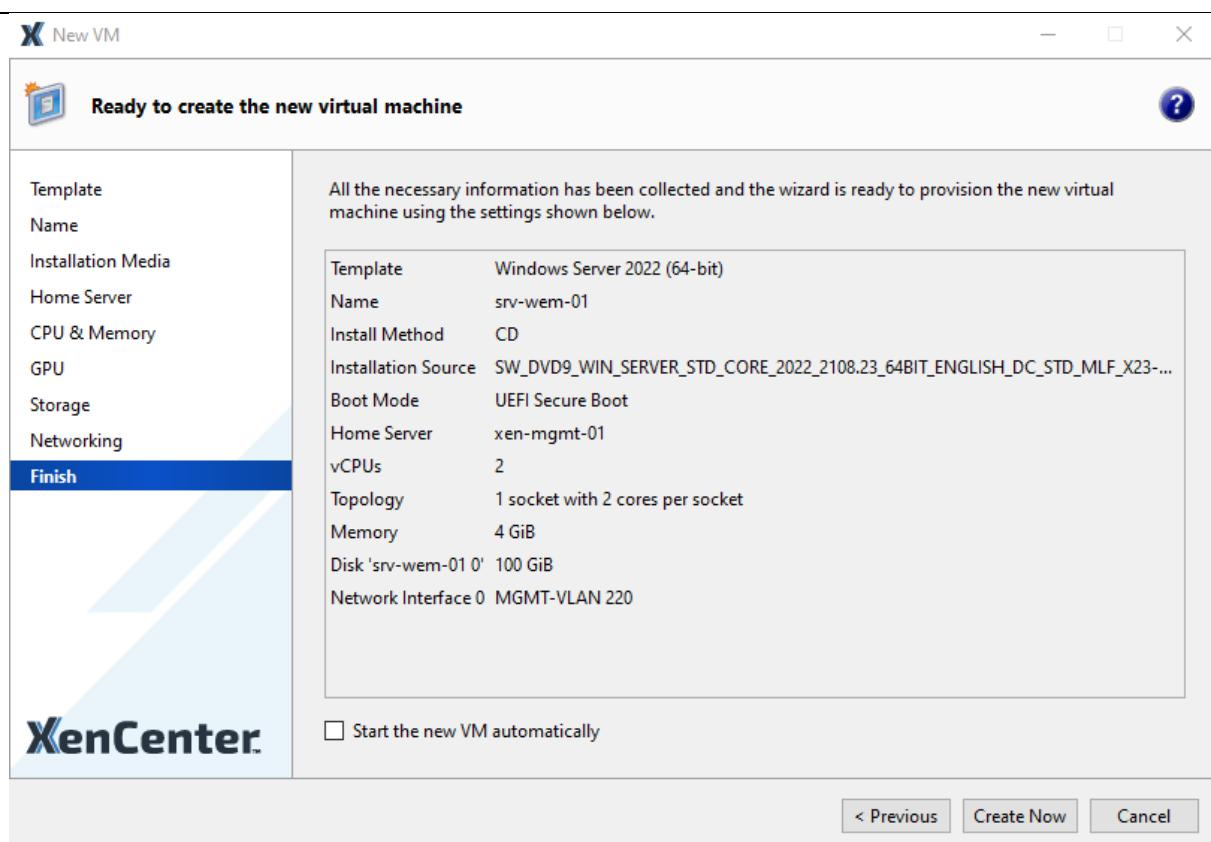
<https://docs.xenserver.com/en-us/xenserver/8/vms/windows/vm-tools>

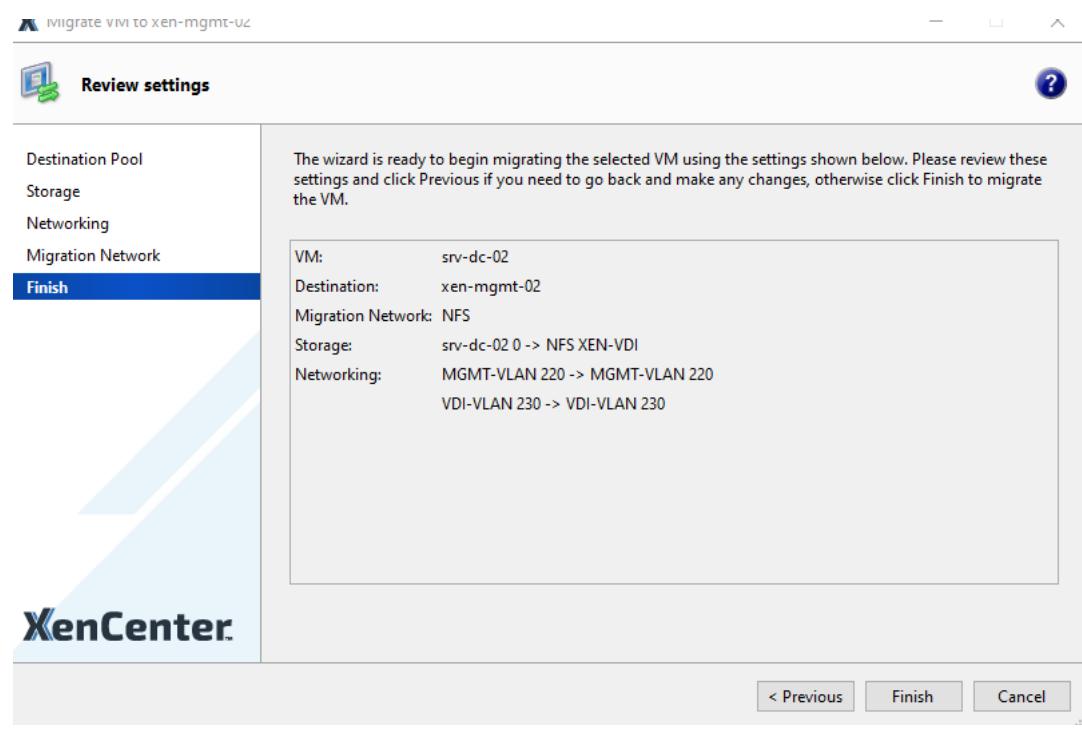
<https://docs.citrix.com/en-us/licensing/current-release/system-requirements>











5 Konfiguration Hauptspeicher

Der Hauptspeicher spielt eine grosse Rolle in dieser Infrastruktur. Er wird für mehrere Funktionen verwendet, wie als Speicherort für die VMs, für die Verwaltung von Backups und als Ablage für Projektdateien. Daher ist es umso wichtiger, diese Dateien auch an einem anderen Ort zu sichern, um sie im Falle eines Vorfalls wiederherstellen zu können.

Das Synology NAS wurde früher als Hauptspeicher in der produktiven Umgebung eingesetzt und später durch ein anderes System ersetzt. Für die Datensicherheit wurde das Synology im High-Availability-Modus betrieben, in einem Active-Active-Modell. In diesem Projekt wird als PoC auf diesen Betriebsmodus verzichtet, jedoch könnte er eine mögliche Lösung für die Zukunft darstellen.

Basis Netzwerkeinstellungen

Der Speicher war bereits vom vorherigen Einsatz gepatcht und musste nicht neu verkabelt werden. Jedoch war es notwendig, neue Ports zu definieren, die anschliessend im externen Rechenzentrum umgesteckt wurden. Bevor das Umstecken erfolgen konnte, musste noch die Netzwerkkonfiguration angepasst werden.

Allgemein	Netzwerk	Speicher	Dienst	Geräteanalyse
^ Allgemeine Informationen				
Servername				srv-data-01 (Bearbeiten)
DSM-Version				DSM 7.2-64570 Update 1
Synology-Konto				- (Bearbeiten)
QuickConnect ID				- (Bearbeiten)
^ Hardware				
Seriennummer				2270PSN046900
Modellname				FS6400
CPU				INTEL Xeon Silver 4110
Prozessor-Taktrate				2.1 GHz
CPU(s)				2
CPU-Kerne				16
CPU1-Kerne				8
CPU2-Kerne				8
Arbeitsspeicher insgesamt				128 GB
Netzteil1				In Ordnung
Netzteil2				In Ordnung
Thermal-Status				● Normal
Lüftermodus				Stiller Modus
PCIe Slot 1				Synology E25G21-F2

	LAN 1 Verbunden	MGMT Netz	Statische IP 192.168.220.15
	LAN 2 Getrennt		DHCP 169.254.178.122
	LAN 3 Getrennt		DHCP 169.254.230.119
	LAN 4 Verbunden	NFS Netz	Statische IP 192.168.210.16
	LAN 5 Verbunden		DHCP 169.254.177.211
	LAN 6 Getrennt		DHCP 169.254.246.60
	LAN 7 Verbunden	NFS Netz	Statische IP 192.168.210.17

Der Hauptspeicher verfügt über eine redundante Verbindung im NFS-Netz, allerdings lässt sich kein Multipathing konfigurieren, da hierfür auch eine redundante Verbindung vom Server erforderlich wäre. Über die MGMT-IP kann der Speicher verwaltet und ebenfalls als Dateiallage-Share genutzt werden. Hierfür war die Einrichtung einer Firewall-Policy notwendig.

NFS-Ordner

Nach Abschluss der Grundnetzwerkkonfiguration ist der Speicher nun erreichbar. Jetzt können die ersten freigegebenen Ordner erstellt werden, die später als NFS-Speicherorte im XenCenter eingebunden werden können.

Zunächst muss sichergestellt werden, dass NFS korrekt konfiguriert ist.

Systemsteuerung

SMB AFP NFS FTP rsync Erweitert

NFS-Dienst aktivieren

Maximales NFS-Protokoll: NFSv4.1

NFS-Bereich: NFSv2, NFSv3, NFSv4, NFSv4.1

Erweiterte Einstellungen

Hinweis: Sie können NFS Berechtigungen für gemeinsame Ordner auf der Bearbeiten-Seite von [Freigegebener Ordner](#) bearbeiten.



Alle freigegebenen Ordner sind mit einem Passwort verschlüsselt. Es wurden zwei freigegebene Ordner erstellt: "ISO-LIB" dient als Ablage für Installationsmedien und verfügt über ein Kontingent von 200 GB. "nfs_xen" dient als Speicherort für alle zukünftig erstellten VMs und hat kein definiertes Kontingent.

Wichtig ist die NFS-Berechtigung zu konfigurieren, sonst kann keine Verbindung errichtet werden.

Freigegebenen Ordner ISO-LIB bearbeiten

Allgemein Verschlüsselung Erweitert Berechtigungen Erweiterte Berechtigungen NFS-B

Erstellen Bearbeiten

NFS-Regel bearbeiten

Client ≡ 192.168.210.0/24	Hostname oder IP: 192.168.210.0/24
Berechtigung:	Lesen/Schreiben
Squash:	Keine Zuordnung
Sicherheit:	sys,krb5i

Asynchron aktivieren
 Verbindungen von nicht-privilegierten Ports (Ports über 1024) zulassen
 Benutzern den Zugriff auf bereitgestellte Unterordner erlauben

Abbrechen Speichern

Domain Join

Für die zukünftige Authentifizierung der Dateiallage über das Active Directory muss das Synology NAS der Domäne beigetreten sein. Dafür muss jedoch zunächst eine Domäne erstellt werden. Der Prozess der Einrichtung des Domain Controllers wird im nächsten Kapitel „Einrichtung Domain Controllers“ beschrieben.

Assistent für das Beitreten zu Domain

Domain-Informationen eingeben

Domain: DOM-POC.LOCAL

DNS-Server: 192.168.230.20

Verwaltungsmodus: Vertrauenswürdige Domains

Domain-Konto *: domainadmin

Domain-Kennwort: *****

DC IP/FQDN: 192.168.230.20 i

DNS-Schnittstelle registrieren: Alle Netzwerk-Schnittstellen

Computerkonten auf einer bestimmten OU registrieren

* Dies ist ein Pflichtfeld.

[Zurück](#) [Weiter](#)

Assistent für das Beitreten zu Domain

Domain überprüfen und dieser beitreten

DNS-Einträge überprüfen
Alle DNS-Einträge sind korrekt

Netzwerk überprüfen
Netzwerkeinstellungen sind normal

Domaindienst überprüfen
Alle Domaindienste funktionieren einwandfrei

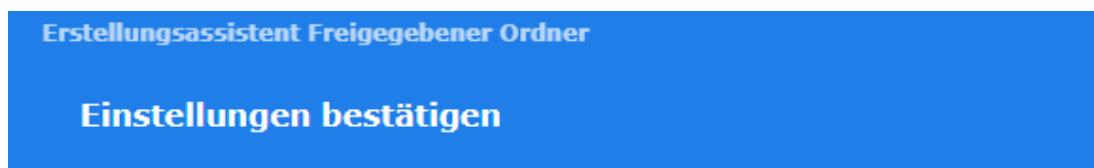
Dem Verzeichnis beitreten
Erfolgreich als Verzeichnis-Client beigetreten

Domainfunktionalität überprüfen
Alle Domaindienste funktionieren einwandfrei

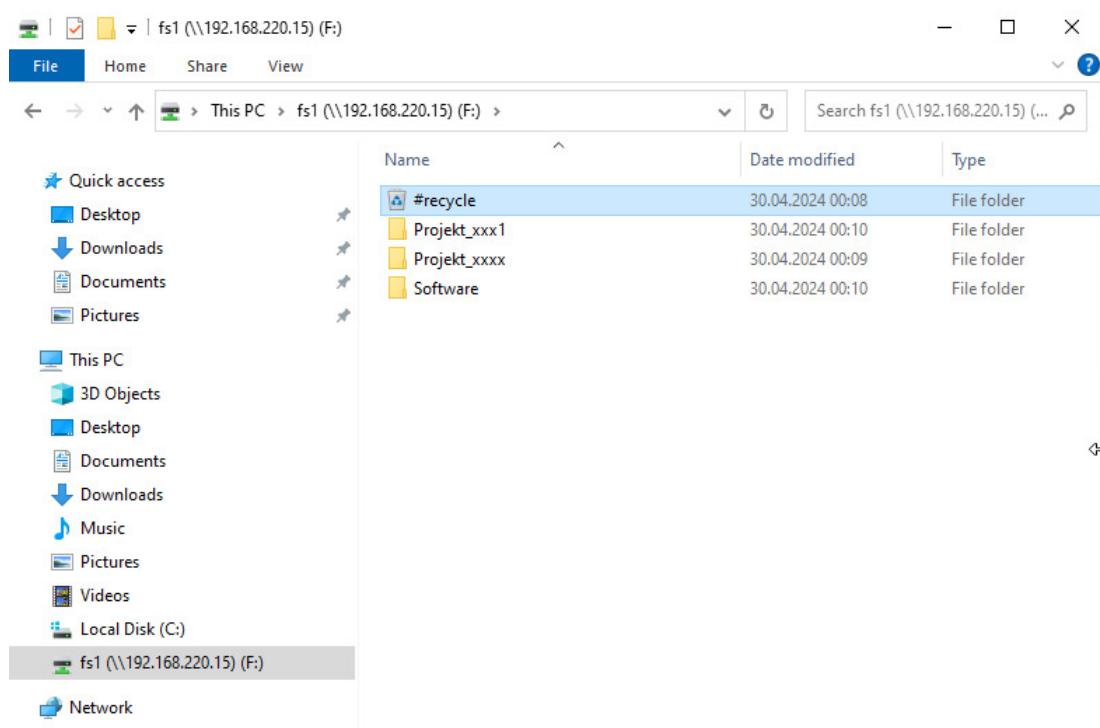
[Zurück](#) [Weiter](#)

Dateiablage Projektdaten

Es wurde eine Dateiablage eingerichtet, die allen Projektmitarbeitenden zur Verfügung steht. Die verschiedenen Projekte und Ordner sind entsprechend den Active Directory-Gruppenberechtigungen zugänglich gemacht worden. Zusätzlich wurde ein Ordner mit dem Namen "Software" erstellt, der als Ablage für IT-relevante Software dient und ausschliesslich für die IT-Abteilung zugänglich ist.



Element	Wert
Name	fs1
Beschreibung	
Ort	Volume 1: Btrfs
Sichtbarkeit	
Papierkorb	Aktiviert, nur Administratoren
Verschlüsselung	Aktiviert
Datenintegritätsschutz	
Dateikomprimierung	
Quote	10 TB



Um den Zugriff auf den Ordner „Software“ ausschliesslich für die IT-Abteilung zu ermöglichen, wurden IT-Accounts erstellt und in eine Administratorengruppe eingebunden.

Name	Type	Description
Sirak Yosef	User	

New Object - User

Create in: dom-poc.local/Confidential Projects/Users

First name: Initials:

Last name:

Full name: Shipinyuan Su

User logon name: gp-ssu @dom-poc.local

User logon name (pre-Windows 2000): DOM-POC\gp-ssu

< Back Next > Cancel

Name Größe Dateityp

#recycle

Projekt_xxx1

Projekt_xxxx

Software

Eigenschaften

Allgemein

Berechtigungs-Editor

Domain: DOM-POC

Benutzer oder Gruppe: DOM-POC\Admins

Übernehmen von: <Keine>

Typ: Zulassen

Anwenden auf: Alle

Berechtigung

Administration

Berechtigungen ändern

Eigentümerschaft übernehmen

Lesen

Ordner durchqueren/Dateien ausführen

Ordner auflisten/Daten lesen

Attribute lesen

Erweiterte Attribute lesen

Leseberechtigungen

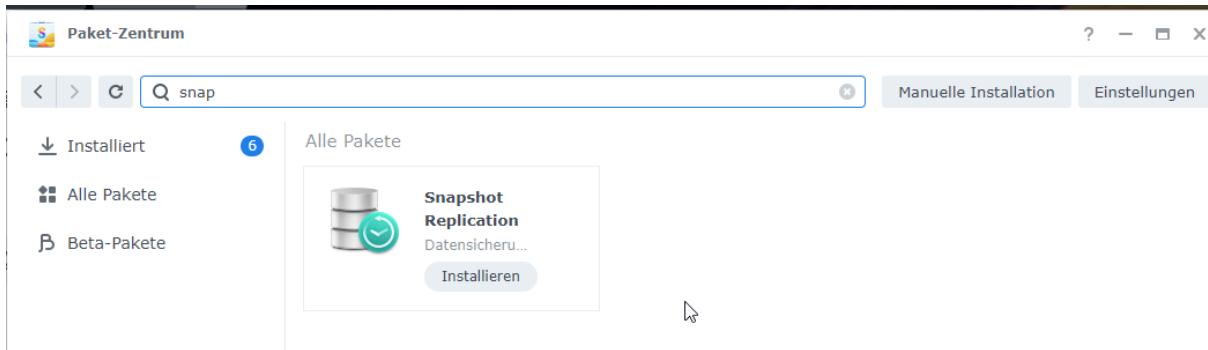
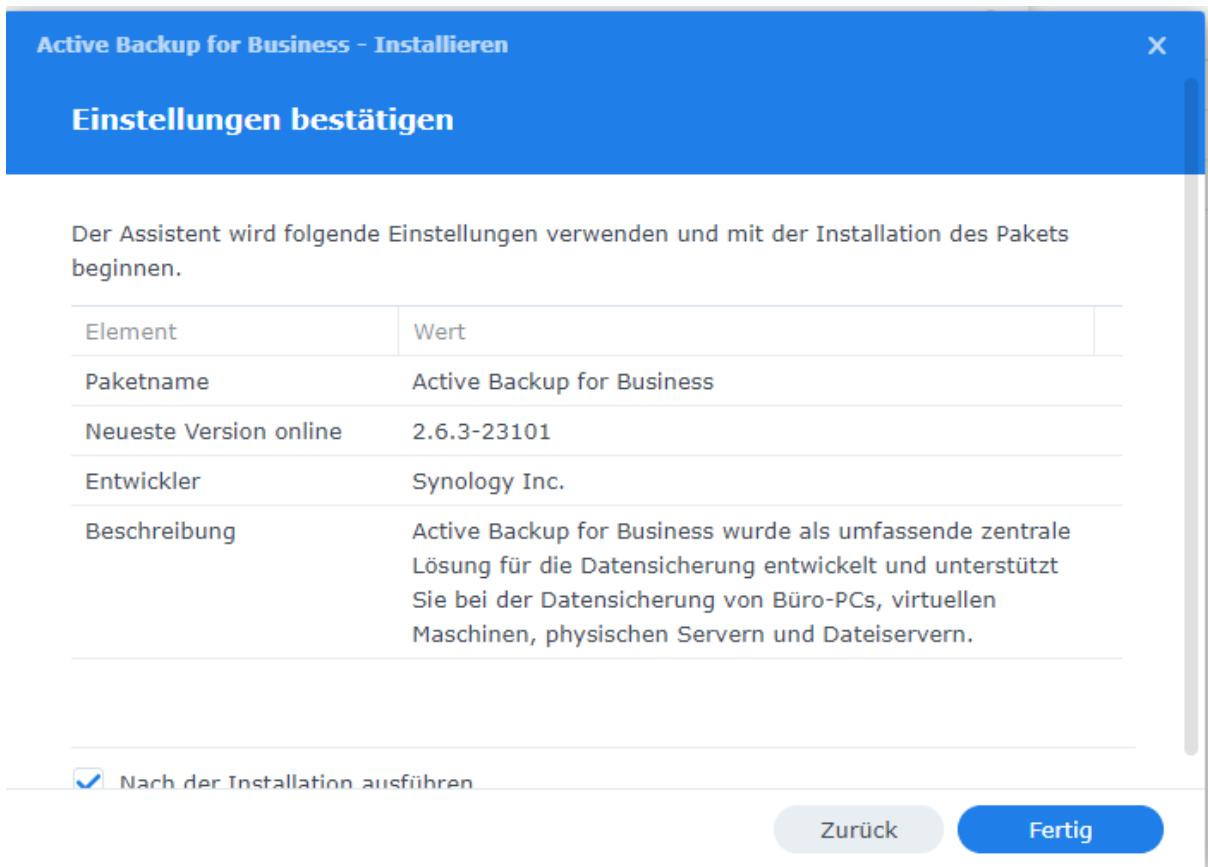
Abbrechen Fertig

Snapshots und Backups

Für Snapshots und Backups werden die von Synology zur Verfügung gestellten Tools verwendet. Die Installationsdateien für diese Tools können entweder von der Synology-Website heruntergeladen oder direkt über den Paket-Zentrum auf der Weboberfläche des Synology NAS installiert werden. Letzteres setzt allerdings voraus, dass das Synology NAS eine Internetverbindung besitzt.

<https://www.synology.com/en-af/support/download/FS6400?version=7.2#packages>

Es kommen primär zwei Tools zum Einsatz: Active Backup for Business (ABB) und Snapshot Replication. ABB wird verwendet, um die VMs zu sichern, während Snapshot Replication für die Sicherung der Projektdaten genutzt wird.



Es können nun Backups gemäss Aufgabenliste vom Detailkonzept erstellt werden.

Snapshots

Einstellungen X

Zeitplan Aufbewahrung Erweitert

Schnappschuss-Zeitplan aktivieren

Tage auswählen:

Erste Ausführungszeit:

Häufigkeit:

Letzte Ausführungszeit:

Unveränderliche Schnappschüsse aktivieren i

Schutzdauer:

Abbrechen OK

Einstellungen X

Zeitplan Aufbewahrung Erweitert

Aktivieren Sie eine Aufbewahrungsrichtlinie, um nur gewünschte Schnappschüsse zu behalten und Speicherplatz freizugeben. Ohne Aufbewahrungsrichtlinie werden alle Schnappschüsse im System gespeichert.

Aufbewahrungsrichtlinie aktivieren

Anzahl der zu behaltenden letzten Schnappschüsse

Alle Schnappschüsse behalten für

Erweiterte Aufbewahrungsrichtlinie

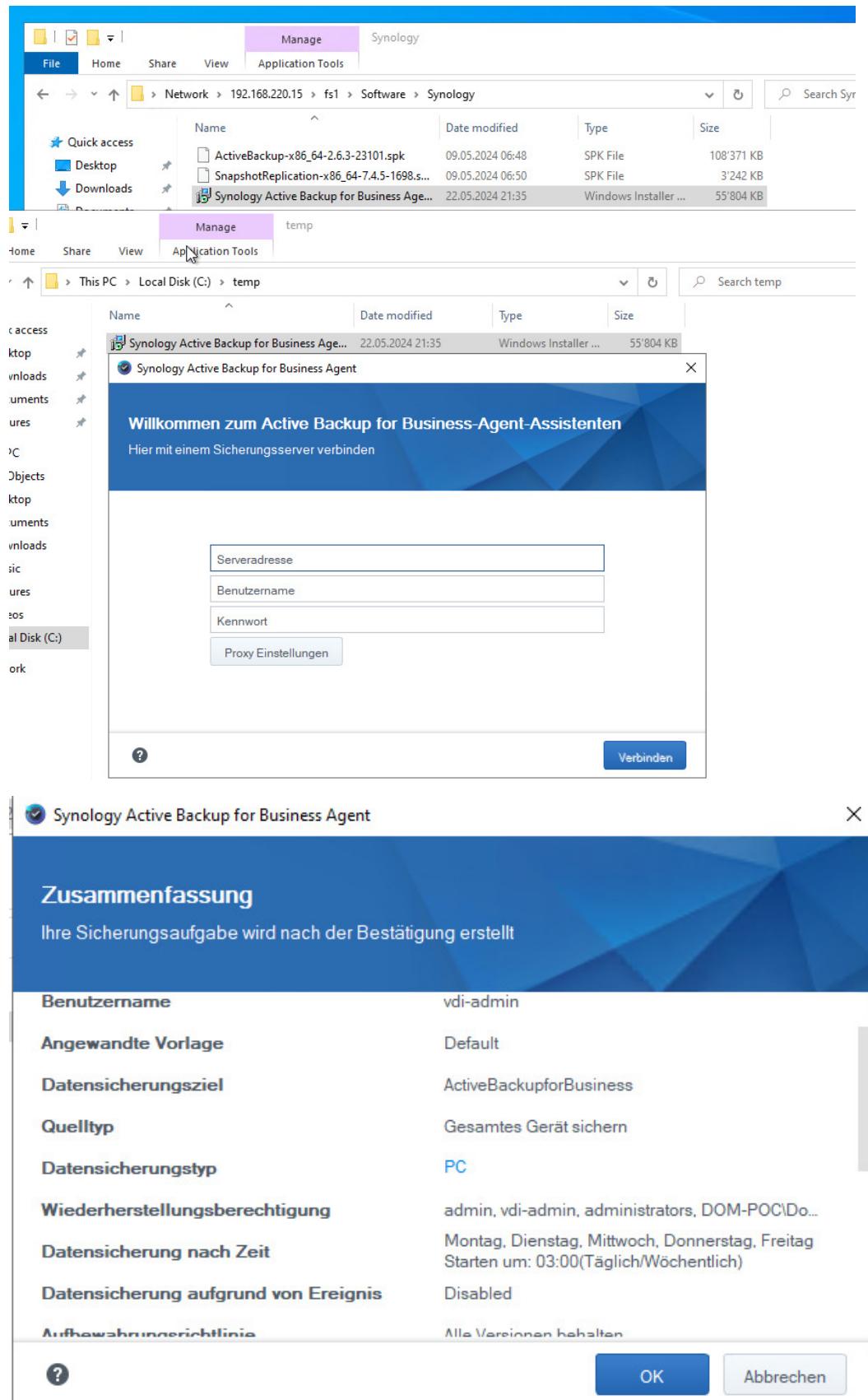
Hinweis: Die Speicherplatzrückgewinnung kann einige Zeit dauern, nachdem Schnappschüsse gelöscht wurden. Sie können [hier](#) einen Zeitplan für die Speicherplatzrückgewinnung einrichten, um sie in Zeiten geringerer Auslastung auszuführen. Dies hilft, die Auswirkungen auf die Leistung von Diensten zu minimieren.

Ein freigegebener Ordner kann bis zu insgesamt 1024 Schnappschüsse in seinen Schnappschuss- und Replikationsaufgaben haben.

Abbrechen OK

Active Backup for Business

Mit Active Backup for Business kann man vollständige Backups der virtuellen Server erstellen. Da Citrix nativ nicht unterstützt wird, muss ein Agent installiert werden. Dieser ist auf der Synology-Website zu finden.



Assistent zur Agent-Sicherungserstellung

Datensicherungsziel

Suchen

Freigegebener Ordner	D...	Komprimierung...	Verschlüsselung...	Verfügbarer
ActiveBackupforBusiness	bt...	Nein	Nein	66.2 TB	
Backup_VDI-srv-data-01	bt...	Verfügbar	Verfügbar	66.2 TB	
fs1	bt...	--	--	66.2 TB	
Golden	bt...	Verfügbar	Verfügbar	66.2 TB	
ISO-LIB	bt...	--	--	66.2 TB	
nfs_xen	bt...	--	--	66.2 TB	

Aufgabe bearbeiten

Allgemein Zeitplan Aufbewahrung

Aufgabenname: Daily-Server-fslogix

Quelltyp:

- Gesamtes Gerät
- Externe Festplatte sichern
- System-Volume
- Benutzerdefiniertes Volume: --- Auswählen

Datenübertragung Einstellungen:

- Datenübertragungskomprimierung aktivieren
- Datenübertragungsverschlüsselung aktivieren
- Beschränkung des Bandbreitenverbrauchs aktivieren
0 KB/s

Energieeinstellungen für Computer:

- Computer nach Abschluss der zeitbasierten, geplanten Datensicherung herunterfahren
- Verhindern, dass Computer während der Sicherung in den Energiesparmodus wechselt

Abbrechen OK

Aufgabe bearbeiten

Allgemein Zeitplan Aufbewahrung

Aufgabenplaner

Manuelle Datensicherung

Geplante Datensicherung

Datensicherung nach Zeit

Ausführen am Täglich

Starten um 23 : 00

Einmal pro Stunde ausführen

Datensicherung aufgrund von Ereignis

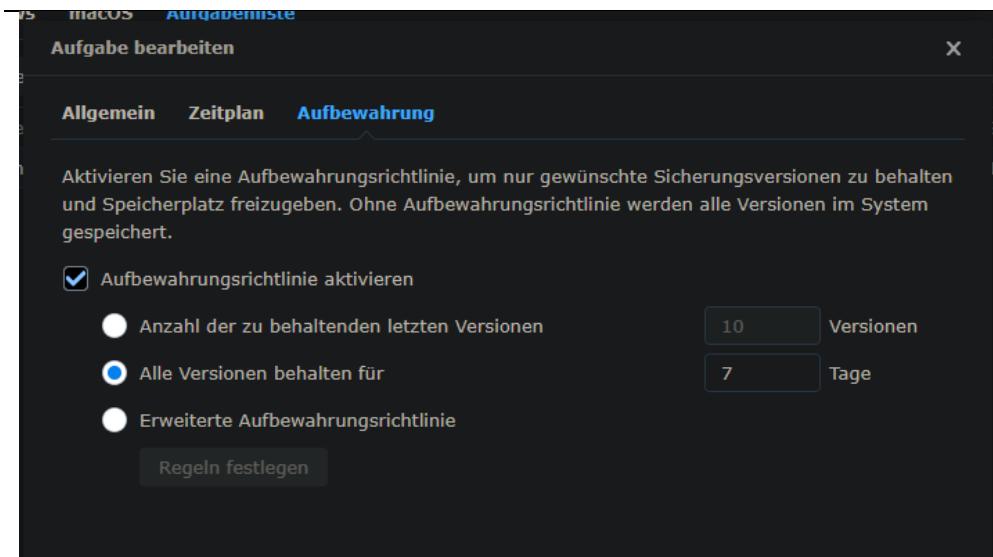
Ereignis Alle

Sicherungsintervall: 1 Stunde

Voreinstellungen

Sicherungsaufgaben nur in den angegebenen Zeitfenstern ausführen

Abbrechen OK

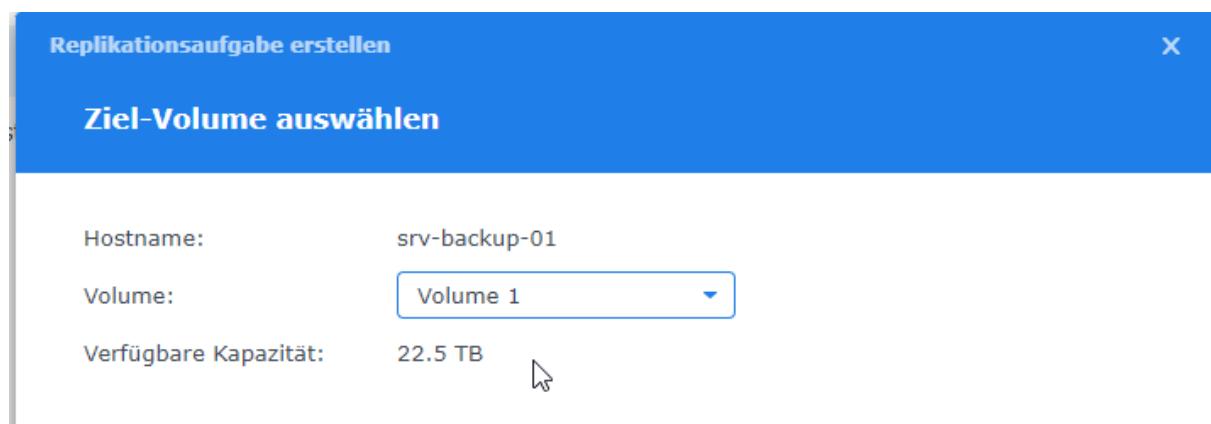
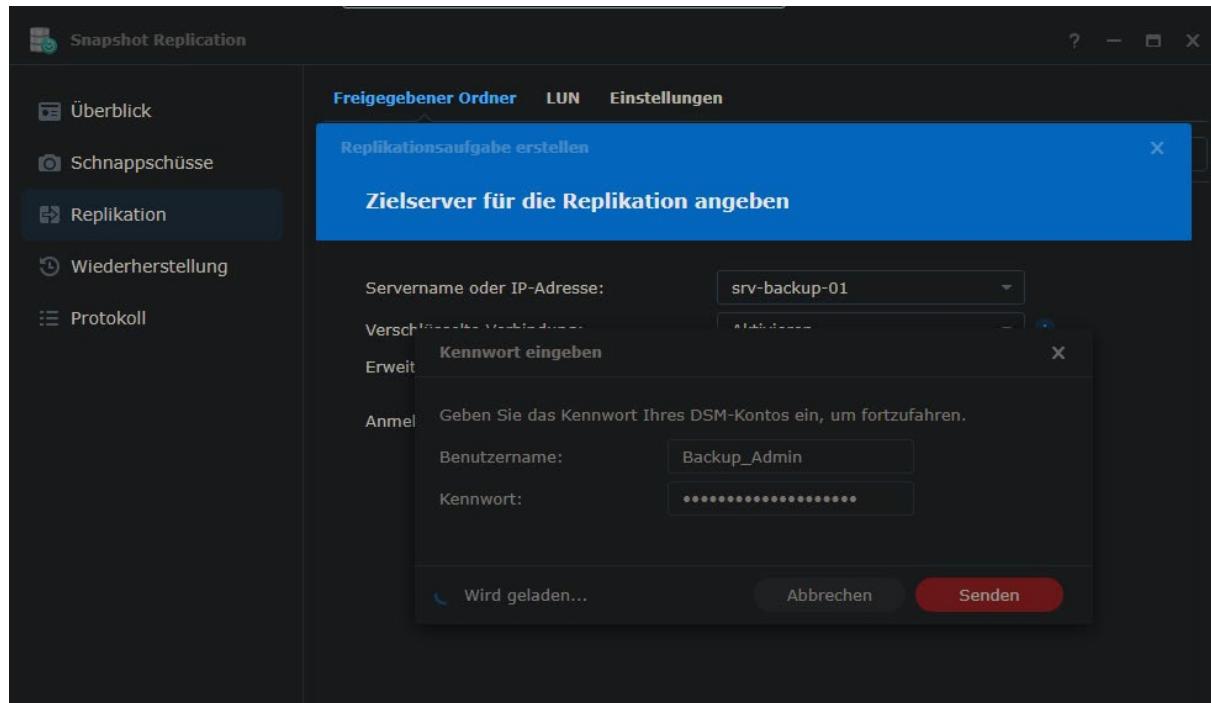


Assistent zur Agent-Sicherungserstellung	
Aufgabenzusammenfassung	
Element	Wert
Aufgabename	weekly-server-fslogix
Gerät	SRV-FSLX-01
Sicherungsziel	/Backup_VDI-srv-data-01
Quelltyp	Gesamtes Gerät (einschließlich externe Fes...)
Plattform	Windows
Datenübertragungskomprimierung	Aktivieren
Datenübertragungsverschlüsselung	Aktivieren
Beschränkung des Bandbreitenverbrauchs	Deaktivieren
Computer nach Abschluss der zeitbasierten, g...	Deaktivieren
Verhindern, dass Computer während der Sich...	Deaktivieren
Computer für geplante Sicherung aus dem En...	Deaktivieren
Komprimierung in Sicherungsziel	Deaktivieren
Verschlüsselung in Sicherungsziel	Aktivieren

Aufgabename	Letzte Sicherung	Status	Versionen
vdi-admin-Default	Noch nicht gesichert	Nächste Sicherung: 23.05.2024 03:00	Link

Replikation

Mit Snapshot Replication ist es möglich, freigegebene Ordner auf eine andere Synology zu replizieren. Dafür muss eine Replikationsaufgabe erstellt werden, die die Anmeldedaten des Backup-Servers benötigt.



This is the third step of the replication setup. The title is 'Replikationsaufgabe erstellen' and the sub-titler is 'Daten für Replikation auswählen'. It displays a table of volumes and their replication status:

	Name	Volume	Repliziert von
<input type="checkbox"/>	ActiveBackupforBusi...	Volume 1	
<input checked="" type="checkbox"/>	Backup_VDI-srv-dat...	Volume 1	
<input checked="" type="checkbox"/>	fs1	Volume 1	
<input type="checkbox"/>	Golden	Volume 1	
<input checked="" type="checkbox"/>	ISO-LIB	Volume 1	
<input type="checkbox"/>	nfs_xen	Volume 1	

Replikationsaufgabe erstellen

Erste Replikation

Größe der ersten Kopie für die replizierten Daten: 56.2 GB

- Erste Kopie über das Netzwerk übertragen
Geschätzter Abschluss in 9 Minuten bei 104.0 MB/s
- Sofort nach Erstellung der Replikationsaufgabe synchronisieren
- Erste Kopie mithilfe des Speichergerätes übertragen

Geben Sie den Speicherort zum Exportieren der ersten Kopie an

Replikationsaufgabe erstellen - Zeitplan für Replikation einstellen

Das System nimmt Schnappschüsse auf und sendet diese entsprechend dem Zeitplan für Replikation an den Partnerserver.

Zeitplan für Replikation aktivieren

Zeitplan für Replikation aktivieren

Tage auswählen: Täglich

Erste Ausführungszeit: 21 : 00

Häufigkeit: Täglich

Letzte Ausführungszeit: 21:00

Timeout-Benachrichtigungseinstellung für die geplante Synchronisierung

Wartezeit (Minuten): 720

Schnappschüsse nur innerhalb des Übertragungszeitfensters senden

Übertragungszeitfenster festlegen

Unveränderliche Schnappschüsse auf Partnerserver aktivieren i

Schutzdauer: 7 Tage

Replikationsaufgabe erstellen

Aufbewahrungsrichtlinie für Speicherziel einstellen

Aktivieren Sie eine Aufbewahrungsrichtlinie, um nur gewünschte Schnappschüsse zu behalten und Speicherplatz freizugeben. Ohne Aufbewahrungsrichtlinie werden alle Schnappschüsse im System gespeichert.

Aufbewahrungsrichtlinie aktivieren

Anzahl der zu behaltenden letzten Schnappschüsse 128

Alle Schnappschüsse behalten für 7 Tage

Erweiterte Aufbewahrungsrichtlinie

Hinweis: Die Speicherplatzrückgewinnung kann einige Zeit dauern, nachdem Schnappschüsse gelöscht wurden. Sie können hier einen Zeitplan für die Speicherplatzrückgewinnung einrichten, um sie in Zeiten geringerer Auslastung auszuführen. Dies hilft, die Auswirkungen auf die Leistung von Diensten zu minimieren.

Ein freigegebener Ordner kann bis zu insgesamt 1024 Schnappschüsse in seinen Schnappschuss- und Replikationsaufgaben haben.

Replikationsaufgabe erstellen

Einstellungen bestätigen

Element	Wert
Zielserver	srv-backup-01
Ziel-Volume	Volume 1
Name des Replikationsziels	Backup_VDI-srv-data-01, fs1, ISO-LIB
Erste Replikation	Über das Netzwerk
Zeitplan	Täglich, Beginnend um 21:00, Täglich, Wiederholen bis 2...
Benachrichtigen, wenn di...	720 Min.
Übertragungszeitfenster	Deaktiviert
Unveränderliche Schnapp...	Replizierte Schnappschüsse sind 7 Tage lang geschützt

Hinweis: Um eine erfolgreiche Replikation sicherzustellen, wendet das System für Ihre lokalen Schnappschüsse eine Aufbewahrungsregel an. Um die Regel zu ändern, gehen Sie zu **Schnappschüsse > Einstellungen > Aufbewahrung**.

[Zurück](#) [Fertig](#)

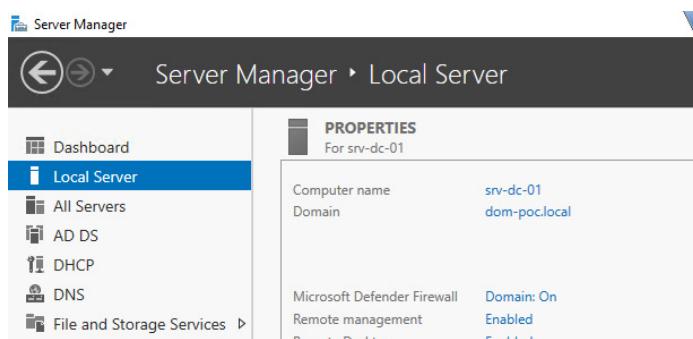
Freigegebener Ordner		LUN	Einstellungen
Erstellen	Info	Aktion ▾	<input type="text"/> Suche
 Backup_VDI-srv-data-01 - Warten auf erste Replikation	Befindet sich auf Volume 1, Btrfs, Repliziert zu [srv-backup-01] Backup_VDI-srv-data-01		▼
 fs1 - Warten auf erste Replikation	Befindet sich auf Volume 1, Btrfs, Repliziert zu [srv-backup-01] fs1		▼
 ISO-LIB - Warten auf erste Replikation	Befindet sich auf Volume 1, Btrfs, Repliziert zu [srv-backup-01] ISO-LIB		▼

6 Einrichtung Domain Controllers

In diesem Kapitel wird die Einrichtung der Domain Controller beschrieben. Zudem umfasst es das Erstellen der Domäne sowie das Einrichten der Dienste.

Erster DC und Domäne

Nachdem die virtuelle Maschine (VM) über den XenCenter hochgezogen und gestartet wurde, musste zuerst die Domäne eingerichtet werden, was gemeinsam mit der Erstellung des ersten Domain Controllers erfolgte. Zunächst wurde der Hostname auf den festgelegten Standard «srv-dc-01» geändert, die Netzwerkkarte entsprechend konfiguriert und anschliessend über den Server Manager die Active Directory-Domänen Dienste installiert. In der folgenden Abbildung ist zu sehen, nachdem die Dienste installiert wurden und der Domain Controller hochgestuft wurde.



OU-Struktur

Nachdem die Domäne erstellt und der Domain Controller (DC) hochgestuft wurde, wurde die Organizational Unit (OU)-Struktur gemäss dem Detailkonzept erstellt. Das Ergebnis sieht wie folgt aus.

Zudem wurde im Administrationscenter die Papierkorb-Funktion aktiviert, sodass im Falle, wenn ein Objekt (wie ein Benutzer oder ein Computer) versehentlich gelöscht wird, dieses einfach wiederhergestellt werden kann.

The screenshot shows the 'Active Directory Users and Computers' snap-in. The left pane displays the organizational unit structure:

- Active Directory Users and Computers [srv-dc-01]
- Saved Queries
- dom-poc.local
 - Builtin
 - Computers
 - Confidential Projects
 - Access-Groups
 - Folder Permissions
 - VDI-Profile
 - Servers
 - Member Servers
 - XenServers
 - Service Accounts
 - Users
 - VDI-Machine
 - Domain Controllers
 - ForeignSecurityPrincipals

DNS-Konfiguration

Als nächstes wurde das Domain Name System (DNS) auf dem Domain Controller (DC) eingerichtet. Dieses ist sowohl für die interne als auch für die externe Namensauflösung wichtig. Dabei wurden beide Netzwerke (VDI und MGMT) berücksichtigt.

The screenshot shows the Windows DNS Manager interface. On the left, a tree view shows the DNS node, followed by SRV-DC-01, Forward Lookup Zones (containing _msdcs.dom-poc.local and dom-poc.local), Reverse Lookup Zones (containing 220.168.192.in-addr.a and 230.168.192.in-addr.a), Trust Points, and Conditional Forwarders. On the right, a table lists DNS records:

Name	Type	Data	Timestamp
dc	Start of Authority (SOA)	[12], srv-dc-01.dom-poc.l...	static
domains	Name Server (NS)	srv-dc-01.dom-poc.local.	static
gc	(same as parent folder)		
pdc	(same as parent folder)		
71f7a5b5-6bce-4290-a6c0-9...	Alias (CNAME)	srv-dc-01.dom-poc.local.	02.05.2024

DHCP-Konfiguration

Nach der Konfiguration des DNS war das Dynamic Host Configuration Protocol (DHCP) an der Reihe. Der DHCP-Scope für das VDI-Netz wurde eingerichtet. Der IP-Bereich, wie bereits im Detailkonzept definiert, erstreckt sich von 192.168.230.30 bis 192.168.230.200 und die Lease-Time dauert 8 Tage. In der folgenden Abbildung sind zudem Gateway und DNS-Server ersichtlich.

The screenshot shows the Windows DHCP Manager interface. On the left, a tree view shows the DHCP node, followed by srv-dc-01.dom-poc.local, IPv4, Scope [192.168.230.30-192.168.230.200], and various sub-options like Address Pool, Address Leases, Reservations, Scope Options, Policies, and Filters. On the right, a table lists DHCP options for the selected scope:

Option Name	Vendor	Value	Policy Name
003 Router	Standard	192.168.230.1	None
006 DNS Servers	Standard	192.168.230.20, 192.168.230.21	None
015 DNS Domain Name	Standard	dom-poc.local	None

Zweiter DC

Nachdem der erste DC bereit war, konnte der zweite DC eingerichtet werden. Dort wurde auch wie beim ersten DC zuerst der Hostname, Netzwerkkarte angepasst und die Active Directory-Domänendienste installiert. Der DC wurde dann zu einem bestehenden DC hochgestuft.

Die Replizierung wurde für Active Directory und DNS überprüft und diese konnte erfolgreich durchgeführt werden. Nur DHCP kann nicht automatisch replizieren, aber dafür wurde ein DHCP-Failover auf beide Server konfiguriert.

The screenshot shows the Active Directory Users and Computers (ADUC) interface. On the left, the navigation pane lists several organizational units: Saved Queries, dom-poc.local (which is expanded to show Builtin, Computers, Confidential Projects, Servers, and Domain Controllers), and ForeignSecurityPrincipals. The 'Domain Controllers' folder under 'Servers' is highlighted. On the right, a table displays the details of the two domain controllers:

Name	Type	DC Type
SRV-DC-01	Computer	GC
SRV-DC-02	Computer	GC

The screenshot shows the Windows DHCP management console. The left pane displays the hierarchy: DHCP, srv-dc-02.dom-poc.local (expanded to show IPv4 and IPv6), and IPv4 (expanded to show Server Options, Scope [192.168.230.0] VDI-Netz, Policies, and Filters). The right pane is titled 'Contents of DHCP Server' and lists the following items: Server Options, Scope [192.168.230.0] VDI-Netz, Policies, and Filters.

7 Konfiguration NAS-Backup

Das NAS-Backup ist ein vom Hauptspeicher und Standort getrennter Speicher, der als Ablage für gesicherte Dateien dient. Dieser Speicher verfügt nicht über eine Management-IP und muss daher im Vorfeld korrekt konfiguriert werden. Zunächst wird der Backup-Speicher im internen Netzwerk konfiguriert. Zu Beginn erhält der Speicher eine DHCP-Adresse, die mithilfe des Synology Assistants oder des Advanced IP-Scanners ermittelt werden kann. Ähnlich wie beim Hauptspeicher werden die grundlegenden Konfigurationen durchgeführt. Auch hier wird ein Freigegebener Ordner erstellt, welcher als Speicherort dient für die zukünftigen gesicherten Dateien. Ebenfalls ist es hier wichtig die NFS-Berechtigungen zu konfigurieren.

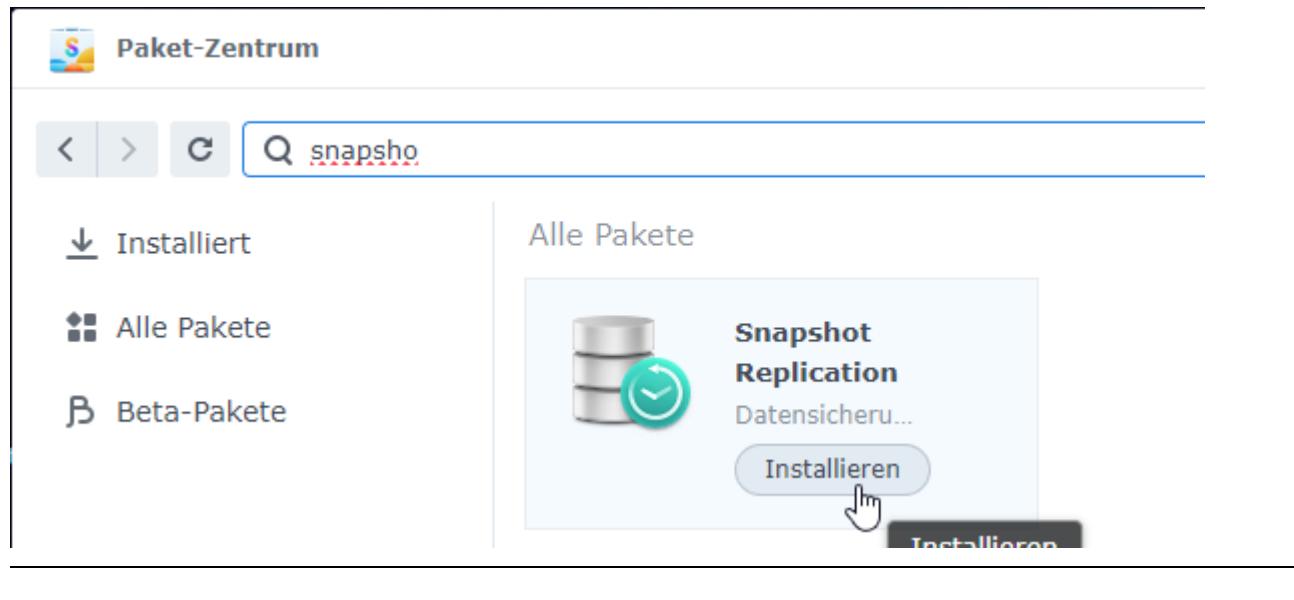
The screenshot shows the 'Systemsteuerung' (System Control) interface. In the left sidebar, 'Freigegebene' is selected under 'Dateifreigabe'. A modal window titled 'NFS-Regel erstellen' (Create NFS Rule) is open, showing fields for 'Hostname oder IP:' (192.168.210.0/24), 'Berechtigung:' (Read/Write), 'Squash:' (Keine Zuordnung), and 'Sicherheit:' (sys). There are also checkboxes for 'Asynchron aktivieren' (Enable asynchronous), 'Verbindungen von nicht-privilegierten Ports (Ports über 1024) zulassen' (Allow connections from non-privileged ports (Ports above 1024)), and 'Benutzern den Zugriff auf bereitgestellte Unterordner erlauben' (Allow users access to shared subfolders). At the bottom are 'Abbrechen' (Cancel) and 'Speichern' (Save) buttons.

Sobald alles vorbereitet ist, kann das gewünschte Ethernet-Interface mit der korrekten IP-Adresse im NFS-Netz eingerichtet und anschliessend am vorgesehenen Ort in Betrieb genommen werden.

Nachdem die Einrichtung des Backup-Speichers abgeschlossen ist, kann der NFS-Share auf dem Hauptspeicher als Remote-Ordner angehängt werden. Dadurch lässt sich dieser Remote-Ordner als Zielort für Backups auswählen, was eine Datensicherung an einem externen Standort ermöglicht.

The screenshot shows the 'File Station' interface. On the left, a tree view shows 'srv-data-01' with subfolders 'Backup_VDI-srv-data-01', 'Golden', 'ISO-LIB', 'NetBackup', 'nfs_vmware3', and 'nfs_xen'. A specific folder 'Backup_VDI-srv-data-01' is selected. A modal window titled 'Remote-Ordner bereitstellen' (Mount Remote Folder) is open, showing 'Dateiprotokoll:' (NFS), 'Ordner:' (192.168.210.15:/volume1), 'Version:' (v4), 'Übertragungsprotokoll:' (TCP), and 'Anhängen an:' (/Backup_VDI-srv-data-01/). There is also a checked checkbox 'Beim Start automatisch bereitstellen' (Mount automatically at startup). At the bottom are 'Schließen' (Close) and 'Anhängen' (Mount) buttons.

