KonsortSWD
NFDI4Society

13 | Working Paper

Remote-Desktop-Verarbeitung sensibler Forschungsdaten: Ein Referenzsystem

Neil Murray,
Kenny Pedrique

September 2025

konsortswd.de

nfdi

Remote-Desktop-Verarbeitung sensibler Forschungsdaten: Ein Referenzsystem

Neil Murray, nmurray@diw.de, SOEP am DIW Berlin

Kenny Pedrique, SOEP am DIW Berlin

September 2025

Abstract

Das RDCnet (Research Data Center Network) verfolgt das Ziel, ein nationales Netzwerk von gesicherten Datenzugangsstellen aufzubauen, indem gesicherte Arbeitsplätze verschiedener Forschungsdatenzentren miteinander vernetzt werden. Dieses Netzwerk wird durch den Einsatz von Remote-Desktop-Systemen realisiert: Die Nutzenden erhalten Zugang zu virtuellen Desktops, die nicht lokal, sondern ausschließlich auf den Servern der datengebenden Partei betrieben werden. Die Implementierung eines solchen Remote-Desktop-Systems ist mit erheblichem technischem Aufwand verbunden und kann für ein Forschungsdatenzentrum eine anspruchsvolle Herausforderung darstellen. Um diesen Prozess zu unterstützen, wird in diesem Arbeitspapier ein Referenzsystem auf Basis von Omnissa Horizon vorgestellt, das als Orientierung und Hilfestellung dienen kann. Im Fokus stehen dabei die zugrunde liegenden Metriken, die Systemarchitektur sowie die Kosten für die Implementierung eines solchen Systems.

Keywords: Forschungsdateninfrastruktur, Remote Access, Forschungsdatenzugang, Sensible Forschungsdaten

1. Konzept des RDCnet

Viele Datensätze, die in der Forschung in den Sozial-, Verhaltens-, Bildungs- und Wirtschaftswissenschaften genutzt werden, sind so sensibel, dass sie ausschließlich lokal an gesicherten Arbeitsplätzen analysiert werden dürfen- diese gesicherten Arbeitsplätze werden im Folgenden als „Gastwissenschaftsarbeitsplätze" (GWAP) bezeichnet. Das RDCnet schafft einen Rahmen, um die GWAP von teilnehmenden Forschungsdatenzentren miteinander zu vernetzen und so ein System sicherer Datenzugangsstellen aufzubauen.

Jedes teilnehmende FDZ stellt dabei einen GWAP in Form eines restriktiv konfigurierten Thin Clients[1] innerhalb eines geschützten Datensicherheitsraums bereit. Über diesen GWAP kann mittels Secure Remote Access auf virtuelle Desktops anderer FDZ zugegriffen werden. Wichtig ist hervorzuheben, dass die Verarbeitung der Forschungsdaten ausschließlich auf den Servern des datenhaltenden FDZ erfolgt, ein physischer Transfer der Daten findet zu keinem Zeitpunkt statt.

Durch die Vernetzung und den erleichterten Zugang können die Forschungsdatenzentren die Zahl der Datennutzenden erhöhen, während gleichzeitig die Reise- und Aufenthaltskosten für Forschende gesenkt werden. Die Kontrolle über den tatsächlichen Zugriff auf die Datensätze verbleibt jedoch bei den jeweiligen