Snapshot Replication installieren, damit Replikationen auf diesen Synology gemacht werden können.



8 Konfiguration VDI-Server

Der VDI-Server ist eine zentrale Komponente dieses Services. Gemäss Konzept betreibt dieser Server alle laufenden VDIs, weshalb er die meiste Leistung benötigt.

Dieser Server war ursprünglich als Test-VDI-Server gedacht, wurde jedoch aufgrund der hohen Nachfrage nach VDIs in die produktive Umgebung integriert. Mit der Bestellung neuer Hardware konnte dieser Server nun wieder für seine ursprüngliche Anwendung genutzt werden, für die er auch geplant war. Leider konnten die neu bestellten Server nicht rechtzeitig integriert werden und die aktuell laufenden VDIs auf dem VDI-Server nicht verschoben werden. Daher konnte dieser VDI-Server leider nicht für die Diplomarbeit eingesetzt werden.

The screenshot shows the vSphere Web Client interface for the host `vditest01.gph.ch`. The top navigation bar includes tabs for Summary, Monitor, Configure, Permissions, VMs, Datastores, Networks, and Updates. The `Summary` tab is currently selected.

Host Details:

- Hypervisor: VMware ESXi, 7.0.3, 22348816
- Model: SYS-220U-MTNR
- Processor Type: Intel(R) Xeon(R) Gold 5317 CPU @ 3.00GHz
- Logical Processors: 48
- NICs: 7
- Virtual Machines: 15
- State: Connected
- Uptime: 171 days

Capacity and Usage:

- CPU:** 64.7 GHz free (7.3 GHz used)
- Memory:** 690.68 GB free (332.94 GB used)
- Storage:** 7.22 TB free (34.6 TB used)

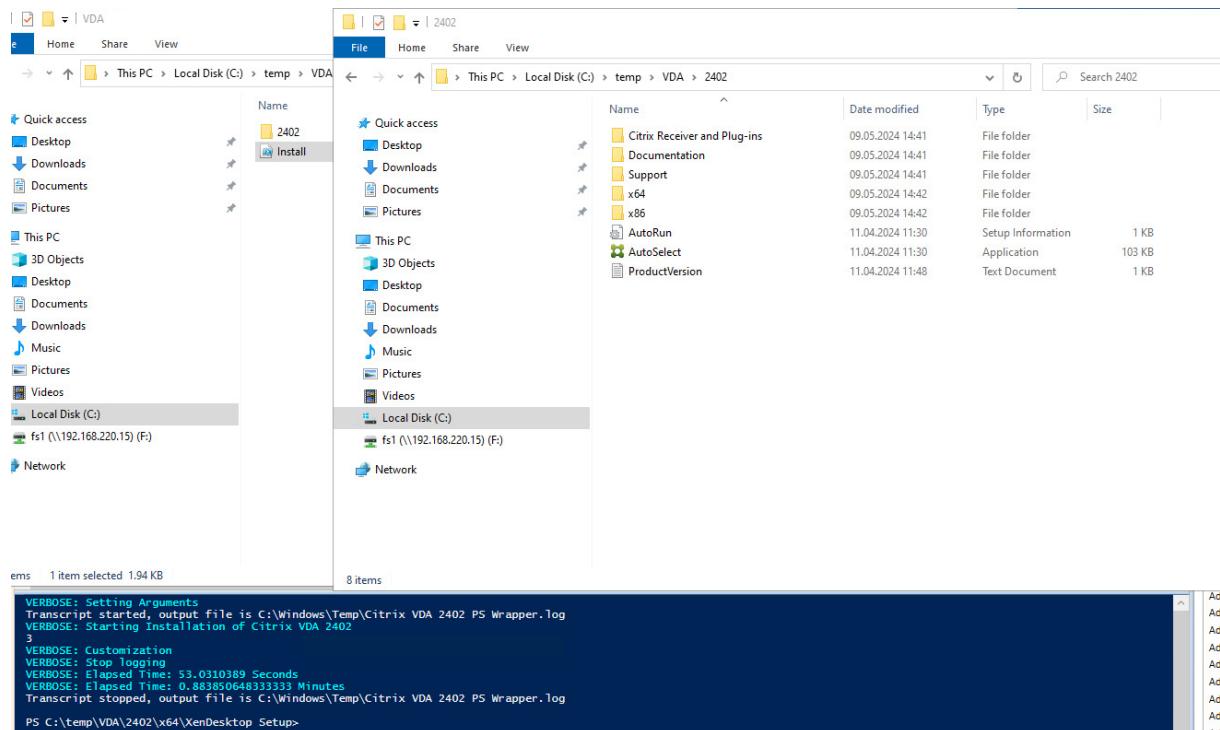
A "VIEW STATS" link is located at the bottom of the Capacity and Usage section.

9 Einrichtung Citrix Services

Nach der Fertigstellung der Installation der Windows-Server auf dem MGMT-Server für die verschiedenen Dienste können wir beginnen, die Dienste zu installieren und zu konfigurieren. In diesem Kapitel werden die verschiedenen Schritte dokumentiert, die benötigt werden, um die erste VDI über den Citrix Workspace zu starten. Dies erfolgt jedoch noch ohne kosmetische Einstellungen wie Profil- oder Sicherheitsrichtlinien

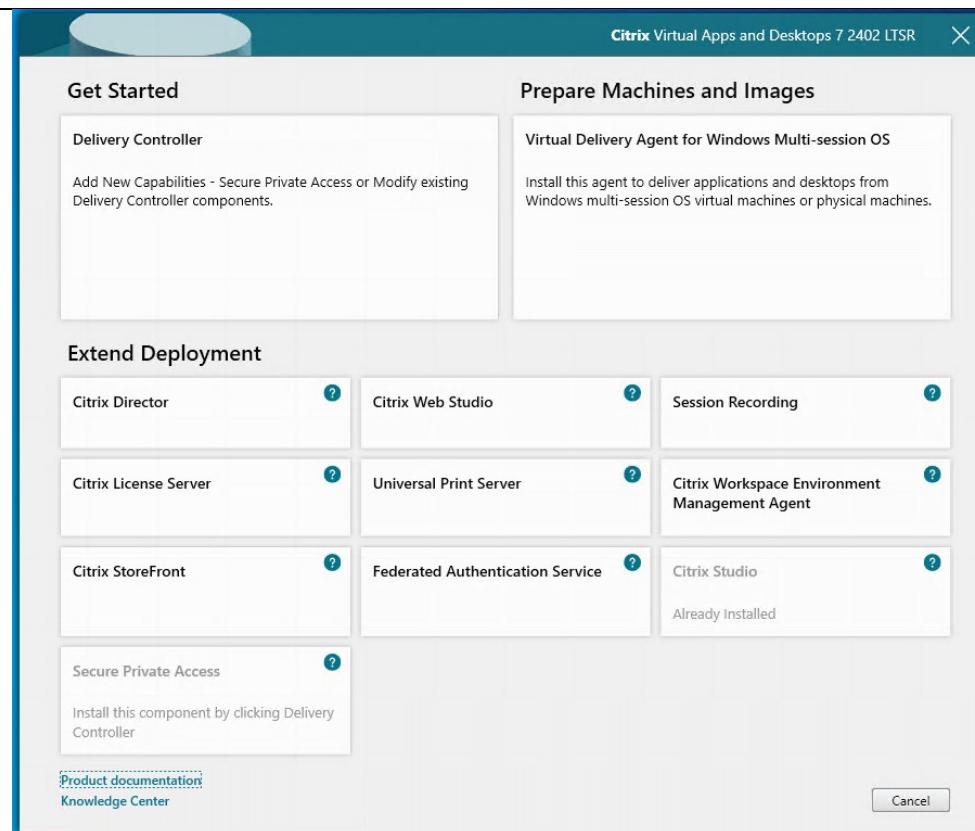
Source

Ein Citrix-Experte hat einen Source-Ordner zur Verfügung gestellt. Darin war eine .exe-Datei enthalten, die alle nötigen Dienste installieren kann. Es gab auch einen PowerShell-Installer, dieser war jedoch nicht für diese Umgebung angepasst. Daher wurde alles manuell über die GUI installiert und konfiguriert.



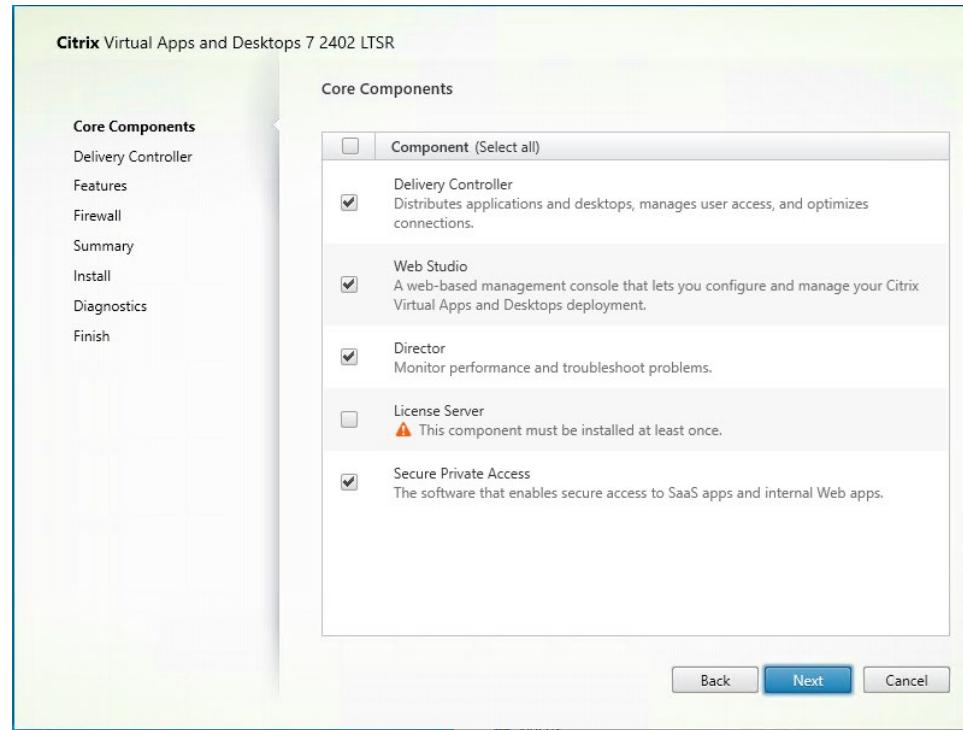
Installation Desktop Delivery Controller

Der DDC gehört zu den Hauptkomponenten des Citrix Service und übernimmt Aufgaben wie die Bereitstellung und Verwaltung der virtuellen Desktops.



Delivery Controller

Der DDC wurde ohne License Server installiert, da dieser auf einer dedizierten Instanz laufen wird.



Delivery Controller

✓ Core Components

Delivery Controller

Features

Firewall

Summary

Install

Diagnostics

Finish

To add a Delivery Controller to the list, enter its address and then click Add. Specify one or more Delivery Controllers for the site that you want to manage with Studio and monitor with Director.

To update the list for Studio, use the Studio configuration tool. To update the list for Director, use Group Policy or the Director configuration tool.

Configuration

srv-ddc-01.dom-poc.local [Edit](#) [Delete](#)

Controller address: (Enter the FQDN, IP addresses are not supported.)

[Test connection](#)[Add](#)[Back](#)[Next](#)[Cancel](#)**Firewall**

The default ports are listed below.

[Printable version](#)

Delivery Controller	Web Studio	Director	Secure Private Access
80 TCP	443 TCP	80 TCP	443 TCP
89 TCP		443 TCP	4443 TCP
443 TCP			

Configure firewall rules:

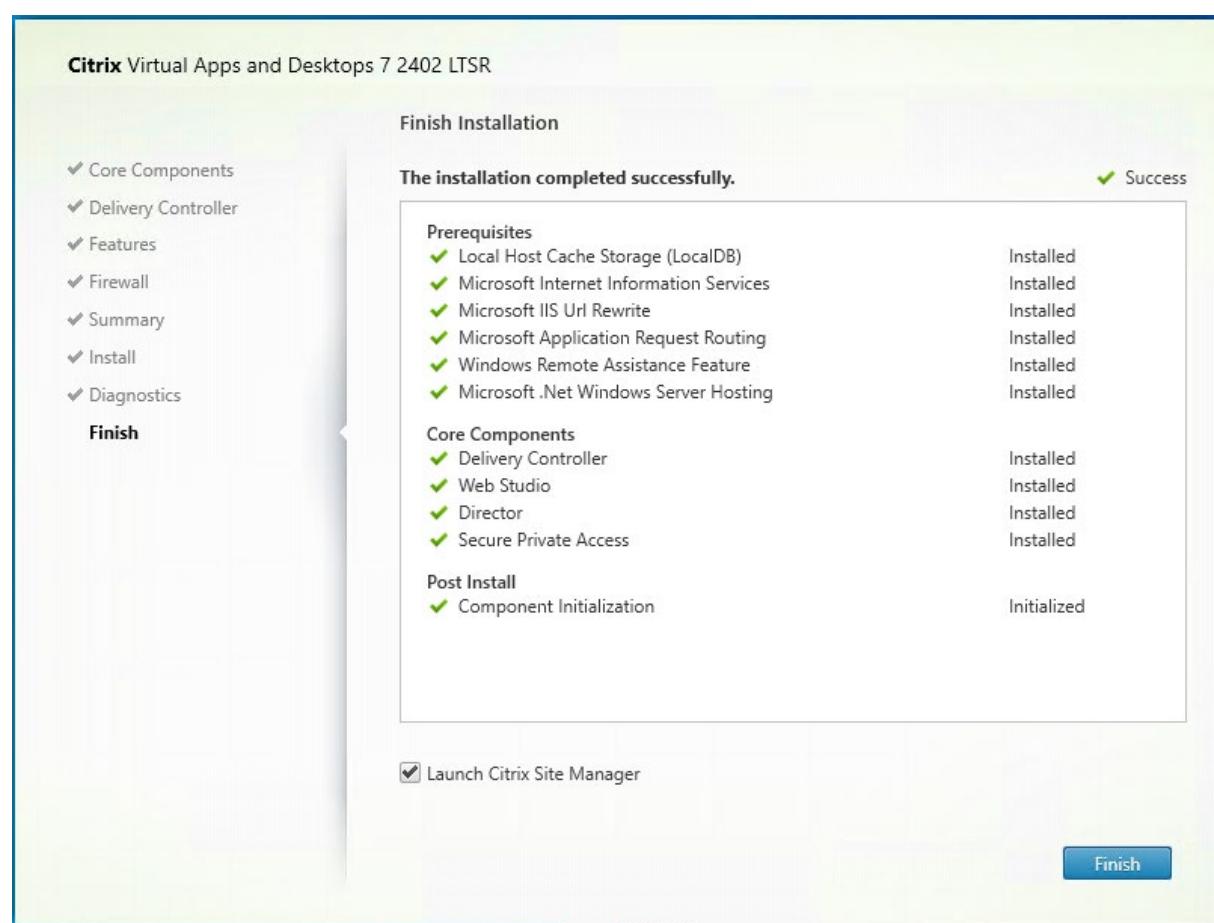
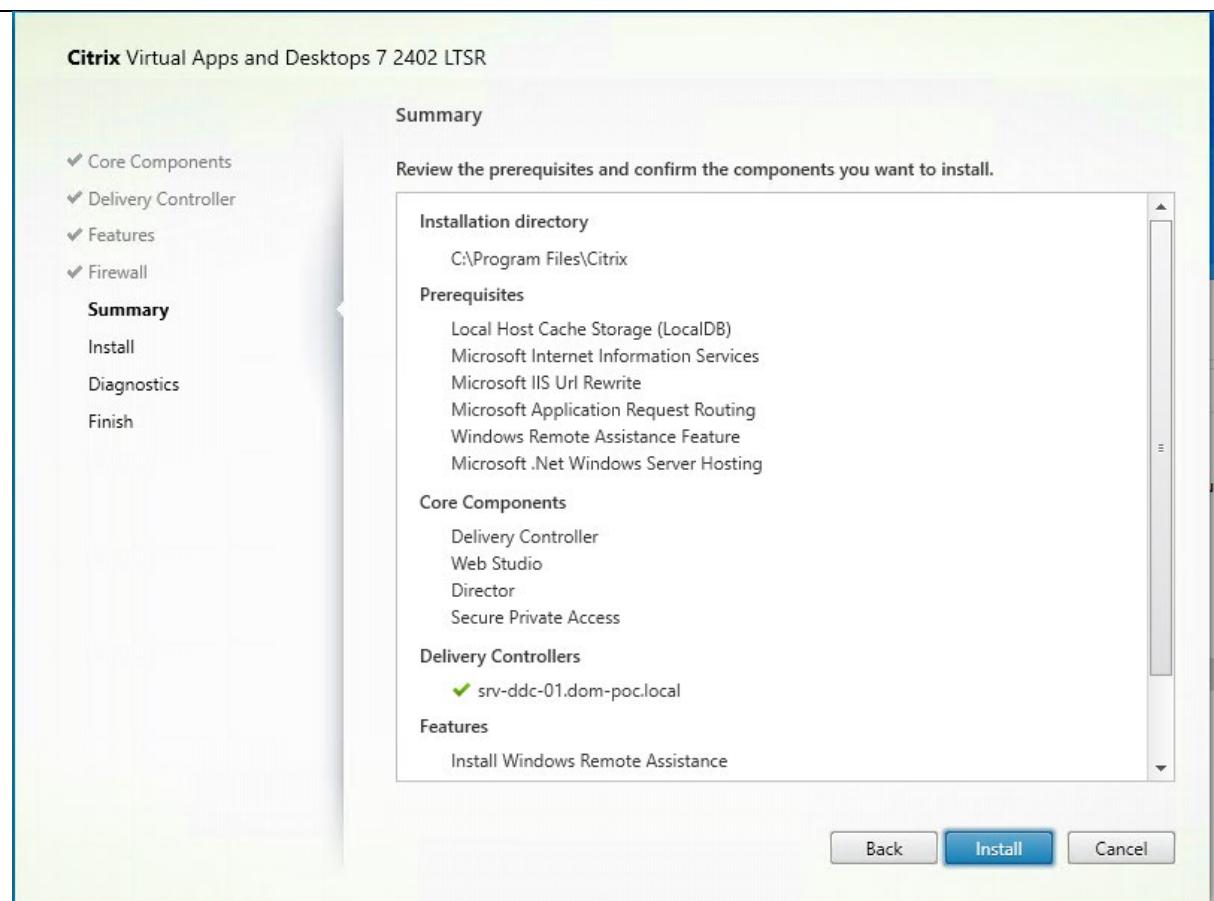
 Automatically

Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.

 Manually

Select this option if you are not using Windows Firewall or if you want to create the rules yourself.

[Back](#)[Next](#)[Cancel](#)



Lizenzserver

Der Lizenzserver wird mit der gleichen Source installiert.

Citrix Virtual Apps and Desktops 7 2402 LTSR

Firewall

The default ports are listed below.

[Printable version](#)

License Server
7279 TCP
27000 TCP
8083 TCP

Configure firewall rules:

Automatically
Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.

Manually
Select this option if you are not using Windows Firewall or if you want to create the rules yourself.

Back **Next** **Cancel**

Citrix Virtual Apps and Desktops 7 2402 LTSR

Finish Installation

The installation completed successfully. ✓ Success

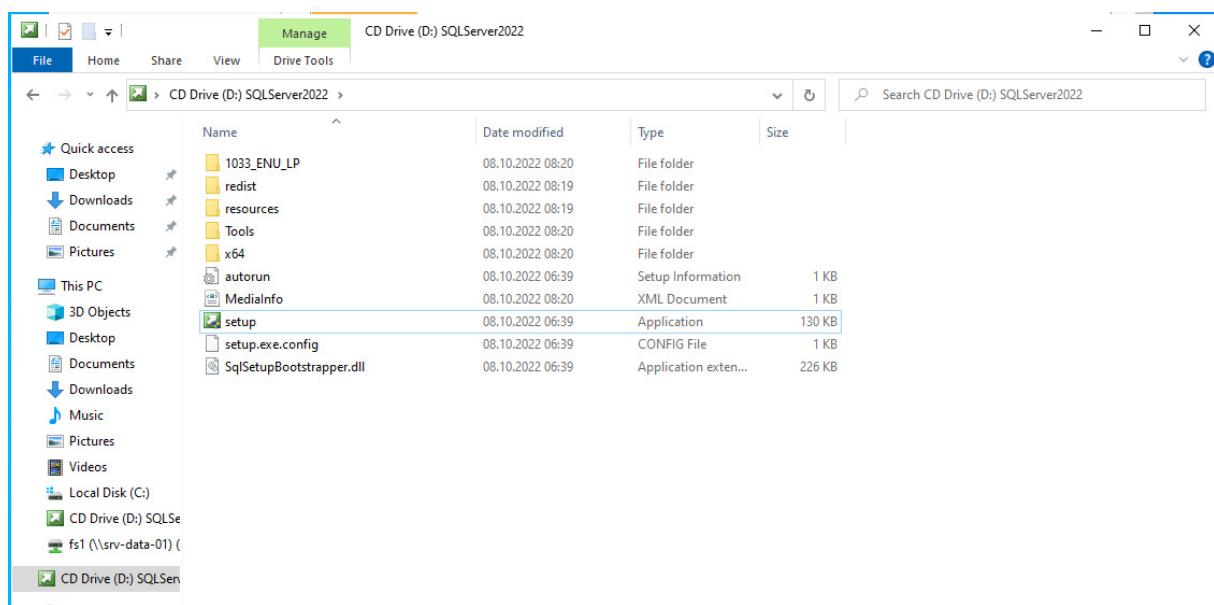
Core Components	✓ License Server Installed
Post Install	✓ Component Initialization Initialized

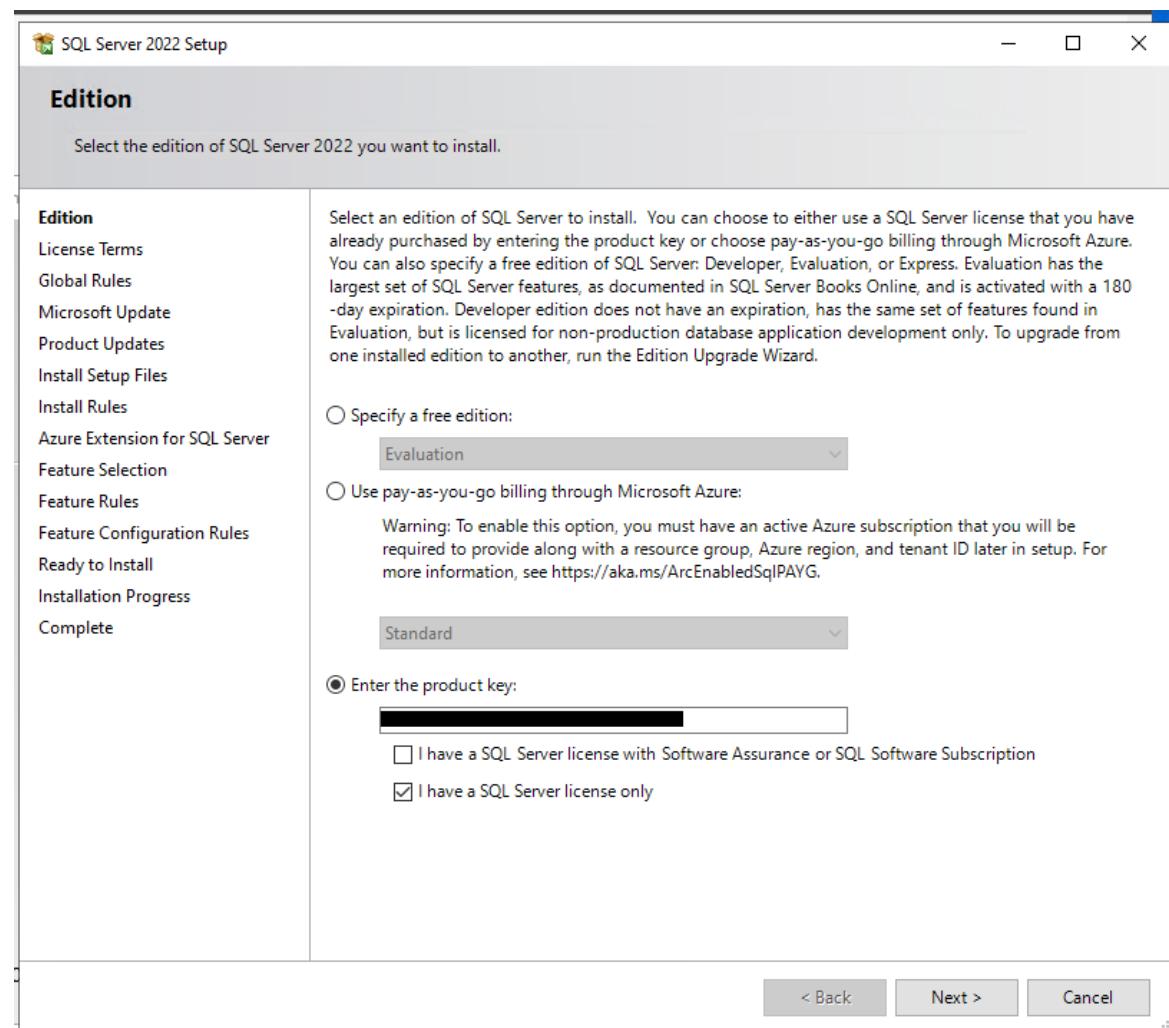
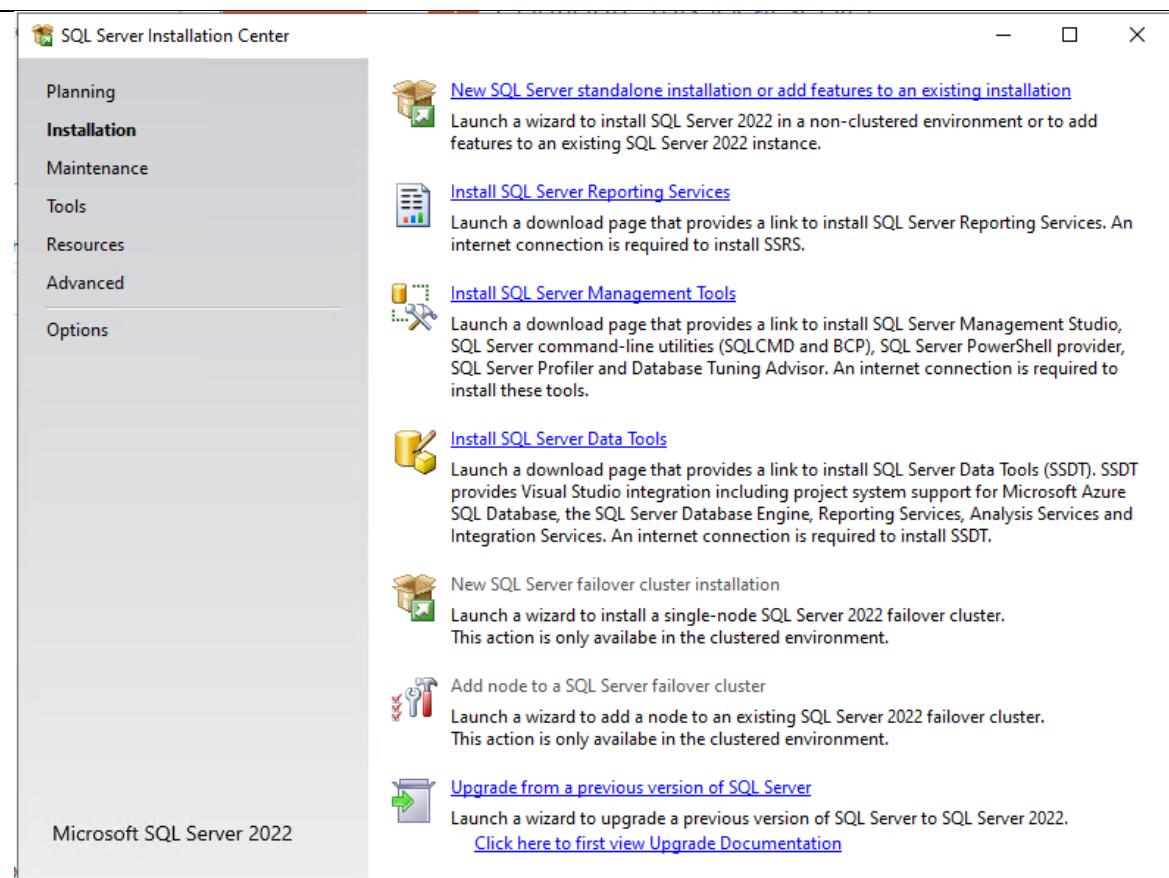
Finish

The screenshot shows the Citrix Licensing Manager interface. At the top, it displays "Citrix Licensing Manager", "License Server Version 11.17.2.0 build 47000", and a greeting "Hello, DOM-POCdo...". Below this is a navigation bar with links for "Dashboard", "Historical Use", "Install Licenses", "Update Licenses", and "Product Information". The main content area is titled "License Usage" and contains a table with two rows of license information. The columns are "PRODUCT-EDITION", "MODEL", "IN USE/INSTALLED", and "AVAILABLE". The first row shows "Citrix Start-up License" as a "Server" model with 0/10000 used and 10000(100%) available. The second row shows "Citrix License Server Diagnostics License" as a "Server" model with 0/10000 used and 10000(100%) available. A "More" link is located at the end of each row. At the bottom of the page, there is a sidebar with icons for "Citrix", "Citrix Licensing Manager", and three Windows Server icons.

Installation SQL-Server

Die SQL-Instanz wird dediziert betrieben, um die Skalierbarkeit und Verfügbarkeit gezielter steuern zu können. Dafür wurde die Windows SQL ISO in die ISO Library hochgeladen. Nach der Installation des Windows Servers konnte die Installation mit der .exe-Datei von der gemounteten ISO gestartet werden.





SQL Server 2022 Setup

Install Rules

Setup rules identify potential problems that might occur while running Setup. Failures must be corrected before Setup can continue.

Edition
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Azure Extension for SQL Server
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete

Operation completed. Passed: 4. Failed 0. Warning 1. Skipped 0.

Hide details << Re-run

[View detailed report](#)

Result	Rule	Status
	Machine Learning Server shared feature support	Passed
	Consistency validation for SQL Server registry keys	Passed
	Computer domain controller	Passed
	Windows Firewall	Warning
	Microsoft .NET Framework 4.7.2, or newer, is required	Passed

SQL Server 2022 Setup

Feature Selection

Select the Standard features to install.

Edition
License Terms
Global Rules
Product Updates
Install Setup Files
Install Rules
Azure Extension for SQL Server
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete

Looking for Reporting Services? [Download it from the web](#)

Features:

Instance Features

Database Engine Services
 SQL Server Replication
 Machine Learning Services and Language Ext.
 Full-Text and Semantic Extractions for Search
 Data Quality Services
 PolyBase Query Service for External Data
 Analysis Services

Shared Features

Data Quality Client
 Integration Services
 Scale Out Worker

Redistributable Features

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on the same computer.

Prerequisites for selected features:

Already installed:
 Windows PowerShell 3.0 or higher
 Microsoft Visual C++ 2017 Redistributable

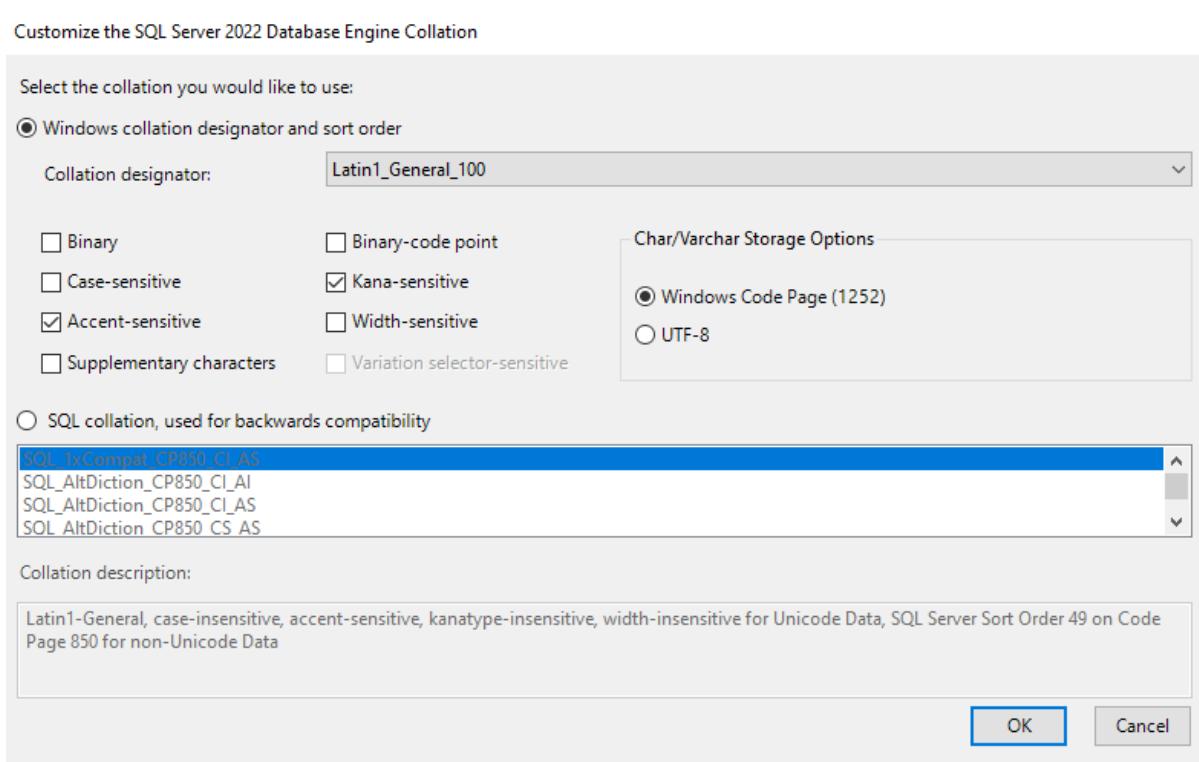
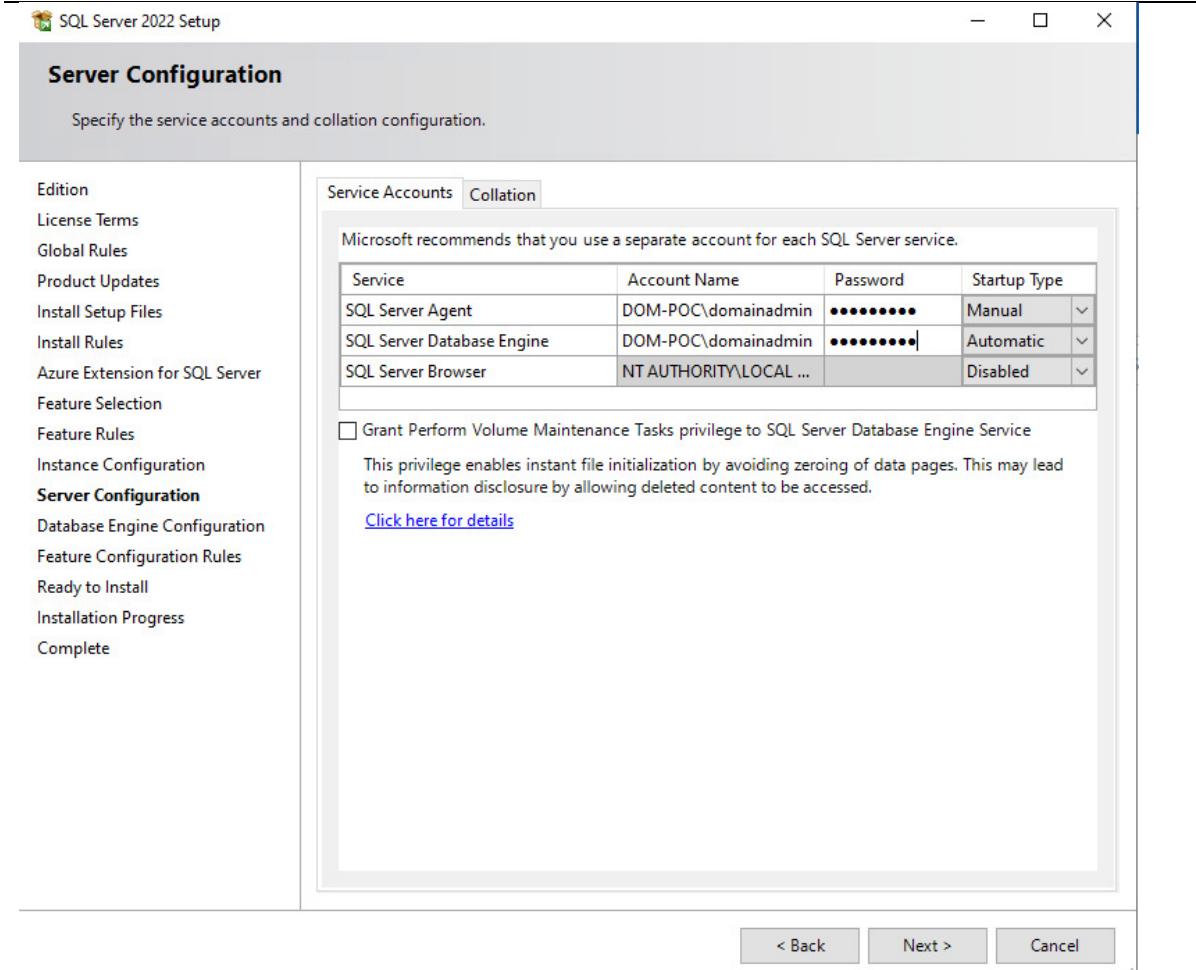
Disk Space Requirements

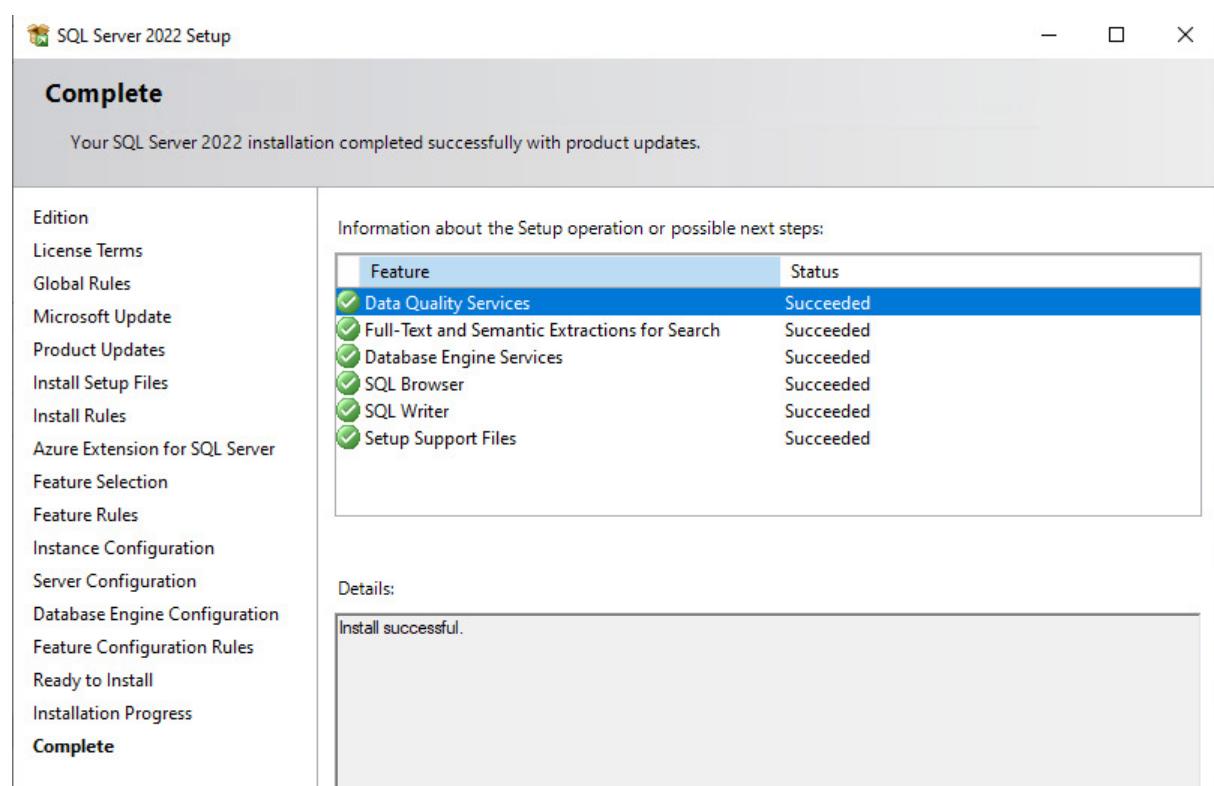
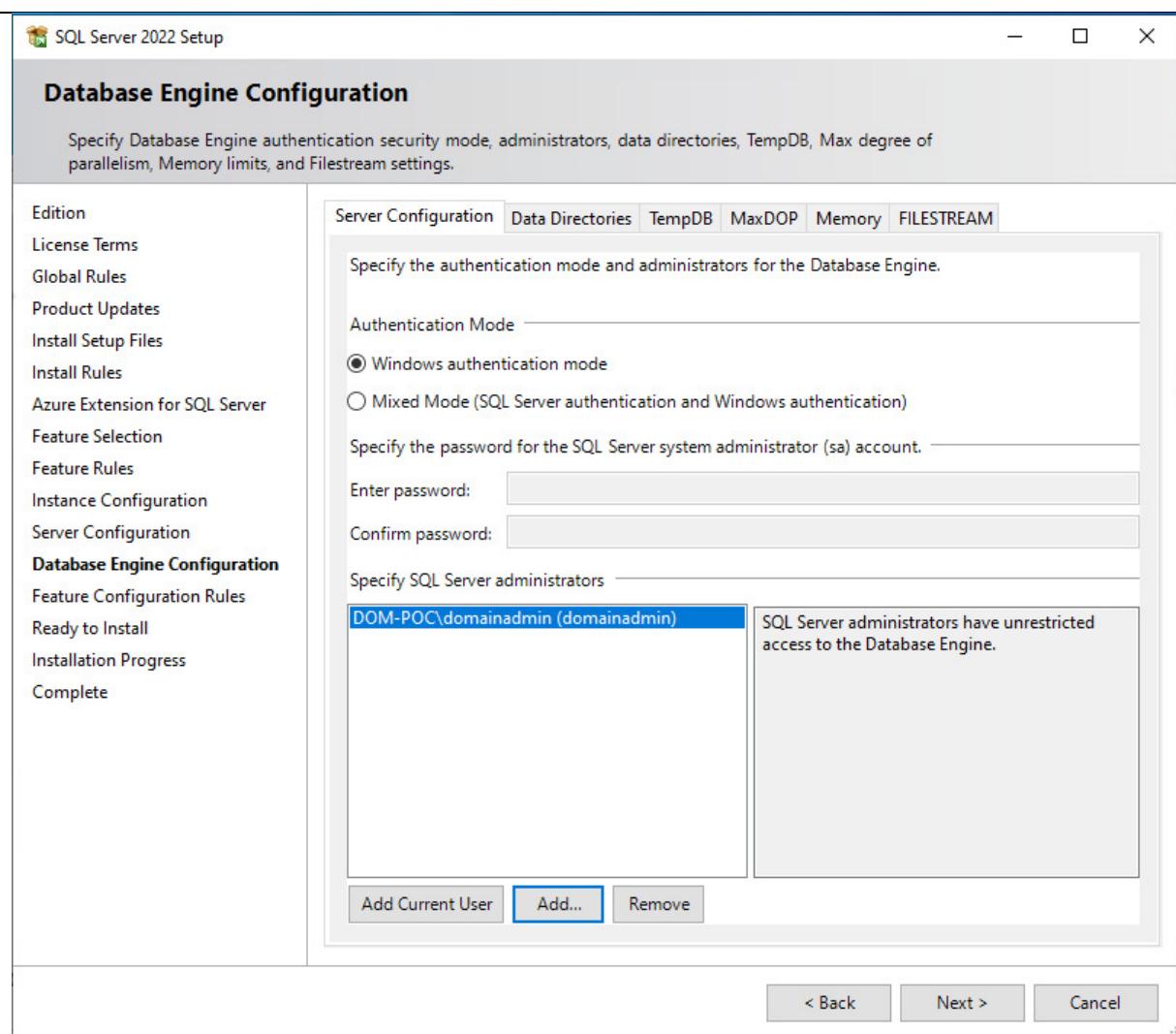
Drive C: 994 MB required, 181558 MB available

Instance root directory: C:\Program Files\Microsoft SQL Server\
Shared feature directory: C:\Program Files\Microsoft SQL Server\
Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

Select All Unselect All

< Back Next > Cancel





Nach der Installation des SQL-Servers, muss man noch die Management Tools installieren.

Learn / SQL / SQL Server /

⊕ 🔍 ⋮

Download SQL Server Management Studio (SSMS)

Article • 04/09/2024 • 49 contributors

Feedback

In this article

[Download SSMS](#)

[Available languages](#)

[What's new](#)

[Previous versions](#)

[Show 8 more](#)

Applies to: ✓ SQL Server ✓ Azure SQL Database ✓ Azure SQL Managed Instance ✓ Azure Synapse Analytics ✓
✓ SQL analytics endpoint in Microsoft Fabric ✓ Warehouse in Microsoft Fabric

SQL Server Management Studio (SSMS) is an integrated environment for managing any SQL infrastructure, from SQL Server to Azure SQL Database. SSMS provides tools to configure, monitor, and administer instances of SQL Server and databases. Use SSMS to deploy, monitor, and upgrade the data-tier components used by your applications and build queries and scripts.

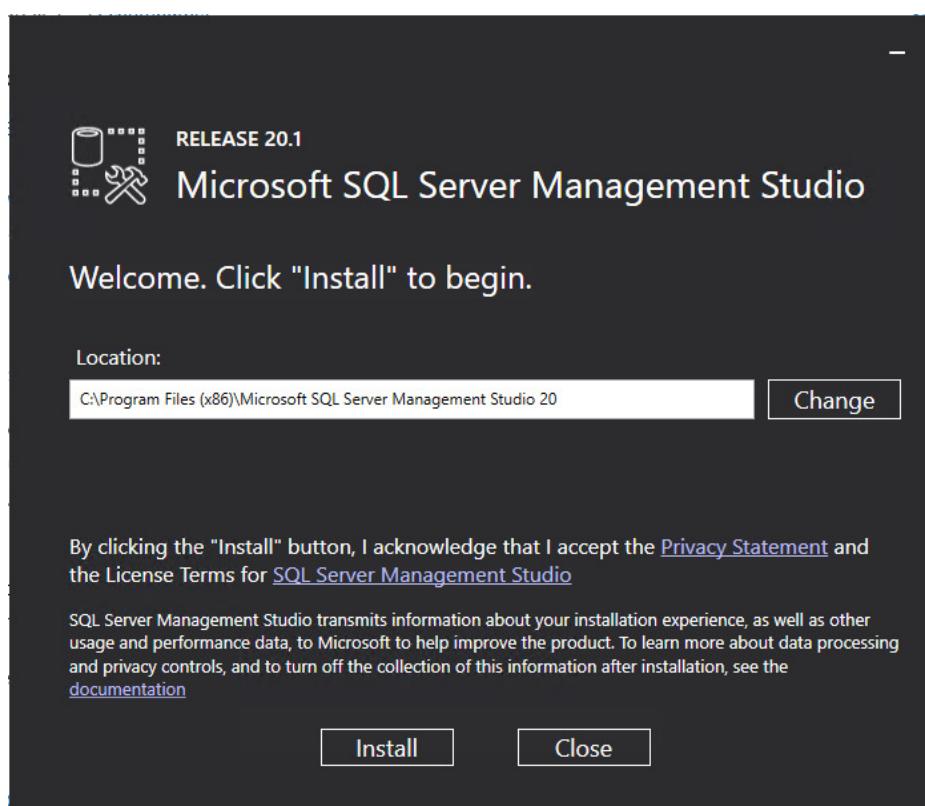
Use SSMS to query, design, and manage your databases and data warehouses, wherever they are - on your local computer or in the cloud.

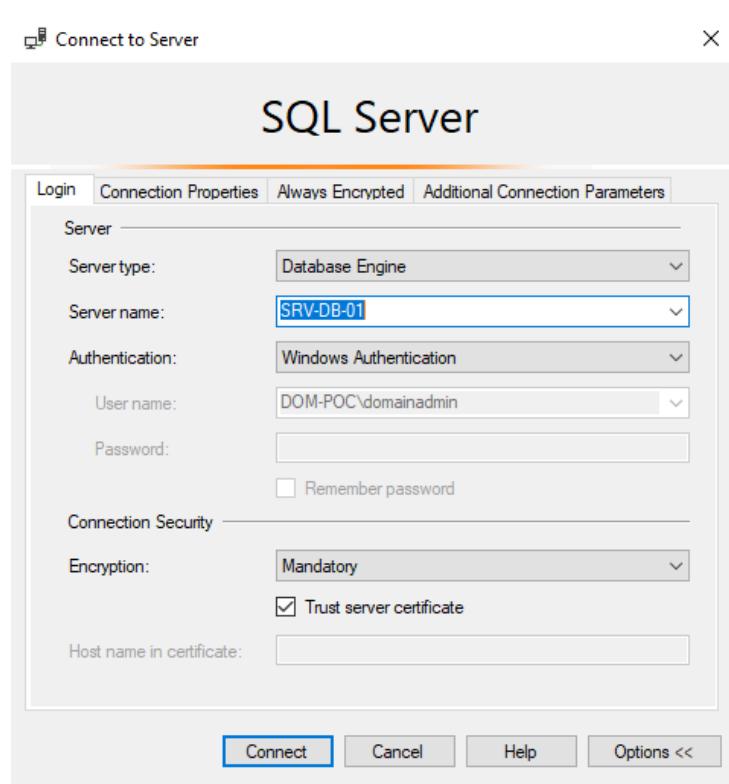
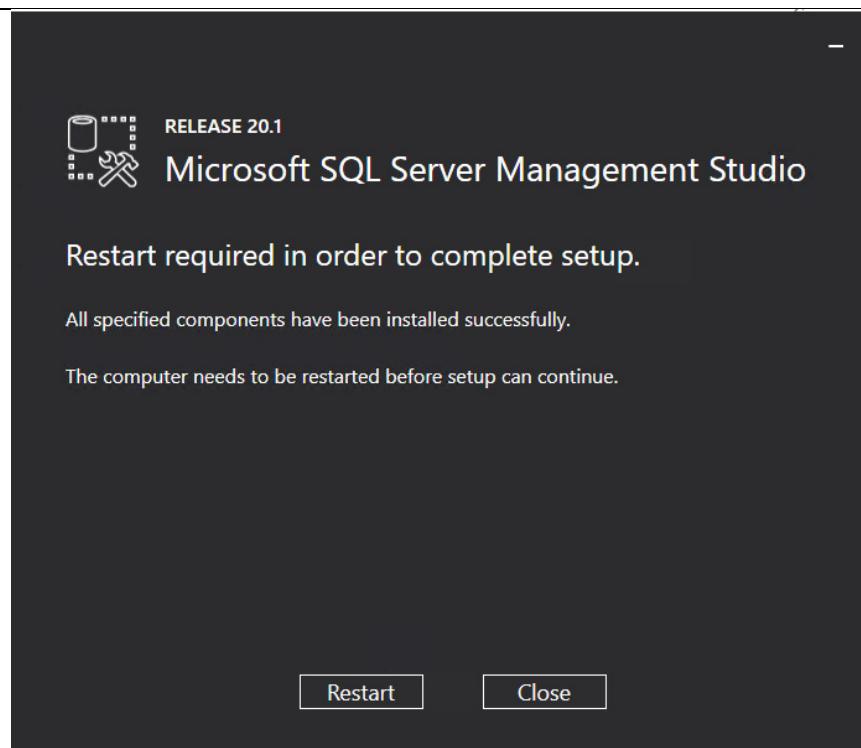
For customers needing a cross-platform companion to SSMS for managing SQL and other Azure databases, use [Azure Data Studio](#).

For details and more information about what's new in this release, *including important security changes*, see [Release notes for SQL Server Management Studio \(SSMS\) 20.1](#).

Download SSMS

[↓ Download SQL Server Management Studio \(SSMS\) 20.1 ↗](#)





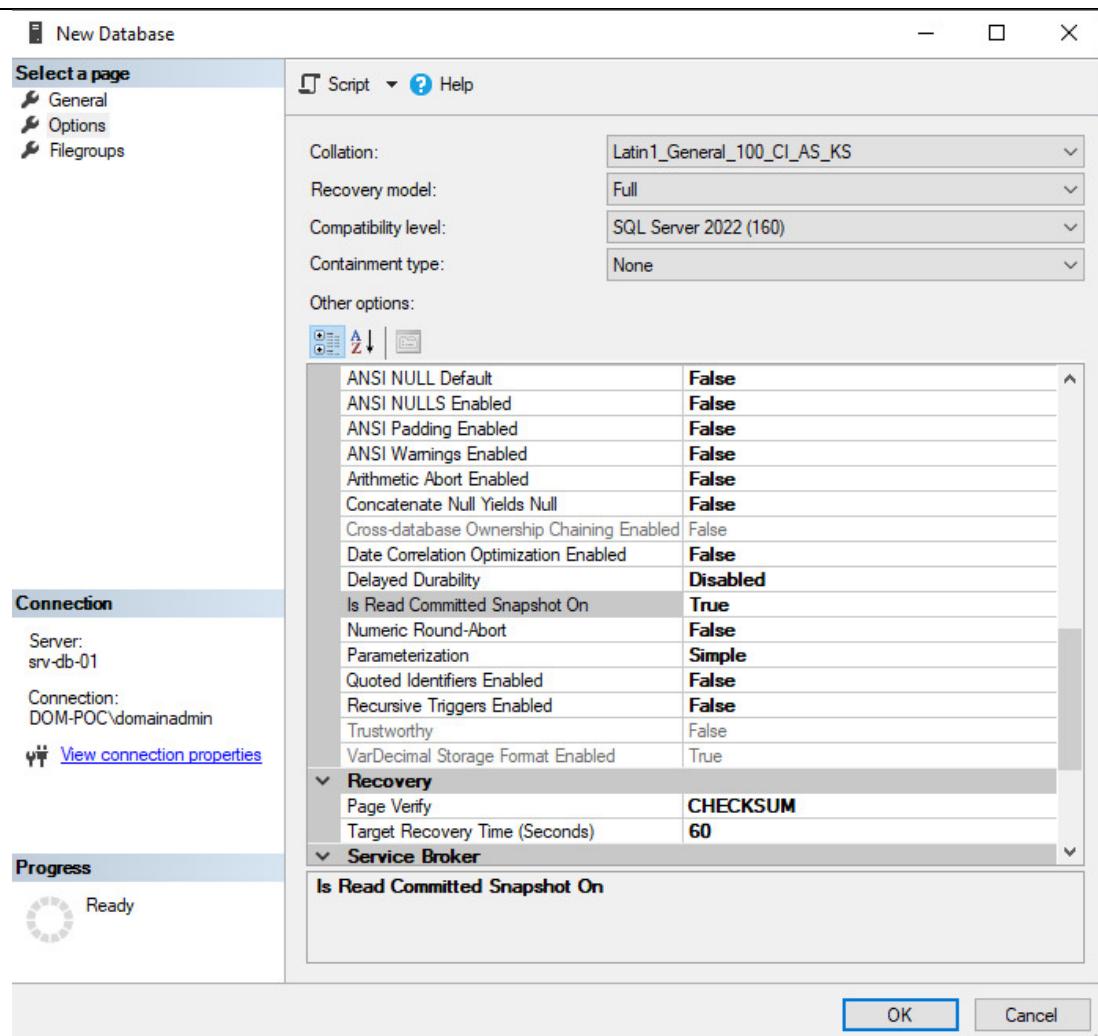
Konfiguration SQL-Server

Drei Datenbanken erstellen mit diesen Einstellungen:

Collation: Latin1_General_100_CI_AS_KS

Is Read Committed Snapshot On = True

CitrixLogging, CitrixMonitoring, CitrixSite



Connect

SRV-DB-01 (SQL Server 16.0.1000.6 - DOM-POC\domainadmin)

- Databases
 - System Databases
 - Database Snapshots
 - CitrixLogging
 - CitrixMonitoring
 - CitrixSite**
- Security

Database Scripts Guide - Notepad

File Edit Format View Help

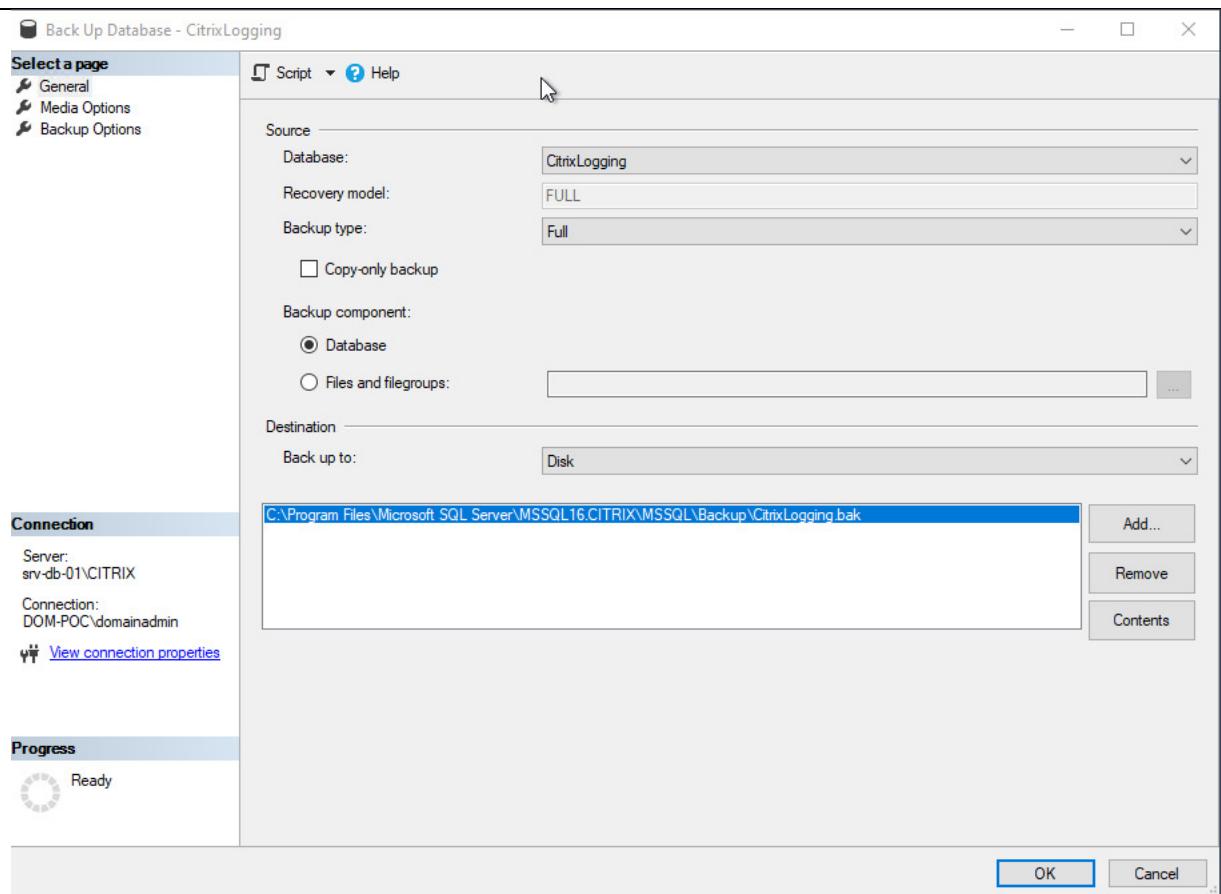
Database Scripts Guide.

Use these scripts to set up databases that are remote from the Delivery Controllers (that is, the databases are not installed on the same server as the Controller).

Create three SQL Server databases: site, monitoring, and logging.
 Use a collation that ends with ".CI_AS_KS". Citrix recommends using a collation that ends with ".100_CI_AS_KS_WS".
 For optimum performance, ensure that the SQL Server Read-Committed Snapshot option is enabled. For details, see <http://support.citrix.com/article/CTX137161>.
 Configure high availability for the databases, if desired.

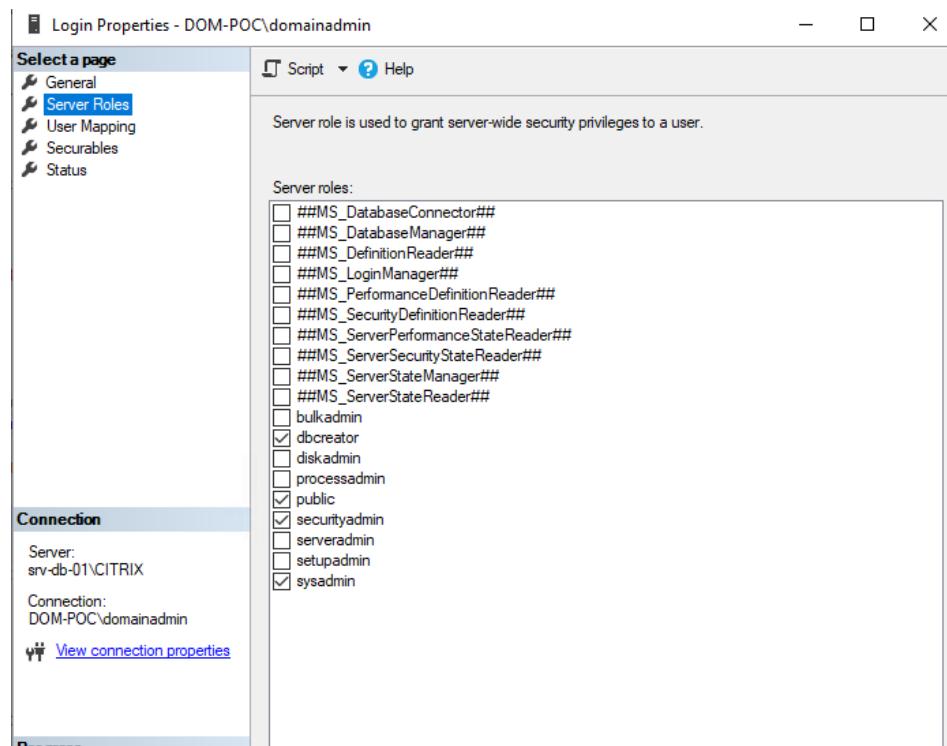
To run the scripts, use the SQLCMD command-line utility, or SQL Server Management Studio in SQLCMD mode. See the Microsoft documentation for details.
 Run each of the xxx_Principal.sql scripts on the principal SQL Server database instances.
 If you configured high availability, for the database run the appropriate xxx_Replicas.sql script on each of the high availability SQL Servers.

Best Practise gemäss Citrix

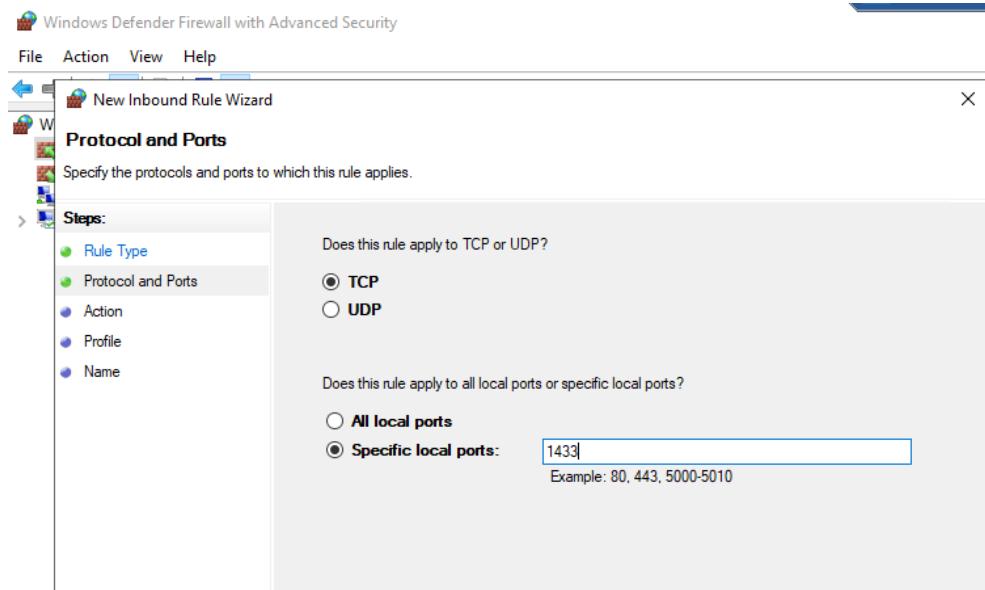


Task starten von den einzelnen Datenbanken und ein lokales Backup erstellen.

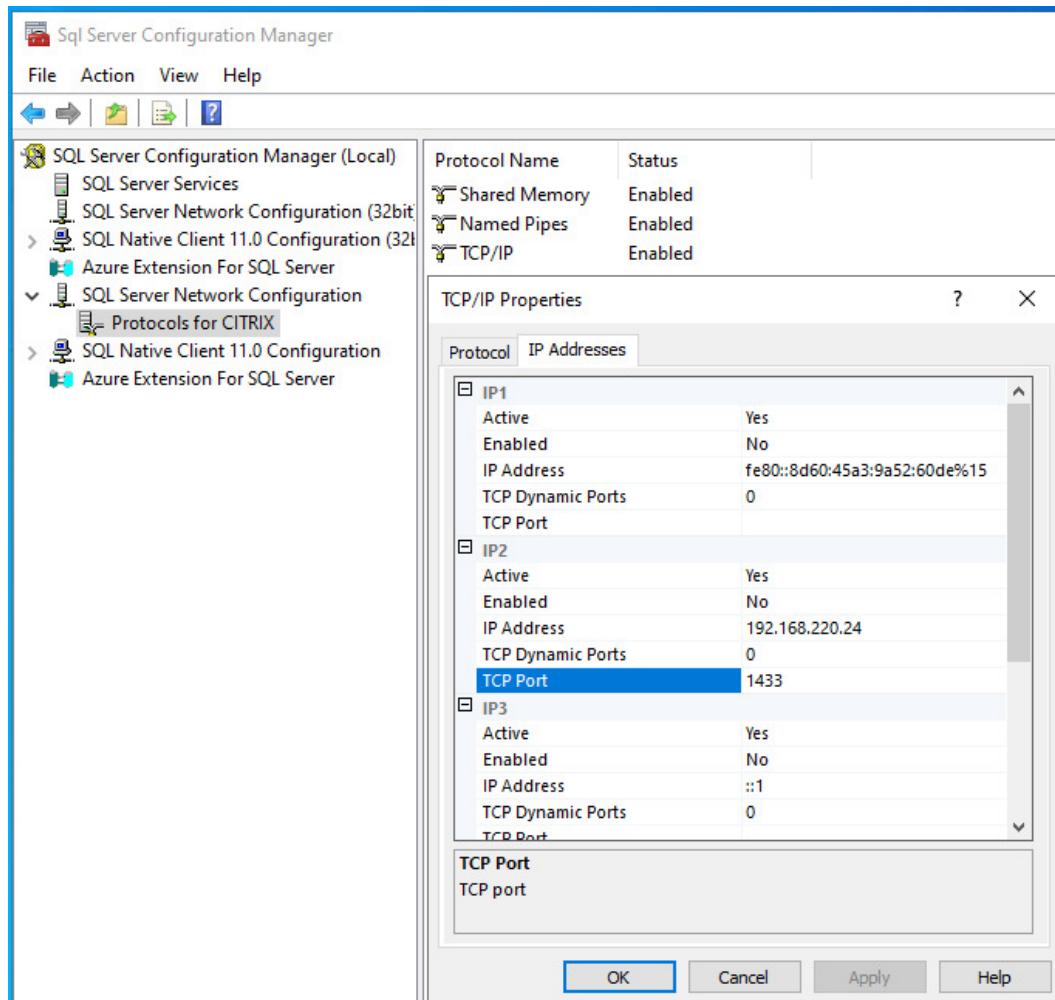
Datenbank Admin sollte diese Rollen haben.



Kontrollieren dass Port 1433 TCP und UDP eingeschaltet ist und sonst Ports öffnen.



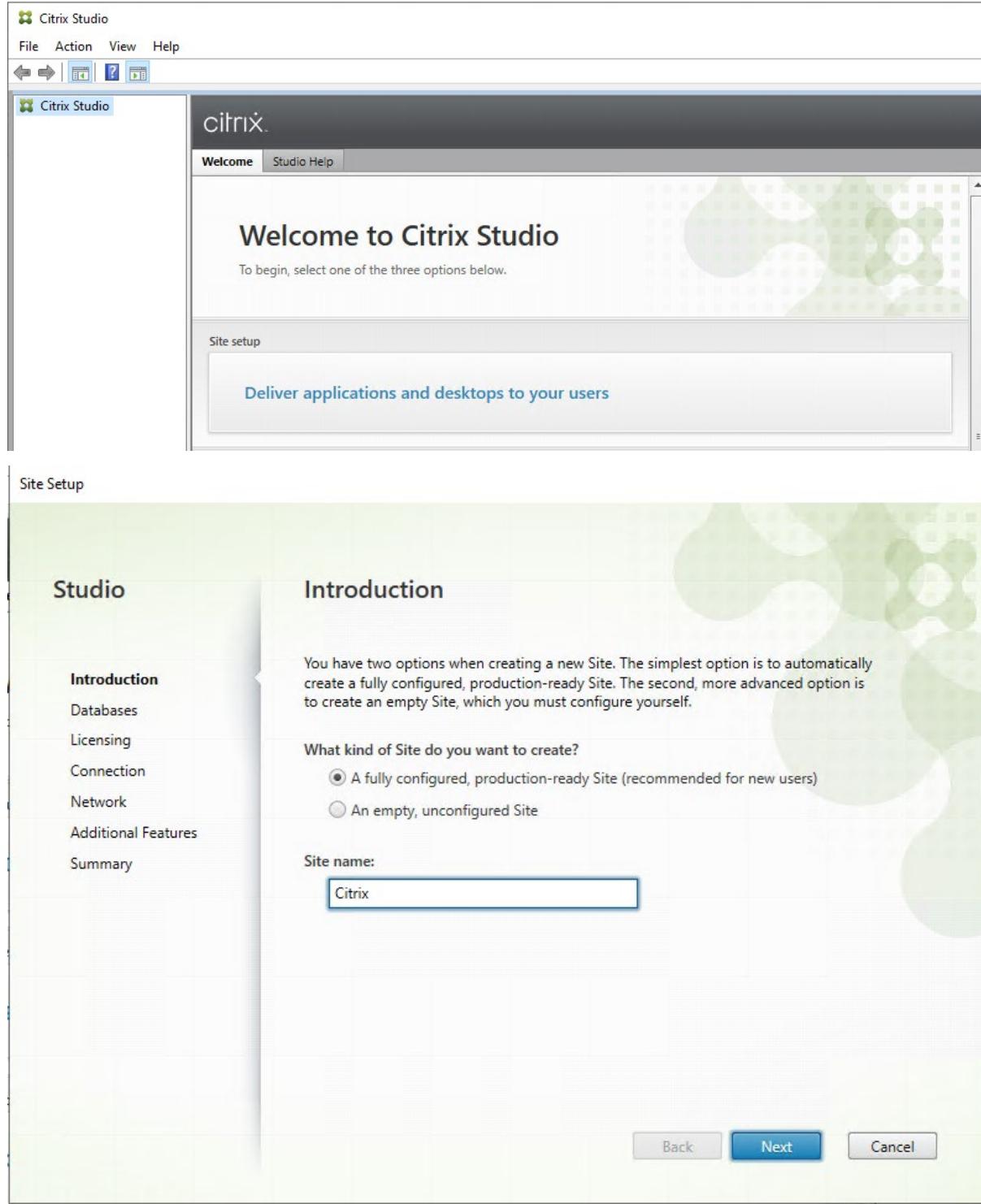
TCP Port 1433 als Standard Port für SQL konfigurieren.



Die Grundeinstellungen sind nun in der Datenbank eingerichtet. Die Konfiguration wird nun auf dem DDC mit der Erstellung einer Site fortgesetzt. Bei der Erstellung der Site muss die Datenbank angegeben werden, wobei die benötigten Konfigurationen automatisch vom Service durchgeführt werden. Ob diese Konfigurationen erfolgreich durchgeführt wurden und wie dies verifiziert werden kann, wird weiter unten beschrieben.

Citrix Site

Auf dem DDC kann nun die erste Site erstellt werden, sobald der Lizenzserver und die SQL-Datenbank bereit sind.



Studio

Databases

Databases store information about Site setup, configuration logging and monitoring. Choose how you want to set up the databases. [Learn more](#)

Create and set up databases from Studio
(You can provide details of existing empty databases)

Generate scripts to manually set up databases on the database server

Provide database details

Data type	Database name	Location (formats)
Site:	CitrixSite	srv-db-01
Monitoring:	CitrixMonitoring	srv-db-01
Logging:	CitrixLogging	srv-db-01

For an AlwaysOn Availability Group, specify the group's listener in the location.

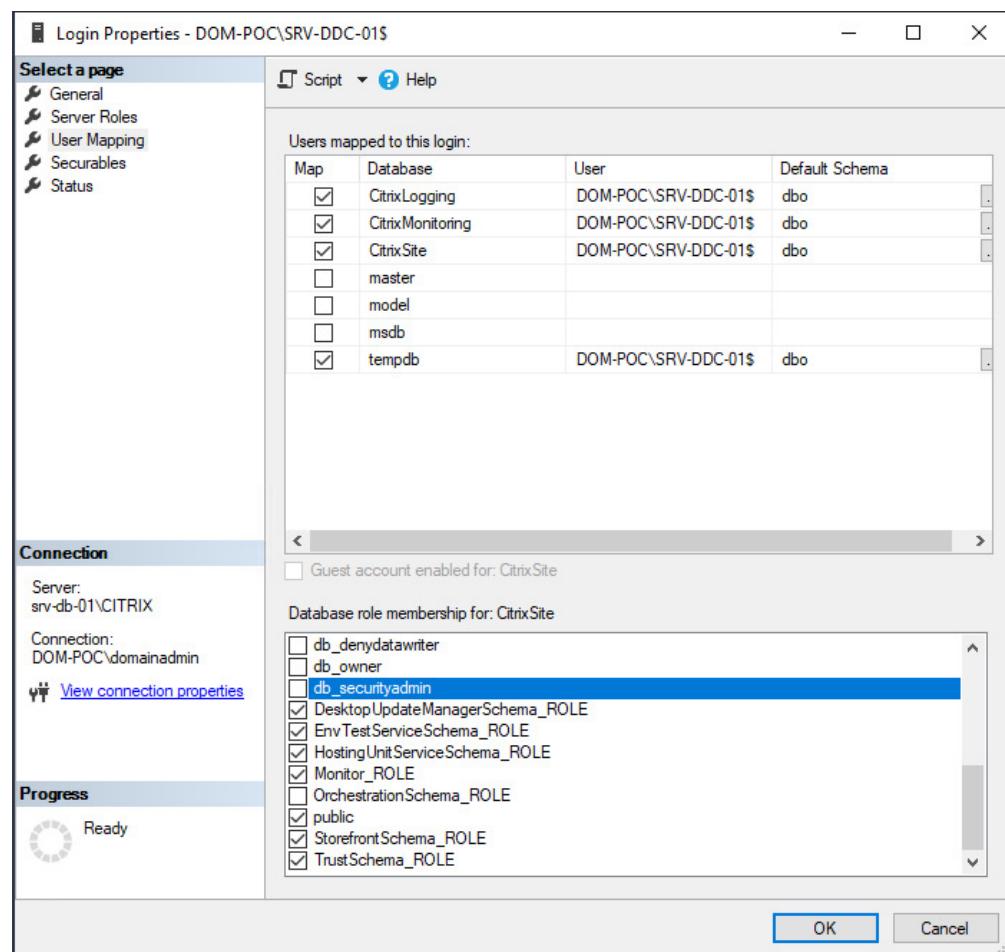
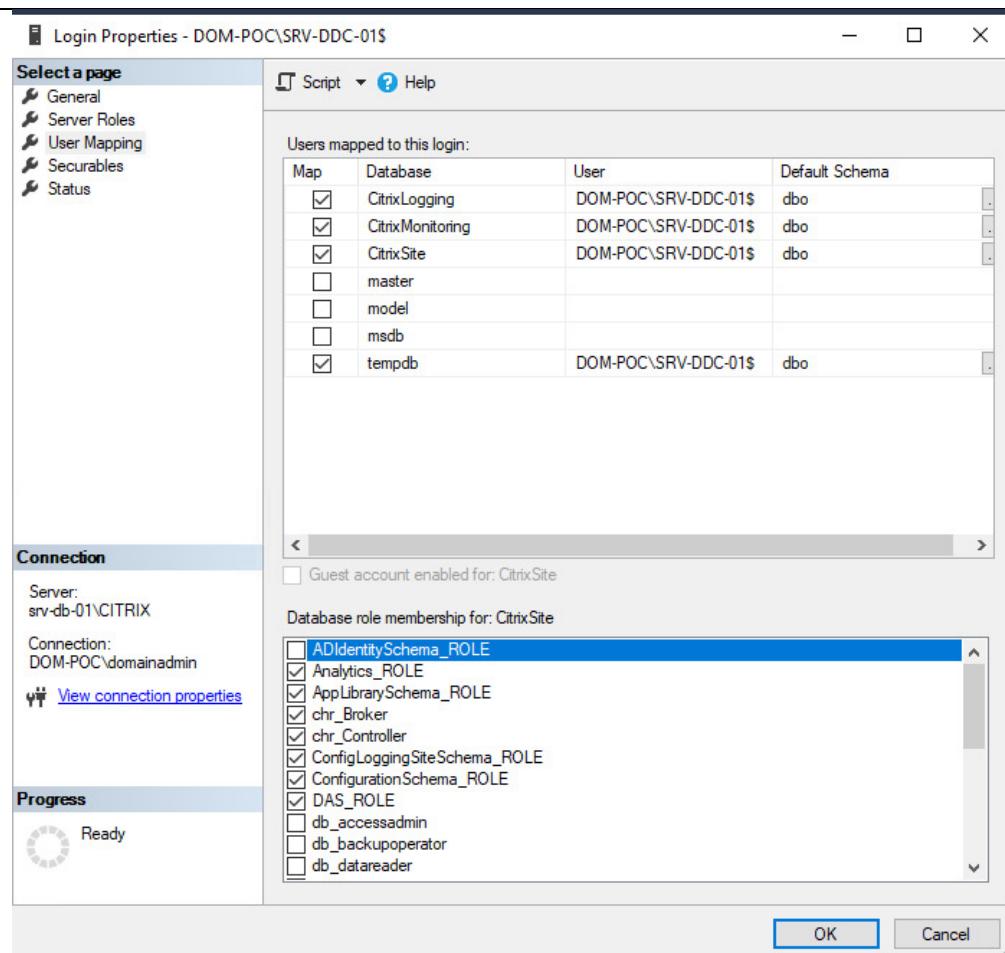
Specify additional Delivery Controllers for this Site [Learn more](#) [Select...](#)

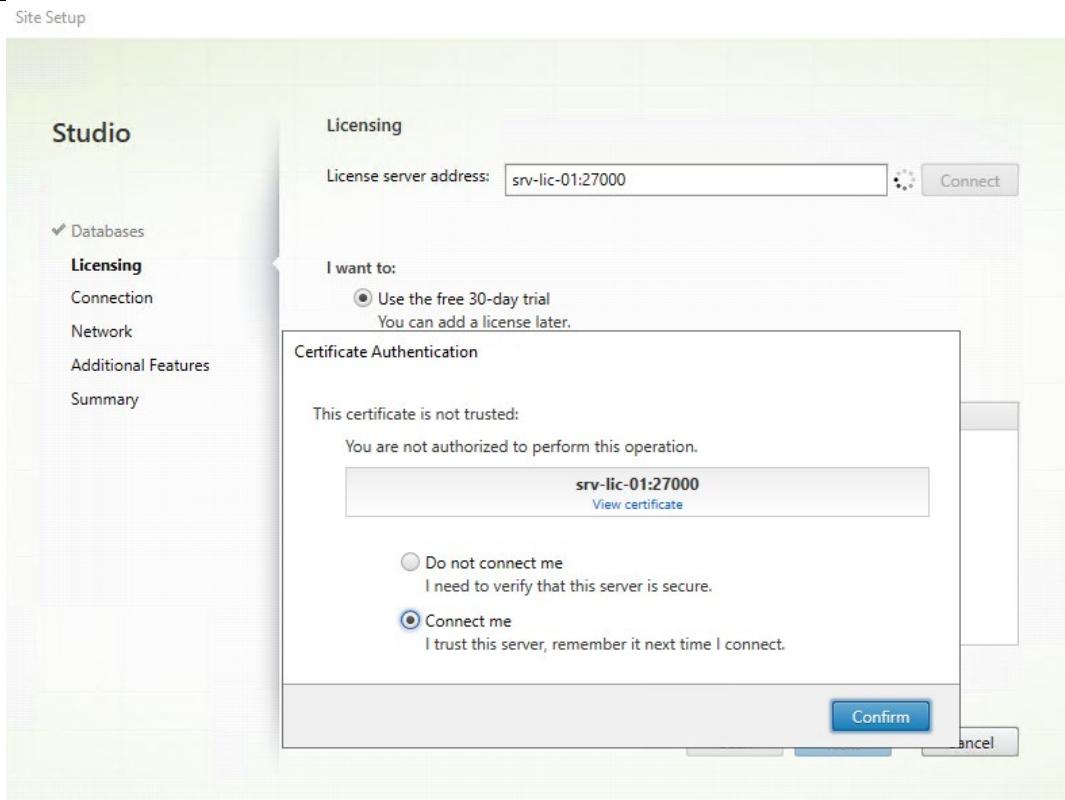
1 selected

[Back](#) [Next](#) [Cancel](#)

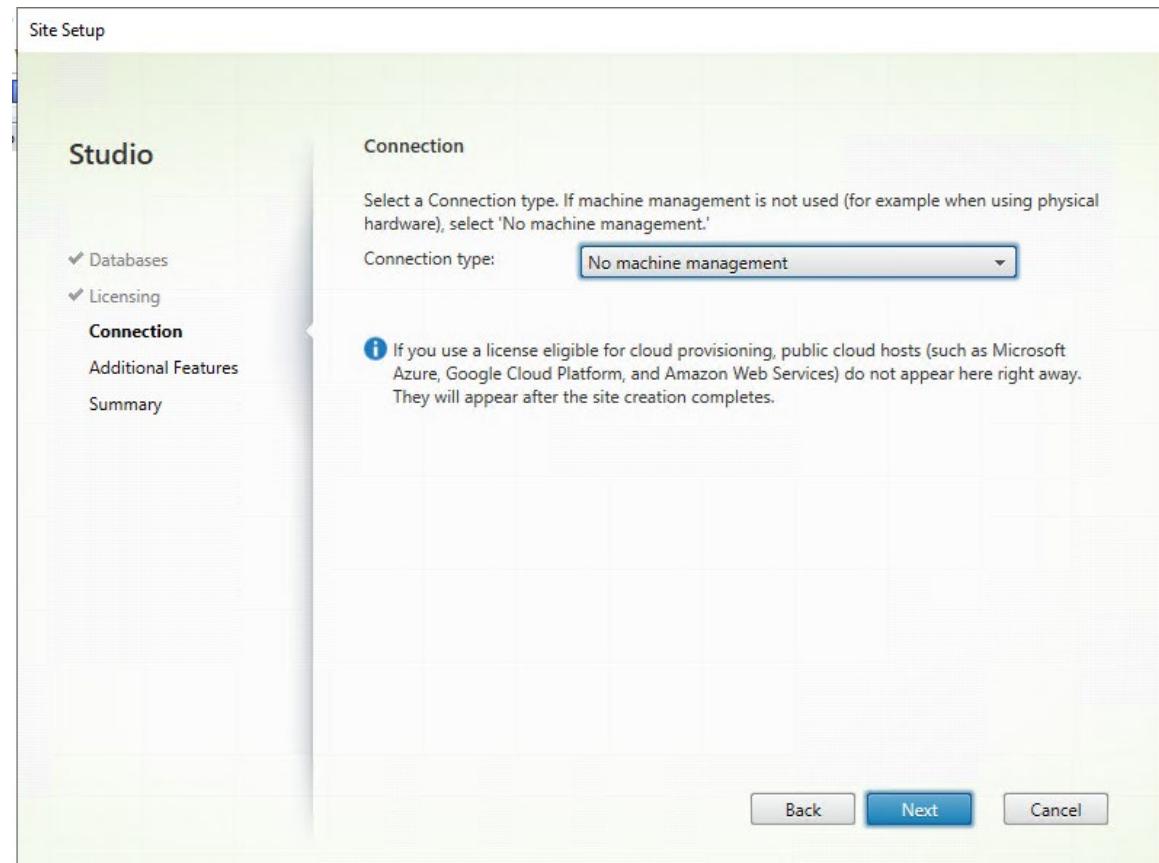
The screenshot shows the 'Databases' configuration screen in Citrix Studio. On the left, a sidebar lists steps: 'Introduction' (marked with a checkmark), 'Databases' (selected), 'Licensing', 'Connection', 'Network', 'Additional Features', and 'Summary'. The main area has a heading 'Databases' with a sub-instruction: 'Databases store information about Site setup, configuration logging and monitoring. Choose how you want to set up the databases.' Below this are two radio button options: 'Create and set up databases from Studio' (selected) and 'Generate scripts to manually set up databases on the database server'. A note says '(You can provide details of existing empty databases)'. A table titled 'Provide database details' lists three entries: 'Site' (CitrixSite, Location: srv-db-01), 'Monitoring' (CitrixMonitoring, Location: srv-db-01), and 'Logging' (CitrixLogging, Location: srv-db-01). A note below the table says 'For an AlwaysOn Availability Group, specify the group's listener in the location.' At the bottom, it says 'Specify additional Delivery Controllers for this Site' with a 'Select...' button, showing '1 selected'. Navigation buttons at the bottom right are 'Back', 'Next', and 'Cancel'.

Nach diesem Schritt kann überprüft werden, ob die Konfiguration korrekt durchgeführt wurde, indem auf der Datenbank nach dem Benutzer DOM-POC\SRV-DDC-01 und seinen Rollen kontrolliert wird.





Der MGMT-Server wurde im Setup noch nicht hinzugefügt, sondern später manuell.



Site Setup

Studio

Summary

Site name:	citrix
Site database:	CitrixSite srv-db-01 (no high availability)
Monitoring database:	CitrixMonitoring srv-db-01 (no high availability)
Logging database:	CitrixLogging srv-db-01 (no high availability)
Delivery Controllers:	srv-ddc-01.dom-poc.local
License server:	srv-lic-01:27000

Summary

Back **Finish** **Cancel**

Citrix Studio

File Action View Help

Back Forward Home Search Help

Citrix Studio (citrix)

- Search
- Machine Catalogs
- Delivery Groups
- Applications
- Policies
- Logging
- Configuration**

 - Administrators
 - Controllers
 - Hosting
 - Licensing
 - StoreFront
 - App-V Publishing
 - Zones

citrix.

Full Deployment Actions PowerShell Studio Help

Site Setup

Follow these steps to set up and deploy your virtual desktop infrastructure.

Configuration

1 Configuration Successful Test site configuration

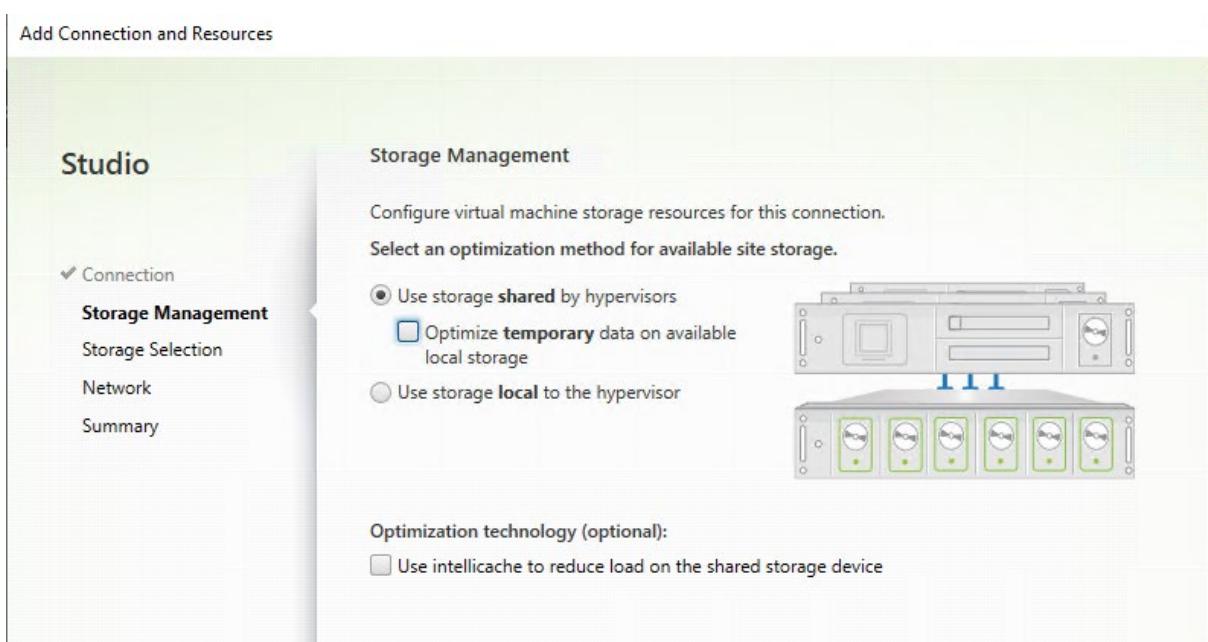
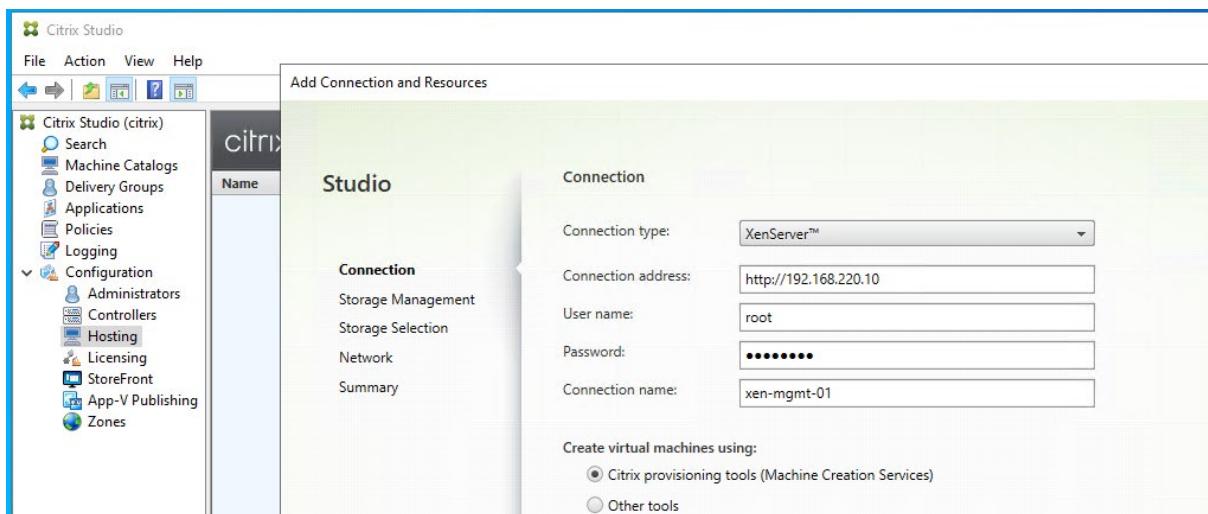
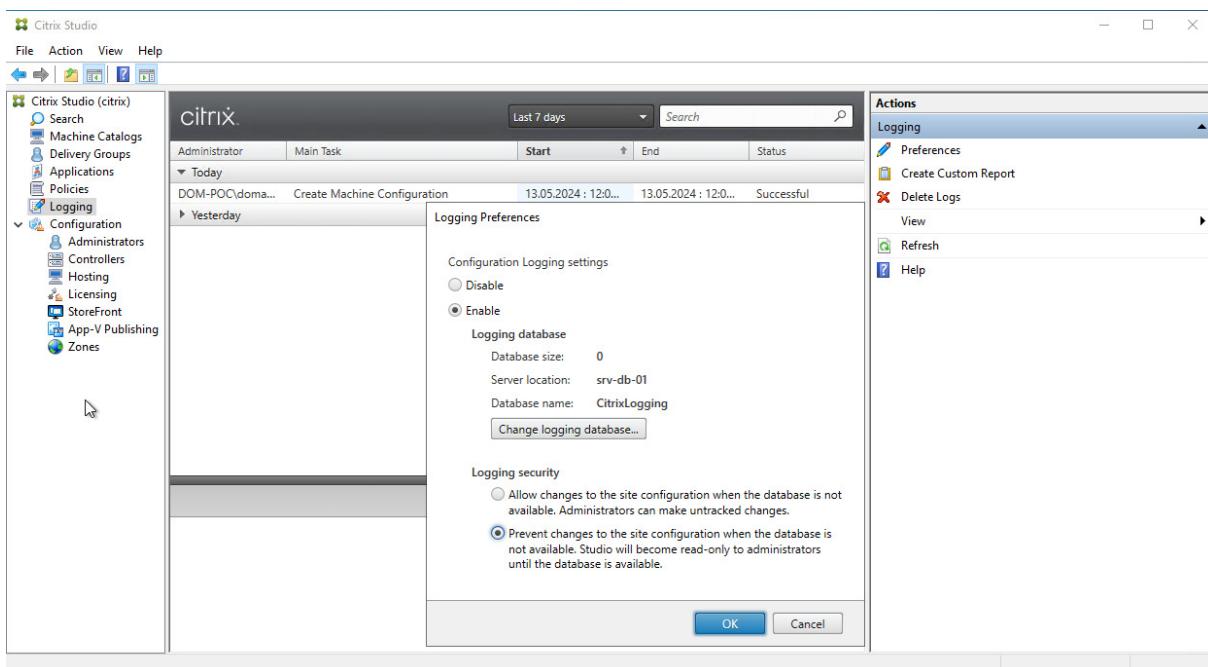
Machine Catalogs

2 Set up machines for desktops and applications or remote PC access Test catalog

Delivery Groups

3 Set up Delivery Groups to assign desktops and applications to your users Test delivery group

Einige Einstellungen und Konfigurationen vornehmen.



Add Connection and Resources

Studio

✓ Connection
✓ Storage Management
Storage Selection
Network
Summary

Storage Selection

When using shared storage, you must select the type of data to store on each shared storage device; machine operating system data, personal user data, and if not storing temporary data locally, temporary data. At least one device must be selected for each data type.

Select data storage locations:

Name	OS	Temporary
NFS XEN-VDI2	<input type="checkbox"/>	<input type="checkbox"/>
NFS XEN-VDI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add Connection and Resources

Studio

✓ Connection
✓ Storage Management
✓ Storage Selection
Network
Summary

Network

Name for these resources:
VDI-GP-Basic-Cluster

The name helps identify the storage and network combination associated with the connection.

Select one or more networks for the virtual machines to use:

Name
MGMT-VLAN 220
NFS
VDI-VLAN 230

Do you want to use graphics virtualization?

No
 Yes

Select a GPU type and group:
NVIDIA A16-4Q (Group of NVIDIA Corporation De... ▾)

3776MB video RAM per virtual machine.
This group allocates GPU resources on demand.

Back Next Cancel

Add Connection and Resources

Studio

Summary

Connection type:	XenServer™
Connection address:	http://192.168.220.10
Connection name:	xen-mgmt-01
Create virtual machines with:	Citrix provisioning tools (Machine Creation Services)
Connection zone:	Primary
Networks:	VDI-VLAN 230
Graphics virtualization:	On
GPU group:	Group of NVIDIA Corporation Device 25b6 GPUs
GPU type:	NVIDIA A16-4Q (3776MB video RAM per VM) This group allocates GPU resources on demand.
Virtual machine OS storage:	NFS XEN-VDI
IntelliCache:	Disabled
Virtual machine temporary storage:	NFS XEN-VDI
Scopes:	All

Back **Finish** **Cancel**

Add Connection and Resources

Studio

Summary

Connection type:	XenServer™
Connection address:	http://xen-mgmt-01.dom-poc.local
Connection name:	MGMT-Server
Create virtual machines with:	Citrix provisioning tools (Machine Creation Services)
Connection zone:	Primary
Networks:	VDI-VLAN 230
Graphics virtualization:	On
GPU group:	Group of NVIDIA Corporation Device 25b6 GPUs
GPU type:	NVIDIA A16-8Q (7616MB video RAM per VM) This group allocates GPU resources on demand.
Virtual machine OS storage:	NFS XEN-VDI
IntelliCache:	Disabled
Virtual machine temporary storage:	NFS XEN-VDI
Scopes:	All

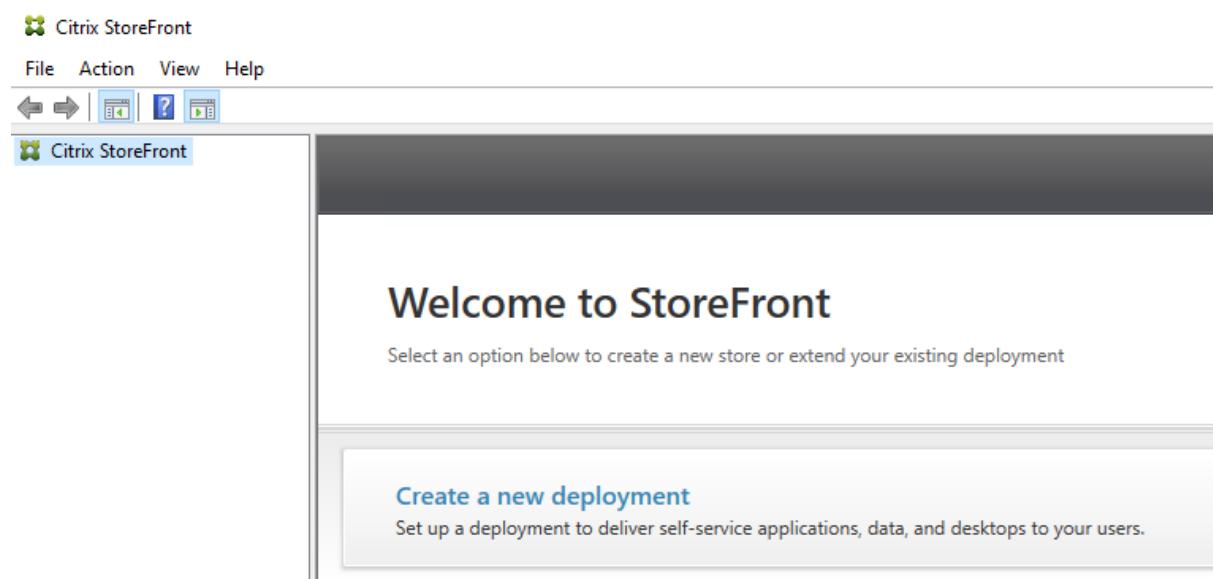
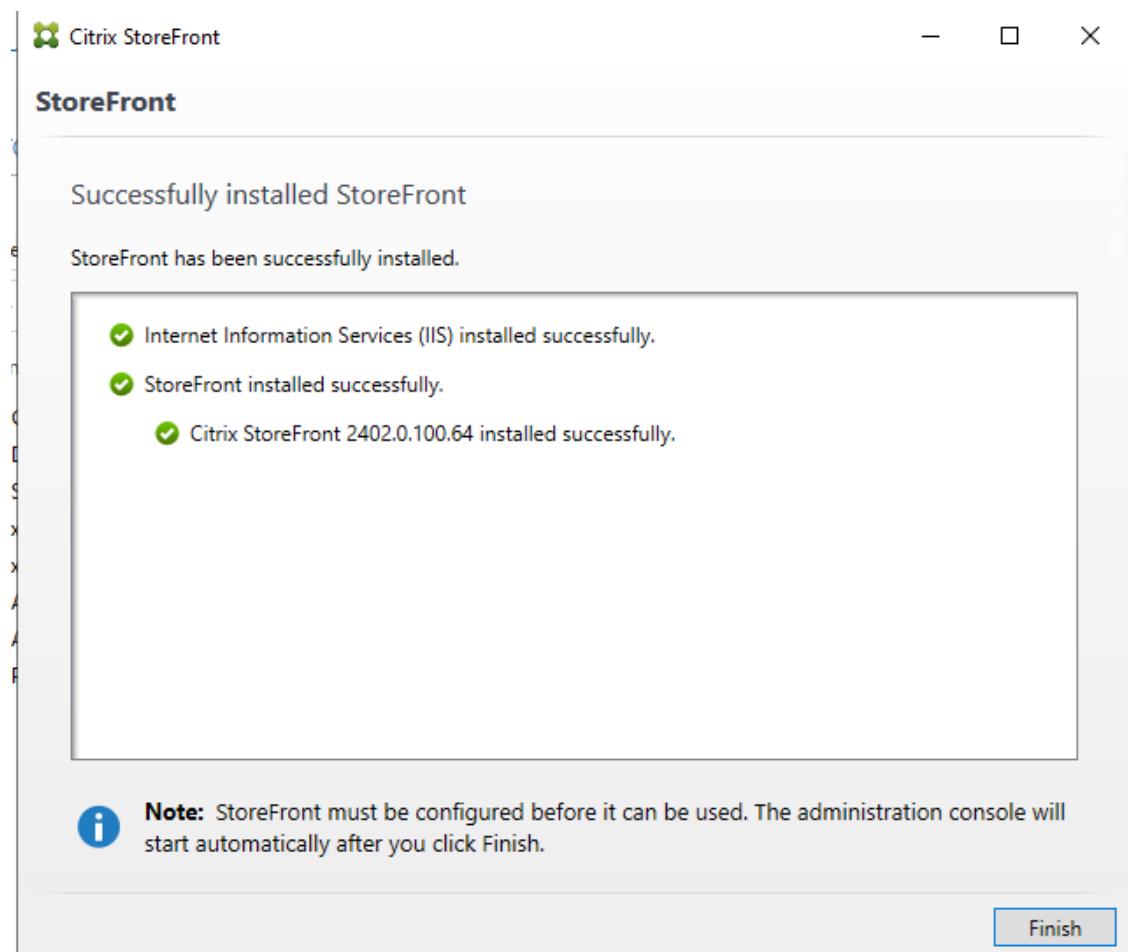
Back **Finish** **Cancel**

Auf diesen Server können nun VDIs mit diesen Ressourcen erstellt werden. Schritte und Voraussetzungen werden weiter unten beschrieben.

Installation StoreFront

Der StoreFront ist das Haupttor zur Umgebung und gehört somit zu den Hauptkomponenten des Services. Er ermöglicht den Benutzern den Zugriff auf ihre Anwendungen und Desktops, indem er eine zentrale Plattform für die Authentifizierung und Bereitstellung bietet. Eine ordnungsgemäße Konfiguration des StoreFronts ist unerlässlich für einen reibungslosen und sicheren Zugang.

Die Installation wieder mit der Source starten.

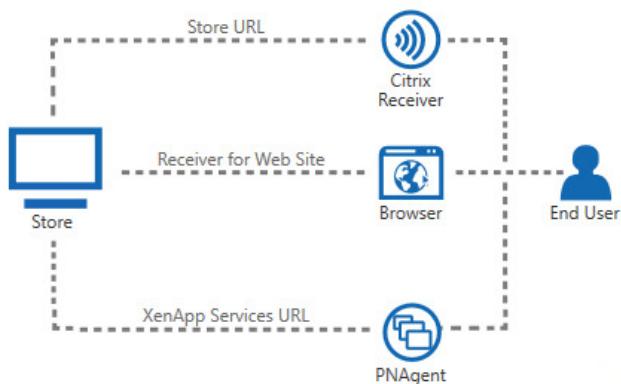


StoreFront**Getting Started**

- Store Name
- Delivery Controllers
- Remote Access
- Authentication Methods
- XenApp Services URL
- Summary

Getting Started

StoreFront stores provide your users with access to their Windows desktops and applications, mobile applications, external software-as-a-service (SaaS) applications, and internal web applications through a single portal from all their devices.

**Next****Cancel****StoreFront**

- Getting Started
- Store Name**
- Delivery Controllers
- Remote Access
- Authentication Methods
- XenApp Services URL
- Summary

Store name and access

Enter a name that helps users identify the store. The store name appears in Citrix Receiver/Workspace app as part of the user's account.

i **Store name and access type cannot be changed, once the store is created.**

Store Name:

Allow only unauthenticated (anonymous) users to access this store
Unauthenticated users can access the store without presenting credentials.

Receiver for Web Site Settings

Set this Receiver for Web site as IIS default

When this is checked, the Receiver for Web site created with the store will be set as the default IIS website. This setting will override any previous defaults configured for the IIS sites.

Back**Next****Cancel**

Edit Delivery Controller

Display name:

Type: Citrix Virtual Apps and Desktops
 Secure Private Access

Servers (load balanced):
Add... Edit... Remove
 Servers are load balanced

Transport type: !

Port:

Advanced Settings

Configure delivery controller communication timeouts and other advanced settings using the 'Settings' dialog.