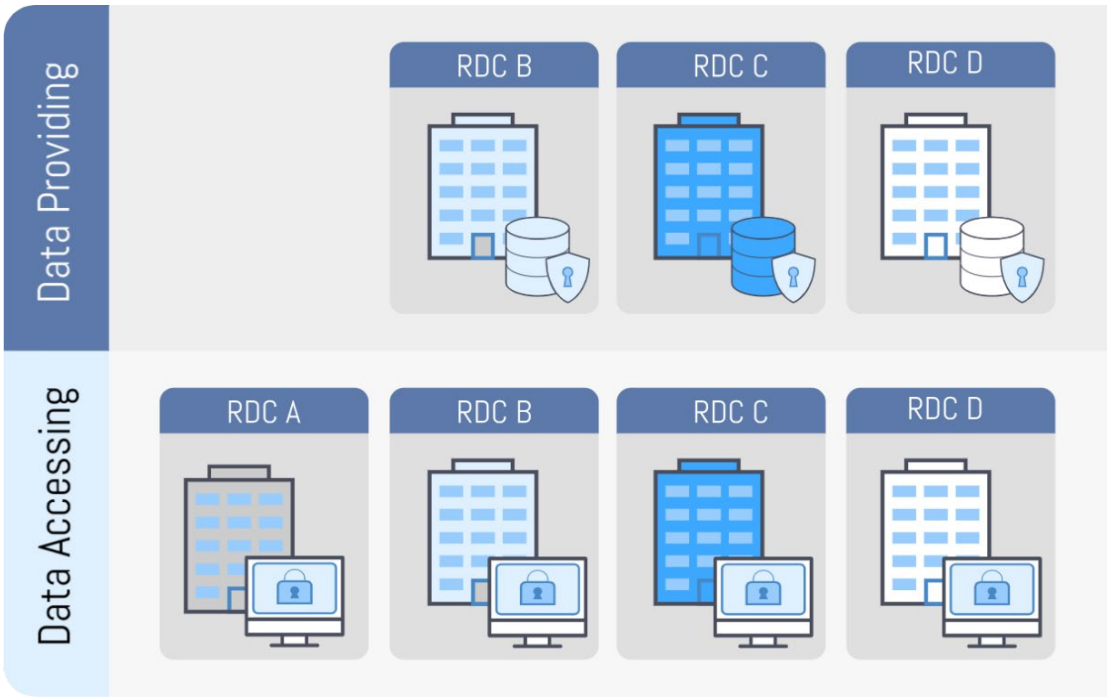


Abbildung 1: Jedes FDZ übernimmt im RDCnet mindestens die Rolle als datenempfangende Partei und optional die Rolle als datengebende Partei.

[1] Ein Thin Client ist ein Computer, der nur grundlegende Ein- und Ausgabefunktionen bereitstellt und alle wesentlichen Anwendungen und Daten von einem zentralen Server bezieht.

datenhaltenden FDZ. So wird sichergestellt, dass individuelle Datenschutz- und Sicherheitsstandards weiterhin eingehalten werden.

Neben vertraglichen Regelungen (Murray & Goebel, 2023) ist die Definition technischer Standards eine zentrale Voraussetzung für den Aufbau eines interoperablen, effizienten und vor allem skalierbaren Netzwerks. Die technische Umsetzung orientiert sich eng am Konzept des „FDZ-im-FDZ" (Bender & Heinig, 2011) und wird im Folgenden erörtert. Innerhalb des RDCnet kann jedes teilnehmende FDZ zwei Rollen einnehmen (siehe Abbildung 1):

- **Datenempfänger (GWAP-Partei):** Bereitstellung eines GWAP zur Nutzung durch Forschende, um auf Daten anderer FDZ sicher zugreifen zu können. Diese Rolle ist für alle Teilnehmenden verpflichtend.
- **Datengeber (Daten-Partei):** Optionale Bereitstellung eines Remote-Desktop-Systems, über die eigene Forschungsdaten für andere FDZ zugänglich gemacht und analysiert werden können.

Ein solches Netzwerk von sicheren Datenzugangsstellen kann durch den Einsatz von „Remote-Desktop-Systemen" realisiert werden. Dabei werden den Nutzenden virtuelle Desktops zur Verfügung gestellt, die jedoch nicht lokal an den GWAP, sondern auf den Servern der datengebenden FDZ gehostet werden. Konkret wird dabei ausschließlich das Bild des virtuellen Desktops von den Servern des datenbereitstellenden FDZ an den GWAP übertragen, an dem sich die Nutzenden befinden. Forschende können den virtuellen Desktop vom GWAP aus bedienen, dessen Inhalte einsehen und auf dieser