[Settings](#)

[OK](#)

[Cancel](#)

Create Store

StoreFront

✓ Getting Started
✓ Store Name
✓ Delivery Controllers
✓ Remote Access

Authentication Methods

XenApp Services URL
Summary

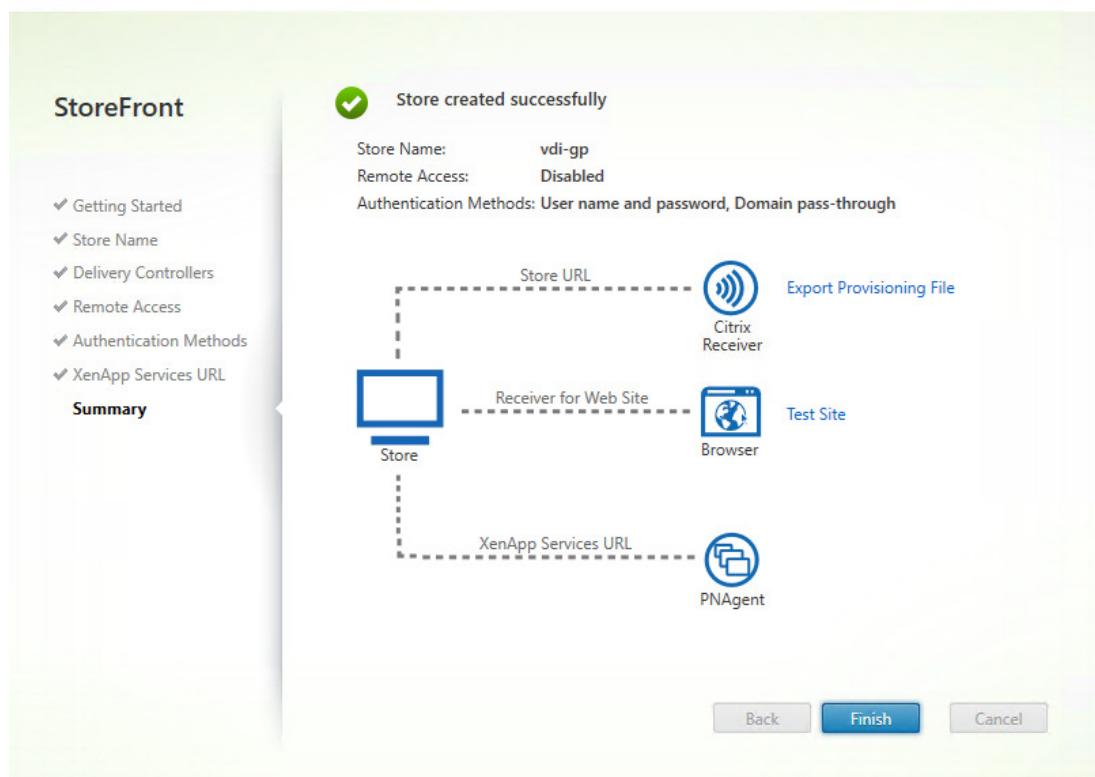
Configure Authentication Methods

Select the methods which users will use to authenticate and access resources.

Method
<input checked="" type="checkbox"/> User name and password
<input type="checkbox"/> SAML Authentication
<input checked="" type="checkbox"/> Domain pass-through Can be enabled / disabled separately on Receiver for Web sites
<input type="checkbox"/> Smart card Can be enabled / disabled separately on Receiver for Web sites
<input type="checkbox"/> HTTP Basic
<input type="checkbox"/> Pass-through from Citrix Gateway

[Back](#) [Next](#) [Cancel](#)

Create Store



Einstellungen und Konfigurationen vornehmen auf dem StoreFront.

Manage Authentication Methods - vdi-gp

Select the methods which users will use to authenticate and access resources.

Method	Settings
<input checked="" type="checkbox"/> User name and password	[Settings]
<input type="checkbox"/> SAML Authentication	[Settings]
<input checked="" type="checkbox"/> Domain pass-through Can be enabled / disabled separately on Receiver for Web sites	[Settings]
<input type="checkbox"/> Smart card Can be enabled / disabled separately on Receiver for Web sites	[Settings]
<input type="checkbox"/> HTTP Basic	[Settings]
<input type="checkbox"/> Pass-through from Citrix Gateway	[Settings]

Installing and uninstalling the authentication methods and the authentication service settings are included in the advanced options.

Create Store Export Multi-Store Provisioning File

Configure Trusted Domains

Allow users to log on from: Trusted domains only

Trusted domains: dom-poc.local

Edit Receiver for Web site - /Citrix/vdi-gpWeb

Customize Receiver for Web Appearance

Logon branding: Logo: C:\temp\Logo_Gruen_1280px.png

Header branding (Post logon): Logo: Upload from local computer

Background color: #0070C0

Text and icon color: #FFFFFF

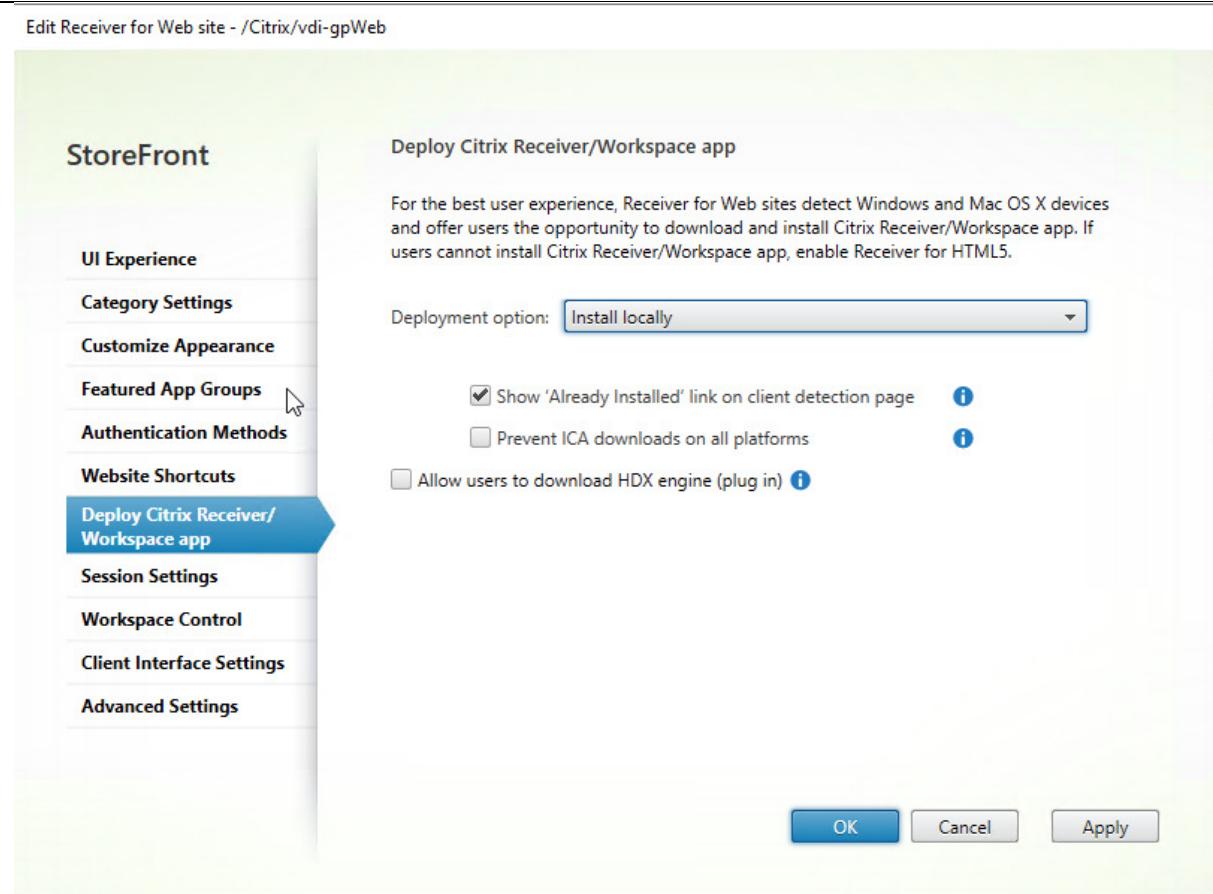
Content branding (Post logon): Link color: #0070C0

Actions

- Create Store
- Export Multi-Store Provisioning File
- Manage Citrix Gateways
- Manage Beacons
- Set Default Website
- View
- Refresh
- Help

vdi-gp

- Manage Delivery Controllers
- Configure Unified Experience
- Manage Authentication Methods
- Manage Receiver for Web Sites → (highlighted with a red arrow)
- Configure Remote Access Settings
- Configure XenApp Services Support
- Configure Store Settings
- Export Provisioning File
- Remove Store
- Help



DNS-Eintrag auf der produktiven Umgebung erstellen, damit die IP auch über DNS aufgelöst werden kann.

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], bedc5.gph.ch., hostmaster.gph.ch.
(same as parent folder)	Name Server (NS)	bedc5.gph.ch.
srv-sfs-01	Host (A)	192.168.220.21

StoreFront mit HTTPS verbinden

Damit die Verbindung vom Client zum StoreFront über HTTPS verläuft, muss ein SSL-Zertifikat im IIS des StoreFronts installiert werden. Dafür wird ein Self-Signed Certificate erstellt.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[1], bedc5.gph.ch., hostmaster.gph.ch.	static
(same as parent folder)	Name Server (NS)	bedc5.gph.ch.	static
srv-sfs-01	Host (A)	192.168.220.21	
vdi	Host (A)	192.168.220.21	

Für die Vereinfachung kann auch ein DNS-Eintrag auf beiden Systemen erstellt werden, um die Webanfrage zu vereinfachen. Vdi.dom-poc.local => srv-sfs-01.dom-poc.local/citrix/vdi-gpWeb/

The screenshot shows the IIS Manager interface. In the left navigation pane, 'SRV-SFS-01 (DOM-POC) dom' is selected. Under 'Sites', 'Default Web Site' is expanded, and 'vdi-gp' is selected. The 'Server Certificates' section displays a table with one row for 'vdi-gp'. The 'Actions' menu on the right has a red box around the 'Create Self-Signed Certificate...' option.

Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store
vdi-gp	srv-sfs-01.dom-poc.local	srv-sfs-01.dom-poc.local	17.05.2025 17:00:00	4445507A69591D5CBAA2188D...	WebHosting

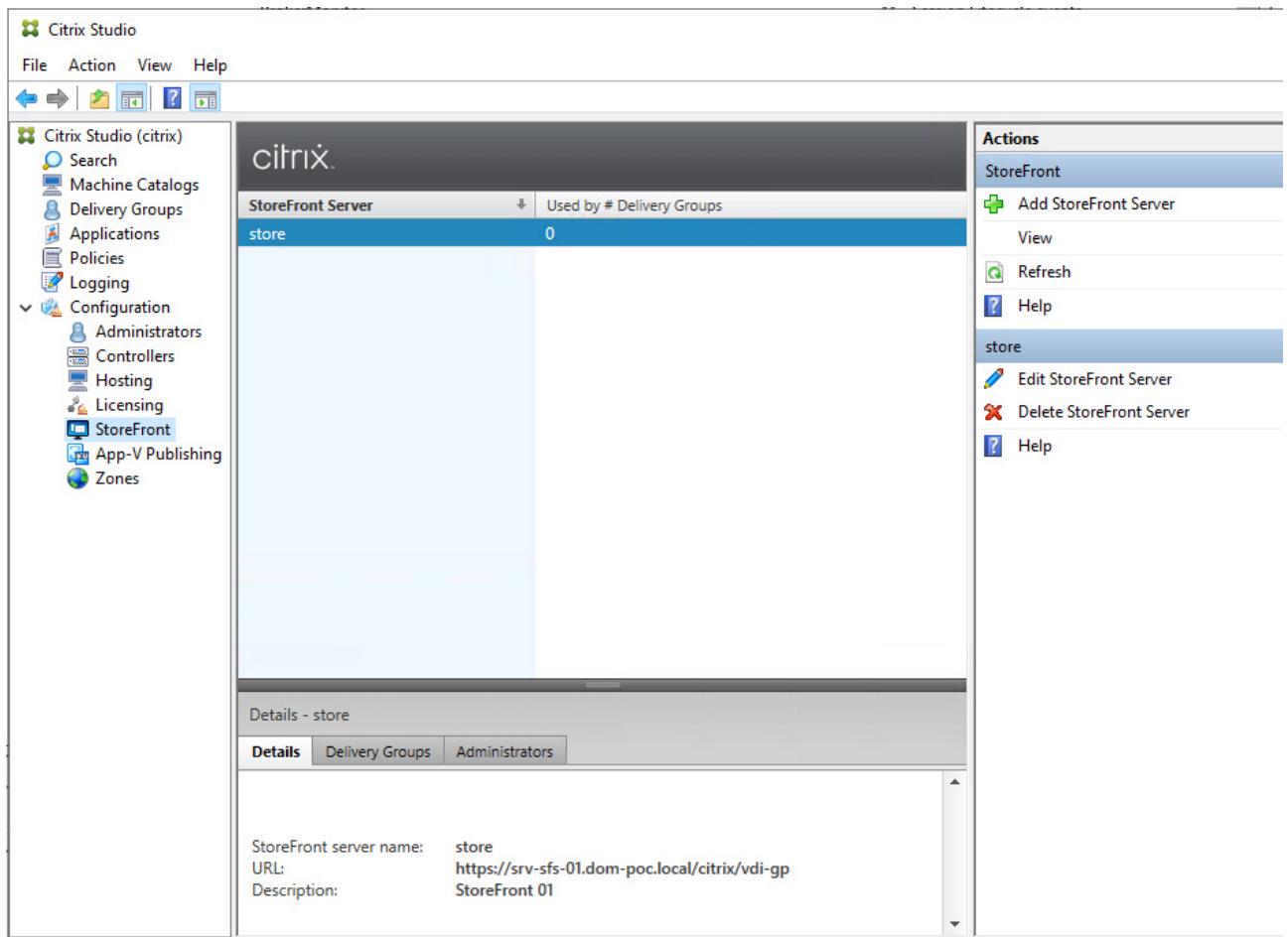
Nach der Erstellung des Zertifikates, muss das Zertifikat bei jedem Client ins Stammzertifizierungsstelle importiert werden.

The screenshot shows the Windows Certificate Snap-in. The left pane shows a tree view with 'Konsolenstamm' expanded, showing 'Certification Authority (Local)' and 'Zertifikat - Aktueller Benutzer'. Under 'Zertifikat - Aktueller Benutzer', there are 'Eigene Zertifikate' and 'Vertrauenswürdige Stammzertifizierungsstellen'. The 'Vertrauenswürdige Stammzertifizierungsstellen' node is expanded, showing 'Zertifikate'. The right pane is a table listing certificates under 'Ausgestellt für' and 'Ausgestellt von'. A red box highlights the 'Zertifikate' folder under 'Vertrauenswürdige Stammzertifizierungsstellen'.

Danach kann die Website mit HTTPS aufgerufen werden.

The screenshot shows a web browser window. The address bar contains 'srv-sfs-01.dom-poc.local/Citrix/vdi-gpWeb/'. A red box highlights the 'Sicherheit' (Security) button in the top-left corner. The main content area shows the 'finitia.' logo. On the right side, there is a login form with fields for 'Benutzername:' (Username), 'Kennwort:' (Password), and 'Domäne:' (Domain). The 'Domäne:' dropdown is set to 'dom-poc.local'. At the bottom right is a blue 'Anmelden' (Login) button.

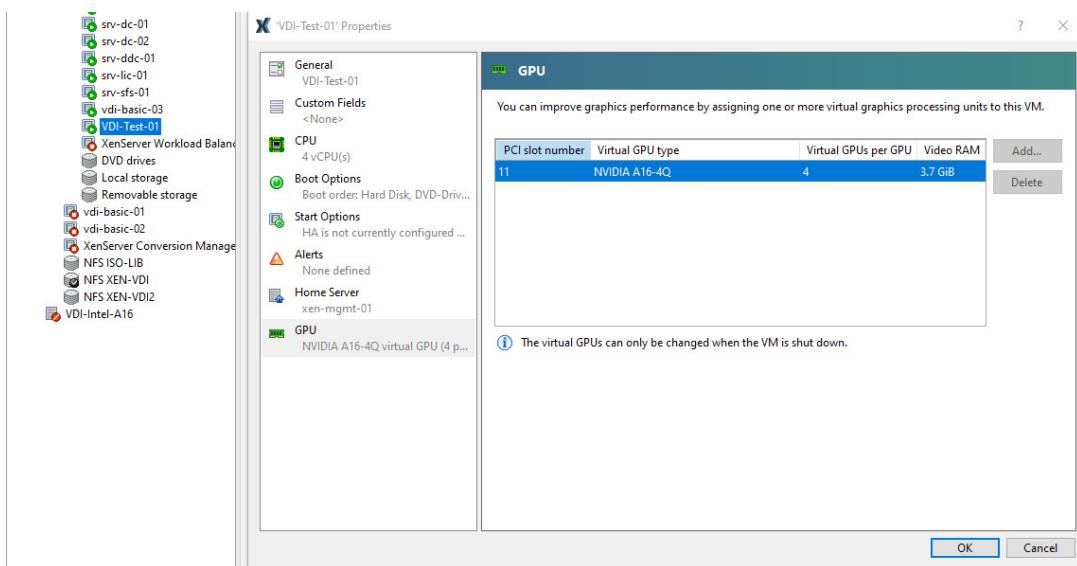
Nach der Fertigstellung des StoreFrontes, kann im DDC der StoreFront als https hinzugefügt werden.



Bereitstellung von Desktops: Golden Image

Die Grundinfrastruktur ist nun so vorbereitet, dass die Konfiguration vorgenommen werden kann, um VDI bereitzustellen. In diesem Abschnitt wird gezeigt, wie dies mit den grundlegenden Funktionen ohne kosmetische Einstellungen bereitgestellt werden kann.

Als erstes muss eine virtuelle Maschine mit dem gewünschten Betriebssystem vorbereitet werden. Dabei werden auch die Hardwareeigenschaften anhand der Werten im Detailkonzept angewendet.



Nach der Konfiguration des Betriebssystems und des Netzwerks muss zwingend der Virtual Delivery Agent installiert werden. Dafür wird wieder die allgemeine Source verwendet.

Citrix Virtual Apps and Desktops 7 2402 LTSR X

Get Started

Delivery Controller

Cannot be installed on this operating system.

Prepare Machines and Images

Virtual Delivery Agent for Windows Single-session OS

Install this agent to deliver applications and desktops from Windows single-session OS virtual machines or physical machines.

Environment

Configuration

I want to:

Create a master MCS image
Select this option if you plan to use Citrix Machine Creation Services (MCS) to provision virtual machines from this master image.

Create master image to be used for Citrix Provisioning (PVS) streaming
Select this option if you plan to use PVS streaming of the target device.

Remote PC Access or machine provisioned with other technologies.
Select this option to install VDA on a physical machine or virtual machine provisioned with technologies other than Machine Creation Service or Citrix Provisioning. This option allows VDAs to be configured with Websockets or similar technologies.

Delivery Controller

Configuration

How do you want to enter the locations of your Delivery Controllers?

Do it later (Advanced)

Do it manually

Choose locations from Active Directory

Let Machine Creation Services do it automatically

Controller address: (Enter the FQDN. IP addresses are not supported.)

srv-ddc-01.dom-poc.local ✓

Test connection Add

Features

<input type="checkbox"/>	Feature (Select all)
<input checked="" type="checkbox"/>	Use Windows Remote Assistance Enable Windows Remote Assistance. Learn more
<input checked="" type="checkbox"/>	Use Real-Time Audio Transport for audio Uses UDP ports 16500 - 16509. Learn more
<input type="checkbox"/>	Use Screen Sharing Use TCP ports 52525 - 52625. Learn more
<input type="checkbox"/>	Is this VDA installed on a VM in the Cloud (i.e. Azure, AWS, Google)? Communicates to Citrix that the VDA is installed in a cloud VM. Learn more

Firewall

The default ports are listed below.

[Printable version](#)

Controller Communications

80 TCP
443 TCP
1494 TCP
2598 TCP
8008 TCP
443 UDP
1494 UDP
2598 UDP

Configure firewall rules:

Automatically

Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.

Summary

Review the prerequisites and confirm the components you want to install.  Restart required

Installation directory

C:\Program Files\Citrix

Core Components

Virtual Delivery Agent

Additional Components: (2)

Citrix Profile Management
Citrix Profile Management WMI plug-in

Delivery Controllers: (1)

 srv-ddc-01.dom-poc.local

Features

Remote Assistance

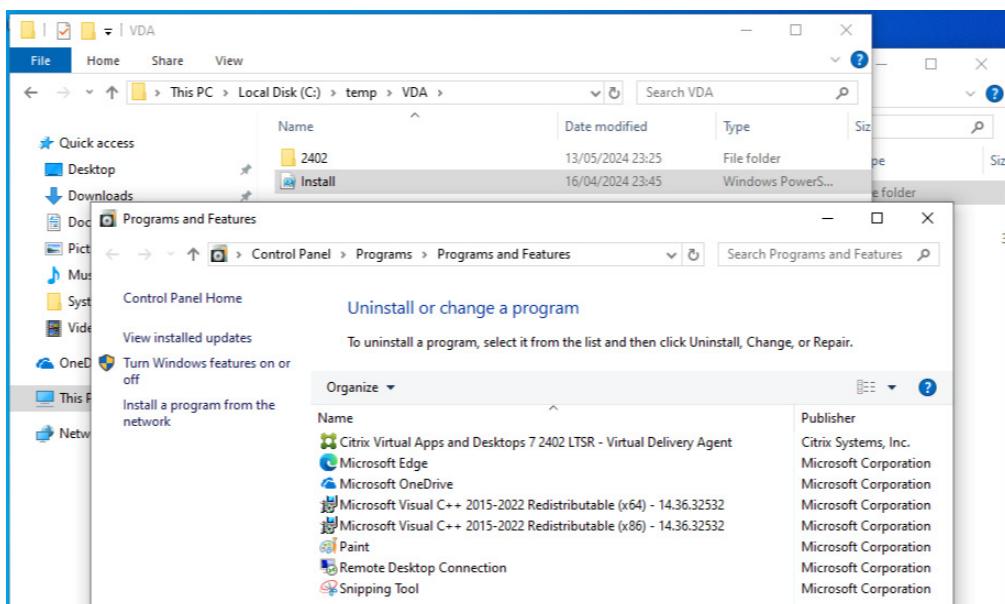
Firewall

UDP Ports: 443, 1494, 2598

TCP Ports: 80, 443, 1494, 2598, 8008

Summary

Review the prerequisites and confirm the components you want to install. ! Restart required



Sobald die VM fertig eingerichtet ist, muss ein Snapshot erstellt werden, der als Image für die Bereitstellung der VDI dient.

Bereitstellung von Desktops: DDC – Machine Catalogs und Delivery Groups

Diese beiden Elemente spielen eine zentrale Rolle bei der Bereitstellung und Verwaltung der virtuellen Desktops. Der Machine Catalog definiert die Maschinen, die für die Bereitstellung verwendet werden, und die Delivery Group ist eine Sammlung von Benutzern und Desktops, die ihnen basierend auf den Maschinen im Machine Catalog zugewiesen werden.

Machine Catalog Setup

The screenshot shows the 'Operating System' step in the 'Machine Catalog Setup' wizard. On the left, a sidebar lists navigation options: Introduction, Operating System (which is selected and highlighted in blue), Machine Management, Desktop Experience, Master Image, Virtual Machines, Computer Accounts, and Summary. The main pane title is 'Operating System' with the sub-instruction 'Select an operating system for this Machine Catalog.' Below this, three radio button options are shown: 'Multi-session OS' (description: 'The multi-session OS machine catalog provides hosted shared desktops for a large-scale deployment of standardized Windows multi-session OS or Linux OS machines.'), 'Single-session OS' (selected, description: 'The single-session OS machine catalog provides VDI desktops ideal for a variety of different users.'), and 'Remote PC Access' (description: 'The Remote PC Access machine catalog provides users with remote access to their physical office desktops, allowing them to work at any time.'). A note at the bottom states: 'There are currently no power management connections suitable for use with Remote PC Access, but you can create one after completing this wizard. Then edit this machine catalog to specify that connection.'

Resources bezieht sich auf die bei der Site erstellte Ressource.

Machine Catalog Setup

The screenshot shows the 'Machine Management' step in the 'Machine Catalog Setup' wizard. The sidebar includes: Introduction, Operating System, Machine Management (selected and highlighted in blue), Desktop Experience, Master Image, Virtual Machines, Computer Accounts, and Summary. The main pane title is 'Machine Management' with the sub-instruction 'This Machine Catalog will use:'. Two radio button options are listed: 'Machines that are power managed (for example, virtual machines or blade PCs)' (selected) and 'Machines that are not power managed (for example, physical machines)'. Below this, the sub-instruction 'Deploy machines using:' is shown with two options: 'Citrix Machine Creation Services (MCS)' (selected) and 'Another service or technology'. Under 'Citrix Machine Creation Services (MCS)', it specifies 'Resources: VDI-GP-Basic-Cluster (Zone: Primary)'. A note at the bottom states: 'Note: For Linux OS machines, consult the administrator documentation for guidance.'

Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Management
- Desktop Experience**
- Master Image
- Virtual Machines
- Computer Accounts
- Summary

Desktop Experience

Which desktop experience do you want users to have?

- I want users to connect to a new (random) desktop each time they log on.
 I want users to connect to the same (static) desktop each time they log on.

Do you want to save any changes that the user makes to the desktop?

- Yes, create a dedicated virtual machine and save changes on the local disk.
 No, discard all changes and clear virtual desktops when the user logs off.

Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Management
- ✓ Desktop Experience
- Master Image**
- Virtual Machines
- Computer Accounts
- Summary

Master Image

The selected master image will be the template for all virtual machines in this catalog. (A master image is also known as a clone, golden, or base image.)

Select a snapshot (or a virtual machine):

- ▶ srv-db-01 ⓘ
- ▶ srv-dc-01 ⓘ
- ▶ srv-dc-02 ⓘ
- ▶ srv-ddc-01 ⓘ
- ▶ srv-lic-01 ⓘ
- ▶ srv-sfs-01 ⓘ
- ▼ VDI-Test-01 ⓘ
 - ▶ Citrix_XD_VDI-Test ⓘ
 - mai_01 ⓘ**
 - ▶ XenServer Conversion Manager ⓘ
 - ▶ XenServer Workload Balancing ⓘ

i Select the minimum functional level for this catalog:

2206 (or newer)

Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog. [Learn more](#)**Studio**

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Management
- ✓ Desktop Experience
- ✓ Master Image
- Virtual Machines**
- Computer Accounts
- Summary

Virtual Machines

How many virtual machines do you want to create?

2

Configure your machines.

Total memory (MB) on each machine:

8000

Configure a cache for temporary data on each machine.

 Memory allocated to cache (MB):256 Disk cache size (GB):10

By default, both check boxes are cleared. (Temporary data is written to OS storage for each VM.) To cache temporary data, a current MCSIO driver must be installed on the VM, in addition to selecting one or both check boxes and values above.

[Learn more](#)

Machine Catalog Setup

Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Management
- ✓ Desktop Experience
- ✓ Master Image
- ✓ Virtual Machines

Computer Accounts

- Summary

Active Directory Computer Accounts

Each machine in a Machine Catalog needs a corresponding Active Directory computer account.

Select an Active Directory account option:

Create new Active Directory accounts
 Use existing Active Directory accounts

Active Directory location for computer accounts:

Domain:



Selected location:

Account naming scheme:

vdi-test-01

Machine Catalog Setup

Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Management
- ✓ Desktop Experience
- ✓ Master Image
- ✓ Virtual Machines
- ✓ Computer Accounts

Summary

Provisioning method:	Machine creation services (MCS)
Desktop experience:	Users connect to a new desktop each time they log on
Resources:	VDI-GP-Basic-Cluster
Master Image name:	mai_01
VDA version:	2206 (or newer)
Number of VMs to create:	2
Virtual CPUs:	4
Memory (MB):	8000
Hard disk (GB):	300
Enable temporary data cache:	No

Machine Catalog name:

Machine Catalog description for administrators: (Optional)

To complete the deployment, assign this Machine Catalog to a Delivery Group by selecting Delivery Groups and then Create or Edit a Delivery Group.

Citrix Studio

File Action View Help

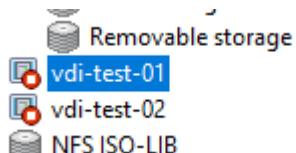
Search Machine Catalogs Delivery Groups Applications Policies Logging Configuration Administrators Controllers Hosting Licensing StoreFront App-V Publishing Zones

Machine Catalog

Machine Catalog	Machine type	No. of machines	Allocated machines
VDI-Test	Single-session OS (Virtual)	2	0
	Allocation Type: Random User data: Discard	Provisioning method: Machine creation ser...	

Details - VDI-Test

Details	Machines	Administrators
Name: VDI-Test	Disk Image: mai_01	
Machine Type: Single-session OS (Virtual)	Virtual CPUs: 4	
Provisioning Method: Machine creation services	Memory: 8000 MB	
Allocation Type: Random	Hard disk: 300 GB	
Set to VDA Version: 2206 (or newer)	Graphics memory: 3776 MB	
Resources: VDI-GP-Basic-Cluster	Installed VDA Version: Unknown	
Scopes: All	Operating System: Unknown	
Zone: Primary		



Create Delivery Group

Studio

Machines

Select a Machine Catalog.

Catalog	Type	Machines
VDI-Test	VDI MCS Random	2

Choose the number of machines for this Delivery Group:

Create Delivery Group

Studio

✓ Introduction
✓ Machines
Users
Applications
Desktops
Summary

Users

Specify who can use the applications and desktops in this Delivery Group. You can assign users and user groups who log on with valid credentials.

Allow any authenticated users to use this Delivery Group.
 Restrict use of this Delivery Group to the following users:

DOM-POC\Admins

Add... Remove

Sessions must launch in a user's home zone, if configured.

Create Delivery Group

Studio

✓ Introduction
✓ Machine
✓ Users
✓ Applications
Desktop
Summary

Add Desktop

Display name: VDI-Test
Description: Example: Assigned desktops for Finance Dept.
The name and description are shown in Citrix Workspace app.

Restrict launches to machines with tag:

Allow everyone with access to this Delivery Group to use a desktop
 Restrict desktop use to:

DOM-POC\Admins

Add... Remove

Enable desktop
Clear this check box to disable delivery of this desktop.

OK Cancel

Create Delivery Group

Studio

Summary

Machine Catalog:	VDI-Test
Machine type:	Single-session OS
Allocation type:	Random
Machines added:	DOM-POC\vd़-test-01 DOM-POC\vd़-test-02 2 unassigned
Users:	DOM-POC\Admins
Desktops:	VDI-Test
Launch in user's home zone:	No
Autoscale:	On (configure it in Edit Delivery Group)

Delivery Group name:

Delivery Group description, used as label in Citrix Workspace app (optional):

Back **Finish** **Cancel**

Search results for "Delivery Group Is "DG_VDI-Basic-DE""

Single-session OS Machines (3) **Multi-session OS Machines (0)** **Sessions (0)** Clear search

Name	Machine Catalog	Delivery Group	User	Maintenance Mode	Persist User Changes	Power State	Registration State
vdi-basic-01.dom-poc.local	MC_VDI-Basic-DE	DG_VDI-Basic-DE	-	Off	Discard	Off	Unregistered
vdi-basic-02.dom-poc.local	MC_VDI-Basic-DE	DG_VDI-Basic-DE	-	Off	Discard	Off	Unregistered
vdi-basic-03.dom-poc.local	MC_VDI-Basic-DE	DG_VDI-Basic-DE	-	Off	Discard	On	Registered

Sobald die Maschinen aufgebaut sind und mit der Delivery Group verteilt worden sind, kann man sich über Web oder App auf die zugewiesene Ressource verbinden.

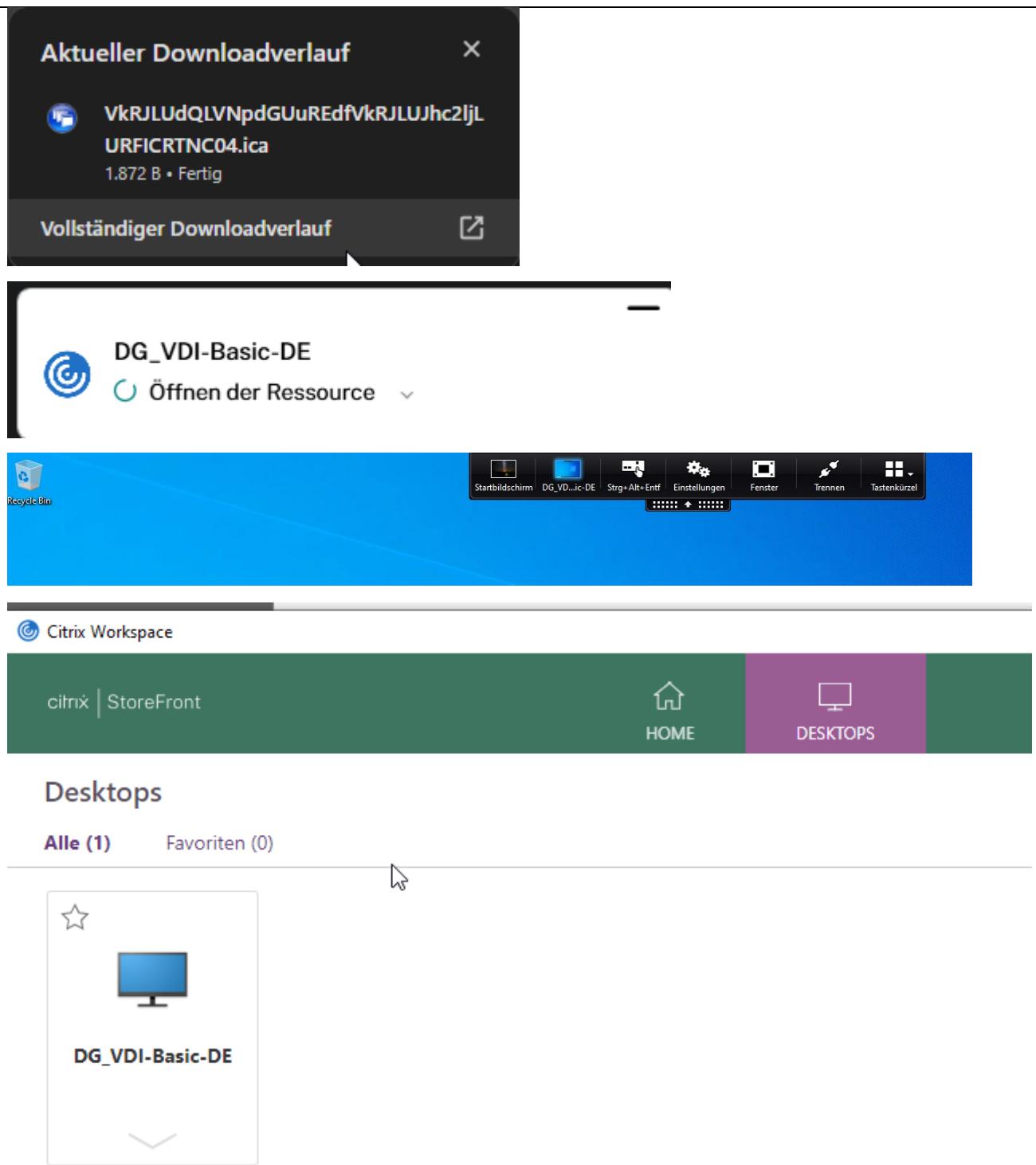
srv-sfs-01.dom-poc.local/Citrix/vdi-gpWeb/

Freshservice - Ticket... DeepL Translate – D... Geschäft TrendMicro Backup Library Privat Pure Keeper® Passwort... Altiris Workflow

citrix | StoreFront HOME DESKTOPS

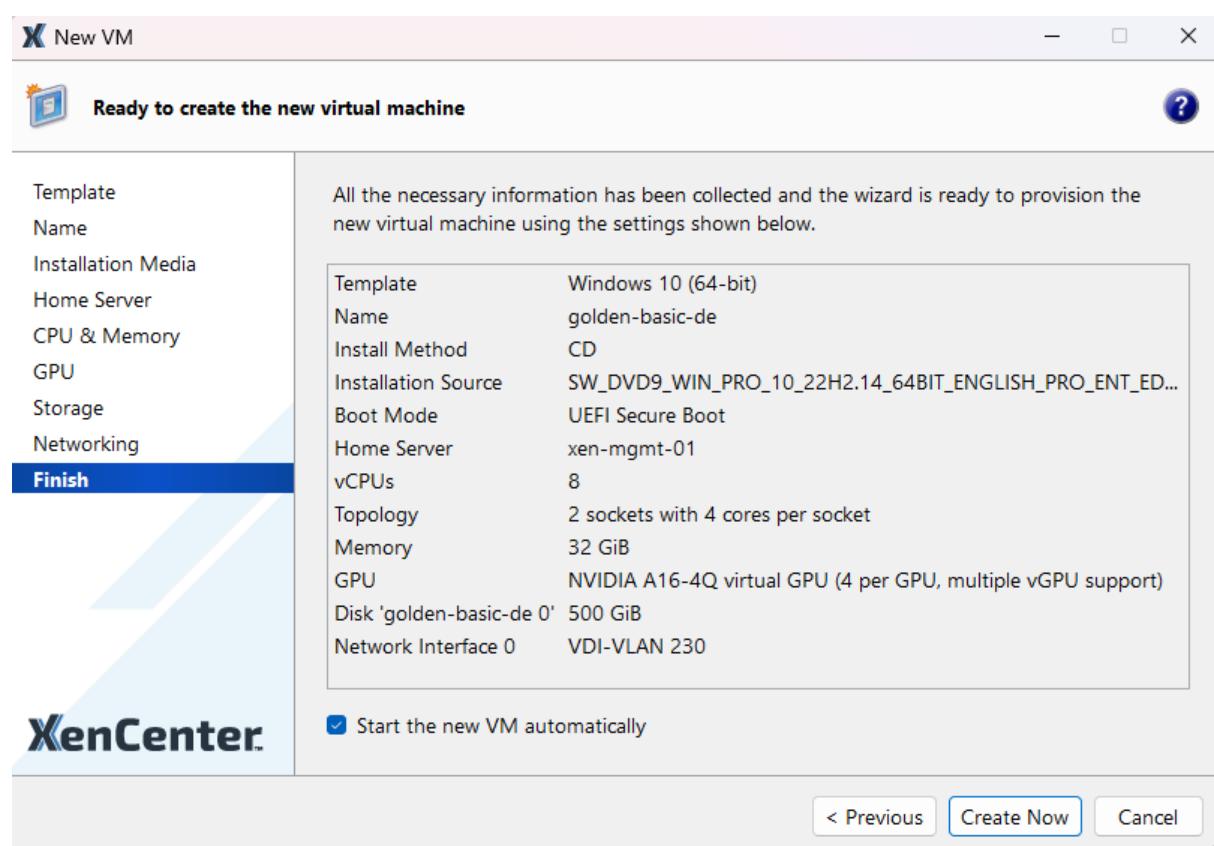
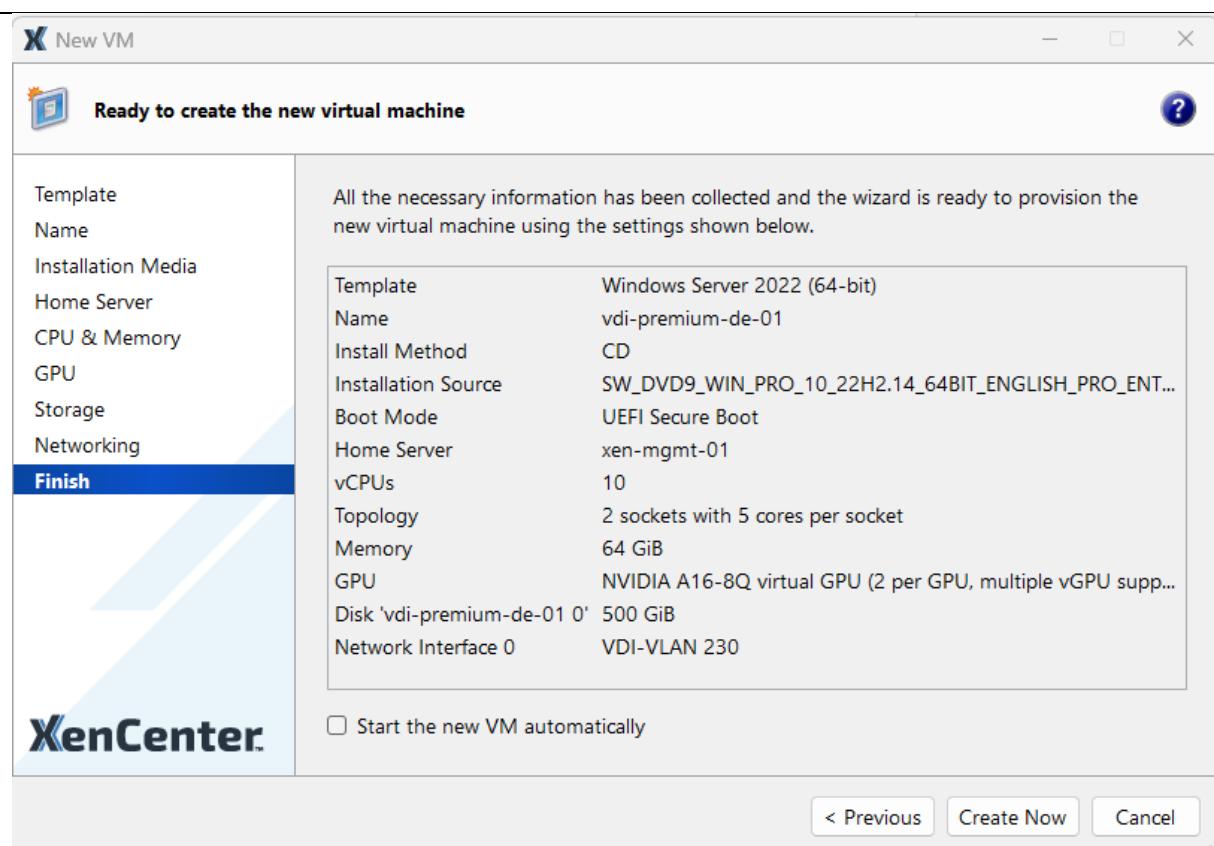
Desktops
Alle (1) Favoriten (0)

DG_VDI-Basic-DE



Konfiguration der Golden Images

Es wurden zwei Golden Images erstellt, die gemäss Detailkonzept für die zwei Abo-Stufen angepasst sind. Diese wurden mit ein paar Testprogramme ausgestattet, die für die Live-Demo verwendet werden.



10 Einrichtung Citrix Services Redundanz

In der Realisierung wurde ein Desktop PC mit XenServer implementiert. Dieser verwaltet verschiedene virtuelle Server, die vorhandene Dienste redundant ergänzen oder ausfallsicher machen sollen.

Xen-mgmt-02 einrichten

Netzwerktechnisch wurde der zweite MGMT-Server genauso wie der erste MGMT-Server eingerichtet. Nach der Grundeinrichtung wurde versucht, den neuen Server in den vorhandenen MGMT-Pool hinzuzufügen. Leider gab es aufgrund der netzwerktechnischen Konfiguration Komplikationen, weshalb dies aus Zeitgründen nicht mehr durchgeführt werden konnte. Große Nachteile entstehen dadurch jedoch nicht.

The screenshot shows the XenCenter interface for managing the server 'xen-mgmt-02'. The 'Networking' tab is selected in the top navigation bar. The left sidebar lists other servers in the pool, including 'xen-mgmt-01' and its associated VMs ('vdi-basic-de-01', 'vdi-prem-de-01', 'vdi-prem-de-03'), and 'xen-mgmt-02' which has a 'VDI-Intel-A16' VM. The main pane displays the 'Server Networks' table:

Name	Description	NIC	VLAN	Auto	Link Status	MAC	MTU	SR-IOV
MGMT-VLAN220		-	No	<None>	-	1500	No	
VDI-VLAN 230		-	No	<None>	-	1500	No	
MGMT/VDI		NIC 0	-	Yes	Connected	ac:1f:6b:dd:fd:0e	1500	No
Network 1		NIC 1	-	Yes	Disconnected	ac:1f:6b:dd:fd:0f	1500	No
Network 2		NIC 2	-	Yes	Disconnected	20:67:7c:01:9bc8	1500	No
NFS		NIC 3	-	Yes	Connected	20:67:7c:01:9bcc	1500	No

Below the table are buttons for 'Add Network...', 'Properties', and 'Remove Network'. The 'IP Address Configuration' section shows the following table:

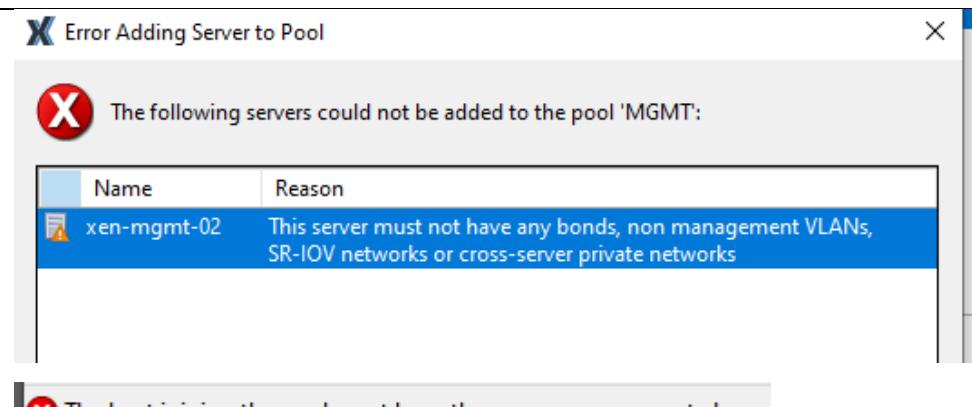
Server	Interface	Network	NIC	IP Setup	IP Address	Subnet mask	Gateway	DNS
xen-mgmt-02	Management	MGMT/VDI	NIC 0	Static	192.168.220.11	255.255.255.0	192.168.220.1	192.168.230.20,1

An overlaid dialog box contains the following text and buttons:

You are attempting to add the server 'xen-mgmt-02' to a pool that is configured to use AD authentication. All pool members must use the same authentication method.

Do you want to enable AD authentication on your server and join it to the same domain as the pool?

Yes No



X The host joining the pool must have the same management vlan.

Der neue Server wurde auch in die Domäne genommen.

Filter by Status ▾ Filter by Server ▾ Filter by Date ▾ Dismiss All ▾

Message	Server / Pool	Date	Actions
Enabling Active Directory Authentication on pool 'xen-mgmt-02'	xen-mgmt-02	May 21, 2024 6:44 PM	Dismiss ▾

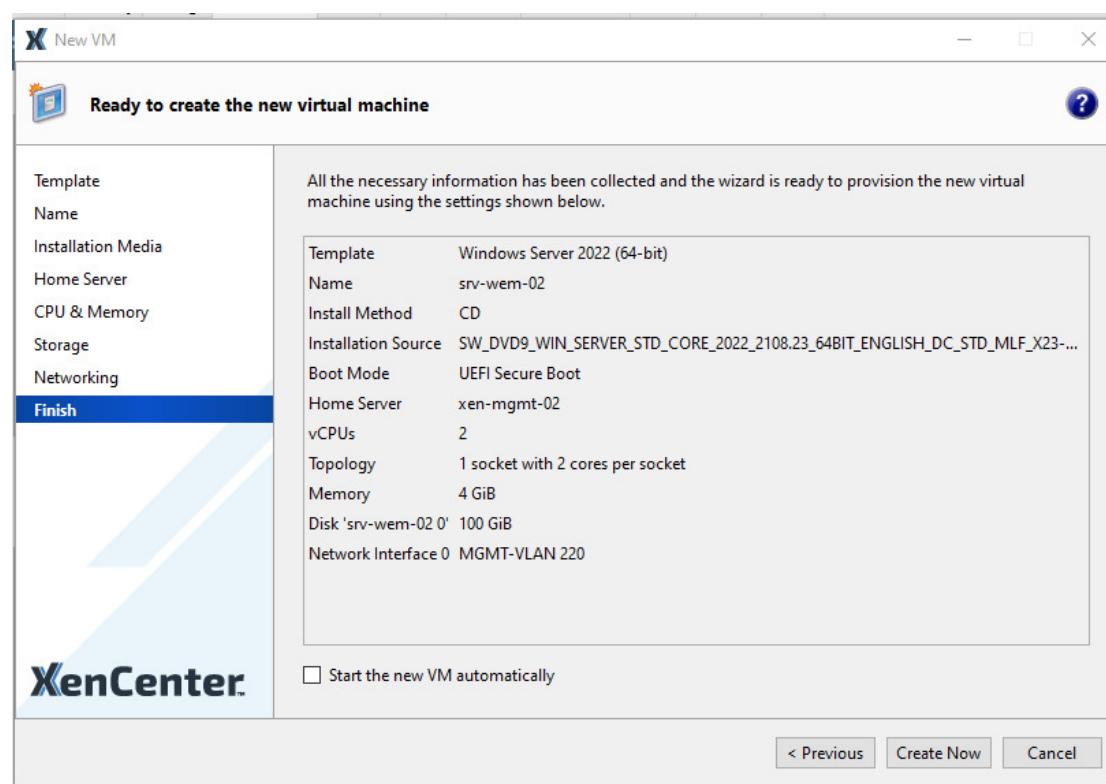
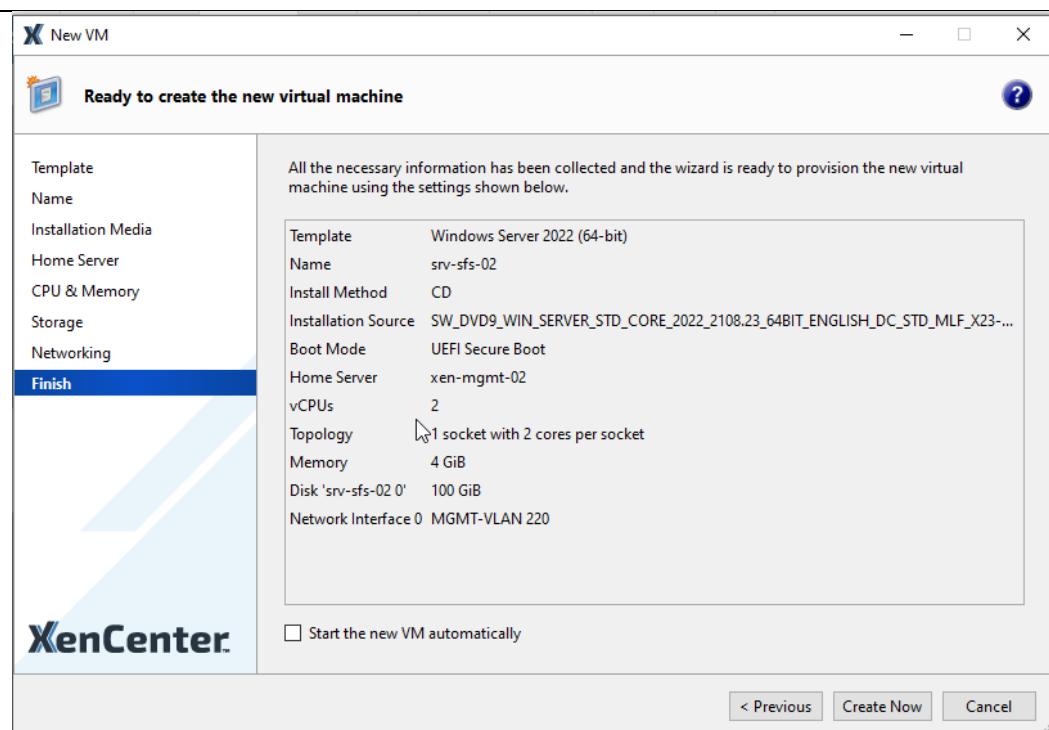
Erstellung der virtuellen Server:

The screenshot shows the "New VM" wizard in XenCenter. The "Finish" step is selected. The summary table shows the following configuration:

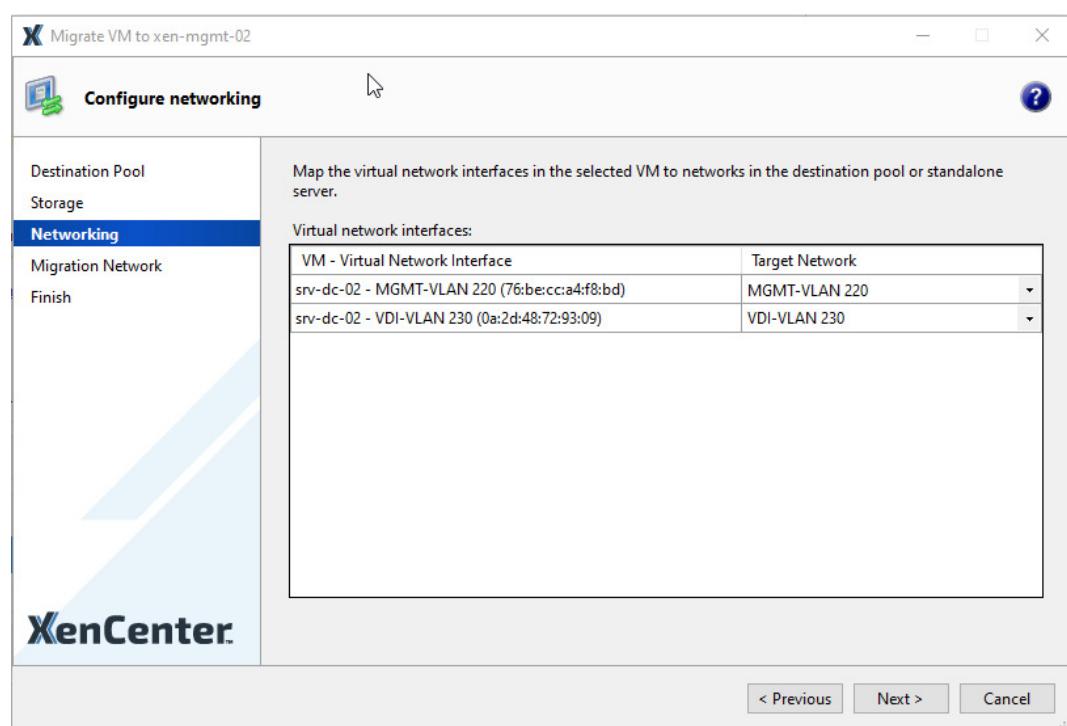
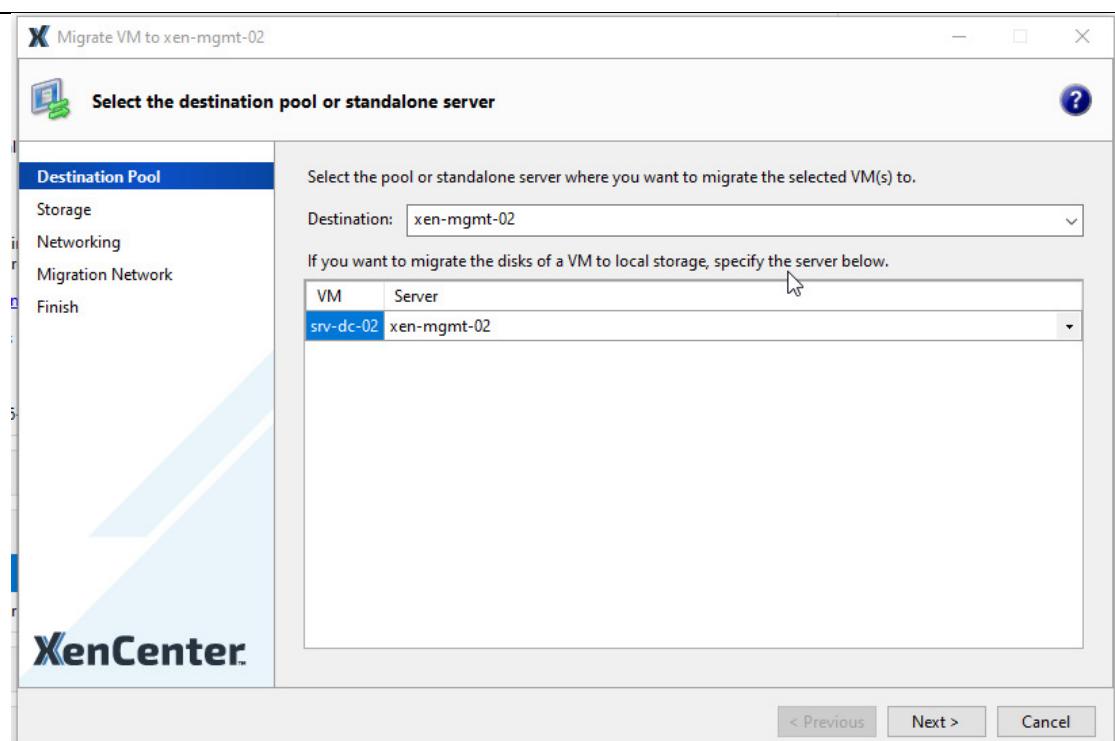
Template	Windows Server 2022 (64-bit)
Name	srv-ddc-02
Install Method	CD
Installation Source	SW_DVD9_WIN_SERVER_STD_CORE_2022_2108.23_64BIT_ENGLISH_DC_STD_MLF_X23...
Boot Mode	UEFI Secure Boot
Home Server	xen-mgmt-02
vCPUs	4
Topology	2 sockets with 2 cores per socket
Memory	8 GiB
Disk 'srv-ddc-02 0'	100 GiB
Network Interface 0	MGMT-VLAN 220

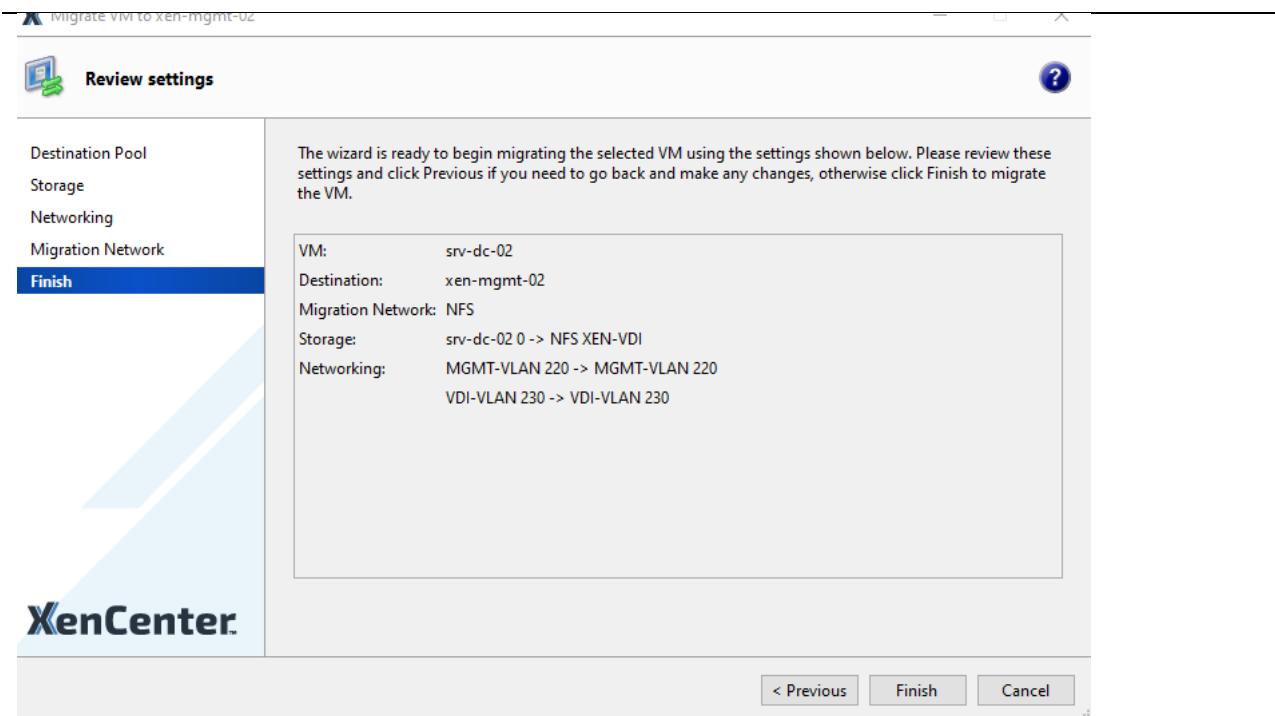
Start the new VM automatically

< Previous Create Now Cancel



Der zweite DC war schon erstellt, somit wurde dieser nun auf den zweiten Server verschoben.

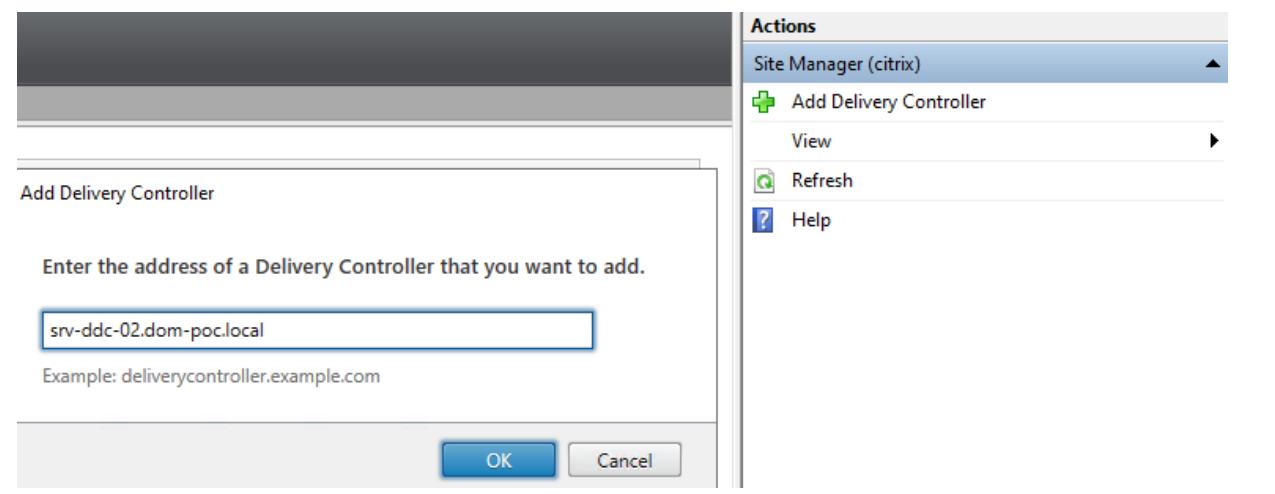




Srv-ddc-02 konfigurieren

Der DDC ist ein wichtiger Service, der redundant eingerichtet werden sollte. Dies dient nicht nur der Ausfallsicherheit, sondern auch einer besseren Lastverteilung.

Den DDC-Dienst ähnlich wie beim ersten DDC installieren. Nach der Installation den neuen DDC zum bestehenden DDC hinzufügen. Die Datenbankinformationen werden bei diesem Prozess automatisch für den neuen DDC konfiguriert.



Citrix Site Manager

File Action View Help

192.168.220.23

Site Manager (citrix)

citrix

Site Overview

Settings

Site name: citrix

Controllers

Name	Version	Status	Last Updated
srv-ddc-01.dom-poc.local	7.41.100.0	Active	0 minutes ago
srv-ddc-02.dom-poc.local	7.41.100.0	Active	0 minutes ago

Databases

Datastore	Database Name	Server Address	Mirror Server Address
Site	CitrixSite	srv-db-01	
Logging	CitriLogging	srv-db-01	
Monitoring	CitriMonitoring	srv-db-01	

Nach der erfolgreichen Einrichtung des zweiten DDCs muss man beim VDA den neuen DDC in der Installation hinzufügen.

Citrix Virtual Apps and Desktops 7 2402 LTSR - Virtual Delivery Agent

Zusammenfassung

✓ Protokoll und Port
✓ Delivery Controller

Zusammenfassung

Neu konfigurieren
Diagnose
Fertig stellen

Kernkomponenten

Virtual Delivery Agent

Delivery Controller: (2)

- ✓ srv-ddc-01.dom-poc.local
- ✓ srv-ddc-02.dom-poc.local

Firewall

UDP-Ports: 443, 1494, 2598
TCP-Ports: 80, 443, 1494, 2598, 8008

Neustart erforderlich

Zurück Neu konfigurieren Abbrechen

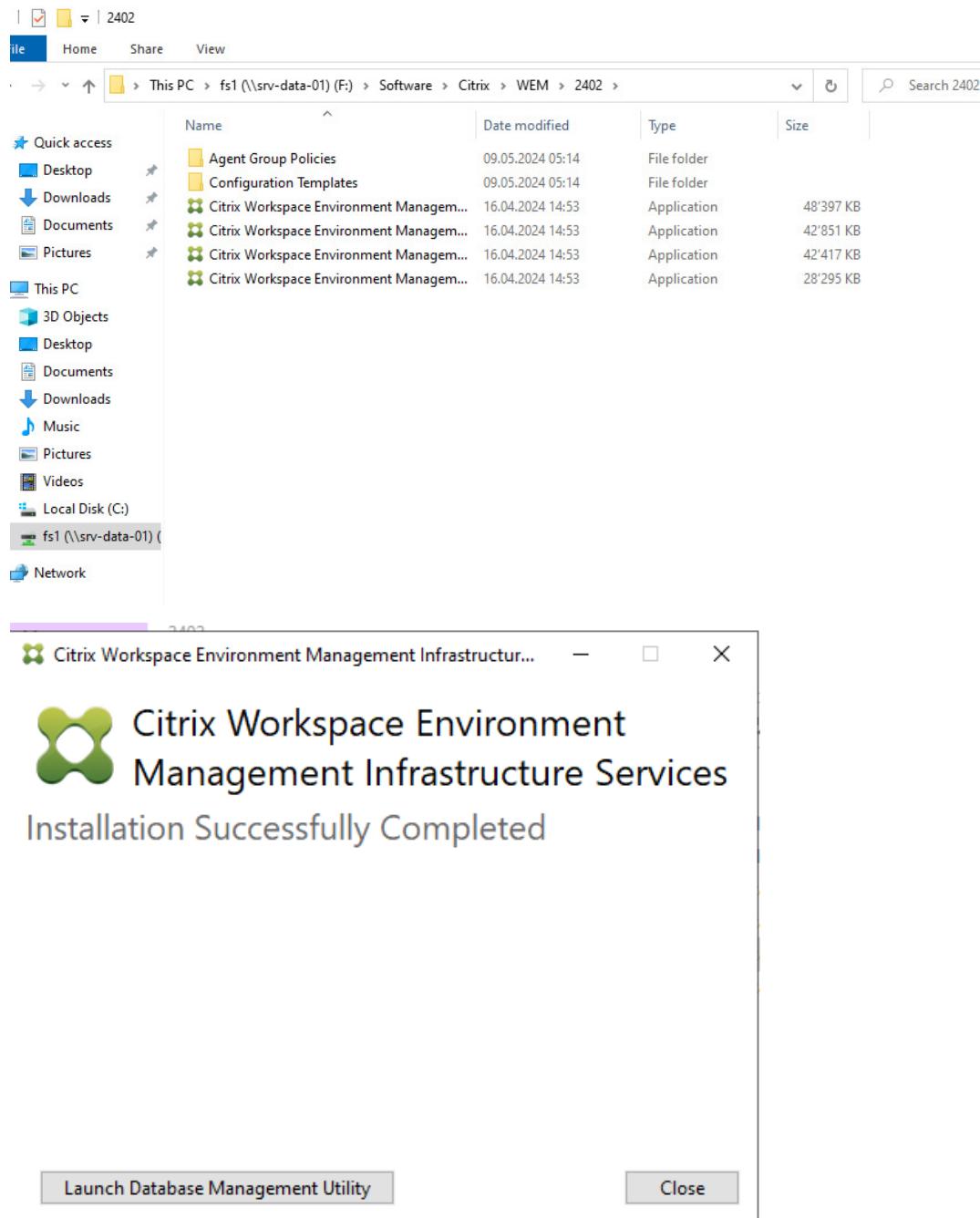
11 Einrichtung WEM und FSLogix

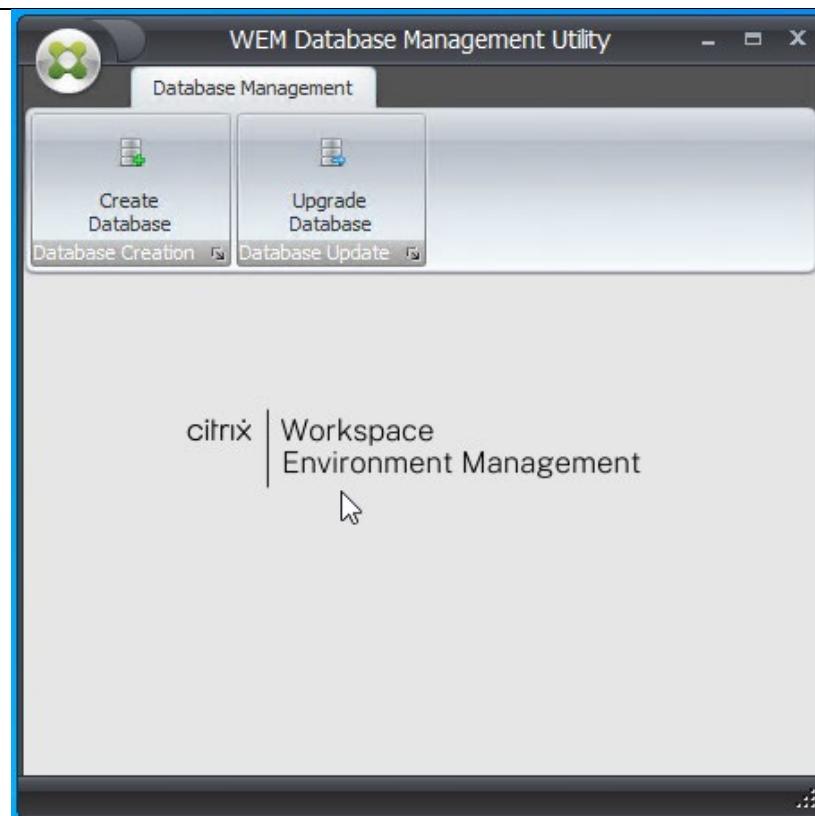
Um die Benutzerfreundlichkeit zu erhöhen, werden Dienste wie WEM und FSLogix eingesetzt. Diese Dienste sollen eine höhere Effizienz ermöglichen, indem sie es Benutzern erlauben, ihre Arbeitsumgebungen, wie Menü-Layouts oder Shortcuts, zu speichern. Mit WEM können die VDI-Umgebungen an verschiedene Projekte angepasst werden.

WEM Broker

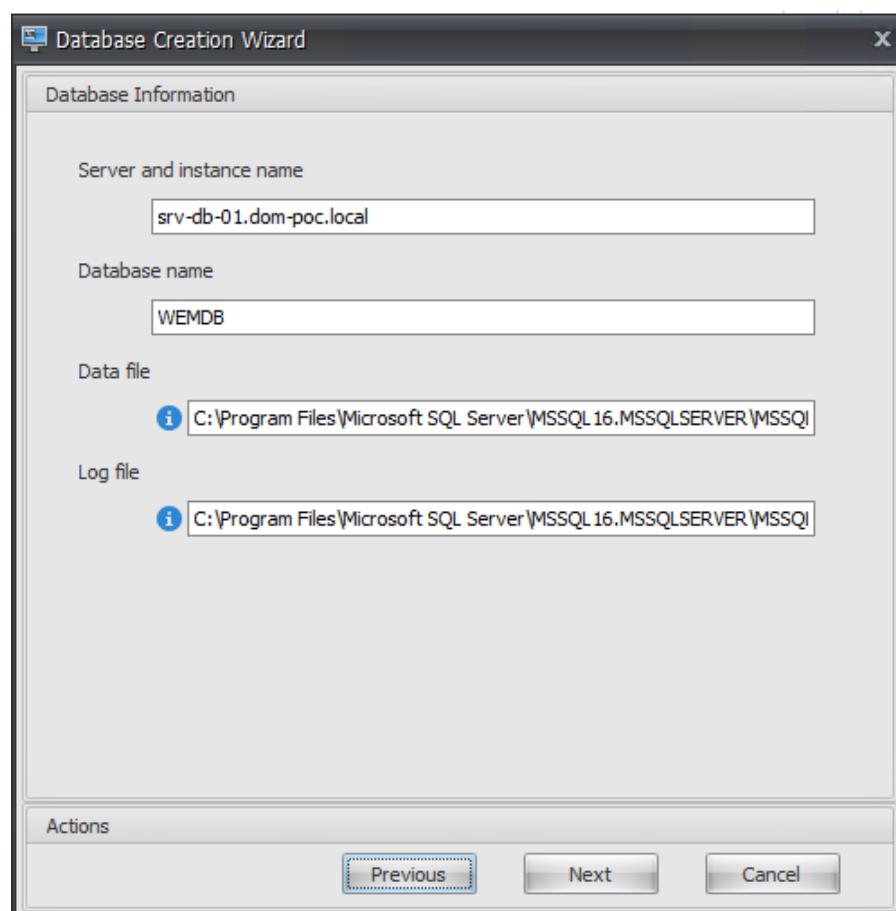
Der WEM Broker ist die Ansprechperson für die VDIs, um die WEM-Konfigurationen zu erhalten. Dabei kommuniziert der WEM Broker mit dem SQL-Server. Verwaltet wird der WEM Broker über die WEM Admin-Konsole. Sowohl die Admin-Konsole als auch der WEM Broker sind auf dem Server srv-wem-01 installiert.

Installation des Brokers sowie der Admin Konsole:

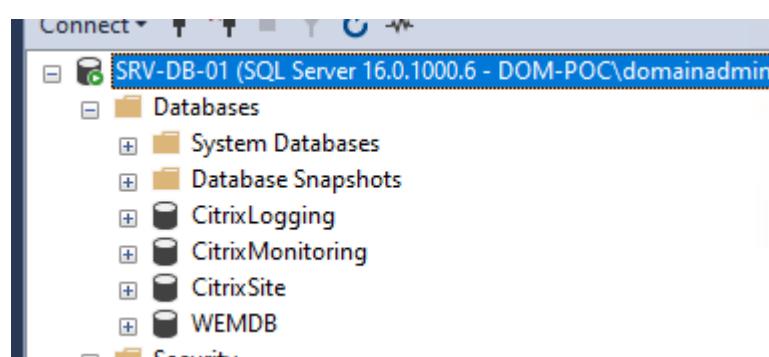
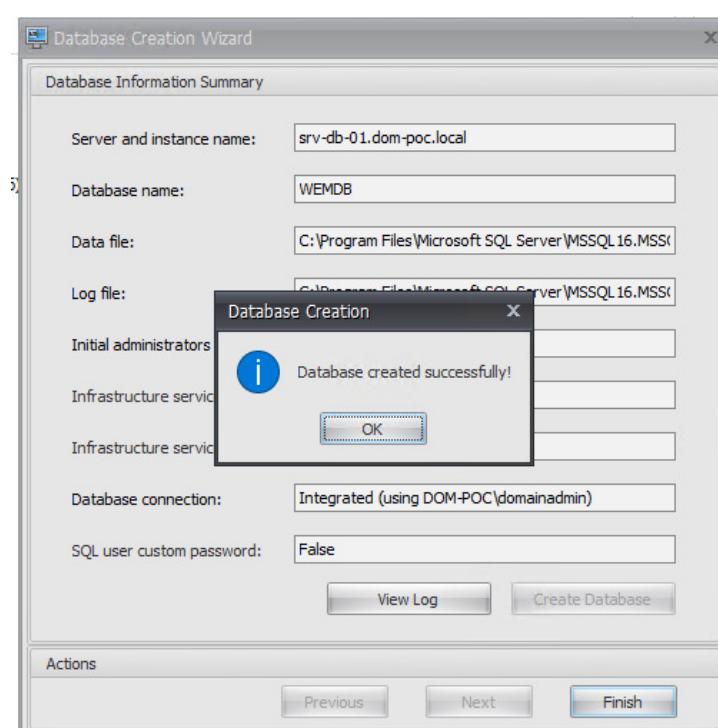
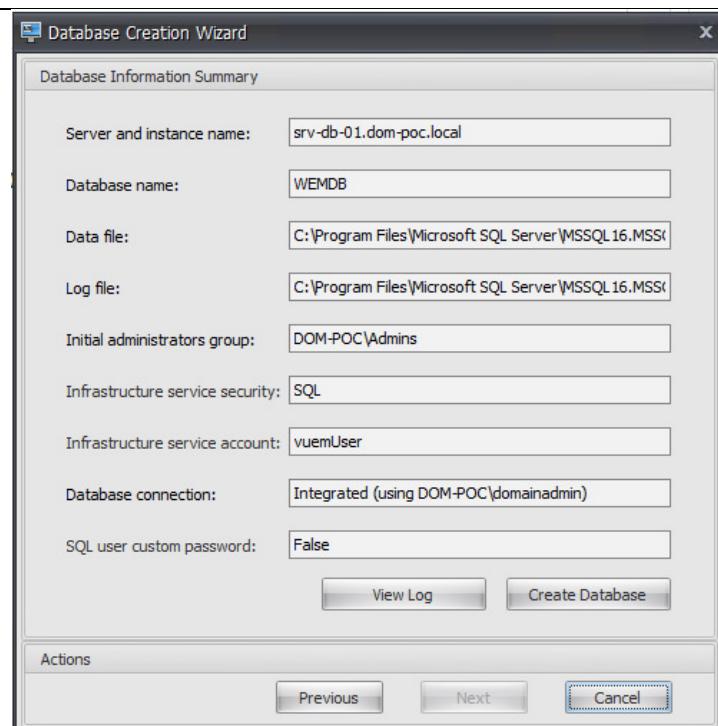


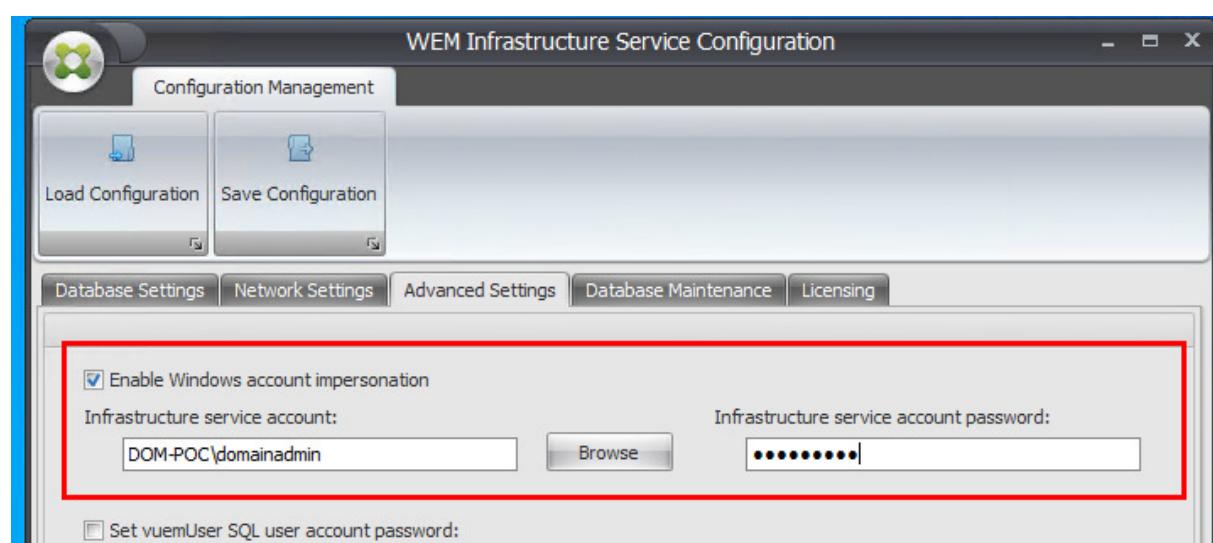
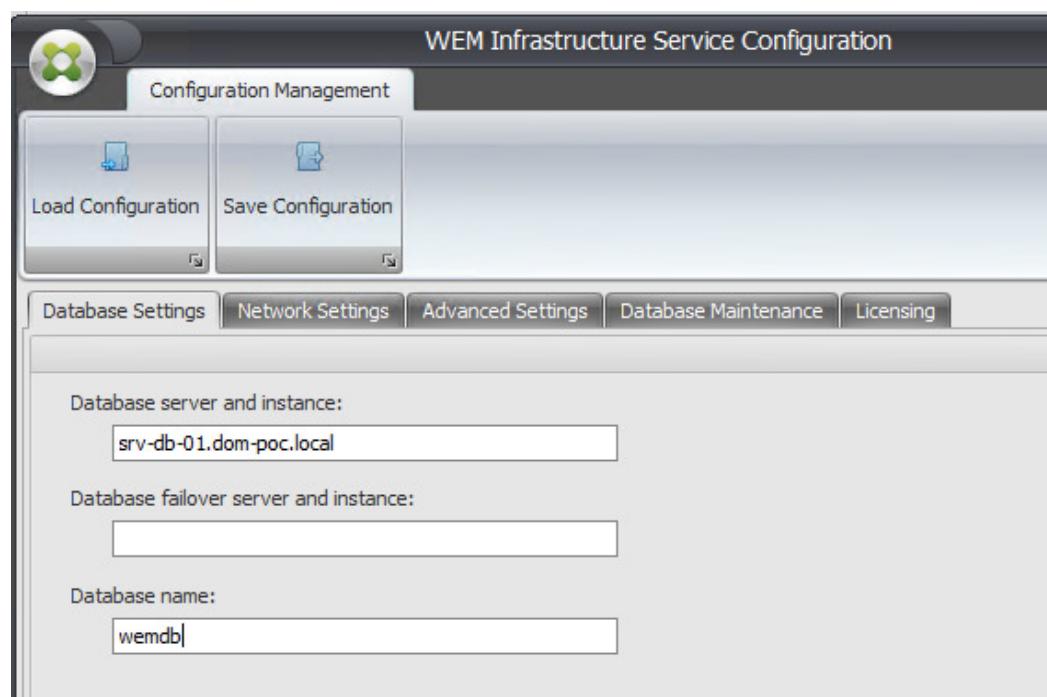
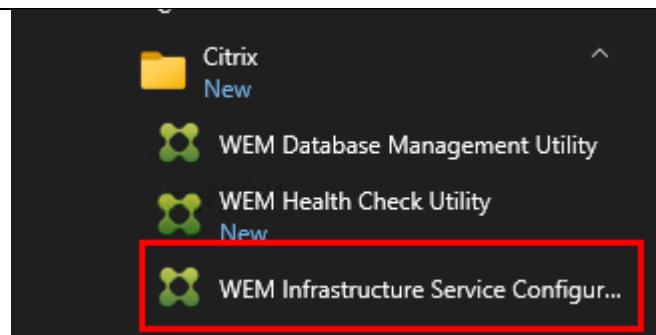


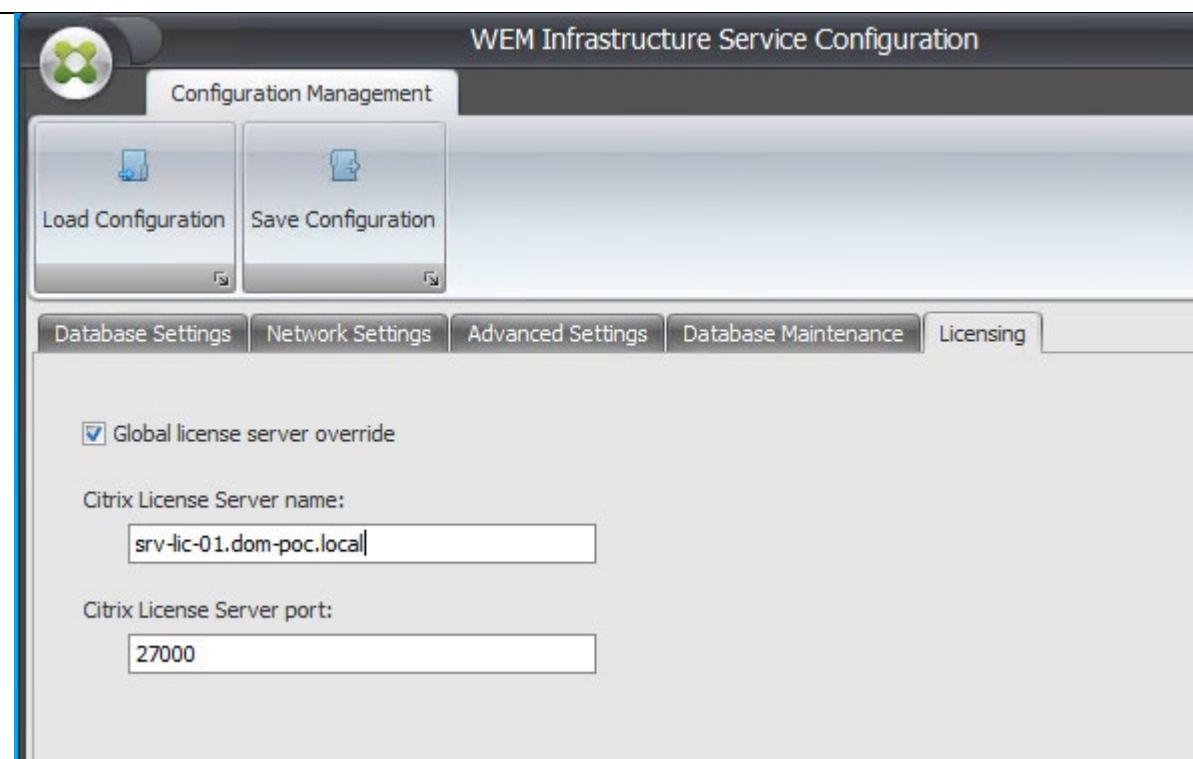
Create Database



Pfad korrigieren gemäss Pfad auf dem Datenbank Server



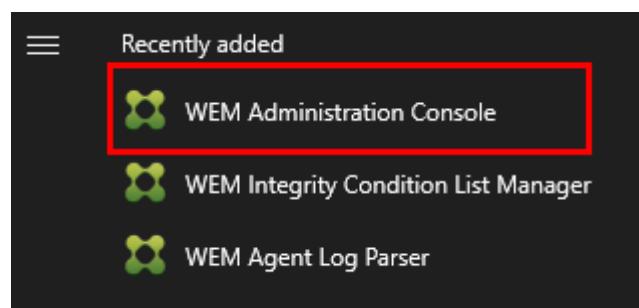




Admin Konsole installieren

> This PC > Local Disk (C:) > temp > 2402

Name	Date modified
Agent Group Policies	09.05.2024 05:14
Configuration Templates	19.05.2024 18:00
Citrix Workspace Environment Management Agent	16.04.2024 14:53
Citrix Workspace Environment Management Console	16.04.2024 14:53
Citrix Workspace Environment Management Infrastructure Services	16.04.2024 14:53
Citrix Workspace Environment Management Web Console	16.04.2024 14:53



Premium Lizenzen einspielen

Für WEM braucht es Premium Lizenzen dafür wurde vom Citrix Experten Lizenzen zur Verfügung gestellt. Diese mussten auf dem Lizenzserver eingespielt werden.

Product Information

Install Licenses

Choose the method to install licenses on the License Server.

License Server Information	
Hostname: srv-lic-01	IP Address: 192.168.220.25

You can choose to install licenses by using the license access code or a license file (.lic).

Use license access code	Use downloaded license file
-------------------------	-----------------------------

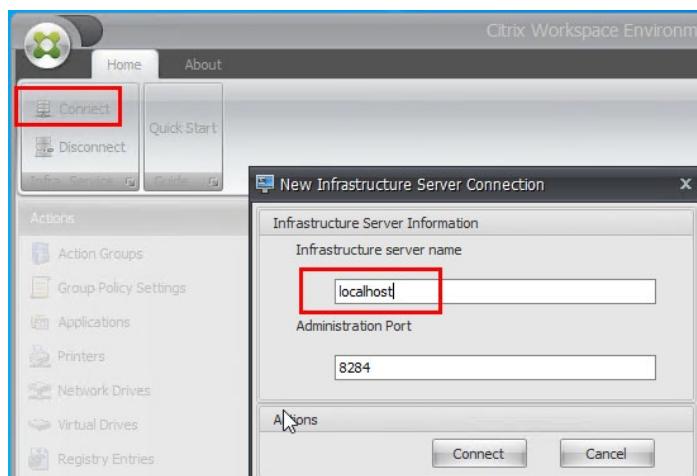
License File

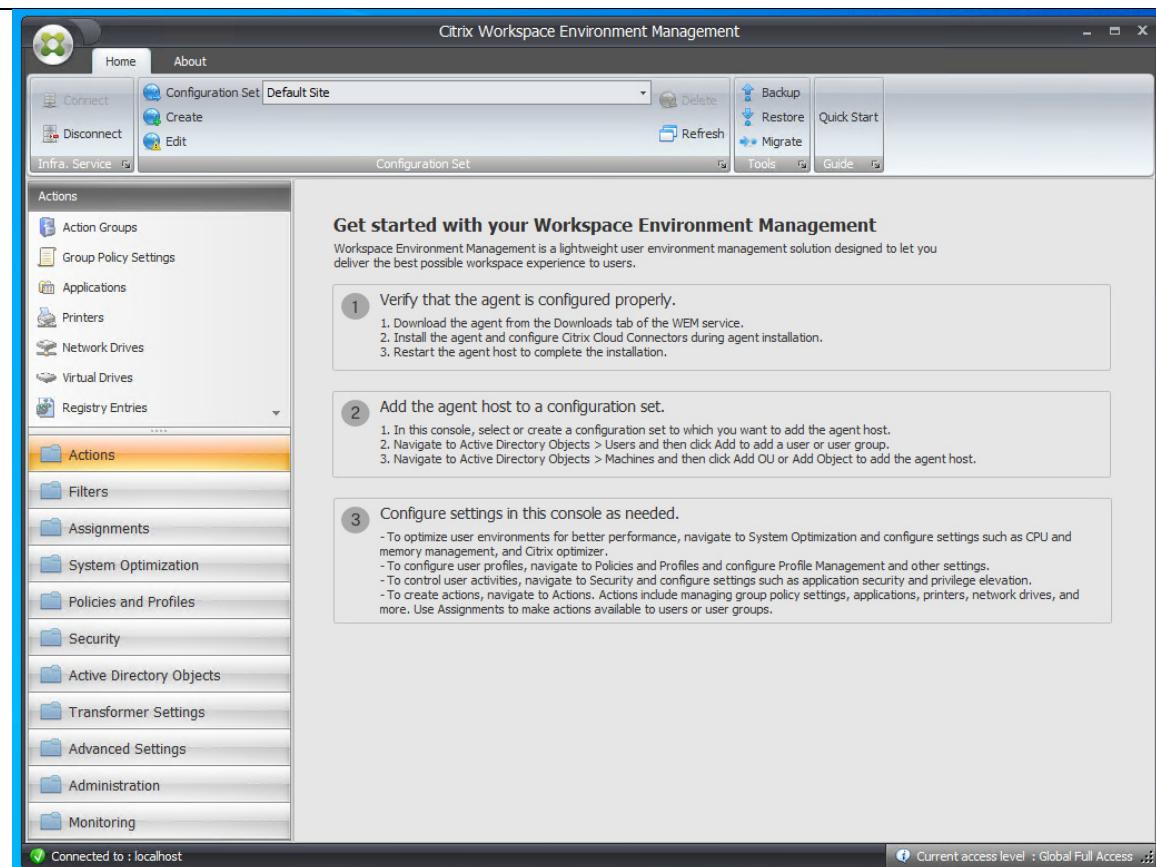
Uploading and rereading FID_ddbc2faa_0dal_4a89_bf27_a4ee61683cb5.lic

Citrix Start-up License	Server	<input type="radio"/> 2/10000	9998(99.98%)	>
Citrix License Server Diagnostics License	Server	<input type="radio"/> 0/10000	10000(100%)	>
Citrix Provisioning for Desktops	Concurrent	<input type="radio"/> 0/21	21(100%)	>
Citrix Provisioning	Concurrent	<input type="radio"/> 0/21	21(100%)	>
Citrix Virtual Apps and Desktops Premium	User/Device	<input type="radio"/> 0/11	11(100%)	>

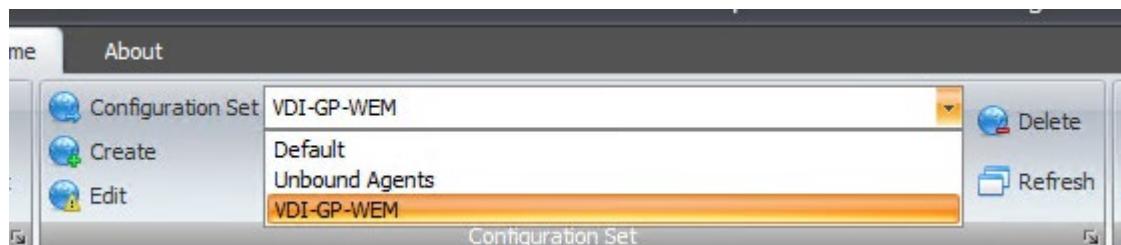
WEM konfigurieren

Mit der Konsole auf dem Broker anmelden, welcher Lokal ist.

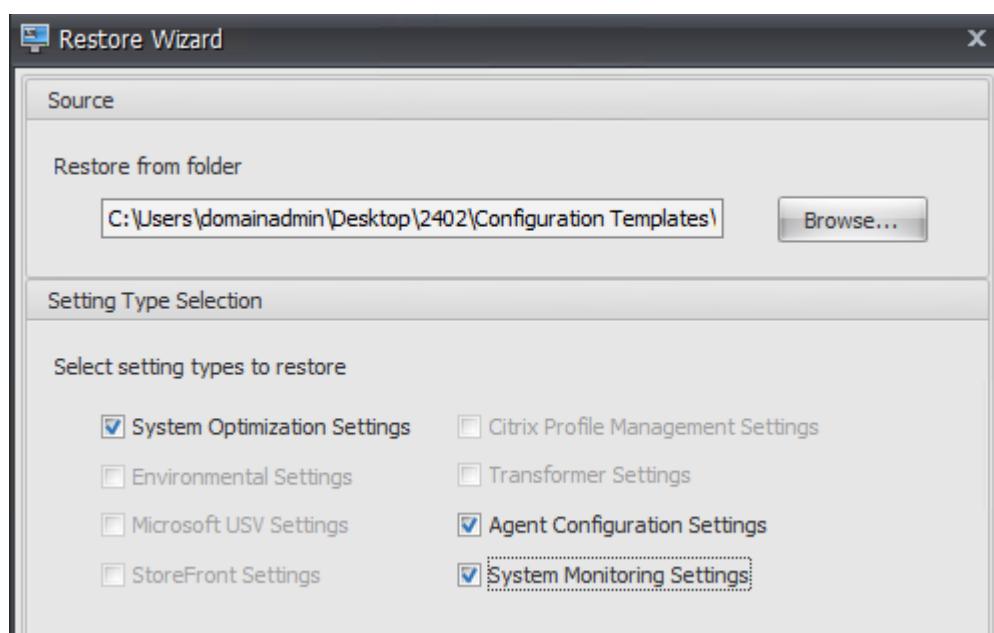




Neuer Configuration Set erstellen



Ein Restore durchführen, mit den Configuration Templates, welche im Installation Order sind.



Unter "Actions" können Objekte wie Netzlaufwerke, Drucker und Registry-Einträge erstellt werden. In diesem Fall wurde ein Netzlaufwerk erstellt, das für alle Benutzer einer Gruppe beim Start der VDI eingebunden werden soll. Unter "Active Directory Object" können diese Gruppen aus dem AD hinzugefügt werden. Anschliessend kann man unter "Assignments" die Actions den Gruppen zuweisen.

The screenshot shows the Citrix Workspace Environment Management interface. The left sidebar has a tree view with nodes like Connect, Disconnect, Infra. Service, Home, Configuration Set (Default Site), Actions Assignment, Modeling Wizard, and others. The main area has tabs for Action Assignment and Configuration Set. Under Action Assignment, there's a 'Users' section with a search bar and a table showing users: 'Everyone' and 'DOM-POC\AG_WEM-Projekt0001-DE'. Both users have priority 100 and are marked as active. Below this is an 'Assignments' section with tabs for Available and Assigned. The Available pane shows categories like Action Groups, Group Policy Settings, Actions, Applications, Printers, Drives, Network, Registry Entries, Environment Variables, Ports, Ini Files, External Tasks, Folders and Files, User DSN, and File Associations. The Assigned pane shows the same categories, with 'Projektablage' selected under Network. At the bottom, there's a table of assignments:

User	Description	Priority
Everyone	A group that includes all users, even anonymous ...	100
DOM-POC\AG_WEM-Projekt0001-DE		100

Below this is another 'Assignments' section with Available and Assigned panes. The Available pane shows the same list of categories. The Assigned pane shows 'Projektablage' selected under Network, with two informational icons: 'Filter : Always True' and 'Drive Letter : F'. The status bar at the bottom indicates 'Connected to : localhost' and 'Current access level : Global Full Access'.

WEM Agent konfigurieren

Der WEM Agent wird auf den Golden Images installiert und ist dafür zuständig die Konfiguration vom WEM Broker zu holen.

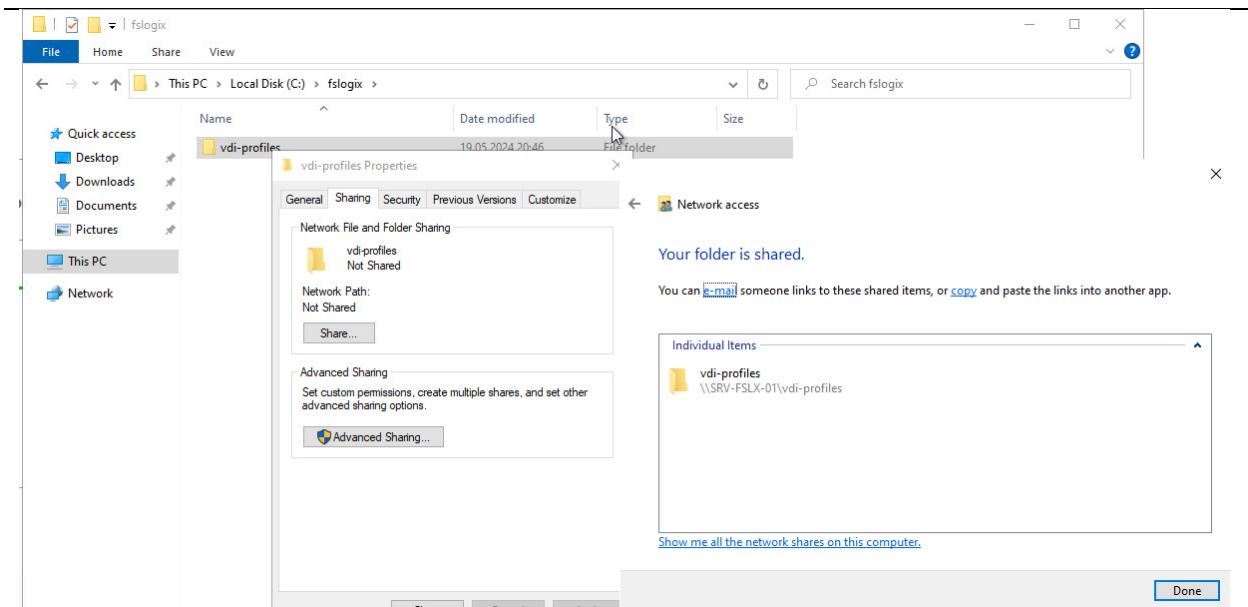
The screenshot shows the 'Citrix Workspace Environment Management Agent Setup' window. The 'Infrastructure Service Configuration' tab is selected. It asks to specify the infrastructure service to which the agent connects. Two options are available: 'Skip Configuration' (unchecked) and 'Configure the Infrastructure Service' (checked). Under 'Configure the Infrastructure Service', the FQDN or IP address is set to 'srv-wem-01.dom-poc.local'. The 'Agent service port (default 8286)' is set to '8286' and the 'Cached data synchronization port (default 8288)' is set to '8288'. At the bottom are 'Back', 'Next', and 'Cancel' buttons, with 'Next' being highlighted.

Name	Publisher
Citrix Virtual Apps and Desktops 7 2402 LTSR - Virtual ...	Citrix Systems, Inc.
Citrix Workspace Environment Management Agent	Citrix Systems, Inc.

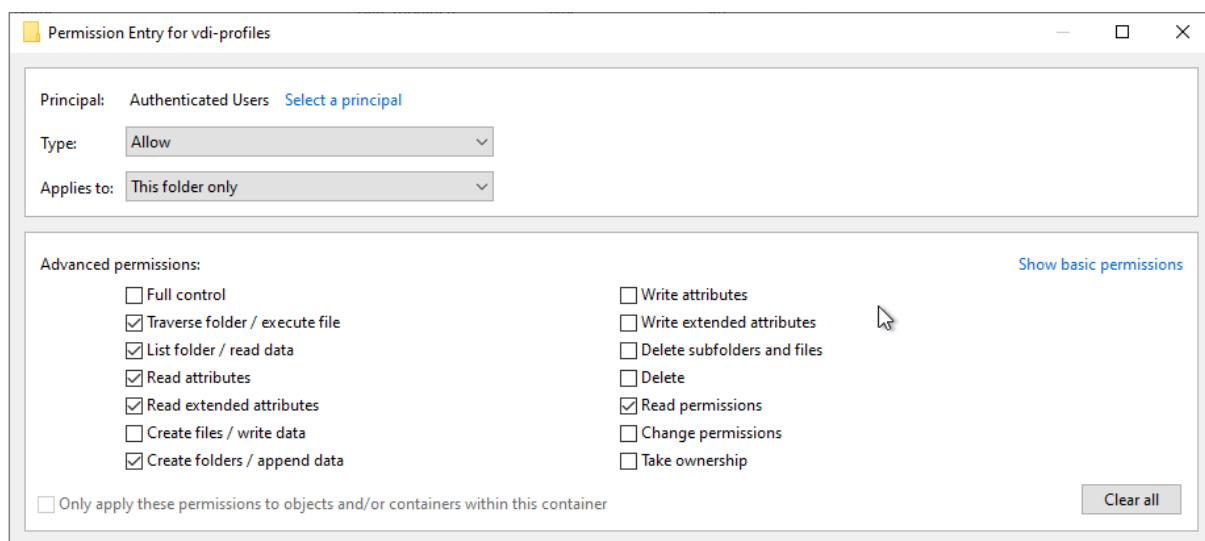
Nach der Installation muss das Golden Image neu gestartet und danach heruntergefahren werden. Sobald es heruntergefahren ist, kann man ein Snapshot des Golden Image erstellen und dieses auf dem DDC freigeben.

FSLogix

FSLogix wird eingesetzt, um Benutzerprofile in Container auf einem dedizierten Server zu verlagern. Dies verkürzt die Anmeldezeiten und speichert verschiedene Benutzereinstellungen.

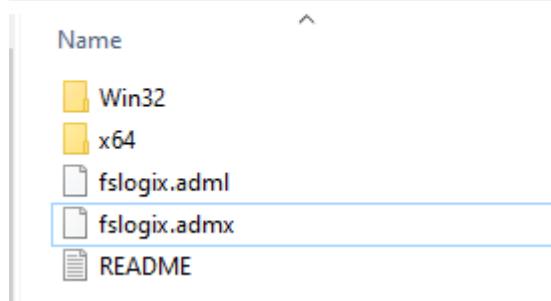


Zuerst muss auf dem FSLogix-Server ein Share erstellt werden, auf dem die Profile abgelegt werden. Die Berechtigungen für authentifizierte Benutzer müssen angepasst werden. Wichtig ist, dass sie die Berechtigung "Create folders / append data" haben.



Der nächste Schritt ist, die GPO-Regeln zu erstellen. Im FSLogix-Download-Ordner sind zwei Dateien enthalten: fslogix.adml und fslogix.admx. Diese müssen als Vorlage für die GPO hinzugefügt werden.

downloads > FSLogix_Apps_2.9.8884.27471



Die Datei fslogix.admx muss in den Ordner "PolicyDefinitions" kopiert werden, und die Datei fslogix.adml in den Sprachordner "en-US". Danach kann der gesamte Ordner "PolicyDefinitions" in den "Sysvol"-Ordner kopiert werden, damit diese Templates für alle Domänencontroller verfügbar sind.

The screenshot shows two windows side-by-side. The left window is a File Explorer window titled 'PolicyDefinitions' showing files in the 'C:\Windows\PolicyDefinitions' folder. The right window is also a File Explorer window titled 'Policies' showing the 'PolicyDefinitions' folder within the 'SYSVOL\sysvol\dom-poc.local\Policies' directory. Below these is a screenshot of the 'Group Policy Management Editor' showing the 'Computer Configuration\Policies\Administrative Templates' node expanded to reveal various FSLogix policy definitions.

File Explorer (Left):

Name	Date modified	Type	Size
fslogix.admx	28.04.2024 10:22	ADMX File	72 KB
fthsvc.admx	08.05.2021 10:15	ADMX File	3 KB
Globalization.admx	08.05.2021 10:15	ADMX File	34 KB
GroupPolicy.admx	08.05.2021 10:15	ADMX File	33 KB

File Explorer (Right):

Name
{6AC1786C-016F-11D2-945F-00C04fB984...}
{31B2F340-016D-11D2-945F-00C04FB984...}
{53428DC8-ED4A-4C44-833B-3458F79EC6...}
PolicyDefinitions

Group Policy Management Editor:

- Computer Configuration
 - Policies
 - Administrative Templates: Policy definitions (ADMX files) retrieved from the central store.
 - Control Panel
 - FSLogix
 - Cloud Cache Service
 - Logging
 - ODFC Containers
 - Profile Containers
 - Network

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
DOM-POC\Domain Admins	Edit settings, delete, modify security	No
DOM-POC\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

FSLogix/Profile Containers

Policy	Setting	Comment
Size In MBs	Enabled Size In MBs 30000	
VHD Locations	Enabled VHD Locations \\srv-fsik-01\vdiprofiles	

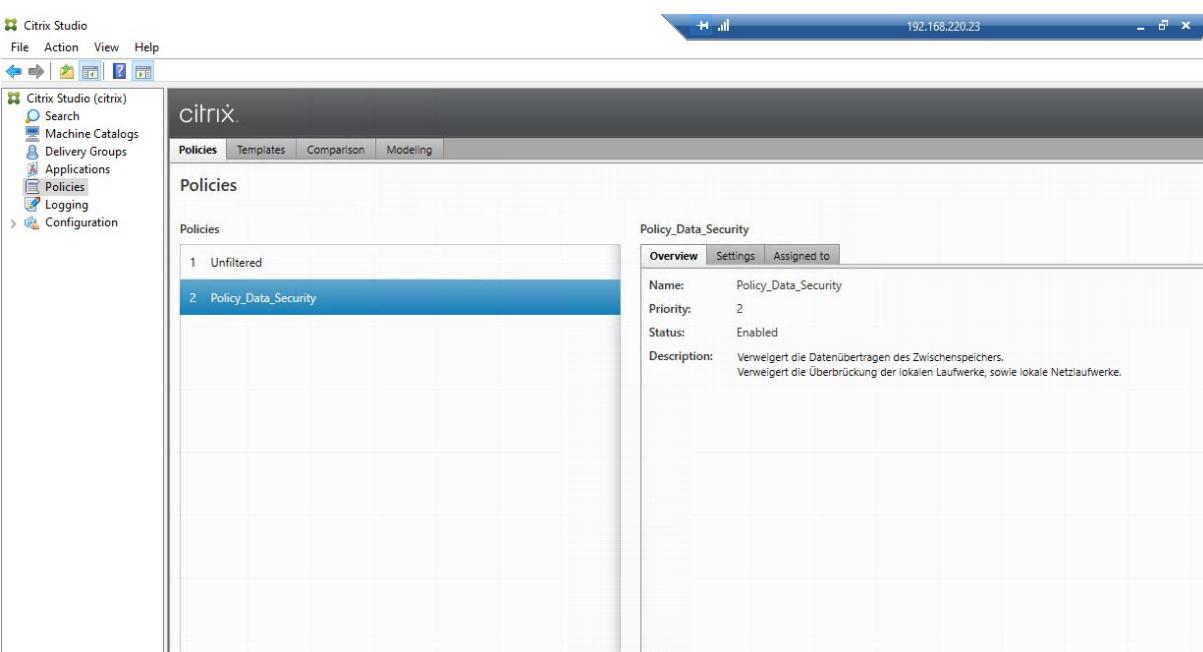
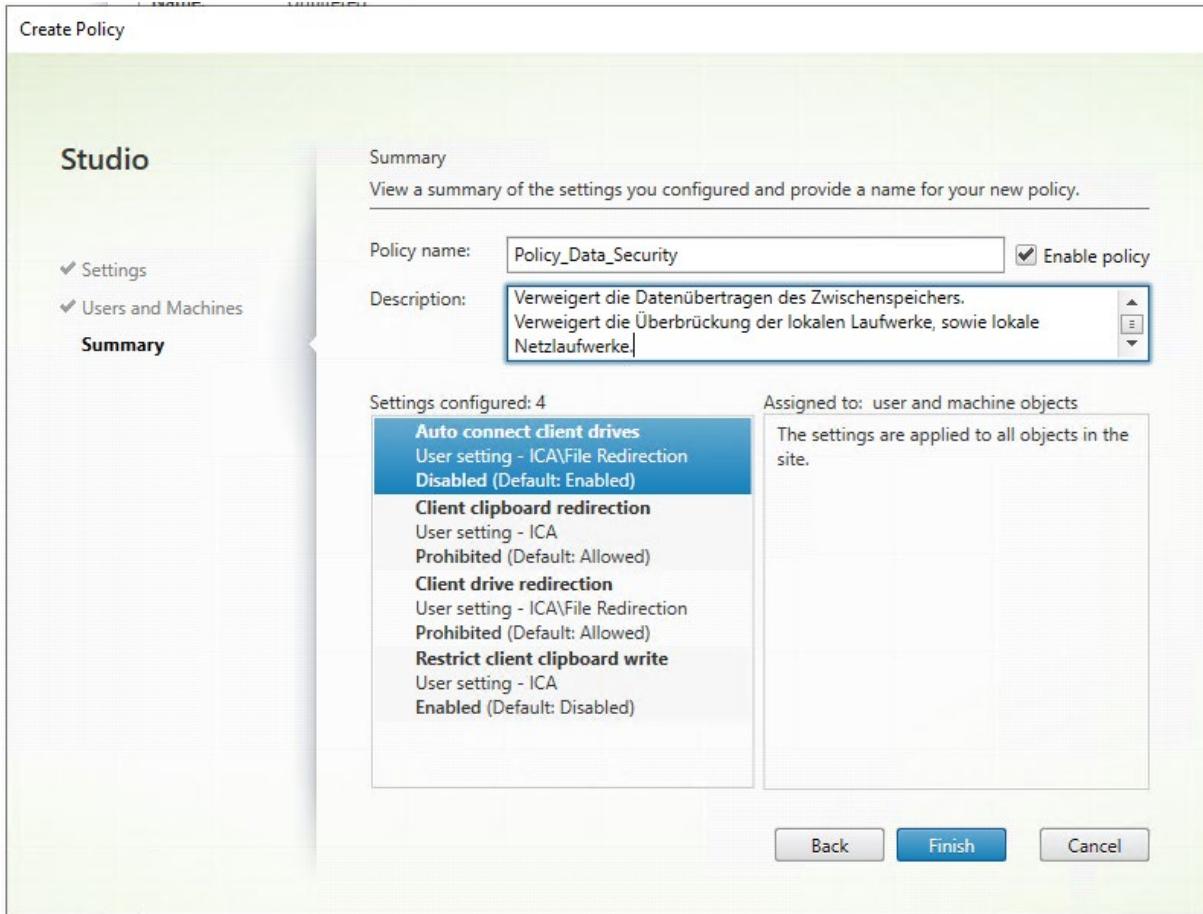
Diese GPO muss für die korrekten OUs erstellt werden, in denen die verschiedenen Benutzer verwaltet werden.

12 Sonstige Konfigurationen

Zur Erfüllung verschiedener Anforderungen und zur Optimierung der Benutzererfahrung wurden zusätzliche Änderungen vorgenommen.

DDC Policy

Auf dem DDC in der Studio-Verwaltungsoberfläche besteht die Möglichkeit, verschiedene Policies zu erstellen. In diesem Fall wurden bestimmte Funktionen deaktiviert oder verweigert.



Lokale Gruppenrichtlinien auf den Projektnotebooks

Zur Einschränkung von Screenshots oder Bildschirmaufnahmen wurden die vorinstallierten Programme für diese Funktionen über die lokalen Gruppenrichtlinien gesperrt.

The screenshot shows the Windows Local Group Policy Editor window. The left pane displays a tree structure under 'Tablet PC' with various policy categories like 'Cursor', 'Eingabebereich', and 'Zubehör'. The right pane shows a table titled 'Einstellung' (Setting) with four entries. The fourth entry, 'Ausführung des Snipping Tools nicht zulassen' (Disallow execution of Snipping Tools), is highlighted and has a status of 'Aktiviert' (Enabled).

Einstellung	Status
Ausführung von InkBall nicht zulassen	Nicht konfig...
Ausführung von Windows-Journal nicht zulassen	Nicht konfig...
Druckausgabe an Journalnotizdruck nicht zulassen	Nicht konfig...
Ausführung des Snipping Tools nicht zulassen	Aktiviert

Nvidia Grid Lizenzierung

Damit die zur Verfügung gestellten Grafikkartenleistung verwendet werden können, muss man die Nutzung lizenziieren. Dafür wurden die internen Lizenzen zu Verfügung gestellt.

Den Lizenztoken auf dem Golden Image implementieren:

The screenshot shows a Windows File Explorer window with the path 'This PC > Local Disk (C:) > Program Files > NVIDIA Corporation > vGPU Licensing > ClientConfigToken'. A file named 'client_configuration_token_10-19-2023-1...' is selected, showing it is a TOK File of size 3 KB.

Nvidia Service neustartnen

The screenshot shows the Windows Task Manager Services tab. It lists three services: 'Network Store Interface Ser...', 'NVIDIA Display Container LS', and 'NVWMI'. All three services are listed as 'Running' with 'Automatic' startup type and are categorized as 'Local Service'.

Danach müsste es automatisch versuchen die Lizenz zu ziehen

License Edition:



Your system is licensed for NVIDIA RTX Virtual Workstation, expiring at 2024-5-29 0:30:32 GMT.

License Server Details

Primary Server Address:

api.ds.licensing.nvidia.com

Port Number:

443

Secondary Server Address:

Port Number:

Dies ist nur möglich, wenn die VDI auch die externe Adresse erreicht. Daher muss hierfür eine Ausnahme gemacht werden.

Rule status

Rule name *

VLAN-230-to-WAN

Description

Enter Description

Rule group

TEST-SHIPI

Action

Accept

Log firewall traffic

Logs traffic, matching this firewall rule, on the appliance [by default] or on the configured syslog server.

Source

Select the source zones, networks, and devices.

The rule applies to traffic from these sources during the scheduled time period.

Source zones *

TEST_Shipi

Source networks and devices *

TEST-SHIPI-VLAN-230

During scheduled time

All the time

Select to apply the rule to a specific time period and day of the week.

Destination and services

Select the destination zones, networks, devices, and services.

The rule applies to traffic to these destinations.

Destination zones *

WAN

Destination networks *

*.nvidia.com

Services *

Any

Danach muss das Golden Image neu ausgerollt werden.

Anhang F2



Testbericht

VDI as a Service

Auftraggeber	Micha Bucher
Projektleiter	Shipinyuan Su, Sirak Yosef
Autor	Shipinyuan Su, Sirak Yosef
Klassifizierung	Intern
Status	Von AG abgesegnet

Änderungsverzeichnis

Datum	Version	Änderung	Autor
19.05.2024	0.1	Dokument erstellt	Shipinyuan Su, Sirak Yosef
22.05.2024	1.0	Dokument fertiggestellt	Shipinyuan Su, Sirak Yosef

Tabelle 1: Änderungsverzeichnis

Inhaltsverzeichnis

1	Einleitung	5
2	Komponententests	6
3	Integrationstests.....	13
4	Systemtests	28
5	Abnahmetests	36

Tabellenverzeichnis

Tabelle 1: Änderungsverzeichnis	1
Tabelle 2: TF-01 Funktionalität der Sophos Firewall	6
Tabelle 3: TF-01 Ergebnis.....	6
Tabelle 4: TF-02 Funktionalität der Netzwerk-Switches	7
Tabelle 5: TF-02 Ergebnis.....	7
Tabelle : TF-03 XenServer Management 1	8
Tabelle : TF-03 XenServer Management 1	8
Tabelle : TF-04 XenServer Management 2	9
Tabelle : TF-04 Ergebnis.....	9
Tabelle : TF-05 XenServer VDI	10
Tabelle : TF-05 Ergebnis.....	10
Tabelle : TF-06 Hauptspeicher Synology NAS	11
Tabelle : TF-06 Ergebnis.....	11
Tabelle : TF-07 Backupspeicher Synology NAS.....	12
Tabelle : TF-07 Ergebnis.....	12
Tabelle : TF-08 Netzwerk VLAN 210 NFS.....	13
Tabelle : TF-08 Ergebnis.....	14
Tabelle : TF-09 Netzwerk VLAN 220 MGMT	15
Tabelle : TF-09 Ergebnis.....	16
Tabelle : TF-10 Netzwerk VLAN 230 VDI	17
Tabelle : TF-10 Ergebnis.....	17
Tabelle : TF-11 Erstellung der Domäne	18
Tabelle : TF-11 Ergebnis.....	19
Tabelle : TF-12 Konfiguration DNS Server	20
Tabelle : TF-12 Ergebnis.....	21
Tabelle : TF-13 Konfiguration DHCP Server	22
Tabelle : TF-13 Ergebnis.....	23
Tabelle : TF-14 Replikation auf zweiten Domain Controller.....	24
Tabelle : TF-14 Ergebnis.....	25
Tabelle : TF-15 Backup erfolgt automatisch täglich.....	26
Tabelle : TF-15 Ergebnis.....	26
Tabelle : TF-16 Auf VDI läuft ein Antivirus	27
Tabelle : TF-16 Ergebnis.....	27
Tabelle : TF-17 Anmeldung auf die isolierte Umgebung.....	28
Tabelle : TF-17 Ergebnis.....	28
Tabelle : TF-18 Schutz gegen Geräteverlust oder Diebstahl	29
Tabelle : TF-18 Ergebnis.....	29
Tabelle : TF-19 Durchführung von Benutzermutationen	30
Tabelle : TF-19 Ergebnis.....	31
Tabelle : TF-20 Intuitiv Performance und Verfügbarkeit	32
Tabelle : TF-20 Ergebnis.....	32
Tabelle : TF-21 Skalierung während dem laufenden Betrieb	33
Tabelle : TF-21 Ergebnis.....	33
Tabelle : TF-22 Redundanz	34
Tabelle : TF-22 Ergebnis.....	34
Tabelle : TF-23 Benutzeranpassungen der VDI-Umgebung	35
Tabelle : TF-23 Ergebnis.....	35
Tabelle : TF-24 Fernzugriff.....	36
Tabelle : TF-24 Ergebnis.....	36
Tabelle : TF-25 Kollaboration mit Projektmitarbeitern.....	37
Tabelle : TF-25 Ergebnis.....	37
Tabelle : TF-26 VDI hat kein Internetzugang.....	38
Tabelle : TF-26 Ergebnis.....	38

Tabelle : TF-27 Vordefinierte Programme sind auf der VDI installiert.....	39
Tabelle : TF-27 Ergebnis.....	39
Tabelle : TF-28 Sicherheitsfunktionen.....	40
Tabelle : TF-28 Ergebnis.....	40

1 Einleitung

Dieser Testbericht dokumentiert die Ergebnisse der durchgeführten Testfälle im Rahmen des Projekts. Die Tests wurden gemäss den im Testkonzept definierten Anforderungen durchgeführt und decken verschiedene Bereiche ab. Die durchgeführten Tests umfassen die Funktionalität von Netzwerkgeräten, Servern, Speicherlösungen und der VDI-Umgebung selbst.

Dieser Testbericht soll einen umfassenden Überblick über die Implementierung geben und aufzeigen, was den Diplomanden gelungen ist und was nicht.

2 Komponententests

Testfallbeschreibung

ID / Bezeichnung: TF-01 Funktionalität der Sophos Firewall

Sicherstellung, dass die Sophos Firewall die Netzwerksicherheit durch Kontrolle und Überwachung des Datenverkehrs, einschliesslich der Funktion VLAN effektiv unterstützt.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Erreichbarkeit der Firewall über das produktive Netzwerk mit dem folgenden Befehl. - PING (IP von Firewall)	Die Firewall ist erreichbar.
2	Zugriff auf das Webinterface der Firewall über das produktive Netzwerk mit einem Browser.	Man kann sich auf der Firewall mit den Zugangsdaten anmelden.
3	Überprüfung, ob VLANs und Richtlinien auf der Firewall erstellt werden können.	Neue VLANs und Richtlinien können auf der Firewall eingerichtet werden.

Tabelle 2: TF-01 Funktionalität der Sophos Firewall

Testdurchführung und Ergebnis

Testdatum	20.05.2024
Tester	Tester Netzwerk/Security
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	Firewall ist erreichbar.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 3: TF-01 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-02 Funktionalität der Netzwerk-Switches

Wie bei der Sophos Firewall, muss auch hier die Funktionalität der Netzwerk-Switches geprüft werden, um die erforderlichen Konfigurationen erfolgreich implementieren zu können.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Erreichbarkeit der Switches über das produktive Netzwerk mit dem folgenden Befehl. - PING (IP von Switch)	Die Switches sind erreichbar.
2	Zugriff auf das Webinterface der Switches über das produktive Netzwerk mit einem Browser.	Man kann sich auf die Switches mit den Zugangsdaten anmelden.
3	Überprüfung, ob VLANs auf die Switches erstellt werden können.	Neue VLANs können auf die Switches eingerichtet werden.

Tabelle 4: TF-02 Funktionalität der Netzwerk-Switches

Testdurchführung und Ergebnis

Testdatum	20.05.2024
Tester	Tester Netzwerk/Security
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	Switches sind erreichbar.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 5: TF-02 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-03 XenServer Management 1

Überprüfung der Funktionalität aller eingebauten Komponenten des XenServer Management Servers.

Schritt	Beschreibung	Erwartetes Ergebnis
1	Verfügbarkeit des Servers über das Netzwerk prüfen mit dem Befehl: PING 192.168.220.10	Server ist über das produktive Netzwerk erreichbar.
2	Verbindung zum Server über XenCenter herstellen.	Verbindung über XenCenter ist erfolgreich.
3	Ressourcen im XenCenter überprüfen.	Alle Komponenten sind ersichtlich und laufen einwandfrei.
4	Version des Servers im XenCenter überprüfen.	XenServer Version 8.0 wird angezeigt.

Tabelle 6: TF-03 XenServer Management 1

Testdurchführung und Ergebnis

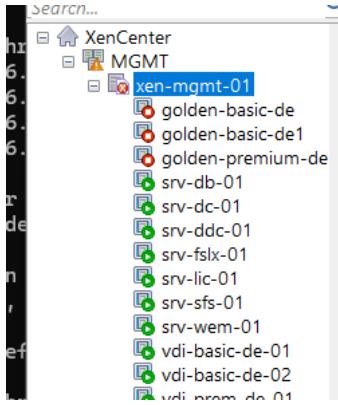
Testdatum	20.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	MGMT XenServer 1 ist erreichbar und alle Testschritte konnten erfolgreich durchgeführt. 
*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel	

Tabelle 7: TF-03 XenServer Management 1

Testfallbeschreibung

ID / Bezeichnung: TF-04 XenServer Management 2

Überprüfung der Funktionalität aller Komponenten vom XenServer MGMT-2.

Schritt	Beschreibung	Erwartetes Ergebnis
1	Verfügbarkeit des Servers über das Netzwerk prüfen mit dem Befehl: PING 192.168.220.11	Server ist über das Netzwerk erreichbar.
2	Verbindung zum Server über XenCenter herstellen.	Verbindung über XenCenter ist erfolgreich.
3	Ressourcen im XenCenter überprüfen.	Alle Komponenten sind ersichtlich und laufen einwandfrei.
4	Version des Servers im XenCenter überprüfen.	XenServer Version 8.0 wird angezeigt.

Tabelle 8: TF-04 XenServer Management 2

Testdurchführung und Ergebnis

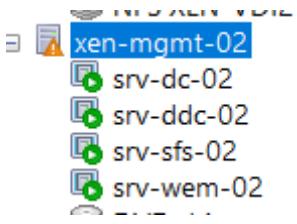
Testdatum	20.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	MGMT XenServer 2 ist erreichbar und alle Testschritte wurden erfolgreich durchgeführt. 
*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel	

Tabelle 9: TF-04 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-05 XenServer VDI

Überprüfung der Funktionalität aller Komponenten des XenServer VDI Servers.

Schritt	Beschreibung	Erwartetes Ergebnis
1	Verfügbarkeit des Servers über das Netzwerk prüfen mit dem Befehl: PING 192.168.220.13	Server ist über das Netzwerk erreichbar.
2	Verbindung zum Server über XenCenter herstellen.	Verbindung über XenCenter ist erfolgreich.
3	Ressourcen im XenCenter überprüfen.	Alle Komponenten sind ersichtlich und laufen einwandfrei.
4	Version des Servers im XenCenter überprüfen.	XenServer Version 8.0 wird angezeigt.

Tabelle 10: TF-05 XenServer VDI

Testdurchführung und Ergebnis

Testdatum	20.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	2
Mängelbeschreibung	Dieser Test konnte nicht durchgeführt werden, da der geplante VDI-Server noch in Gebrauch ist. Daher laufen alle virtuellen Desktops auch auf den Management-Servern.
Bemerkungen	Dies stellt jedoch kein Problem dar, da gemäss Migrationskonzept mit diesem Szenario gerechnet wurde. Daher konnte die alternative Lösung umgesetzt werden. Es muss jedoch beachtet werden, dass die Management-Server dadurch ausgelasteter sein könnten, da jetzt auch die virtuellen Desktops darauf laufen.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 11: TF-05 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-06 Hauptspeicher Synology NAS

Überprüfung der Festplattenkonfiguration und des Updatestands des Hauptspeichers.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Verbindung über das Webinterface auf Synology NAS mit der folgenden URL: https://192.168.220.15	Verbindung ist über das Netzwerkinterface möglich.
2	Überprüfung, ob ein RAID auf dem NAS eingerichtet wurde.	Ein RAID wurde eingerichtet, um Ausfallsicherheit bei einem Festplattenausfall zu gewährleisten.
3	Überprüfung des Updatestands des Synology NAS.	Das NAS ist auf dem neuesten Stand.

Tabelle 12: TF-06 Hauptspeicher Synology NAS

Testdurchführung und Ergebnis

Testdatum	20.05.2024														
Tester	Tester Serverinfrastruktur														
Mängelklasse	0														
Mängelbeschreibung	Keine Mängel vorhanden.														
Bemerkungen	<p>NAS ist auf dem aktuellen Updatestand und RAID 6 ist konfiguriert. Somit wurden alle Testschritte erfolgreich durchgeführt.</p> <p>Allgemeine Informationen</p> <table> <tbody> <tr> <td>Servername</td> <td>srv-data-01 (Bearbeiten)</td> </tr> <tr> <td>DSM-Version</td> <td>DSM 7.2.1-69057 Update 5</td> </tr> <tr> <td>Synology-Konto</td> <td>- (Bearbeiten)</td> </tr> <tr> <td>QuickConnect ID</td> <td>- (Bearbeiten)</td> </tr> </tbody> </table> <p>Info</p> <table> <tbody> <tr> <td>RAID-Typ:</td> <td>RAID 6 (Mit Datenschutz)</td> </tr> <tr> <td>Gesamtkapazität:</td> <td>69.7 TB</td> </tr> <tr> <td>Maximale Anzahl Laufwerke pro RAID:</td> <td>24</td> </tr> </tbody> </table>	Servername	srv-data-01 (Bearbeiten)	DSM-Version	DSM 7.2.1-69057 Update 5	Synology-Konto	- (Bearbeiten)	QuickConnect ID	- (Bearbeiten)	RAID-Typ:	RAID 6 (Mit Datenschutz)	Gesamtkapazität:	69.7 TB	Maximale Anzahl Laufwerke pro RAID:	24
Servername	srv-data-01 (Bearbeiten)														
DSM-Version	DSM 7.2.1-69057 Update 5														
Synology-Konto	- (Bearbeiten)														
QuickConnect ID	- (Bearbeiten)														
RAID-Typ:	RAID 6 (Mit Datenschutz)														
Gesamtkapazität:	69.7 TB														
Maximale Anzahl Laufwerke pro RAID:	24														

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 13: TF-06 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-07 Backupspeicher Synology NAS

Überprüfung der Festplattenkonfiguration und des Updatestands des Backup-Speichers.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	NAS mit Monitor, Tastatur und Maus verbinden, um darauf zuzugreifen, da es sich im geschlossenen NFS-Netz befindet.	Anmeldung auf dem NAS ist erfolgreich.
2	Überprüfung, ob ein RAID auf dem NAS eingerichtet wurde.	Ein RAID wurde eingerichtet, um Ausfallsicherheit bei einem Festplattenausfall zu gewährleisten.
3	Überprüfung des Updatestands des Synology NAS.	Das NAS ist auf dem neuesten Stand.

Tabelle 14: TF-07 Backupspeicher Synology NAS

Testdurchführung und Ergebnis

Testdatum	20.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	NAS ist auf dem aktuellen Updatestand und das RAID 5 ist auch konfiguriert.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 15: TF-07 Ergebnis

3 Integrationstests

Testfallbeschreibung

ID / Bezeichnung: TF-08 Netzwerk VLAN 210 NFS

Überprüfung, ob die Zugriffsrichtlinien vom VLAN 210 ordnungsgemäss funktionieren.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Von srv-dc-01 (VDI-Netz) und srv-ddc-01 (MGMT-Netz) den Backup-Server srv-backup-01 (NFS-Netz) mit folgenden Befehlen anpingen: - PING 192.168.210.15 - PING srv-backup-01	Der Backup-Server ist über diese IP nicht erreichbar, da sowohl das VDI- als auch das MGMT-Netz keinen Zugriff auf das NFS-Netz haben.
2	Von srv-backup-01 den srv-dc-01 und srv-ddc-01 mit folgenden Befehlen anpingen: - PING 192.168.230.20 - PING srv-dc-01 - PING 192.168.220.23 - PING srv-ddc-01	Die DC- und DDC-Server sind vom NFS-Netz nicht erreichbar, da das Netz keinen Zugriff auf das VDI- und MGMT-Netz hat.
3	Von srv-backup-01 den srv-data-01 (NFS-Leitung) mit folgenden Befehlen anpingen: - PING 192.168.210.17 - PING srv-data-01	Der Data-Server ist über diese IP erreichbar, da er sich im gleichen Netz wie der Backup-Server befindet.

Tabelle 16: TF-08 Netzwerk VLAN 210 NFS

Testdurchführung und Ergebnis

Testdatum	20.05.2024
Tester	Tester Netzwerk/Security
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	<p>Alle Testschritte wurden erfolgreich durchgeführt.</p> <p>Von DC aus</p> <pre>C:\Users\domainadmin>hostname srv-dc-01 C:\Users\domainadmin>ping 192.168.210.15 Pinging 192.168.210.15 with 32 bytes of data: Request timed out. Request timed out. Request timed out.</pre> <p>Von NAS aus</p> <pre>ash-4.4# sudo ping -I eth0 192.168.230.20 PING 192.168.230.20 (192.168.230.20) from 192.168.210.15 ash-4.4# sudo ping -I eth0 192.168.210.17 PING 192.168.210.17 (192.168.210.17) from 192.168.210.15 64 bytes from 192.168.210.17: icmp_seq=1 ttl=64 time=0.30 64 bytes from 192.168.210.17: icmp_seq=2 ttl=64 time=0.32 64 bytes from 192.168.210.17: icmp_seq=3 ttl=64 time=0.32</pre>

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 17: TF-08 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-09 Netzwerk VLAN 220 MGMT

Überprüfung, ob die Zugriffsrichtlinien vom VLAN 220 ordnungsgemäss funktionieren.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Von produktivem Netzwerk den MGMT-XenServer anpingen mit folgendem Befehl: - PING 192.168.220.10	XenServer ist mit dieser IP erreichbar.
2	Von MGMT-XenServer einen Client im produktiven Netzwerk anpingen.	Client ist nicht erreichbar, da das MGMT-Netzwerk keinen Zugriff auf das produktive Netz hat.
3	Internetzugang überprüfen von srv-ddc-01 mit dem folgenden Befehl: - PING 8.8.8.8	Da sich srv-ddc-01 im MGMT-Netz befindet und dieser Internetzugang hat, sollte der PING erfolgreich ausgeführt werden.
5	Vom srv-ddc-01 den srv-dc-01 anpingen mit dem folgenden Befehl: - PING 192.168.230.20 - PING srv-dc-01	DC ist vom MGMT-Netz erreichbar.

Tabelle 18: TF-09 Netzwerk VLAN 220 MGMT

Testdurchführung und Ergebnis

Testdatum	20.05.2024
Tester	Tester Netzwerk/Security
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	<p>Alle Testschritte konnten erfolgreich durchgeführt werden.</p> <p>Screenshots vom DDC</p> <p>C:\Users\domainadmin>ping 8.8.8.8</p> <pre>Pinging 8.8.8.8 with 32 bytes of data: Reply from 8.8.8.8: bytes=32 time=4ms TTL=115 Reply from 8.8.8.8: bytes=32 time=4ms TTL=115</pre> <p>C:\Users\domainadmin>ping 192.168.230.20</p> <pre>Pinging 192.168.230.20 with 32 bytes of data: Reply from 192.168.230.20: bytes=32 time=1ms TTL=127 Reply from 192.168.230.20: bytes=32 time<1ms TTL=127</pre> <p>C:\Users\domainadmin>ping srv-dc-01</p> <pre>Pinging srv-dc-01.dom-poc.local [192.168.230.20] with 32 bytes of data: Reply from 192.168.230.20: bytes=32 time<1ms TTL=127 Reply from 192.168.230.20: bytes=32 time<1ms TTL=127</pre>

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 19: TF-09 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-10 Netzwerk VLAN 230 VDI

Überprüfung, ob die Zugriffsrichtlinien vom VLAN 230 ordnungsgemäss funktionieren.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Von einer VDI-Maschine die folgende URL abrufen: - www.google.com	Die URL kann nicht aufgelöst werden, da es keinen Internetzugang vom VDI-Netzwerk gibt.
2	Vom srv-dc-01 den srv-ddc-01 anpingen mit dem folgenden Befehl: - PING 192.168.220.23 - PING srv-ddc-01	Der DDC-Server ist vom VDI-Netz nicht erreichbar.

Tabelle 20: TF-10 Netzwerk VLAN 230 VDI

Testdurchführung und Ergebnis

Testdatum	20.05.2024
Tester	Tester Netzwerk/Security
Mängelklasse	1
Mängelbeschreibung	Der DC kann den DDC-Server anpingen und dem entsprechend ist dieser Testfall nicht erfolgreich. <pre>C:\Users\domainadmin>ping srv-ddc-01 Pinging srv-ddc-01.dom-poc.local [192.168.220.23] with 32 bytes of data: Reply from 192.168.220.23: bytes=32 time<1ms TTL=127 Reply from 192.168.220.23: bytes=32 time<1ms TTL=127 Reply from 192.168.220.23: bytes=32 time<1ms TTL=127</pre>
Bemerkungen	Beim Erstellen dieses Testfalls wurde nicht berücksichtigt, dass die Verbindung für den Agenten benötigt wird. Daher wurde dieser Testfall als belangloser Mangel eingestuft.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 21: TF-10 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-11 Erstellung der Domäne

Die erfolgreiche Einrichtung der Domäne «dom-poc.local» gemäss den definierten Anforderungen wird überprüft, ebenso wie die ordnungsgemässe Funktion des dedizierten Domain Controllers als primärer Authentifizierungsserver. Zusätzlich wird die Active Directory Struktur kontrolliert.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung, ob der Domain Controller (DC) im Netzwerk erreichbar ist, indem die statische IP-Adresse der VM angepingt wird.	Die DC ist erreichbar.
2	Anmeldung auf DC über Remote Desktop (RDP) mit Domain-Admin und Überprüfung, ob die Active Directory-Domänen-dienste installiert sind.	Erfolgreiche Anmeldung und die Active Directory-Domänendienste sind installiert.
3	Überprüfung, ob die Domäne «dom-poc.local» in der Active Directory angezeigt wird.	Die Domäne «dom-poc.local» wird in der Active Directory angezeigt
4	Überprüfung der Active Directory (AD) Struktur gemäss Detailkonzept.	Die AD-Struktur ist wie im Detailkonzept beschrieben erstellt.

Tabelle 22: TF-11 Erstellung der Domäne

Testdurchführung und Ergebnis

Testdatum	20.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	<p>Der DC ist erreichbar und die Domänendienste sind installiert. Der DC befindet sich im Domänennetzwerk und die AD-Struktur wurde gemäss Detailkonzept umgesetzt. Somit wurden alle Testschritte erfolgreich durchgeführt.</p> <p>Printscreens von Domain Controller.</p> <p>Who and what can access your networks.</p> <p> Domain network (active) Firewall is on.</p> <p> Private network Firewall is on.</p> <p> Public network Firewall is on.</p> <pre> -> dom-poc.local > Builtin > Computers <-- Confidential Projects > Access-Groups > Folder Permissions > VDI-Profile > Servers > Member Servers > XenServers > Service Accounts > Users > VDI-Machine </pre>

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 23: TF-11 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-12 Konfiguration DNS Server

Die erfolgreiche Einrichtung und Konfiguration des DNS-Servers gemäss den definierten Anforderungen wird bestätigt, wobei sichergestellt wird, dass der DNS-Server im VDI-Netz nur interne und im MGMT-Netz sowohl interne als auch externe Namen und IP-Adressen auflöst.

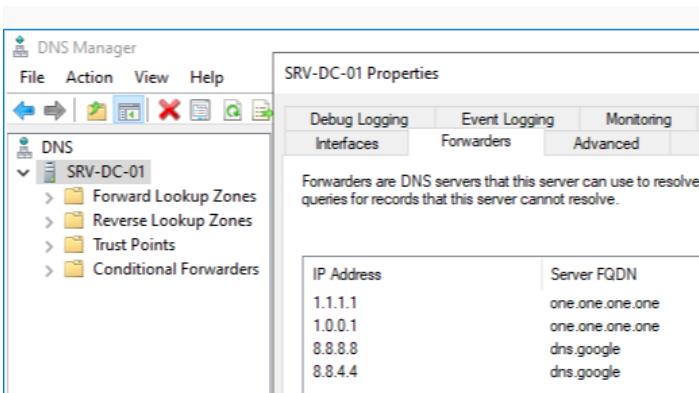
Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung der DNS-Server-Konfiguration auf dem Domain Controller, um sicherzustellen, dass er sowohl das MGMT- als auch das VDI-Netz auflöst.	Die DNS-Server-Konfiguration zeigt, dass der Domain Controller korrekt konfiguriert ist und Anfragen für das MGMT-Netz (192.168.220.0) und das VDI-Netz (192.168.230.0) auflösen kann.
2	Überprüfung der Namensauflösung im MGMT-Netz durch Anfragen an den DNS-Server für sowohl interne als auch externe Adressen durch folgende Befehle: - NSLOOKUP srv-lic-01 - NSLOOKUP 192.168.220.25 - NSLOOKUP www.google.com - NSLOOKUP 8.8.8.8	Die DNS-Anfragen für interne und externe Adressen werden korrekt aufgelöst.
3	Überprüfung der Namensauflösung im VDI-Netz durch Anfragen an den DNS-Server für interne Adressen mit dem folgenden Befehl: - NSLOOKUP srv-dc-02 - NSLOOKUP 192.168.230.21	Die DNS-Anfragen für interne Adressen im VDI-Netz werden korrekt aufgelöst, während Anfragen für externe Adressen fehl-schlagen.
4	Überprüfung der Namensauflösung im VDI-Netz für externe Adressen - NSLOOKUP www.google.com - NSLOOKUP 8.8.8.8	Namensauflösung nicht möglich.

Tabelle 24: TF-12 Konfiguration DNS Server

Testdurchführung und Ergebnis

Testdatum	20.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	1
Mängelbeschreibung	Die interne und externe Namensauflösung funktioniert für das MGMT-Netz einwandfrei. Für das VDI-Netz funktioniert die interne und externe Namensauflösung ebenfalls, was die externe Namensauflösung jedoch nicht tun sollte. Das Problem liegt darin, dass es nur eine DNS-Konfiguration für die beiden Netzwerke gibt.
Bemerkungen	Dieser Mangel ist jedoch sehr gering und beeinträchtigt den Service nicht.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel



IP Address	Server FQDN
1.1.1.1	one.one.one.one
1.0.0.1	one.one.one.one
8.8.8.8	dns.google
8.8.4.4	dns.google

Tabelle 25: TF-12 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-13 Konfiguration DHCP Server

Die erfolgreiche Einrichtung und Konfiguration des DHCP-Servers gemäss den definierten Anforderungen wird überprüft.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung der DHCP-Server-Konfiguration, um sicherzustellen, dass der IP-Adressbereich (192.168.230.30 - 192.168.230.200), der Gateway (192.168.230.1) und die DNS-Server (192.168.230.20 und 192.168.230.21) korrekt eingetragen sind.	Die DHCP-Server-Konfiguration zeigt, dass der IP-Adressbereich, der Gateway und die DNS-Server korrekt konfiguriert sind.
2	Verbindung auf einer VDI-Maschine und Überprüfung, ob die IP-Adresse automatisch vom DHCP-Server bezogen wird.	Die VDI-Maschine erhält automatisch eine IP-Adresse im Bereich von 192.168.230.30 bis 192.168.230.200.
3	Überprüfung, ob die VDI-Maschine den richtigen Gateway (192.168.230.1) und die richtigen DNS-Server (192.168.230.20 und 192.168.230.21) erhalten hat mit dem folgenden Befehl: - IPCONFIG /ALL	Die VDI-Maschine hat das Gateway 192.168.230.1 und die DNS-Server 192.168.230.20 und 192.168.230.21 zugewiesen bekommen.
4	Überprüfung der Lease-Dauer auf der VDI-Maschine, um sicherzustellen, dass sie auf 8 Tage eingestellt ist.	Die Lease-Dauer der IP-Adresse auf der VDI-Maschine zeigt 8 Tage an.

Tabelle 26: TF-13 Konfiguration DHCP Server

Testdurchführung und Ergebnis

Testdatum	20.05.2024								
Tester	Tester Serverinfrastruktur								
Mängelklasse	0								
Mängelbeschreibung	Keine Mängel vorhanden.								
Bemerkungen	<p>Der DHCP funktioniert einwandfrei und die Clients erhalten die richtige IP-Adresse im vorgesehenen DHCP-Bereich.</p> <p>Printscreen von DHCP-Konfiguration.</p> <table border="1"> <thead> <tr> <th>Option Name</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>003 Router</td> <td>192.168.230.1</td> </tr> <tr> <td>006 DNS Servers</td> <td>192.168.230.20, 192.168.230.21</td> </tr> <tr> <td>015 DNS Domain Name</td> <td>dom-poc.local</td> </tr> </tbody> </table> <p>Printscreen VDI-Maschine:</p> <pre>Connection-specific DNS Suffix . : dom-poc.local Link-local IPv6 Address : fe80::81dc:9871:aef5:72f8%6 IPv4 Address : 192.168.230.42 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.230.1</pre>	Option Name	Value	003 Router	192.168.230.1	006 DNS Servers	192.168.230.20, 192.168.230.21	015 DNS Domain Name	dom-poc.local
Option Name	Value								
003 Router	192.168.230.1								
006 DNS Servers	192.168.230.20, 192.168.230.21								
015 DNS Domain Name	dom-poc.local								

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 27: TF-13 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-14 Replikation auf zweiten Domain Controller

Die regelmässige und vollständige Synchronisation aller Domänendaten zwischen den beiden Domain Controllern wird sichergestellt. Zudem wird die Funktionsfähigkeit des zweiten Domain Controllers überprüft, einschliesslich seiner Fähigkeit, im Falle eines Ausfalls des ersten Domain Controllers die volle Kontrolle über die Domäne zu übernehmen.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Erstellen eines neuen Objekts im Active Directory auf dem ersten Domain Controller (srv-dc-01).	Das neue Objekt erscheint automatisch im Active Directory auf dem zweiten Domain Controller (srv-dc-02).
2	Erstellen einer Datei im SYSVOL-Ordner auf dem ersten Domain Controller (srv-dc-01).	Die Datei erscheint automatisch im SYSVOL-Ordner auf dem zweiten Domain Controller (srv-dc-02).
3	Erstellen eines neuen DNS-Eintrags auf dem ersten Domain Controller (srv-dc-01).	Der neue DNS-Eintrag erscheint automatisch im DNS-Manager auf dem zweiten Domain Controller (srv-dc-02).
4	Erstellen einer Test-GPO (Gruppenrichtlinie) auf dem ersten Domain Controller (srv-dc-01).	Die Test-GPO erscheint automatisch im Gruppenrichtlinien-Manager auf dem zweiten Domain Controller (srv-dc-02).
5	Erstellung einer DHCP-Failover-Konfiguration vom ersten Domain Controller (srv-dc-01) auf dem zweiten.	Die DHCP-Failover-Konfiguration ist auf dem zweiten Domain Controller (srv-dc-02) im DHCP-Manager eingerichtet.
6	Herunterfahren des ersten Domain Controllers (srv-dc-01) und Überprüfung, ob der zweite Domain Controller (srv-dc-02) alle Aufgaben übernimmt.	Der zweite Domain Controller (srv-dc-02) übernimmt erfolgreich alle Aufgaben und die Domäne funktioniert weiterhin ordnungsgemäss.

Tabelle 28: TF-14 Replikation auf zweiten Domain Controller

Testdurchführung und Ergebnis

Testdatum	20.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	<p>Die Replikation funktioniert einwandfrei. Alle Testschritte konnten erfolgreich durchgeführt werden.</p> <p>Screenshot DHCP-Failover.</p>

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 29: TF-14 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-15 Backup erfolgt automatisch täglich

Überprüfung, dass das Backup täglich um 2 Uhr morgens automatisch durchgeführt wird, um die Integrität und Verfügbarkeit der Daten zu gewährleisten.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung der Backup-Konfiguration, um sicherzustellen, dass ein tägliches Backup um 2 Uhr morgens geplant ist.	Die Backup-Konfiguration zeigt, dass ein tägliches Backup um 2 Uhr morgens korrekt geplant ist.
2	Überwachung der Backup-Protokolle am nächsten Tag, um zu bestätigen, dass das Backup erfolgreich durchgeführt wurde.	Die Backup-Protokolle bestätigen, dass das tägliche Backup um 2 Uhr morgens erfolgreich durchgeführt wurde.

Tabelle 30: TF-15 Backup erfolgt automatisch täglich

Testdurchführung und Ergebnis

Testdatum	21 - 22.05.2024	
Tester	Tester Serverinfrastruktur	
Mängelklasse	0	
Mängelbeschreibung	Keine Mängel vorhanden.	
Bemerkungen	<p>Alle Testschritte wurden erfolgreich durchgeführt. Backups werden täglich gesichert.</p> <p><input checked="" type="radio"/> Geplante Datensicherung <input checked="" type="checkbox"/> Datensicherung nach Zeit</p> <p>Ausführen am <input type="button" value="Sonntag"/></p> <p>Starten um <input type="button" value="02"/> : <input type="button" value="00"/></p>	
*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel		

Tabelle 31: TF-15 Ergebnis

Testfallbeschreibung

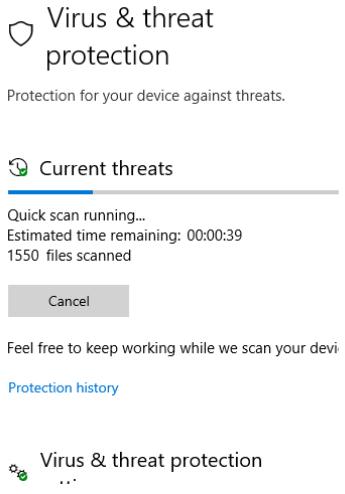
ID / Bezeichnung: TF-16 Auf VDI läuft ein Antivirus

Es wird überprüft, ob der Antivirus sicherstellt, dass alle VDI-Maschinen laufend überwacht werden und vor Malware-Bedrohungen geschützt sind.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung, ob Windows Defender mit Echtzeitschutz den VDI-Maschinen aktiviert ist.	Windows Defender mit Echtzeitschutz ist aktiviert.
2	Durchführung eines vollständigen Systemscans auf einer VDI-Maschine	Der vollständige Systemscan zeigt keine Malware-Bedrohungen an und bestätigt, dass das System überwacht wird.

Tabelle 32: TF-16 Auf VDI läuft ein Antivirus

Testdurchführung und Ergebnis

Testdatum	21.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	<p>Der Windows-Virenschutz ist aktiviert, der Echtzeitschutz ist eingeschaltet und ein Virenscan wurde durchgeführt.</p>  <p>The screenshot shows the Windows Defender interface with a scan in progress. It displays the following text: Virus & threat protection Protection for your device against threats. Current threats Quick scan running... Estimated time remaining: 00:00:39 1550 files scanned Cancel Feel free to keep working while we scan your devi Protection history Virus & threat protection ...</p>

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 33: TF-16 Ergebnis

4 Systemtests

Testfallbeschreibung

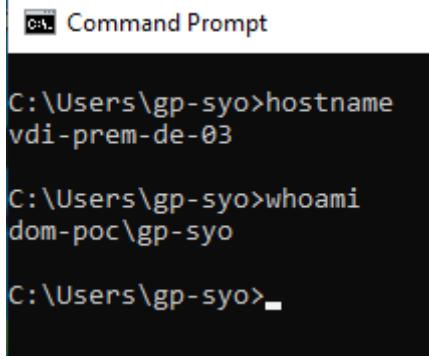
ID / Bezeichnung: TF-17 Anmeldung auf die isolierte Umgebung

Sicherstellen, dass Benutzer sich erfolgreich mit ihren Zugangsdaten über die neue Domäne an der VDI-Umgebung anmelden können.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Anmeldung über die neue Domäne auf der eigenen VDI-Umgebung.	Die Anmeldung war erfolgreich.
2	Nach der Anmeldung überprüfen, mit welchem Benutzer man angemeldet ist, durch den Befehl: - WHOAMI	Als Ausgabe erscheint der eigene Benutzername.

Tabelle 34: TF-17 Anmeldung auf die isolierte Umgebung

Testdurchführung und Ergebnis

Testdatum	21.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	Die Anmeldung eines Domänenbenutzers auf der VDI-Maschine war erfolgreich.  C:\Users\gp-syo>hostname vdi-prem-de-03 C:\Users\gp-syo>whoami dom-poc\gp-syo C:\Users\gp-syo>

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 35: TF-17 Ergebnis

Testfallbeschreibung

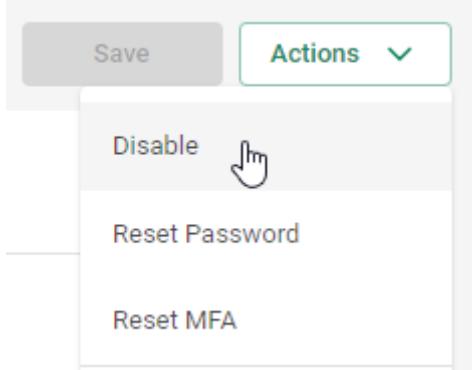
ID / Bezeichnung: TF-18 Schutz gegen Geräteverlust oder Diebstahl

Gewährleistung, dass im Falle von Verlust oder Diebstahl des Arbeitsnotebooks der IT-Administrator in der Lage ist, die gesamte VPN-Verbindung zu unterbrechen, was auch die aktive VDI-Verbindung trennt.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Trennung der VPN-Verbindung eines Notebooks, um den Verlust oder Diebstahl zu simulieren.	Das Notebook kann keine Verbindung mehr zum Firmennetzwerk herstellen, und die aktive VDI-Verbindung wird sofort getrennt.

Tabelle 36: TF-18 Schutz gegen Geräteverlust oder Diebstahl

Testdurchführung und Ergebnis

Testdatum	22.05.2024
Tester	Tester Netzwerk/Security
Mängelklasse	0
Mängelbeschreibung	<p>Die VPN-Verbindung wird über die Cloud verwaltet. Alle vorhandenen VPN-Sessions werden angezeigt. Dabei kann man einzelne Sessions trennen oder sogar deaktivieren.</p> 
Bemerkungen	Das VPN stellt sicher, dass nur autorisierte Benutzer Zugang zur Umgebung haben. Alle Tests konnten erfolgreich durchgeführt werden.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 37: TF-18 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-19 Durchführung von Benutzermutationen

Gewährleistung, dass die Verwaltung von Benutzerkonten in der VDI-Infrastruktur durch den IT-Support effizient und fehlerfrei erfolgen kann.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Ein Testbenutzerkonto wird im Active Directory erstellt und der Benutzer wird der neuen VDI-Umgebung zugewiesen.	Das Testbenutzerkonto wird erfolgreich erstellt und zugewiesen.
2	Anmeldung des Testbenutzers an der VDI-Umgebung, um die Funktionsfähigkeit des Kontos zu überprüfen.	Der Testbenutzer kann sich erfolgreich an der VDI-Umgebung anmelden.
3	Überprüfung, ob der Testbenutzer Zugriff auf die notwendigen Ressourcen und Anwendungen hat, die für seine Rolle vorgesehen sind.	Der Testbenutzer hat Zugriff auf alle zugewiesenen Ressourcen und Anwendungen.
4	Löschen des Testbenutzerkontos und Überprüfung, ob alle zugehörigen Daten und Zugriffe korrekt entfernt wurden.	Das Testbenutzerkonto und alle zugehörigen Daten und Zugriffe werden vollständig entfernt.

Tabelle 38: TF-19 Durchführung von Benutzermutationen

Testdurchführung und Ergebnis

Testdatum	22.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	Nach der Erstellung eines Benutzers müssen die Berechtigungen an verschiedenen Orten angepasst werden. - VDI Abo Stufe (AD) - WEM Profil (AD) - Dateiablage (NTFS oder Synology NAS)

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 39: TF-19 Ergebnis

Testfallbeschreibung

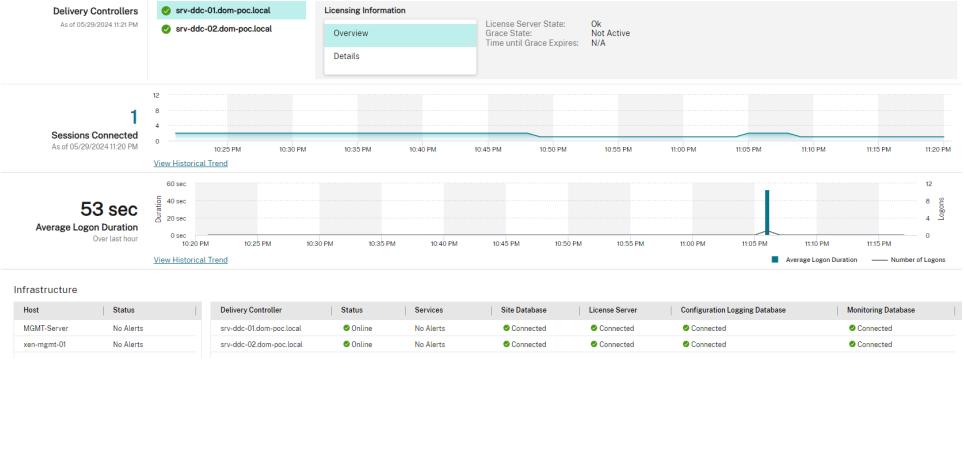
ID / Bezeichnung: TF-20 Intuitiv Performance und Verfügbarkeit

Bestätigung, dass die Performance der VDI-Systeme regelmäßig überwacht wird, um eine leistungsfähige und effiziente Umgebung sicherzustellen.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Überprüfung der Performance und Verfügbarkeit der VDI-Umgebung über das Citrix Dashboard.	Die Performance- und Verfügbarkeitsdaten sind im Citrix Dashboard sichtbar und zeigen keine Auffälligkeiten.
2	Durchführung eines Lasttests auf einer Test-VDI-Umgebung, um die Systemleistung unter hoher Auslastung zu überprüfen.	Das System bleibt auch unter hoher Last stabil und die Performance-Daten werden korrekt im Dashboard angezeigt.

Tabelle 40: TF-20 Intuitiv Performance und Verfügbarkeit

Testdurchführung und Ergebnis

Testdatum	22.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	 <p>The screenshot displays the Citrix Director Dashboard. It includes a 'Sessions Connected' chart showing 1 session at 10:29 PM on May 29, 2024. Below it is a 'Average Logon Duration' chart showing 53 sec over the last hour. The 'Infrastructure' section shows two hosts (MGMT-Server and xen-mgmt-01) with no alerts, and four delivery controllers (srv-ddc-01, srv-ddc-02, and two others) all online. Services, Site Database, License Server, Configuration Logging Database, and Monitoring Database are also listed as connected.</p>
Bemerkungen	Über das Citrix Director Dashboard erhält man eine Übersicht über die VDI-Landschaft und wird bei Fehlern durch verschiedene Alarne benachrichtigt.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 41: TF-20 Ergebnis

Testfallbeschreibung

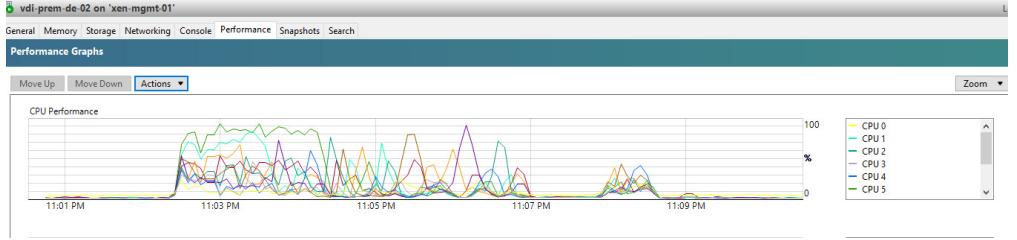
ID / Bezeichnung: TF-21 Skalierung während dem laufenden Betrieb

Es wird bestätigt, dass die VDI-Infrastruktur während des laufenden Betriebs skalierbar ist, um den steigenden Anforderungen gerecht zu werden.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Mehrere Testbenutzer melden sich an und führen einen Lasttest aus.	Im Citrix Dashboard wird angezeigt, dass die Ressourcen ausgelastet sind.
2	Die Testbenutzer, die am meisten Leistung benötigen, erhalten eine VDI-Maschine mit mehr Ressourcen.	Alle anderen Testbenutzer können weiterarbeiten, ohne unterbrochen zu werden.
3	Überprüfung nach Skalierung.	Die Ressourcen liegen innerhalb der akzeptablen Grenzwerte.

Tabelle 42: TF-21 Skalierung während dem laufenden Betrieb

Testdurchführung und Ergebnis

Testdatum	22.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden. 
Bemerkungen	Es kann proaktiv oder bei Bedarf des Kunden eine leistungsstärkere VDI bereitgestellt werden, ohne andere Benutzer zu beeinträchtigen.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 43: TF-21 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-22 Redundanz

Überprüfung der Ausfallsicherheit der Dienste Storefront Server, Desktop Delivery Controller, Domain Controller und Workspace Environment Management

Testschritt	Beschreibung	Erwartetes Ergebnis
1	Verbindung auf XenServer über den XenCenter herstellen.	Verbindung zu XenServer kann erfolgreich hergestellt werden.
2	Um einen Ausfall zu simulieren, werden alle drei Server über XenCenter heruntergefahren: - srv-sfs-01 - srv-ddc-01 - srv-dc-01 - srv-wem-01	VMs werden im XenCenter als heruntergefahren angezeigt.
3	Überprüfen, ob die redundanten Server die Aufgaben übernommen haben, indem eine Testanmeldung auf die VDI-Umgebung durchgeführt wird.	Die Testanmeldung ist erfolgreich, und die redundanten Server haben die Aufgaben übernommen: - srv-sfs-02 - srv-ddc-02 - srv-dc-02 - srv-wem-02

Tabelle 44: TF-22 Redundanz

Testdurchführung und Ergebnis

Testdatum	22.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	3
Mängelbeschreibung	Keine vollständige Einrichtung der Redundanz dieser Dienste: - srv-sfs-01 - srv-wem-01 Restliche Dienste funktionieren redundant.
Bemerkungen	Aufgrund der Notwendigkeit eines Loadbalancers konnten diese beide Dienste zeitlich nicht redundant ausgelegt werden.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 45: TF-22 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-23 Benutzeranpassungen der VDI-Umgebung

Sicherstellung, dass zusätzliche Anpassungen am Standard-Image auf Wunsch des Kunden durchgeführt werden können.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Installation des Programms PDF24 auf dem Standard-VDI-Image.	Die Installation ist für alle VDI-Maschinen verfügbar und bleibt nach einer erneuten Anmeldung des Benutzers erhalten.
2	Der Testbenutzer meldet sich erneut an der VDI-Umgebung an und überprüft, ob die vorgenommenen Anpassungen vorhanden sind.	Das installierte Programm ist nach der erneuten Anmeldung weiterhin vorhanden.
3	Testen der Funktionalität des installierten Programms, um sicherzustellen, dass es ordnungsgemäss funktioniert.	Das Programm funktioniert einwandfrei.

Tabelle 46: TF-23 Benutzeranpassungen der VDI-Umgebung

Testdurchführung und Ergebnis

Testdatum	22.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden. 
Bemerkungen	PDF24 wurde auf dem Basic Image installiert und freigegeben. Das Programm war danach für alle berechtigten Benutzern verfügbar.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 47: TF-23 Ergebnis

5 Abnahmetests

Testfallbeschreibung

ID / Bezeichnung: TF-24 Fernzugriff

Sicherstellung, dass Kunden sicher von jedem Ort auf ihre VDI-Umgebung zugreifen können.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Das eingerichtete VPN auf dem Firmen-notebook starten.	Verbindung zum Firmennetzwerk ist möglich und es erscheint die Citrix Storefront-Anmeldemaske.
2	Anmeldung auf Citrix VDI.	Die Eingabe war erfolgreich.
3	VDI-Umgebung starten und Überprüfung der Verbindung und Funktionalität.	Die VDI-Umgebung startet erfolgreich.

Tabelle 48: TF-24 Fernzugriff

Testdurchführung und Ergebnis

Testdatum	22.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.
Bemerkungen	Die Verbindung wurde mit einem Testgerät hergestellt, auf dem das Stammzertifikat für die HTTPS-Verbindung zu StoreFront installiert wurde. Die Verbindung zur VDI hat problemlos funktioniert

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 49: TF-24 Ergebnis

Testfallbeschreibung

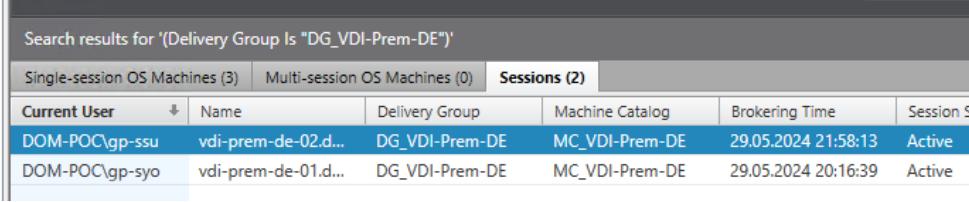
ID / Bezeichnung: TF-25 Kollaboration mit Projektmitarbeitern

Überprüfung, ob mehrere Benutzer gleichzeitig auf die Citrix VDI-Umgebung zugreifen und gemeinsam an Projekten arbeiten können.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Mehrere Testbenutzer melden sich gleichzeitig an der VDI-Umgebung an.	Die Anmeldung ist erfolgreich und die Mitarbeiter blockieren sich nicht gegenseitig.
2	Jeder Projektmitarbeiter hat Zugriff auf die für ihn freigegebenen Daten und Ressourcen.	Die Mitarbeiter können auf die freigegebenen Daten zugreifen und diese nach Absprache gemeinsam bearbeiten.

Tabelle 50: TF-25 Kollaboration mit Projektmitarbeitern

Testdurchführung und Ergebnis

Testdatum	22.05.2024					
Tester	Tester Serverinfrastruktur					
Mängelklasse	0					
Mängelbeschreibung	Keine Mängel vorhanden. 					
Bemerkungen	Verschiedene Benutzer können sich problemlos gleichzeitig mit der VDI verbinden. Die Datenablage wird korrekt über WEM zugewiesen, und ein gemeinsamer Zugriff auf eine zentrale Dateiablage ist möglich.					

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 51: TF-25 Ergebnis

Testfallbeschreibung

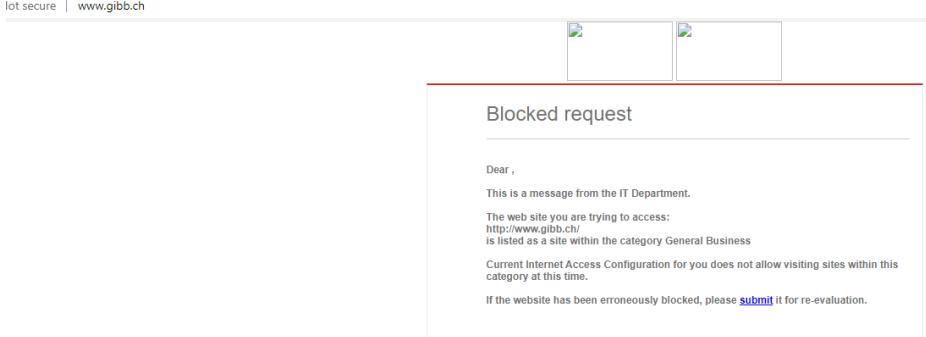
ID / Bezeichnung: TF-26 VDI hat kein Internetzugang

Es wird sichergestellt, dass die VDI-Umgebung keinen Internetzugang ermöglicht und Benutzer ausschliesslich auf interne Netzwerkressourcen zugreifen können.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Einen Webbrower in der VDI-Umgebung öffnen und die folgende Webseite aufrufen: - www.gibb.ch	Der Zugriff auf externe Webseiten ist nicht möglich und es wird eine Fehlermeldung angezeigt.

Tabelle 52: TF-26 VDI hat kein Internetzugang

Testdurchführung und Ergebnis

Testdatum	22.05.2024
Tester	Tester Netzwerk/Security
Mängelklasse	0
Mängelbeschreibung	Keine Mängel vorhanden.  <p>The screenshot shows a browser window with the URL 'www.gibb.ch' in the address bar. A red box highlights a message box titled 'Blocked request'. The message reads: 'Dear, This is a message from the IT Department. The web site you are trying to access: http://www.gibb.ch/ is listed as a site within the category General Business Current Internet Access Configuration for you does not allow visiting sites within this category at this time. If the website has been erroneously blocked, please submit it for re-evaluation.' Below the message box, there are two small thumbnail images.</p>
Bemerkungen	Firewall Regel ins WAN wurde korrekt eingerichtet.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 53: TF-26 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-27 Vordefinierte Programme sind auf der VDI installiert

Es wird sichergestellt, dass die spezifischen, für die Arbeit notwendigen Programme vorab auf der VDI installiert wurden und funktionieren.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Die vorinstallierten Anwendungen in der VDI-Umgebung starten und ihre Funktionalität überprüfen.	Die Anwendungen starten ohne Probleme und funktionieren einwandfrei.
2	Eine Testaufgabe mit jeder der vorinstallierten Anwendungen durchführen, um ihre Leistungsfähigkeit und Stabilität zu prüfen.	Jede Anwendung führt die Testaufgabe erfolgreich aus, ohne Abstürze oder Fehlermeldungen.

Tabelle 54: TF-27 Vordefinierte Programme sind auf der VDI installiert

Testdurchführung und Ergebnis

Testdatum	22.05.2024
Tester	Tester Serverinfrastruktur
Mängelklasse	0
Mängelbeschreibung	Da keine spezifischen Anwendungen angefordert wurden, haben die Tester selbst gewählte Programme installiert und getestet.
Bemerkungen	Der Vectorworks 23 Viewer und Blender wurden mit verschiedenen Demodateien getestet. Beide Programme laufen stabil mit 30 FPS.

*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel

Tabelle 55: TF-27 Ergebnis

Testfallbeschreibung

ID / Bezeichnung: TF-28 Sicherheitsfunktionen

Gewährleistung, dass die implementierten Sicherheitsmassnahmen effektiv aktiviert wurden.

Test-schritt	Beschreibung	Erwartetes Ergebnis
1	Versuchen, Daten von der VDI-Umgebung auf das lokale Notebook zu kopieren und umgekehrt.	Die Kopierfunktion ist blockiert und es können keine Daten vom lokalen Notebook in die VDI-Umgebung oder aus der VDI-Umgebung auf das lokale Notebook kopiert werden.
2	Überprüfung, ob Screenshots oder Videoaufnahmen vom lokalen Notebook aus von der VDI-Umgebung gemacht werden können.	Screenshots und Videoaufnahmen können vom lokalen Notebook aus nicht gemacht werden.
3	Beim Anmeldeprozess in die VDI-Umgebung muss mindestens einmal eine Zwei-Faktor-Authentifizierung (2FA) durchgeführt werden.	Die Multi-Faktor-Authentifizierung ist erfolgreich implementiert und funktioniert einwandfrei.

Tabelle 56: TF-28 Sicherheitsfunktionen

Testdurchführung und Ergebnis

Testdatum	22.05.2024
Tester	Tester Netzwerk/Security
Mängelklasse	1
Mängelbeschreibung	Es wurden keine spezifischen Richtlinien in der Infrastruktur eingerichtet, die Screenshots oder Videoaufnahmen softwareseitig blockieren. Da vordefinierte Projektnotebooks verwendet werden, wird jedoch jede Software mit solchen Funktionen blockiert.
Bemerkungen	<p>Die Zwischenablage von der VDI-Umgebung zur lokalen Maschine sowie umgekehrt wird durch eine Richtlinie verweigert.</p> <p>Die Zwei-Faktor-Authentifizierung ist für das VPN eingerichtet und wird einmal täglich angefordert.</p>
<p>*Mängelklasse: 0 = fehlerfrei, 1 = belangloser Mangel, 2 = leichter Mangel, 3 = schwerer Mangel, 4 = kritischer Mangel</p>	

Tabelle 57: TF-28 Ergebnis

Anhang F3

Abnahmeprotokoll

VDI as a Service

Auftraggeber Micha Bucher
Projektleiter Shipinyuan Su, Sirak Yosef
Autor Shipinyuan Su, Sirak Yosef
Klassifizierung Intern
Status Von AG abgesegnet

Änderungsverzeichnis

Datum	Version	Änderung	Autor
19.05.2024	1.0	Dokument erstellt, bearbeitet & fertiggestellt	Shipinyuan Su, Sirak Yosef

Checkliste

Diese Checkliste dient zur Überprüfung der korrekten Einrichtung und Funktionalität der VDI-Lösung. Die Funktionstests werden vom Auftraggeber persönlich durchgeführt.

Nr.	Funktionstest	Checkbox
1	VPN ist auf dem Notebook installiert	<input type="checkbox"/>
2	VPN-Verbindung ist mit einer Zwei-Faktor-Authentifizierung geschützt	<input type="checkbox"/>
3	Verbindung von externen auf das interne Netzwerk kann hergestellt werden	<input type="checkbox"/>
4	Ohne Zertifikat kann auf die Anmeldemaske über den Browser nicht zugegriffen werden	<input type="checkbox"/>
5	Mit installiertem Zertifikat kann auf die Anmeldemaske zugegriffen werden	<input type="checkbox"/>
6	Mit den erhaltenen Zugangsdaten kann man sich über die Anmeldemaske anmelden	<input type="checkbox"/>
7	Citrix Workspace ist lokal vorinstalliert und der Desktop kann durch Doppelklick gestartet werden	<input type="checkbox"/>
8	CAD-Programm ist installiert und kann gestartet werden	<input type="checkbox"/>
9	Laufwerk für Datenablage ist eingebunden und der Zugriff funktioniert	<input type="checkbox"/>
10	Dokumente können bearbeitet und abgespeichert werden	<input type="checkbox"/>
11	Das Browsen im Internet ist nicht möglich	<input type="checkbox"/>
12	Das Übertragen von Daten von der VDI-Session auf das lokale Notebook oder umgekehrt wird blockiert	<input type="checkbox"/>
14	Jegliche lokalen Aufnahmen von der VDI-Session werden blockiert	<input type="checkbox"/>

Ort / Datum

Unterschrift

Micha Bucher

Anhang F4

Citrix Virtual Apps

Stellen Sie geschäftliche Windows- und Web-Anwendungen auf jedem Endgerät bereit, während Sie gleichzeitig den Datenschutz verbessern, Kosten senken und die Produktivität steigern.

Citrix Virtual Apps ist die führende Lösung für die Bereitstellung von Anwendungen und Desktops, mit über 100 Millionen Nutzern weltweit. Citrix Virtual Apps ermöglicht einen sicheren Remote-Zugriff auf Windows-Anwendungen und Server-Desktops – über jedes beliebige Endgerät und Netzwerk. Anwendungen und Desktops werden im Rechenzentrum abgesichert, sodass vertrauliche Informationen und Unternehmensdaten geschützt werden. Mit Citrix Virtual Apps können Mitarbeiter nun auch virtuelle Linux®-Desktops gemeinsam mit Windows-Ressourcen verwenden, für einen höheren Benutzerkomfort am digitalen Arbeitsplatz.

Warum Citrix Virtual Apps?



Flexibilität

Schnelle Anpassung an veränderte Geschäftsanforderungen

Citrix Virtual Apps kann für zahlreiche Anwendungsfälle genutzt werden. Sie können einen vollständigen Desktop oder ausschließlich Anwendungen bereitstellen, je nach Rolle oder Endgerät des Nutzers. Durch umfassende Funktionen und eine flexible Architektur kann die IT agiler werden und sich schneller an veränderte Arbeitsplätze anpassen.



Sicherheit

Secure by design

Citrix Virtual Apps ist die einzige Lösung in der Branche, die Common-Criteria-zertifiziert ist und eine native FIPS-140-2-Compliance aufweist. Citrix Virtual Apps verringert das Datenverlustrisiko und verhindert unbefugten Zugriff, indem jedem Nutzer ein sicherer Zugriff auf Unternehmensanwendungen bereitgestellt wird, abhängig von dessen Standort sowie endgerätespezifischen Funktionen und Sicherheitseinstellungen.



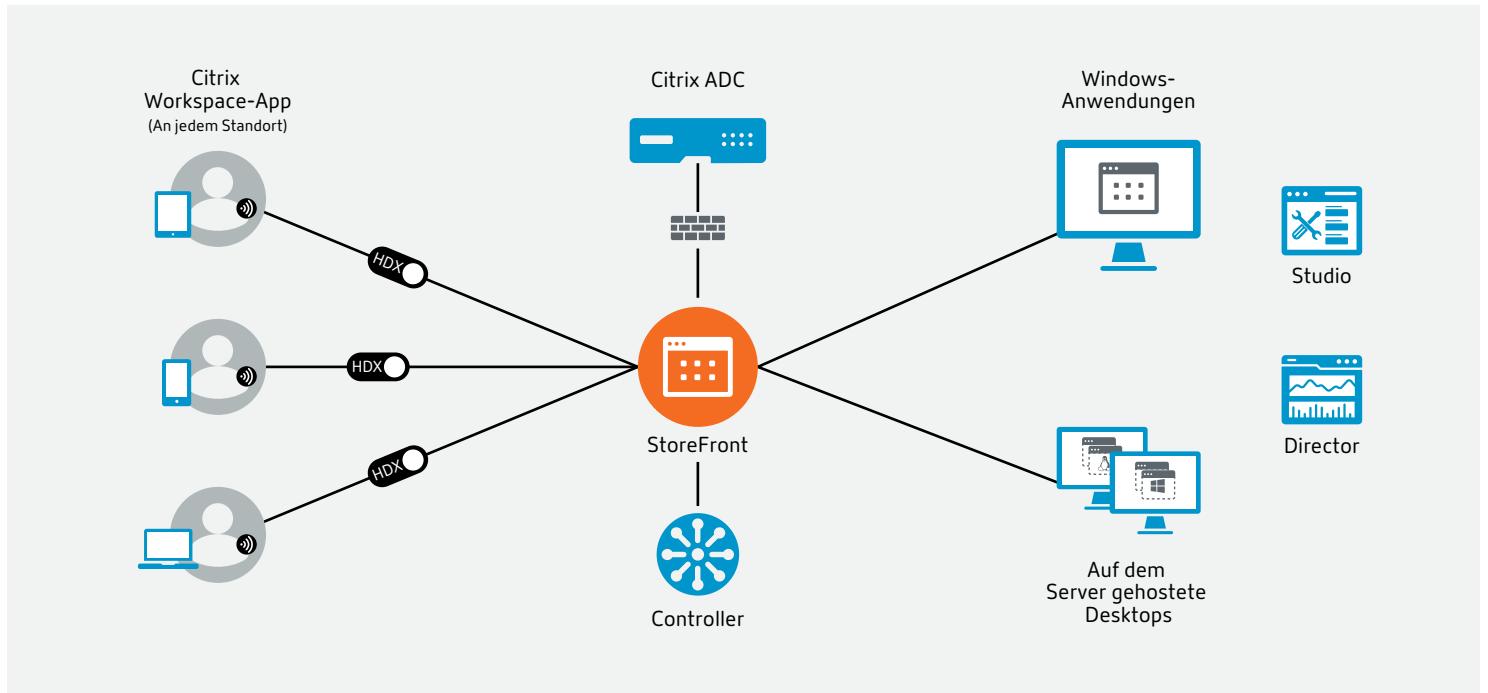
Benutzerkomfort

High-Definition-Performance (HDX) auf jedem Endgerät

Die HDX-Technologie ermöglicht eine erstklassige High-Definition-Performance auf jedem Endgerät. HDX übertrifft Lösungen der Konkurrenz und stellt sicher, dass Mitarbeiter über eine nahezu native Performance verfügen, egal wo sie sich befinden – selbst bei mangelhafter Verbindungsqualität.

Komponenten von Citrix Virtual Apps

- **Citrix Workspace-App.** Anwender greifen über die Citrix Workspace-App auf ihre Anwendungen und Desktops zu. Die Citrix Workspace-App ist ein universeller Client, der praktisch auf jedem Betriebssystem ausgeführt werden kann, einschließlich iOS, Android, Windows, Mac® und Linux.
- **HDX-Technologie.** HDX-Technologie bietet Nutzern virtueller Anwendungen und Desktops eine „High-Definition“ Performance auf jedem Endgerät und über jedes Netzwerk.
- **Citrix Gateway.** Citrix Gateway ist eine Lösung für den sicheren Zugriff auf Anwendungen und Desktops, die Administratoren eine granulare Zugriffskontrolle auf Anwendungs-/Datenebene und Anwendern einen zuverlässigen standortunabhängigen Remote-Zugriff ermöglicht.
- **StoreFront.** StoreFront bietet einen Self-Service-Abonnementsservice über einen Unternehmens-App-Store, sodass Anwender praktischen Zugriff auf alle geschäftlichen Anwendungen und Desktops haben, die sie benötigen.
- **Controller.** Controller verwaltet zentral den Anwenderzugriff auf virtuelle Apps und Desktops im Rechenzentrum über anwender- und computerbasierte Richtlinien.
- **Anwendungen und Desktops.** Mit Citrix Virtual Apps können alle Anwendungsarten sowie auf einem Server gehostete Windows- oder Linux-Desktops – egal ob in einer Private oder Public Cloud – zentral verwaltet und On-Demand für Tausende von Anwendern weltweit bereitgestellt.
- **Studio.** Studio umfasst Servicedesign-Assistenten zum Erstellen und Verwalten der Infrastruktur und Ressourcen, um Anwendungen und Desktops bereitzustellen und so Produktionsbereitstellungen zu vereinfachen.
- **Director.** Director stellt Trend- und Diagnoseinformationen in Echtzeit zu Anwendern, Anwendungen und Desktops bereit, um Helpdesk-Mitarbeiter bei der Fehlerbehebung zu unterstützen.



„Bei Verbindungen mit vielen Anwendern hat das Design-Kollaborationssystem der nächsten Generation mit Citrix Virtual Apps als Grundlage eine höhere Performance und Effizienz gezeigt als das vorhandene System.“

- Moon Kyung Yoon, Information Technology Team Manager, Daewoo Shipbuilding & Marine Engineering

[Vollständiger Bericht](#)

So unterstützt Sie Citrix Virtual Apps

Windows-, Web-, SaaS- und Linux-Anwendungen für unterwegs

Citrix Virtual Apps and Desktops gewährt Mitarbeitern auf jedem Gerät und von überall aus sicheren mobilen Zugriff auf Anwendungen, die in Windows- oder Linux-Betriebssystemen gehostet werden.

Sicherer Zugriff für Auftragnehmer, Partner und Remote-Mitarbeiter

Citrix Virtual Apps bietet eine granulare Zugriffskontrolle, fortschrittliches System-Monitoring und eine von Grund auf sichere Architektur, da der Remote-Zugriff auf Windows-Anwendungen und -Desktops im Rechenzentrum abgesichert ist.

Anwendungen für Design und Konstruktion auf jedem Endgerät bereitstellen

Citrix Virtual Apps ermöglicht einen sicheren Remote-Zugriff in Echtzeit auf zentrale Design-Ressourcen. So können Konstrukteure und Techniker über jedes Endgerät auf professionelle 3D-Grafikanwendungen zugreifen.

Kosten und Komplexität von App- und Desktop-Management verringern

Citrix Virtual Apps ist eine bewährte Lösung, die den Betrieb effizienter gestaltet, Kosten senkt und das Anwendungs-Management optimiert. So können Mitarbeiter über verschiedene Endgeräte sicher auf vertrauliche Unternehmensressourcen zugreifen.

Bring-Your-Own-Device (BYOD) im Unternehmen ermöglichen

Mit Citrix Virtual Apps kann die IT On-Demand-Anwendungen und -Desktops auf jedem beliebigen Endgerät bereitstellen. So kann auf einfache und sichere Weise BYOD im Unternehmen ermöglicht werden.

Citrix Virtual Apps nach Branche

Gesundheitswesen

Citrix Virtual Apps macht mobiles Arbeiten möglich, mit nahtlosem, sicherem Zugriff auf Patientendaten an jedem beliebigen Standort und Endgerät und über jedes Netzwerk. So können sich Ärzte und Pflegekräfte auf die Behandlung von Patienten konzentrieren.

Finanzwesen

Mit Citrix Virtual Apps können sich Finanzinstitute dank des zentralisierten Anwendungsmanagements schnell auf neue gesetzliche Vorgaben einstellen, sich vor Cyberbedrohungen schützen und die Anforderungen von Kunden erfüllen.

Öffentliche Verwaltung

Landes- und Kommunalverwaltungen können mithilfe von Citrix Virtual Apps mehrere hundert Millionen Euro an Steuergeldern einsparen, indem sie Ausgaben verringern und die Effizienz von Behörden und Dienstleistungen steigern.

Produktion

Citrix Virtual Apps beschleunigt die Fertigung in verschiedenen Branchen, darunter Automobilherstellung, Konsumgüter, Luft- und Raumfahrt sowie Verteidigung, indem Anwendungen und Daten auf schnelle Weise in der gesamten Lieferkette bereitgestellt werden.

Unterricht und Ausbildung

Citrix Virtual Apps bietet Schülern und Lehrkräften On-Demand einen sicheren, mobilen Zugriff auf Anwendungen, Daten und Services, die sie für ein unabhängiges Lernen und Forschen benötigen.

Erfahren Sie mehr über Citrix Virtual Apps and Desktops auf
www.citrix.com/de-de/products/citrix-virtual-apps-and-desktops.



Enterprise Sales

Nordamerika | 800-424-8749
Weltweit | +1 408 790 8000

Standorte

Unternehmenszentrale | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, USA
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, USA

©2019 Citrix Systems, Inc. Alle Rechte vorbehalten. Citrix, das Citrix-Logo und andere hierin aufgeführten Marken sind Eigentum von Citrix Systems, Inc. und/oder eines ihrer Tochterunternehmen und sind möglicherweise beim Patent- und Markenamt der Vereinigten Staaten und in anderen Ländern eingetragen. Alle anderen Marken sind Eigentum der jeweiligen Inhaber.

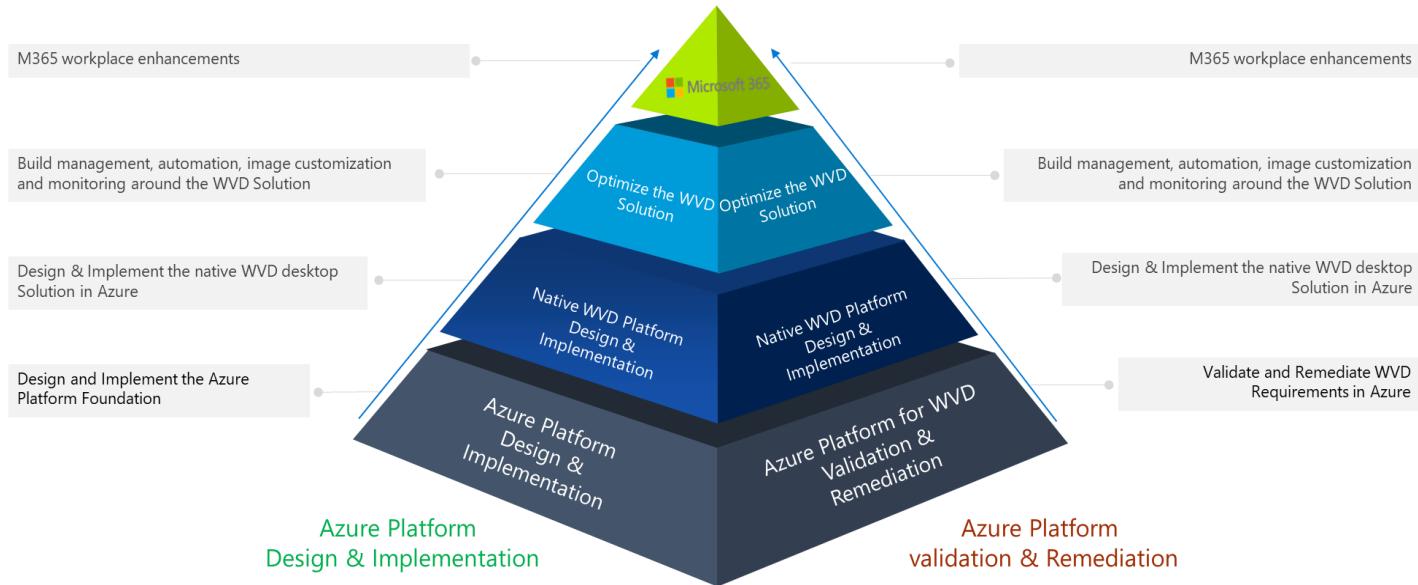
Azure Workloads for Windows Virtual Desktop

Discover, Design, Implement

Virtualization is helping organizations address many business needs around flexibility, security, compliance, and employee-specific requirements. However, deploying and managing an on-premises virtualization infrastructure, especially for desktop scenarios, can be complex and costly for IT and the business.

Windows Virtual Desktop (WVD) is a comprehensive desktop and app virtualization service running in the cloud and offers organizations an option to optimize their desktop virtualization experience and leverage the power of a modern cloud

Two Adoption Paths with the same outcomes



The service can support customers that already have an Azure Cloud infrastructure or those who are about to embark on their journey with Azure by utilizing the existing Azure Cloud Foundation Offering

VDI/RDSH as a Service Management in Azure

Leverage the WVD PaaS to simplify your virtual desktop infrastructure while optimizing the operations

Enable optimizations for Office 365 ProPlus

WVD delivers the best Office 365 ProPlus experience with multi-session virtual scenarios to provide the most productive virtualized experience to your users.

Deploy and scale in minutes

Virtualize and deploy modern and legacy desktop app experiences in minutes with unified management in the Azure portal.

Delivers the only multi-session Windows 10 experience

WVD is the only multi-session Windows 10 virtualized in the cloud that's highly scalable, always up to date, and available on any device.



WVD Discovery & Insights

WVD Design & Implementation

WVD Optimization

- Interview and tooling-based discovery
- Identify customer requirements for the WVD solution
- Identify Azure Platform gaps to deploy WVD
- Remediate Azure Platform gaps to deploy WVD

- Design a native WVD solution based on customer requirements
- Implement a native WVD solution including Hosts Pools, Sessions Hosts, App Groups
- Implementation automation using DevOps practices (optional)

- Build additional imaging, automation and monitoring capabilities on top of Azure WVD native controls
- Includes Azure and M365 enhance security, Monitoring, Management and Automation

The Modern Workplace Approach

Azure Cloud Foundation establish Azure as the platform for your workloads, applications, and services. Design and implement your enterprise-grade, secure by design infrastructure in Azure. Address identity and security requirements to simplify administration and IT processes, and to protect privileged accounts against credential.

Modern Desktop and Devices Essentials is a modular engagement which will align to your organizational requirements and readiness. The overall goal is to help you move your users to the Modern Desktop as quickly as possible. Microsoft Industry Solutions offers four main areas of assistance, that are regularly needed by our customers:

Modern Workplace Security Essentials provides customers with support for enabling key Microsoft 365 security features across the Office 365 suite and Windows 10 clients. The engagement combines security features for securing customer data, the transfer of data, and data at rest—as well as supports information classification and monitoring for potential environmental threats our customers face within their Microsoft 365 portfolio.



Azure Cloud Foundation

WVD Design & Implementation

WVD Optimization

M365 Enhancements

Next steps: Contact your Microsoft representative to learn more. For more information about consulting and support solutions from Microsoft, visit [Microsoft Industry Solutions | Powering your digital transformation](#).

VMware Horizon

A modern platform for secure delivery of virtual desktops and apps

What's new

Flexible deployment options and hybrid and multi-cloud capabilities let organizations leverage the cloud and unlock key use cases. Continuously updated management capabilities in the Horizon Control Plane enable organizations to reduce complexity by unifying management and entitlement across pods and clouds.

At a glance

VMware Horizon is a modern platform for secure delivery of virtual desktops and apps across the hybrid cloud.

VMware's virtualization heritage provides Horizon unique benefits and best-in-class technologies that enable one-to-many provisioning and streamlined management of images, apps, profiles and policies for an agile, lightweight, modern approach that speeds, simplifies and reduces costs. Horizon, powered by the Blast Extreme protocol, delivers an immersive, feature-rich user experience for end users across devices, locations, media and network connections. Enabled by enterprise-grade management capabilities and a deep VMware technology ecosystem, Horizon extends the digital workspace to all apps.

Embracing modern technology has become critical with the growth in remote work, mobility and hybrid cloud and the security that these trends require. These changes give organizations the opportunity to use technology to build a digital-first culture and accelerate business outcomes, but they also introduce challenges for IT and end users. While easy access to corporate apps and data from any device increases end-user productivity and engagement, it also requires the highest level of security. Managing and delivering services across distributed environments to end users with traditional or legacy desktop and app tools has also become increasingly difficult.

VMware Horizon® provides IT with a modern, streamlined approach to deliver, protect and manage Windows and Linux desktops and applications while containing costs and ensuring that end users can work anytime, anywhere, on any device.

Horizon: From on-premises to the hybrid and multi-cloud

Leveraging best-in-class management capabilities and deep integrations with the VMware technology ecosystem, the Horizon platform delivers a modern approach for desktop and app management that extends from on-premises to the hybrid and multi-cloud. The result is fast and simple virtual desktop and application delivery that brings the best digital workspace experience to all applications.

Modern platform for simplicity and speed

You can rapidly deploy full-featured, personalized virtual desktops and apps in seconds by leveraging Instant Clone, VMware App Volumes™, and VMware Dynamic Environment Manager technologies. Instant clone desktops retain user customization and persona from session to session and can be destroyed at logout, an agile provisioning approach that can quickly roll out updated images and apps at the next login. One-to-many provisioning and complete API extensibility of the Horizon platform streamlines and automates day 2 management of images, apps, profiles and policies. IT can take advantage of this lightweight, modern approach that simplifies management, saves time, and reduces costs, but not at the expense of user customization and personalization.

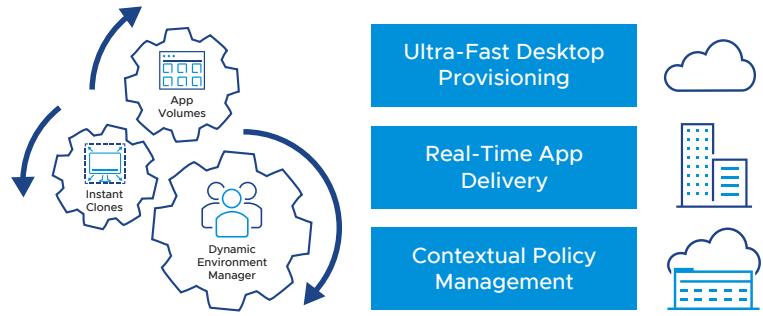


Figure 1: Just-in-time management technologies eliminate cost and complexity.

Hybrid delivery, management and scale

Flexible deployment options across private and public clouds, such as Microsoft Azure, VMware Cloud™ on AWS, and Google Cloud, enable hybrid and multi-cloud architectures. Always up-to-date services in the Horizon Control Plane connect entitlement and management layers across Horizon pods in different data centers and clouds, addressing challenges such as monitoring and image, application and lifecycle management. The integrated Universal Broker delivers a global entitlement layer that lets end users access their personal desktop or app in any connected pod or cloud, providing an optimized user experience based on proximity. These features, coupled with real-time desktop and application delivery and consistent end-to-end security, address key hybrid use cases such as business continuity, real-time bursting, disaster recovery and high availability, simplifying and optimizing your cloud investment.

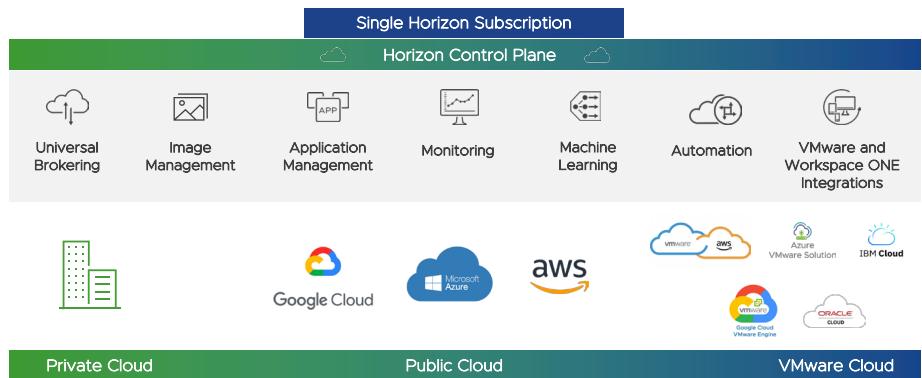


Figure 2: Leverage cloud resources for hybrid delivery and management. Simplify VDI and app management across clouds with the Horizon Control Plane.

End-to-end security from your trusted partner

Horizon delivers secure remote access to corporate resources from bring-your-own or corporate devices and centrally hosted desktops and apps. Intrinsic security that is built into your VMware infrastructure helps provide complete security from the device, across the network, and into the data center and cloud. VMware Workspace ONE® Access establishes and verifies end-user identity with multifactor authentication and serves as the basis for conditional access and network microsegmentation policies for Horizon virtual desktops and apps.

Additional security features that are supported by Horizon, such as VMware NSX® Advanced Load Balancer (formerly known as Avi Networks) and VMware SD-WAN™, are woven into VMware technologies across the network. With next-generation endpoint protection from Carbon Black, IT can further improve security on virtual desktops and apps. These intrinsic elements help provide a Zero Trust access security model across users, apps and endpoints that empowers employees without sacrificing security.

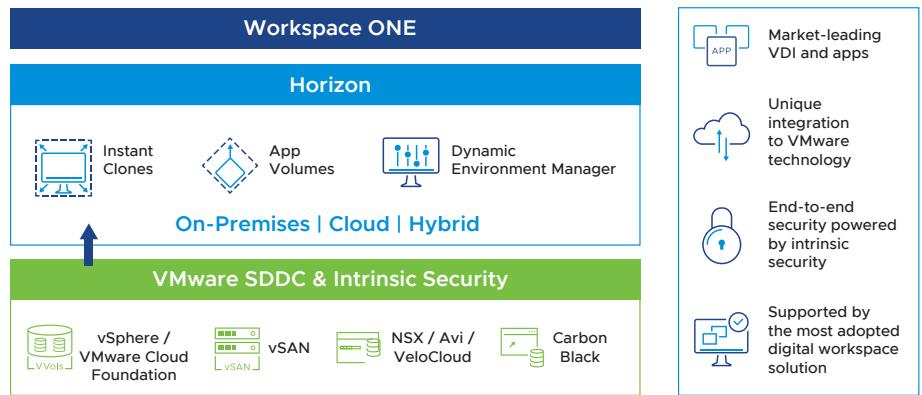


Figure 3: Enable the future-ready workforce with Horizon 8, a modern platform for secure delivery of VDI and apps across the hybrid cloud.

Unique integration with VMware technology

Leveraging VMware's virtualization heritage and leadership in the Software-Defined Data Center and digital workspace technology, Horizon delivers unique benefits across management, networking, security and user experience. Built on VMware Cloud Foundation™, Horizon can leverage the market-leading capabilities of VMware vSphere®, VMware vSAN™ and VMware NSX to deliver real-time desktops and applications, strengthen security, and simplify and automate day 2 operations.

VMware Cloud Foundation forms the bedrock of the leading hyperconverged infrastructure across on-premises and cloud deployments, delivering a seamless turnkey solution that enables just-in-time desktops and apps with Instant Clones, App Volumes, and Dynamic Environment Manager. IT can ultimately eliminate the need to build, test and support disparate storage, virtualization and networking products. To provide the best digital workspace experience for employees, Horizon virtual desktops and apps can be securely accessed directly from Workspace ONE through the Workspace ONE Intelligent Hub.

The best digital workspace experience

By providing access to Horizon virtual desktops and apps through Workspace ONE, IT can further extend the best digital workspace experience to all apps and use cases. Horizon features include single sign-on, session collaboration, and support for hundreds of peripherals. Personalized desktops deliver optimal performance and an immersive, feature-rich user experience across devices, locations, media and network connections. Remote and mobile workers enjoy workstation-class performance and rich 2D and 3D graphics with the Blast Extreme protocol, which offers dynamic optimization in non-ideal, high-latency, low-bandwidth network conditions.

Find out more

For more information, visit vmware.com/go/horizon.

For information or to purchase VMware products, call 877-4-VMWARE, visit vmware.com, or search online for an authorized reseller. For detailed specifications and requirements, refer to the product documentation.

Our relentless pursuit of the best digital workspace experience is enabled by our enterprise-grade management capabilities and technology ecosystem with user-centric performance metrics and monitoring, advanced load balancing, and SD-WAN optimization that extend from on-premises to the hybrid and multi-cloud.

Make the move today

VMware Horizon is available as a subscription SaaS or Term offering.

A Horizon subscription provides a single, flexible entitlement to all Horizon technology, services and deployment options: on-premises, in the cloud, or hybrid and multi-clouds. You can choose from these SaaS licenses:

- **Horizon Universal** – Premium desktop and app delivery with a full suite of cloud management services for multi-cloud deployments
- **Horizon Enterprise Plus** – Advanced desktop and app delivery with select cloud management services for a single cloud deployment
- **Horizon Standard Plus** – Premium desktop and app delivery with a full suite of cloud management services for multi-cloud deployments
- **Horizon Apps Universal** – Powerful app delivery with a full suite of cloud management services for hybrid cloud deployment
- **Horizon Apps Standard** – Simple app delivery with basic cloud management services for on-premises or cloud deployment

If you prefer a Term license:

- **Horizon Enterprise Term** – Desktops and applications delivered with closed-loop management and automation
- **Horizon Advanced Term** – Cost-effective delivery of virtual desktops and applications through a unified workspace
- **Horizon Standard Term** – Simple, powerful virtual desktop infrastructure with a great user experience
- **Horizon Apps Advanced Term** – Powerful application virtualization with closed-loop management and automation. Horizon is also available as part of select Workspace ONE editions.
- **Horizon Apps Standard Term** – Simple, powerful application virtualization with a great user experience

Horizon is also available as part of select Workspace ONE editions.

For information on bundle features, see the [feature comparison matrix for Horizon subscription licenses](#) and [Horizon term licenses](#).

Anhang F5

Benutzeranleitung Anmeldung VDI

Änderungsverzeichnis

Datum	Version	Änderung	Autor
19.05.2024	1.0	Dokument erstellt, bearbeitet und fertiggestellt	Shipinyuan Su, Sirak Yosef

Anmeldung über VPN

Um sich in die VDI-Umgebung anmelden zu können, muss zuerst das VPN gestartet werden, damit das Notebook eine Verbindung zum Firmennetzwerk herstellen kann. Dafür wird die Cato-Applikation verwendet, die bereits auf dem Firmennotebook vorinstalliert ist.

Verbindung zum Internet herstellen:

- Stellen Sie sicher, dass Ihr Notebook mit dem WLAN oder über ein Kabel mit dem Internet verbunden ist

VPN-Verbindung herstellen:

- Starten Sie die Cato-App auf Ihrem Notebook
- Melden Sie sich mit Ihrem Benutzernamen und Passwort an
- Geben Sie den MFA-Code (Multi-Factor Authentication) aus Ihrer Authenticator-App ein
- Nach der Eingabe des MFA-Codes startet die VPN-Verbindung automatisch

Hinweis: Beim ersten Anmelden müssen Sie das MFA auf Ihrem Smartphone einrichten. Dafür erhalten Sie eine E-Mail vom IT-Support.

Die MFA-Abfrage sieht dann wie folgt aus.

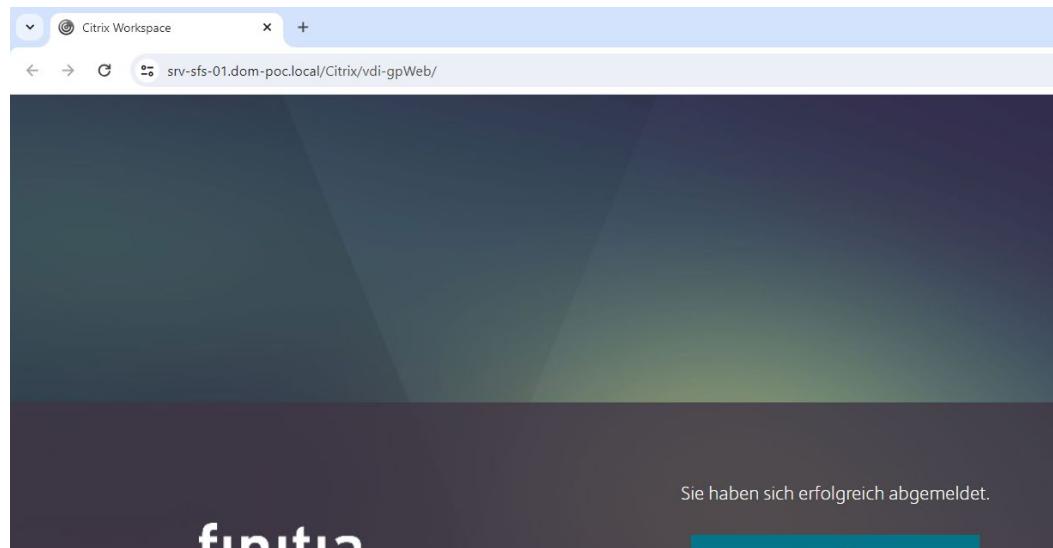
The screenshot shows a web-based MFA authentication interface. At the top, the Cato Networks logo is displayed with the tagline "Join The Network". Below the logo, the text "MFA Authentication" is shown in blue. A large input field is labeled "Enter verification code". At the bottom of the input field is a green "Continue" button. At the very bottom of the page, there is a link that says "Open the [User Portal](#) to set up MFA".

Anmeldung in die Virtuelle Umgebung

Dieser Abschnitt erklärt, wie man sich auf seine eigene VDI-Umgebung anmeldet und die VDI-Maschine startet. Voraussetzung dafür ist, dass die VPN-Verbindung hergestellt werden konnte.

Anmeldeseite öffnen:

Geben Sie folgende URL in Ihren Webbrowser ein, um auf die Anmeldeseite von Citrix zu gelangen:
<https://srv-sfs-01.dom-poc.local/Citrix/vdi-gpWeb/> oder vdi.dom-poc.local



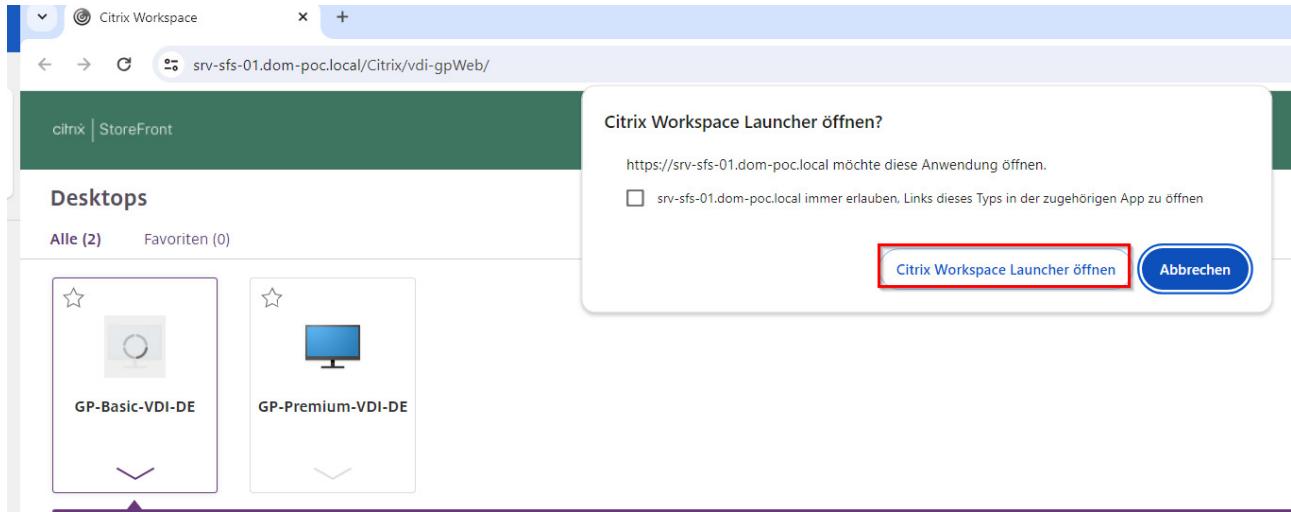
Anmelden:

- Melden Sie sich mit den Zugangsdaten an, die Sie von der IT erhalten haben

A screenshot of a Citrix login form. The form has three input fields: "Benutzername" with the value "gp-syo", "Kennwort" with a redacted value, and "Domäne" with the value "dom-poc.local". Below these fields is a large teal "Anmelden" button. At the bottom of the form, there is a link in blue text that reads "Verwenden Sie eine andere Anmeldeoption". The background of the form is dark.

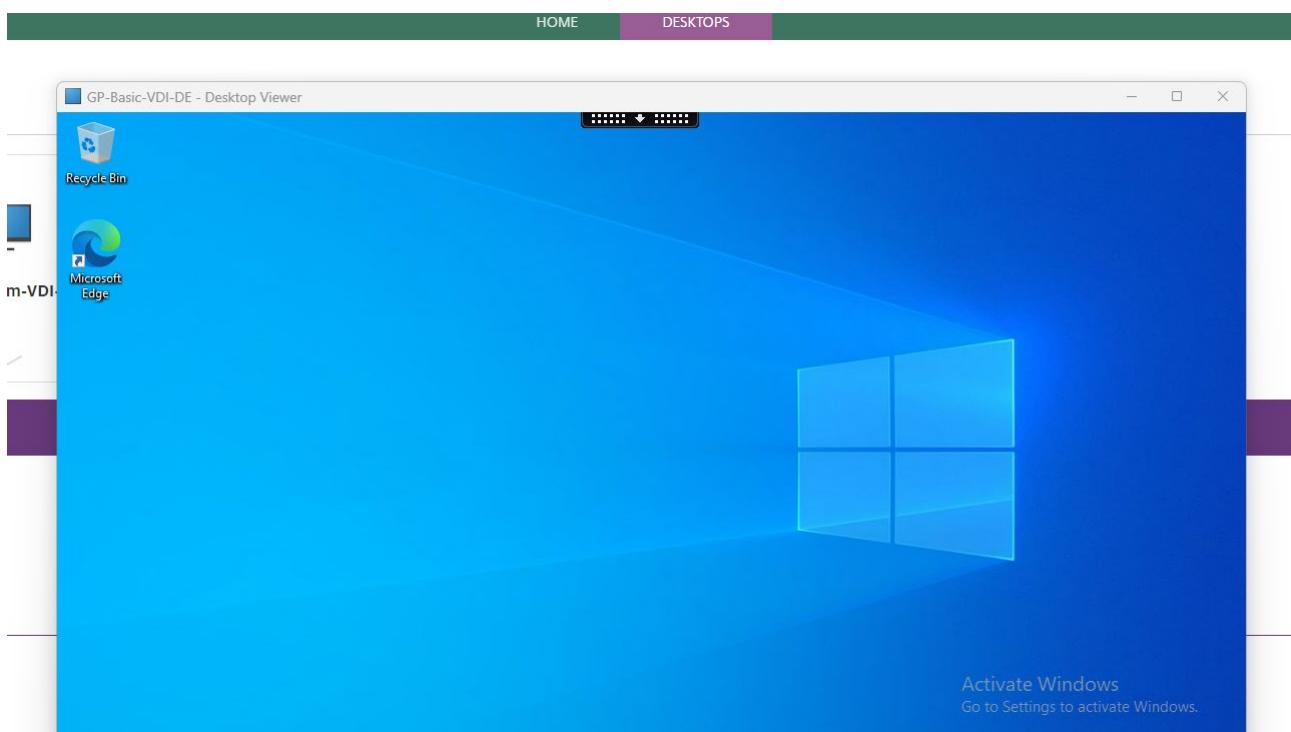
Desktop auswählen und starten:

- Klicken Sie oben auf "Desktop"
- Wählen Sie Ihren eigenen Desktop aus, indem Sie darauf doppelklicken.
- Klicken Sie auf "Citrix Workspace Launcher öffnen".



VDI-Umgebung nutzen:

- Ihr Desktop startet automatisch und Sie befinden sich nun in Ihrer eigenen VDI-Umgebung



Anhang G1



Protokoll Kickoff-Meeting

VDI as a Service

Datum	21.02.2024
Ort	Teams-Online
Autoren	Shipinyuan Su, Sirak Yosef
Sitzungsleiter	Shipinyuan Su, Sirak Yosef
Protokollführer	Shipinyuan Su, Sirak Yosef
Klassifizierung	Intern
Version	1.0
Anwesend	Shipinyuan Su Sirak Yosef Thomas Staub Tenzin Langdun

1 Inhaltsverzeichnis

1	Inhaltsverzeichnis	2
2	Diskussion & Fragen.....	3
3	Administrative Themen	3
3.1	Statusbericht	3
3.2	Zwischenmeeting und Abschlussmeeting	3
3.3	Nächste Schritte	3
4	Technische Themen	3
4.1	Projektauftrag	3
4.2	Lösungsvarianten.....	3

2 Diskussion & Fragen

Im Rahmen des Kickoff-Meetings wurde die Projektidee VDI as a Service vorgestellt. Dabei lag der Fokus auf der Darstellung des Services, der Use Cases und welche Probleme es im Unternehmen löst. Zudem erhielten wir administrative und technische Inputs von den Experten und konnten die Gelegenheit auch nutzen, um offene Fragen zu fragen und zu beantworten.

3 Administrative Themen

3.1 Statusbericht

Es wurde beschlossen, dass in einem Zwei-Wochen-Rhythmus ein Status-Update per E-Mail an die Experten versendet wird, um sie kontinuierlich über den Fortschritt der Diplomarbeit zu informieren.

3.2 Zwischenmeeting und Abschlussmeeting

Für die weiteren Projektphasen wurden zwei wichtige Termine festgelegt: Das Zwischenmeeting ist für den 12.03.2024 um 18:00 Uhr geplant und findet online über Microsoft Teams statt. Das Abschlussmeeting ist für den 04.06.2024 um 9:00 Uhr geplant und wird in Bern vor Ort durchgeführt. Detaillierte Informationen und Einladungen zu den Terminen werden den Experten rechtzeitig per E-Mail zugestellt.

3.3 Nächste Schritte

Als nächste Schritte sind die Fertigstellung der Studie und des Projektauftrags vorgesehen. Diese Unterlagen müssen spätestens zwei Tage vor dem Zwischenmeeting abgeschlossen sein und per Mail an die Experten verschickt werden, damit sie eine angemessene Vorbereitungszeit auf das Meeting haben.

4 Technische Themen

4.1 Projektauftrag

Im Projektauftrag werden basierend auf User Stories sowohl funktionale als auch nicht-funktionale Anforderungen aus Kundenperspektive definiert. Dies dient dazu, im späteren Projektverlauf die Erfüllung dieser Anforderungen überprüfen zu können.

4.2 Lösungsvarianten

In der Studie werden verschiedene Lösungsansätze wie VMWare, Citrix oder MS Azure VDI für den Service untersucht. Besonders die kürzlich erfolgte Übernahme von VMWare durch Broadcom soll dabei, als relevantes Thema behandelt werden.



Protokoll Zwischenmeeting

VDI as a Service

Datum	26.03.2024
Ort	Teams-Online
Autoren	Shipinyuan Su, Sirak Yosef
Sitzungsleiter	Shipinyuan Su, Sirak Yosef
Protokollführer	Shipinyuan Su, Sirak Yosef
Klassifizierung	Intern
Version	1.0
Anwesend	Shipinyuan Su Sirak Yosef Thomas Staub Tenzin Langdun

1 Inhaltsverzeichnis

1	Inhaltsverzeichnis	2
2	Besprechung Studie und Projektauftrag	3
3	Weiteres Vorgehen	3
4	Zusammenfassung	3

2 Besprechung Studie und Projektauftrag

Im Zwischenmeeting wurden die beiden Lieferobjekte, die Studie und der Projektauftrag, eingehend besprochen. Die Experten hatten mehrere Fragen zur Sicherheit und zur Nutzwertanalyse, die geklärt wurden. Durch die detaillierte Besprechung und die vorgelegte Studie erhielten die Experten ein klareres Bild der gesamten Diplomarbeit. Auch von unserer Seite gab es Fragen zu den Abgaben, die von den Experten beantwortet werden konnten.

3 Weiteres Vorgehen

Als nächstes wird mit der Konzeptionierung begonnen. Da das nächste Meeting das Abschlussmeeting am 4. Juni sein wird, wurde die Abgabe der Statusberichte genauer definiert. Diese werden nun an jedem zweiten Mittwoch an die Experten versendet.

4 Zusammenfassung

Zum Abschluss des Meetings wurden die wichtigsten Punkte noch einmal zusammengefasst:

- Die Studie und der Projektauftrag wurden erfolgreich besprochen und offene Fragen geklärt.
- Die nächsten Schritte beinhalten die Konzeptionierung und die regelmässige Abgabe von Statusberichten.

Anhang G2



Präsentationen

VDI as a Service

Auftraggeber	Micha Bucher
Projektleiter	Shipinyuan Su, Sirak Yosef
Autor	Shipinyuan Su, Sirak Yosef
Klassifizierung	Intern
Status	Abgeschlossen

Inhaltsverzeichnis

1	Projektantrag	3
2	Kickoff Meeting	9
3	Zwischen-Meeting	15

1 Projektantrag

finitia.

Projektantrag

VaaS – VDI as a Service

Shipinyuan Su / Sirak Yosef

Agenda

Ausgangslage

IST / SOLL

Ziele

Lieferobjekte

Projektabgrenzung

Unser konzeptioneller Beitrag

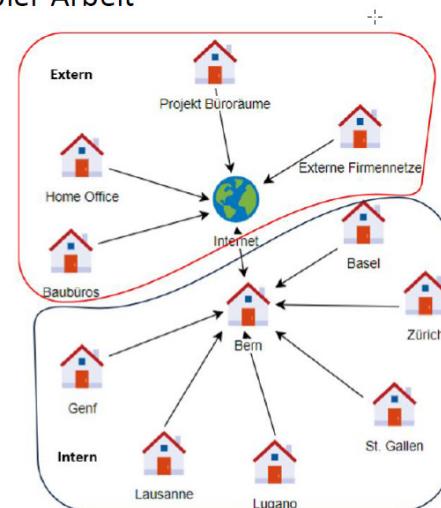
Überschneidung mit den Schulfächern



Ausgangslage

Die aktuelle Lage

- Zunahme von Homeoffice und flexibler Arbeit
- Standortunabhängigkeit
- Erhaltung der Arbeitsperformance
- Digitale Transformation



IST / SOLL

Probleme und Bedürfnisse

IST - Probleme

- Die Covid-Pandemie hat die Anpassung der Arbeitsgewohnheit beschleunigt
- Geografische Verteilung der Kunden
- Die Herausforderung die Arbeitsqualität und –effizienz trotz Flexibilität und Standortunabhängigkeit aufrechtzuerhalten
- Arbeitsmethoden und IT-Infrastruktur überdenken, um Effizienz zu steigern und konkurrenzfähig zu bleiben

IST / SOLL

Probleme und Bedürfnisse

SOLL - Bedürfnisse

- Effiziente und Qualitative Leistung Standortunabhängig
- Zugriff auf leistungsfähige Werkzeuge und Ressourcen
- Technische Ausstattung, sowie Schulungen für die Nutzung digitaler Kommunikationstools
- Die kontinuierliche Verfügbarkeit des Systems muss gewährleistet sein
- Investition in die Digitalisierung von Arbeitsprozessen und IT-Infrastruktur

Ziele

Mit unserer Lösung wollen wir erreichen

- Verbesserung der Work-Life-Balance
- Steigerung der Produktivität
- Erhöhung der Mitarbeiterzufriedenheit
- Mögliche Skalierbarkeit
- Sicherstellung der Geschäftskontinuität
- Schulung neuer Technologie
- Förderung der digitalen Transformation

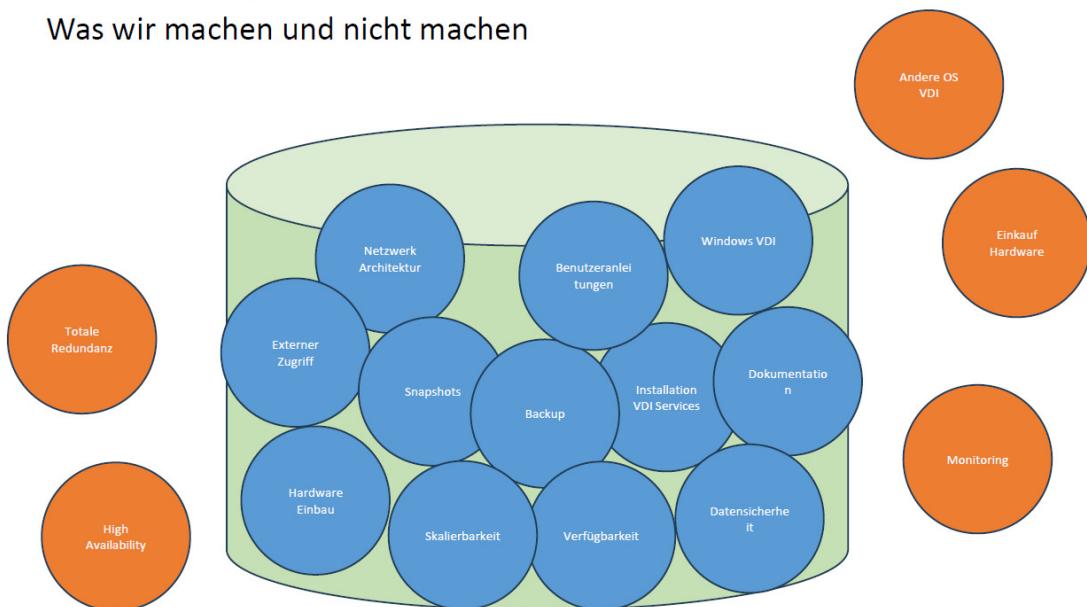
Lieferobjekte

Unsere Lieferobjekte sind

Phase	Lieferobjekte
Initialisierung	<ul style="list-style-type: none"> • Projektplan • Projektauftrag • Präsentation für Kick-off-Meeting • Studie
Konzept	<ul style="list-style-type: none"> • Detailkonzept • Betriebskonzept • Migrationskonzept • Testkonzept • Präsentation mit den wichtigsten Phasenergebnissen

Projektabgrenzung

Was wir machen und nicht machen



Unser konzeptioneller Beitrag

Unsere konzeptionellen Beiträge umfassen folgende Punkte

Gestaltung der Architektur

- Entwicklung einer kosteneffizienten und nachhaltigen VDI-Architektur

Skalierungsstrategie

- Entwurf einer Architektur, die eine schnelle Skalierung der VDI-Ressourcen ermöglicht
- Individuell angepasste Ressourcenzuweisung, gemäss Nachfrage

Verfügbarkeit und Laststrategie

- Gewährleistung einer hohen Verfügbarkeit der VDI-Lösung, um kontinuierlichen und unterbrechungsfreien Zugriff sicherzustellen

Datensicherung

- Sicherstellung der Datenverfügbarkeit durch effektive und zuverlässige Datensicherungsstrategien

Überschneidung mit den Schulfächern

Diese Schulfächer werden für diese Arbeit verwendet

Modul	Angewendetes Wissen
PMM – Project Management Methodology	<ul style="list-style-type: none">• Hermes• Diplombericht• Konzepte
DTR – Digitale Transformation	<ul style="list-style-type: none">• Change-Management• Analysierung der Veränderung der Digitalisierung
ISM – IT Service Management	<ul style="list-style-type: none">• SLA• Break Even Berechnung

Überschneidung mit den Schulfächern

Diese Schulfächer werden für diese Arbeit verwendet

Modul	Angewendetes Wissen
LDS - Leadership	<ul style="list-style-type: none">• Auftrittskompetenz• Zeitmanagement
NB 1&2 – Network Basics	<ul style="list-style-type: none">• Netzwerkaufbau• Netzwerkkonzept• Access Control Lists• Loadbalancer
SA 1&2 – System Administration	<ul style="list-style-type: none">• Server Orchestrieren

finitia.**Ende**

2 Kickoff Meeting

finitia.

Kickoff Meeting

VaaS – VDI as a Service

Shipinyuan Su / Sirak Yosef



finitia.

Agenda

Ausgangslage

Projektziele

Projektorganisation

Projektablauf

Projektbegrenzung

Lieferobjekte

Nächste Schritte

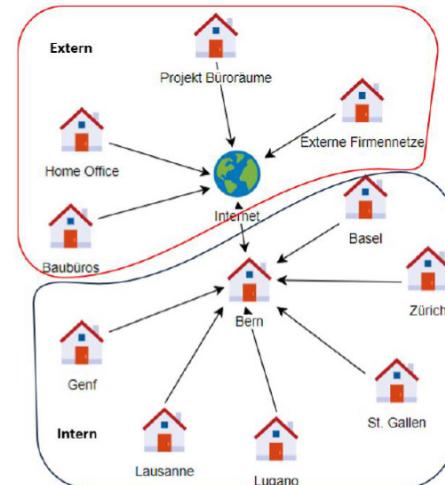
Diskussion/Fragen



Ausgangslage

Die aktuelle Lage

- Zunahme von Homeoffice und flexibler Arbeit
- Standortunabhängigkeit
- Erhaltung der Arbeitsperformance
- Digitale Transformation



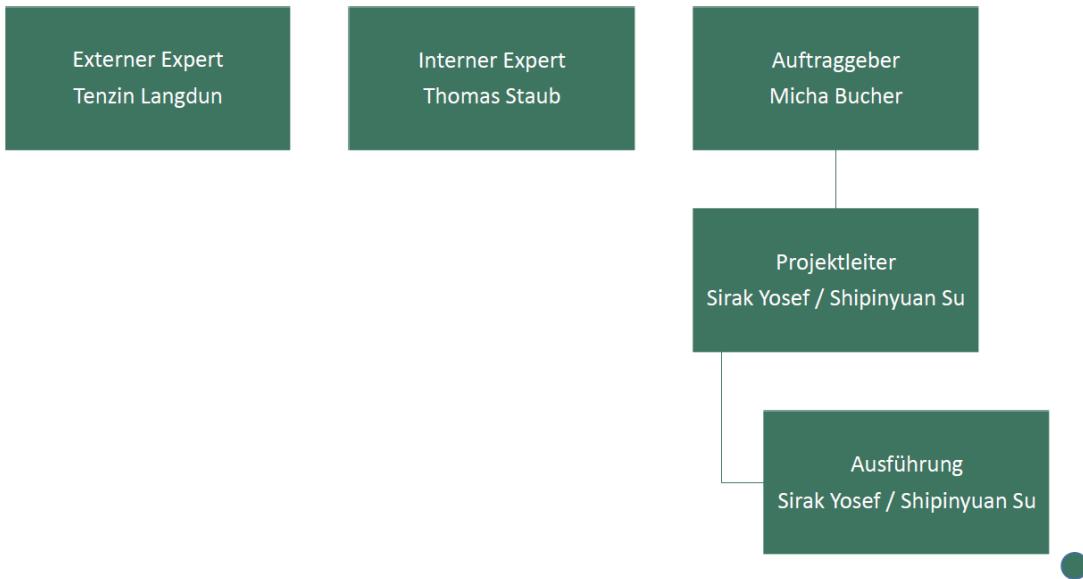
Projektziele

Mit unserer Lösung wollen wir erreichen

- Steigerung der Produktivität und Flexibilität
- Erhöhung der Mitarbeiterzufriedenheit
- Mögliche und schnelle Skalierbarkeit
- Sicherstellung der Geschäftskontinuität
- Schulung neuer Technologie
- Förderung der digitalen Transformation
- Plattformübergreifende Kompatibilität ermöglichen

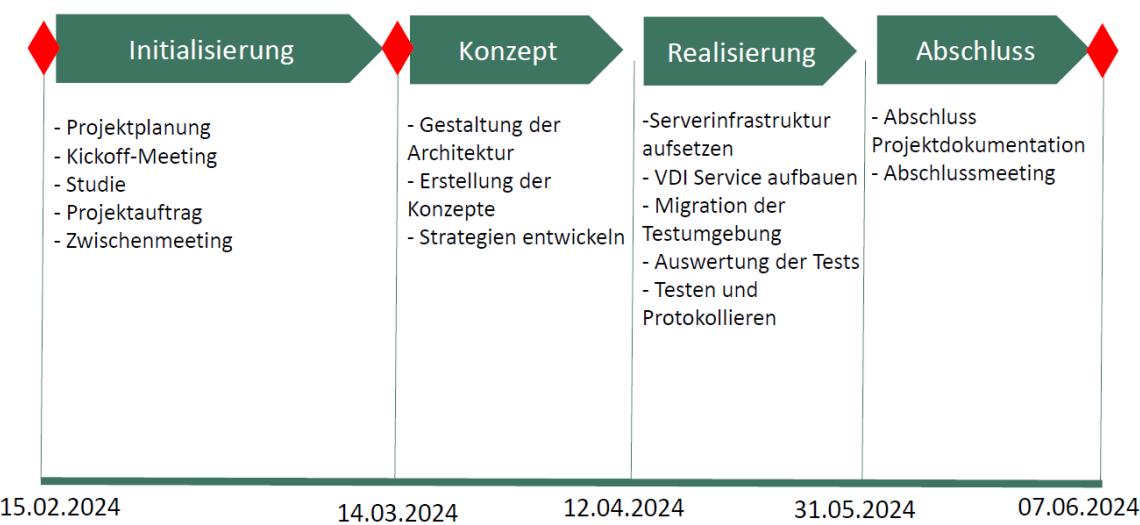
Projektorganisation

Aufbau unserer Projektorganisation



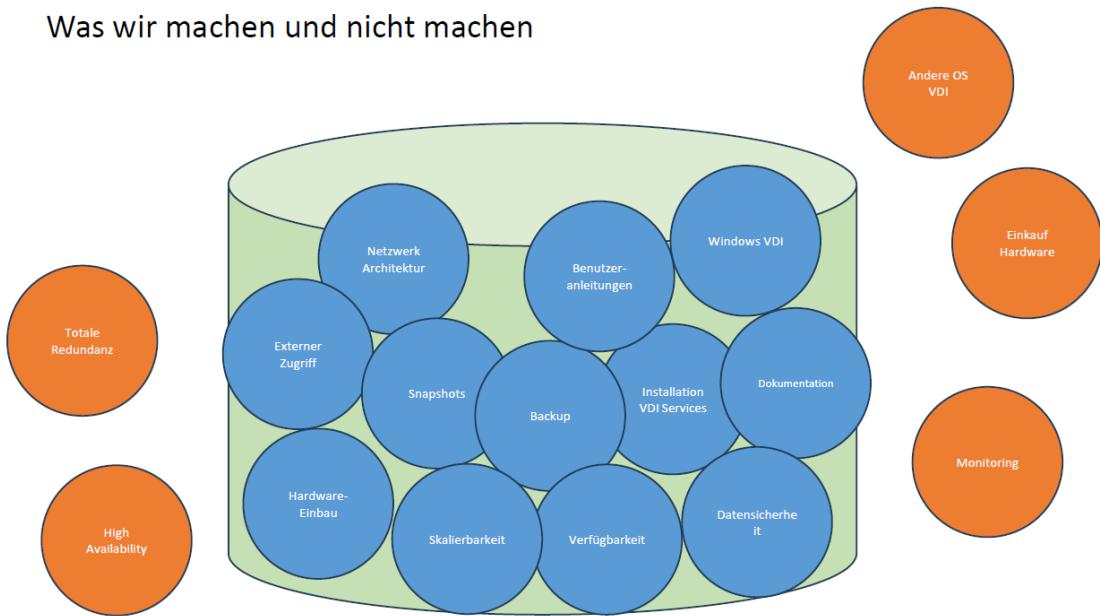
Projektablauf

Ablauf mit den wichtigsten Punkten



Projektabgrenzung

Was wir machen und nicht machen



Lieferobjekte

Unsere Lieferobjekte sind

Phase	Lieferobjekte
Initialisierung	<ul style="list-style-type: none">• Projektplan• Präsentation für Kick-off-Meeting• Projektinitialisierungsauftrag• Studie• Projektauftrag• Zwischenmeeting
Konzept	<ul style="list-style-type: none">• Detailkonzept• Testkonzept• Migrationskonzept• Betriebskonzept

Lieferobjekte

Unsere Lieferobjekte sind

Phase	Lieferobjekte
Realisierung & Einführung	<ul style="list-style-type: none">• Testbericht• Arbeitsprotokoll• Schriftliche Auswertung vom Feedback der Pilotbenutzer• Benutzeranleitung• Abnahmeprotokoll
Abschluss	<ul style="list-style-type: none">• Abschlussbericht• Präsentation

Nächste Schritte

- Erstellung der Studie
- Erstellung des Projektauftrags
- Zwischenmeeting 11-14.03.2024



Diskussion/Fragen



finitia.

Ende



3 Zwischen-Meeting

finitia.

Zwischen-Meeting

VaaS – VDI as a Service

Shipinyuan Su / Sirak Yosef



finitia.

Agenda

Ausgangslage

User Stories

Anforderungen

Lösungsvarianten

Bewertung

Empfehlung

Nächste Schritte

Diskussion/Fragen



Ausgangslage

Die aktuelle Lage

- Mit Auftragsgeber die Situation und Möglichkeiten besprochen
- Gemeinsame Anforderungen/User Stories definiert
- Zeitliche Verzögerungen
 - Abklärungen
 - Projektstart beruflich
 - Schulische Projekte
- Nach der umfassenden Studie, fühlen wir uns nun bereit mit der Konzeptphase zu starten



User Stories

Sicht der verschiedenen Rollen



User Stories

Sicht der verschiedenen Rollen

Als...	Möchte ich...	Sodass...
Projektmitarbeiter	Von mehreren Standorten aus arbeiten können	Ich auch beim Kunden vor Ort effektiv sein kann
Projektmitarbeiter	Trotz der Flexibilität über eine Leistungsfähige Umgebung verfügen	Ich weiterhin produktiv und effizient arbeiten kann
Projektmitarbeiter	Mit meinem Projektteam in Echtzeit kollaborieren können	Die Effizienz unserer Arbeit nicht beeinträchtigt wird
Auftraggeber	Den Service auf monatlicher Basis abrechnen können	Wir eine neue Einkommensquelle haben und den Abrechnungsprozess vereinfachen können
IT-Supporter	Anpassungen an der Umgebung möglichst einfach und ohne Wartungsarbeiten durchführen können	Die Kundenzufriedenheit hoch bleibt

Anforderungen

Funktionale und nicht-funktionale

Anforderungen

Funktionale

Nr.	Anforderungen	Kategorie
1	Die Kunden können sich von jedem Ort aus sicher auf ihre VDI verbinden	M
2	VDI verfügt über keinen direkten Internetzugang	M
3	Das Backup erfolgt automatisch ohne manuellen Eingriff	M
4	Eine aktive Verbindung kann in einem Notfall sofort unterbrochen und blockiert werden	M
5	Der IT-Supporter kann die Leistung (Kerne, RAM, VRAM) der VDI anpassen	S
6	IT-Support kann Änderungen am VDI-Image vornehmen, ohne den laufenden Betrieb zu stören	S
7	Sicherheitsfunktionen, wie das Blockieren von Screenshots und Videoaufnahmen der VDI, werden implementiert	K
8	Das Benutzerendgerät muss in der Lage sein bis zu mindestens vier Sicherheitsfunktionen, wie z.B. sicheres Passwort, Bitlocker, USB Authentifizierung Schlüssel, Deep Freeze ähnliche Produkte zu unterstützen	X
Kategorie: M = Muss, S = Soll, K = Kann, X = wird nicht realisiert		

Anforderungen

Nicht-funktionale

Nr.	Anforderungen	Beschreibung	Messkriterium	Verifizierung
1	Benutzerfreundlichkeit	Die Arbeitsprozesse sind leichtverständlich. Die Oberfläche ist einfach und intuitiv zu bedienen.	Mehr als 80% der Nutzer geben positives Feedback zur Benutzerfreundlichkeit	Direktes Feedback vom Kunden
2	Skalierbarkeit	Das System kann bei steigender oder sinkender Nutzeranzahl effizient Ressourcen zuweisen oder einsparen. Anpassung der Leistung einzelner VDIs möglich	Das System unterstützt ohne Leistungseinbussen die maximale berechnete Anzahl gleichzeitiger Nutzer	Lasttests und Lastmonitoring
3	Verfügbarkeit	Das System ist rund um die Uhr verfügbar und kann Ausfälle einzelner Komponenten überstehen	Die Verfügbarkeit des Systems liegt bei 99% über den Monat	Monitoring der Verfügbarkeit
4	Support	Kunden haben während der Geschäftszeiten Zugang zum Support und können Änderungen anfragen	Antwortzeit gemäss Qualität Management Service (QMS)	Rapport des Ticketing

Lösungsvarianten

Übersicht

- VMware Horizon
- Citrix Virtual Apps und Desktop
- Microsoft Azure Virtual Desktop

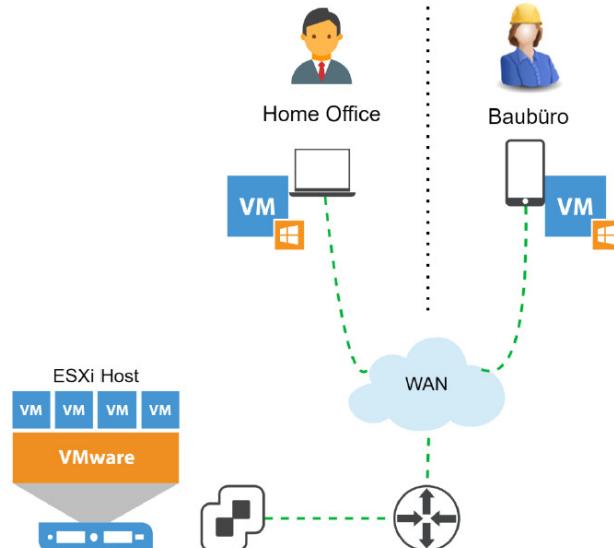


vmware®

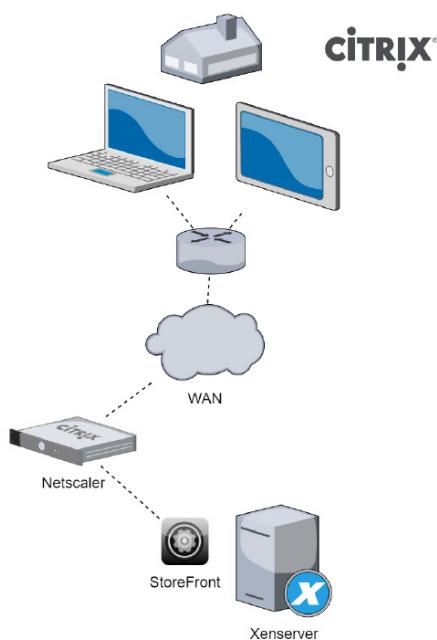


CITRIX

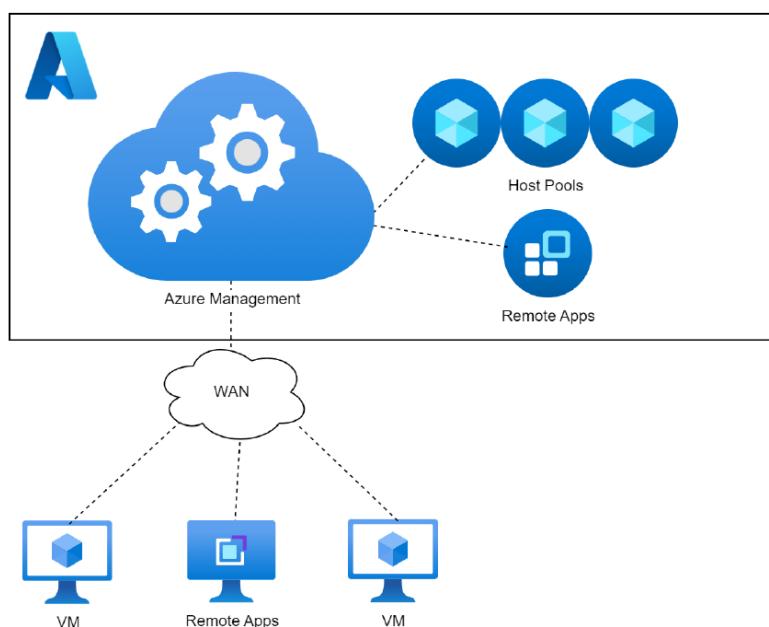
VMware Horizon



Citrix DaaS



MS Azure Virtual Desktop



Bewertung

Abdeckung der Anforderungen

- Grundsätzlich können alle Lösungen alle Anforderungen erfüllen
- Bedingungen
 - Azure müsste als Hybrid Lösung verwendet werden
 - Verwendung von weiteren Tools => Profil Speichern, Monitoring
 - Azure Authentifizierung => neuer Tenant

Bewertung

Diese Analyse zeigt

	Kosten	Anforderungen	Komplexität	Kompatibilität	Benutzerfreundlichkeit	Leistung	Skalierbarkeit	Nachhaltigkeit	Sicherheit	Support und Wartung	Punkte	Gewichtung berechnet	Gewichtung für NWA
Kosten		1	1	2	1.5	1	1	2	1	1	11.5	13	15
Anforderungen	1		2	1.5	1.5	1	1	2	1	1	12	13	15
Komplexität	1	0		1	1	0.5	0.5	1.5	0.5	1	7	8	10
Kompatibilität	0	0.5	1		1	1	1	2	1	1	8.5	9	10
Benutzerfreundlichkeit	0.5	0.5	1	1		0.5	0.5	1.5	0.5	0.5	6.5	7	5
Leistung	1	1	1.5	1	1.5		1	1.5	1	1	10.5	12	10
Skalierbarkeit	1	1	1.5	1	1.5	1		1.5	1	1	10.5	12	10
Nachhaltigkeit	0	0	0.5	0	0.5	0.5	0.5		0	0	2	2	5
Sicherheit	1	1	1.5	1	1.5	1	1	2		1	11	12	10
Support und Wartung	1	1	1	1	1.5	1	1	2	1		10.5	12	10



Bewertung

Diese Analyse zeigt

Kriterien	Erläuterung	Gewichtung (G)	VMware		Citrix		Azure	
			Note (W)	G*W	Note (W)	G*W	Note (W)	G*W
Kosten	günstig: 5 / teuer: 0	15	1	15	3	45	1	15
Anforderungen	alle: 5 / keine 0	15	5	75	5	75	5	75
Komplexität	einfach: 5 / komplex 0	10	2	20	2	20	3	30
Kompatibilität	kompatibel: 5 / nicht kompatibel 0	10	4	40	4	40	4	40
Benutzerfreundlichkeit	Intuitiv: 5 / Komplex 0	5	4	20	4	20	4	20
Leistung	Schnell: 5 / Langsam 0	10	4	40	5	50	4	40
Skalierbarkeit	Skalierbar: 5 / nicht skaliert 0	10	4	40	5	50	5	50
Nachhaltigkeit	Nachhaltig: 5 / nicht Nachhaltig 0	5	5	25	5	25	5	25
Sicherheit	Compliance: 5 / Sicherheitslücken 0	10	5	50	5	50	4	40
Support und Wartung	Innert 24h 5 / mehr als 72h 0	10	3	30	4	40	4	40
Total		100		355		415		375

Empfehlung

Unser Entscheid

- Gewinner der Nutzwertanalyse ist Citrix
- Ausschlaggebende Punkte
 - Kosten (indirekte Partnerschaft)
 - Leistung
 - Vorhandene Ansprechperson

Nächste Schritte

- Korrekturen der Initialisierung
- Erstellung des Konzeptes
- Durchführung Realisation
- Durchführung Einführung und Abnahme
- Abschlussmeeting 04.06.2024



Diskussion/Fragen



Anhang H

Logbuch / Statusbericht

Änderungsverzeichnis

Datum	Version	Änderung	Autor
08.02.2024	0.1	Dokument erstellt	Shipinyuan Su, Sirak Yosef
16.03.2024	0.2	Phase Initialisierung – fortlaufende Dokumentation	Shipinyuan Su, Sirak Yosef
23.03.2024	0.3	Phase Konzept – fortlaufende Dokumentation	Shipinyuan Su, Sirak Yosef
20.04.2024	0.4	Phase Realisierung – fortlaufende Dokumentation	Shipinyuan Su, Sirak Yosef
31.05.2024	1.0	Dokument fertiggestellt	Shipinyuan Su, Sirak Yosef

Datum	Tätigkeit	Wer	Zeit / h	Bemerkung
Initialisierungsphase				
11.12.2023	Erstellung des Projektinitialisierungsauftrags	SSU, SYO	16	Die Idee dokumentieren für die Diplomfreigabe
16.12.2023	Erstellung der Präsentation für das Kick-Off Meeting	SSU, SYO	16	Abgabe für die Diplomfreigabe, sowie für das Kick-Off-Meeting
09.02.2024	Anpassung der Projektziele	SSU, SYO	8	Diplomfreigabe erhalten, Rahmenbedingungen der Kommission einbeziehen
16.02.2024	Vorbereitung des Kick-Off-Meetings	SSU, SYO	8	
21.02.2024	Kick-Off-Meeting	SSU, SYO	2	
25.02.2024	Start der Studie	SSU, SYO	16	
Statusbericht 06.03.2024				
<p>Status: Zurzeit sind wir noch voll dran an der Studie und den Projektauftrag. Es gab und gibt immer noch viele Abklärungen, die wir mit dem Auftraggeber definieren müssen.</p> <p>Abklärungen die noch offen sind:</p> <ul style="list-style-type: none"> - Welche Informationen dürfen wir rausgeben und welche nicht => Standortbeschreibung wie z.B. Inventarliste - Anforderungen definieren für unseren PoC Use-Case => Schwierigkeit erhält von Informationen - Laufende Lizenz Abklärungen, die in die Wirtschaftlichkeit einfließen werden 				
10.03.2024	Studie: Stärken, Schwächen Analyse, Pflichtenheft	SSU, SYO	4	Abklärungen mit dem Auftragsgeber für das Pflichtenheft
14.03.2024	Studie: Pflichtenheft	SSU	4	Fertigstellung des Pflichtenheft mit der Absegnung des Auftragsgebers
14.03.2024	Start des Projektauftrags	SYO	4	
17.03.2024	Studie: Variantenentscheid	SSU	4	Der komplette Variantenentscheid brauchte eine gewisse Zeit, da zwei Produkte neu waren und die Recherchen eher aufwändig war
17.03.2024	Projektauftrag: IST/SOLL Analyse	SYO	4	
22.03.2024	Studie: Anforderungsabdeckung	SSU	4	
22.03.2024	Projektauftrag: Projektziele und Lieferobjekte	SYO	3	

Datum	Tätigkeit	Wer	Zeit / h	Bemerkung
Initialisierungsphase				
23.03.2024 – 24.03.2024	Studie: Nutzwertanalyse, Variantenentscheid und Wirtschaftlichkeit	SSU	14	Durch das unterschätzen der Grösse der Studie haben wir eine Verzögerung des Zeitplans
24.03.2024	Projektauftrag: Vorgehen, Projektplan, Kosten	SYO	10	
Statusbericht 25.03.2024				
<p>Wir möchten euch hiermit auch ein kurzes Update zum aktuellen Stand unserer Diplomarbeit geben. Die Initialisierungsphase hat mehr Zeit in Anspruch genommen als ursprünglich geplant, was zu einigen Verschiebungen im Projektzeitplan geführt hat. Eigentlich war der Start der Konzeptphase bereits für die letzte Woche vorgesehen, jedoch können wir erst diese Woche effektiv damit beginnen.</p> <p>Trotz dieser Verzögerungen behalten wir den Überblick und sind zuversichtlich, den Rückstand aufzuholen zu können. Momentan würden wir den Status unseres Projekts aufgrund dieser Situation mit "Gelb" im Rahmen eines Ampelsystems kennzeichnen.</p> 				
26.03.2024	Vorbereitung des Zwischenmeetings	SSU, SYO	2	Erstellung der Präsentation und Vorbereitung
26.03.2024	Zwischenmeeting	SSU, SYO	2	Durchführung des Zwischenmeeting und somit auch der Abschluss der Initialisierungsphase und Übergang zur Konzeptphase

Datum	Tätigkeit	Wer	Zeit / h	Bemerkung
Konzeptphase				
Statusbericht 03.04.2024				
<p>Aktuell befinden wir uns in der Konzeptphase, in der wir sammeln und präzisieren, wie wir unsere Lösung umsetzen möchten. Zusätzlich stehen weitere Abklärungen mit dem Auftraggeber an.</p> <p>Entsprechend dem Zeitplan sind wir momentan eine Woche im Verzug. Um dies auszugleichen, haben wir beide für die kommenden zwei Wochen Ferien genommen, um uns voll und ganz auf die Diplomarbeit konzentrieren und die verlorene Zeit aufzuholen zu können.</p> <p>Den aktuellen Projektstatus würden wir, basierend auf dem Ampelsystem, zwischen Grün und Gelb setzen.</p> <p>Zur Information: Die Statusberichte werden alle zwei Wochen mittwochs per E-Mail an euch versendet. Der nächste Bericht ist demnach für den 17. April vorgesehen.</p> 				

Datum	Tätigkeit	Wer	Zeit / h	Bemerkung
Konzeptphase				
08.04.2024	Start des Detailkonzeptes	SSU	4	Nach einer Osterpause starten wir mit einer intensiven zweiwöchigen Diplomarbeitsphase
08.04.2024	Start des Testkonzepts	SYO	4	In dieser Woche haben wir auch mit dem Testkonzept angefangen parallel zum Detailkonzept
09.04.2024	Detailkonzept: System-übersicht	SSU	4	Es wurde schon angefangen Abklärungen zu machen mit den Dritt-partner, bezüglich des Netzwerks
09.04.2024	Testkonzept: Testziele, Testorganisation	SYO	2	
10.04.2024	Detailkonzept: System-übersicht	SSU	4	
10.04.2024	Testkonzept: Testablauf	SYO	2	
11.04.2024	Detailkonzept: Komponentenbeschreibung, Schnittstellen	SSU	4	
11.04.2024	Testkonzept: Pflichtenheft von Studie überprüft	SYO	4	
12.04.2024	Detailkonzept: Komponentenbeschreibung, Backupkonzept	SSU	4	
12.04.2024	Testkonzept: Testanforderungen geschrieben	SYO	4	
14.04.2024	Detailkonzept: Komponentenbeschreibung, Backupkonzept Start des Betriebskonzepts	SSU	8	
14.04.2024	Testkonzept: Testfälle anhand Anforderungen erstellt	SYO	8	
15.04.2024	Abgleich des Detailkonzept mit Auftraggeber Betriebskonzept Ports Abklärungen	SSU	4	Es werden schon einige Abklärungen erledigt für die Realisation wie VLAN-Regeln und Port Kontrolle
15.04.2024	Start des Migrationskonzept: Einleitung, Ziele und Migrationsobjekte	SYO	4	Parallel wurde mit dem Migrationskonzept begonnen.
16.04.2024	Betriebskonzept: Organisationsstruktur	SSU	4	Es wurde Ports definiert für die geplante VLANs, damit wir so früh wie

Datum	Tätigkeit	Wer	Zeit / h	Bemerkung
Konzeptphase				
	Meeting mit Drittpartner Abklärung der Switches			möglich mit der Realisation anfangen können
16.04.2024	Migrationskonzept: Migrationsverfahren	SYO	4	
17.04.2024	Betriebskonzept: Betriebsprozesse, Wirtschaftlichkeit	SSU	6	Es wurde angefangen mehr über die Wirtschaftlichkeit zu denken. Eine Break-Even Analyse wird erstellt
17.04.2024	Migrationskonzept: Risiken, Fertigstellung	SYO	6	
Statusbericht 17.04.2024				
<p>Wir nähern uns dem Ende der Konzeptphase, die voraussichtlich diese Woche abgeschlossen wird. Anschliessend beginnen wir mit der Realisierungsphase des Projekts. Aktuell sind wir immer noch eine Woche hinter dem Zeitplan, aber wir hatten in dieser Woche ein Meeting mit dem externen Netzwerkpartner von Finitia. Wir haben unsere Anforderungen besprochen und ihm den Auftrag erteilt, das Netzwerk gemäss unseren Wünschen zu konfigurieren. Dies umfasst das Einrichten der VLANs und der Netzwerkrichtlinien, was eine wichtige Voraussetzung dafür ist, dass wir später den Server aufbauen und konfigurieren können. Durch diese Vorbereitungen hoffen wir, während der Realisierungsphase Zeit zu sparen.</p> <p>Den Projektstatus würden wir dementsprechend wieder zwischen Grün und Gelb setzen.</p> 				
18.04.2024	Betriebskonzept: Betriebsprozesse, Wirtschaftlichkeit	SSU	8	
18.04.2024	Überarbeitung Testkonzept und Erstellung Factsheet	SYO	8	Fehler korrigiert und neue Testfälle hinzugefügt
19.04.2024	Betriebskonzept: Betriebsprozesse, Wirtschaftlichkeit	SSU	7	Backupkonzept und Betrieb gleichzeitig geschrieben
19.04.2024	Betriebskonzept: Betriebsprozesse	SYO	7	
20.04.2024	Betriebskonzept: SLA, Backup	SSU	8	
20.04.2024	Erstellung Testbericht	SYO	8	
Konzeptphase / Realisierungsphase				
21.04.2024	Fertigstellung Detailkonzept, Testkonzept & Betriebskonzept. Start Aufbereitung Infrastruktur	SSU, SYO	8	MGMT-Server wurde aufgebaut und konfiguriert

Datum	Tätigkeit	Wer	Zeit / h	Bemerkung
Konzeptphase				
25.04.2024	Grundinfrastruktur aufbereiten, Erweiterung / Korrektur Architektur Detailkonzept	SSU, SYO	4	Netzwerkconfiguration vom MGMT, Hauptspeicher, Backupspeicher wurden konfiguriert
26.04.2024	Grundinfrastruktur aufbereiten	SSU, SYO	8	Es gab Konfigurationsprobleme des Management Interfaces des MGMT-Servers
27.04.2024	Serverinfrastruktur aufbereiten, Kommunikationsgrafik Detailkonzept	SSU, SYO	8	Netzwerkbasis steht nun. Es wird angefangen Grundkonfigurationen zu machen, wie die Verbindung von den verschiedenen Komponenten
28.04.2024	Serverinfrastruktur aufbereiten, Start vom Führen eines Arbeitsberichtes	SSU, SYO	8	

Datum	Tätigkeit	Wer	Zeit / h	Bemerkung
Realisierungsphase				
Statusbericht 01.05.2024				
Wir befinden uns nun in der Realisierungsphase unseres Projekts. Das Netzwerk, die physischen Server und das Storage sind soweit eingerichtet, dass wir bereits die ersten VMs erstellen konnten. Aktuell sind wir dabei, die Domain Controller einzurichten. Bislang hatten wir keine Probleme, die uns blockiert haben und wir befinden uns auch im Zeitplan. Daher würden wir den Projektstatus auf Grün setzen.				
02.05.2024	Start Installation von Citrix Diensten	SSU	4	DDC, LIC, DB
02.05.2024	Einrichtung Domain Controller und Domäne	SYO	4	Start mit Einrichtung der Domäne und Fortführung des Arbeitsberichts
03.05.2024	Installation von Citrix Diensten	SSU	8	DDC, LIC, DB
03.05.2024	Erstellung Active Directory Struktur, Gruppen und Benutzer	SYO	8	Zusätzlich wurde die Grafik der AD-Struktur im Detailkonzept angepasst, da eine OU (VDI-Machines) gefehlt hat
05.05.2024	Installation von Citrix Diensten	SSU	8	DDC, LIC, DB
05.05.2024	Einrichtung DNS und DHCP-Dienste	SYO	8	Parallel wurde der Arbeitsbericht weitergeführt
09.05.2024	Installation von Citrix Diensten	SSU	8	StoreFront Einrichtung. Das Self-signed certificate hat viel Zeit in Anspruch genommen

Datum	Tätigkeit	Wer	Zeit / h	Bemerkung
Realisierungsphase				
09.05.2024	Einrichtung des zweiten Domain Controller und Replizierung	SYO	8	Bei den DCs hatten wir ein Problem mit der Zeitsynchronisierung. Die Synchronisierung konnten wir dann mit Powershell-Befehlen anstossen
10.05.2024	Konfiguration von Citrix Diensten	SSU, SYO	8	Konfiguration der Dienste bis zu Funktion vom Verbinden einer VDI
12.05.2024	Konfiguration von Citrix Diensten	SSU, SYO	8	Troubleshoot bis zur erfolgreichen Verbindung. War zeitaufwendig, bis die erste Verbindung geklappt hat

Statusbericht 15.05.2024

Wir nähern uns dem Abschluss der Realisierungsphase und hatten bisher keine grösseren Probleme. Es gibt jedoch noch einiges zu tun, wie das Testen nach der Implementierung und die Fertigstellung des Diplomberichts. Da das Abschlussmeeting am 04.06. vorgesehen ist und der Bericht ja vorher fertig sein muss.

Eine Frage an euch: Möchtet ihr den Diplombericht in Papierform erhalten oder reicht es, wenn wir ihn euch digital per Mail zuschicken?

Wenn ihr ihn in Papierform möchtet, benötigen wir eure Adressen, um ihn euch per Post schicken zu können.

Den Projektstatus würden wir zwischen grün und gelb einordnen.



16.05.2024	Konfiguration von WEM und FSLogix	SSU, SYO	8	WEM braucht Premium Lizenzen. Dies musste beim Experten angefragt werden. Durch Ferienabwesenheit des Experten gab es hier Verzögerung dieses Tasks
18.05.2024	Konfiguration von WEM und FSLogix	SSU, SYO	16	Arbeitsbericht fortführend nachtragen
19.05.2024	Backupeinrichten	SSU	8	Das Backupspeicher musste kurz nochmals mit einem Management IP versehen werden, da man noch etwas darauf installieren musste. So mit hat sich das ein wenig verschoben
19.05.2024	Vorbereitung Testbericht, Erstellung des Abnahmeprotokolls und Benutzeranleitung	SYO	8	
20.05.2024	Testbericht ausführen und Diplombericht zusammenfassen	SSU, SYO	8	Kurz vor Ende wird der Diplombericht mit den wichtigsten Informationen zusammengefasst und mit den weiteren Kapiteln ergänzt

Datum	Tätigkeit	Wer	Zeit / h	Bemerkung
Realisierungsphase				
21.05.2024	Testbericht ausführen und Diplombericht zusammenfassen	SSU, SYO	8	
22.05.2024	Testbericht ausführen und Diplombericht zusammenfassen	SSU, SYO	8	
23.05.2024	Diplombericht zusammengefasst	SSU, SYO	16	
24.05.2024	Diplombericht zusammengefasst	SSU, SYO	8	
25.05.2024	Diplombericht zusammengefasst	SSU, SYO	8	
26.05.2024	Diplombericht zusammengefasst	SSU; SYO	16	
27.05.2024	Korrektur der Diplomarbeit	SSU, SYO	8	Aktuellste Version der Diplomarbeit wurde an mehreren Bekannten versendet und für Feedback gefragt
28.05.2024	Korrektur der Diplomarbeit	SSU, SYO	8	
29.05.2024	Korrektur der Diplomarbeit	SSU, SYO	8	
Statusbericht 29.05.2024				
Dies ist der letzte Statusbericht unserer Diplomarbeit. Wir befinden uns nun in der Abschlussphase und nehmen die letzten Korrekturen vor. Ihr erhaltet den Diplombericht am Freitagabend per E-Mail zugeschickt, damit ihr bis nächsten Dienstag Zeit habt, ihn zu lesen. Da nicht mehr viel fehlt, setzen wir den Status auf Grün.				
Kurzer Reminder: Das Abschlussmeeting findet nächsten Dienstag um 9 Uhr bei der Finita AG, Nordring 4A, 3001 Bern statt.				
30.05.2024	Korrektur der Diplomarbeit	SSU, SYO	8	
31.05.2024	Zusammenführen der Dokumente und abschicken an Experten	SSU, SYO	8	
1-3.06.24	Erstellung und Vorbereitung des Abschluss-Meetings	SSU, SYO	16	
04.06.2024	Abschluss-Meeting	SSU, SYO	4	

Anhang I

Glossar

Abkürzung / Fachbegriff	Erklärung / Bedeutung
PoC	<p>Proof of Concept</p> <p>Nachweis der Machbarkeit einer Idee.</p>
VDI	<p>Virtual Desktop Infrastructure</p> <p>Technologie zur Bereitstellung von Desktop-Umgebungen über das Netzwerk.</p>
DDC	<p>Desktop Delivery Controller</p> <p>Tool zur Verwaltung und Steuerung von virtuellen Desktops.</p>
VLAN	<p>Virtual Local Area Network</p> <p>Eine Methode zur Segmentierung eines physischen Netzwerks in mehrere logischen Netzwerke, um die Netzwerksicherheit und -verwaltung zu verbessern.</p>
NFS	<p>Network File System</p> <p>Ein Protokoll, das es ermöglicht, Dateien über ein Netzwerk so zu verwenden, als ob sie auf einem lokalen Datenträger gespeichert wären.</p>
DC	<p>Domain Controller</p> <p>Verwaltet Sicherheitsanforderungen von Windows-Domänen.</p>
DHCP	<p>Dynamic Host Configuration Protocol</p> <p>Ein Netzwerkprotokoll, das IP-Adressen automatisch zuweist und Netzwerkkonfigurationsparameter an Geräte im Netzwerk verteilt.</p>
DNS	<p>Domain Name System</p> <p>Ein Netzwerkprotokoll, für die Namensauflösung von Namen in IP-Adressen oder umgekehrt.</p>
NTFS	<p>New Technology File System</p> <p>Ein Dateisystem von Microsoft, das auf Windows-Betriebssystemen verwendet wird, um Dateien zu speichern, zu organisieren und zu verwalten.</p>
Snapshot	Eine Momentaufnahme des aktuellen Zustands einer virtuellen Maschine oder eines Dateisystems, die zu einem späteren Zeitpunkt zur Wiederherstellung verwendet werden kann.

Abkürzung / Fachbegriff	Erklärung / Bedeutung
LDAP	<p>Lightweight Directory Access Protocol</p> <p>Ein Protokoll zur Abfrage und Modifikation von Verzeichniseinträgen, das häufig zur Authentifizierung und Verwaltung von Benutzerdaten in einem Netzwerk verwendet wird.</p>
Kerberos	<p>Ein Netzwerk-Authentifizierungsprotokoll, das sichere Benutzer- und Dienstauthentifizierung über unsichere Netzwerke ermöglicht.</p>
ISP	<p>Internet Service Provider</p> <p>Ein Unternehmen, das Kunden den Zugang zum Internet bereitstellt.</p>
CLI	<p>Command Line Interface</p> <p>Eine Benutzerschnittstelle, die es ermöglicht, mit einem Computer durch Eingabe von Textbefehlen zu interagieren.</p>
ICA	<p>Independent Computing Architecture</p> <p>Ein von Citrix entwickeltes Protokoll zur Bereitstellung von Anwendungen und Desktops von einem zentralen Server an entfernte Clients.</p>
HDX	<p>High Definition Experience</p> <p>Eine Technologie von Citrix, die eine verbesserte Benutzererfahrung durch Optimierung von Grafik, Audio, Video und allgemeiner Interaktivität in virtuellen Umgebungen bietet.</p>
TCP	<p>Transmission Control Protocol</p> <p>Ein grundlegendes Netzwerkprotokoll des Internets, das eine zuverlässige, geordnete und fehlerfreie Übertragung von Daten zwischen Anwendungen ermöglicht.</p>
UDP	<p>User Datagram Protocol</p> <p>Ein einfaches Netzwerkprotokoll, das eine schnelle, aber unzuverlässige Übertragung von Daten ohne Fehlerkorrektur ermöglicht.</p>
HA	<p>High Availability</p> <p>Eine Eigenschaft eines Systems, die sicherstellt, dass es kontinuierlich und ohne Unterbrechung betriebsbereit ist, oft durch Redundanz und Failover-Mechanismen erreicht.</p>
Active-Passive	<p>Eine Hochverfügbarkeitskonfiguration, bei der ein aktiver (primärer) Server alle Anfragen bedient, während ein passiver (sekundärer) Server nur bei Ausfall des aktiven Servers übernimmt.</p>

Abkürzung / Fachbegriff	Erklärung / Bedeutung
Active-Active	Eine Hochverfügbarkeitskonfiguration, bei der mehrere Server gleichzeitig aktiv sind und Lastverteilung durchführen, um die Verfügbarkeit und Leistung zu maximieren.
XenCenter	Tool für XenServer, das die Verwaltung von virtuellen Maschinen ermöglicht.
RDP	Remote Desktop Protocol Ein Protokoll, das den Zugriff auf Desktops von anderen Computern ermöglicht.
VPN	Virtual Private Network Verschlüsselte Verbindung übers Internet.
MFA	Mutli-Factor Authentication Eine Sicherheitsmassnahme, die mehrere Verifikationsmethoden erfordert.
NAS	Network Attached Storage Dateispeichersystem, das übers Netzwerk Zugriff bietet.
RAID	Redundant Array of Independent Disks Dateispeicher-Technologie, die mehrere physische Festplatten zu einer logischen Einheit kombiniert.
WAN	Wide Area Network Ein Weitverkehrsnetzwerk, das ein grosses geografisches Gebiet abdeckt.
Golden Image	Standardisierte Vorlage für virtuelle Maschinen.
FSLogix	Eine Software zur Optimierung und Verwaltung von Benutzerprofilen.
DEM	Dynamic Environment Manager Tool für die Verwaltung von Benutzereinstellungen oder Konfigurationsdaten.
RBAC	Role-Based Access Control Ein System für die Zuweisung von Zugriffsrechten basierend auf Benutzerrollen.
BitLocker	Verschlüsselungstool von Daten auf der Festplatte.

Abkürzung / Fachbegriff	Erklärung / Bedeutung
DER	Endpoint Detection and Response Tool für die Überwachung von Bedrohungen auf Endgeräten.
Citrix Workspace	Tool für den virtuellen Zugriff auf Citrix VDI Desktops oder Anwendungen.
SLA	Service Level Agreement Vertragliche Vereinbarung zu Qualität und Verfügbarkeit.
PRTG	Paessler Router Traffic Grapher Überwachungstool von IT-Infrastruktur.
Ticketing-Tool	System zur Verwaltung von Supportanfragen.
VRAM	Video Random Access Memory Speicher in Grafikkarten.
CAD	Computer-Aided Design Programme zur Erstellung von Designs.