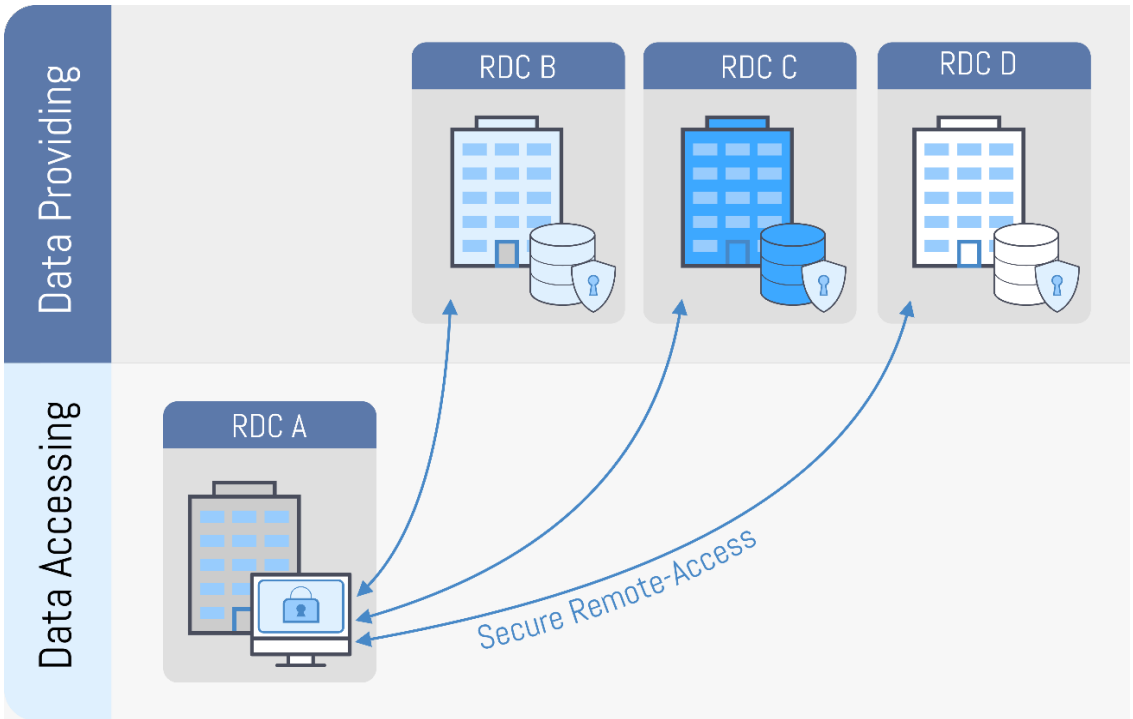


Abbildung 2: Beispiel- Secure Remote Access vom FDZ A zu allen teilnehmenden Datengebenden Parteien.

Basis ihre Analysen durchführen. Wichtig ist hervorzuheben, dass die Verarbeitung der Forschungsdaten ausschließlich auf den Servern des datenhaltenden FDZ erfolgt – ein physischer Transfer der Daten findet zu keinem Zeitpunkt statt. Dadurch wird sichergestellt, dass die Daten weiterhin nur in kontrollierten Umgebungen analysiert werden können und die datengebenden FDZ zu jedem Zeitpunkt die volle Kontrolle über den Zugriff auf die Daten behalten.

Dieses Dokument dient vorrangig der Definition der technischen Anforderungen und Kriterien für den Aufbau eines Remote-Access-Systems in der Rolle des **Datengebers (Daten-Partei).** Im Fokus steht ein Referenzsystem auf Basis der Remote-Desktop-Software Horizon des Anbieters Omnissa, das es ermöglicht, von externen GWAP eine sichere Verbindung zu den eigenen Rechenservern herzustellen. Für die Definition der Anforderungen als **Datenempfänger (GWAP-Partei)** verweisen wir auf Goebel et. al (2023).

Dabei ist zu betonen, dass der Schwerpunkt dieses Dokuments auf dem Remote-Access-System selbst liegt und nicht auf der Ausgestaltung oder dem Betrieb der zugrundeliegenden Rechenserver. Eine detaillierte Beschreibung der Anforderungen an die Serverinfrastruktur, insbesondere hinsichtlich Hardwareausstattung, Softwareumgebung oder Datenmanagement, würde den Rahmen dieses Dokuments sprengen. Zudem variieren die Anforderungen an Rechenserver stark in Abhängigkeit von den jeweils zu analysierenden Daten und den spezifischen Bedürfnissen der Nutzenden. Eine universelle Lösung lässt sich daher nur schwer definieren.

2. Remote Desktop System

2.1. Lösungen

Die Implementierung eines Remote-Desktop-Systems ist mit erheblichem Aufwand für die jeweiligen IT-Abteilungen verbunden, etwa durch Lizenzkosten, Schulungsbedarf und infrastrukturelle Anforderungen. Hinzu kommt, dass eine Vielzahl unterschiedlicher Anbieter und Lösungen für solche Systeme existiert.

Für den Erfolg des RDCnet ist es daher entscheidend, dass die teilnehmenden FDZ auf bestehende technische Strukturen aufbauen und diese weiter nutzen können. Gleichzeitig müssen jedoch alle Remote-Access-Verbindungen zu den datengebenden FDZ auf den jeweiligen GWAP der datenempfangenden FDZ konfiguriert und gepflegt werden. Das bedeutet: Mit jeder zusätzlichen Remote-Desktop-Lösung bzw. Software steigt der Einrichtungsaufwand – insbesondere für die Datenempfänger-Seite. Unter dem Aspekt einer langfristigen Skalierbarkeit stellen die Freiheitsgrade bei der Wahl der eingesetzten Remote-Desktop-Systeme also eine Herausforderung dar.

In Abstimmung mit acht Partner-FDZ[2], die sich an einem Prototyp-Netzwerk beteiligen, wurde daher initial beschlossen, die Wahl des genutzten Remote-Desktop-System zu standardisieren und mithilfe von Omnissa Horizon[3] umzusetzen. Die Wahl fiel auf Omnissa Horizon, da diese Lösung sowohl die Bereitstellung der virtuellen Desktops als auch den Fernzugriff innerhalb einer einheitlichen Produktfamilie ermöglicht. Zudem kann mit dem integrierten Unified Access Gateway (UAG) ein Sicherheits-Gateway genutzt werden, wodurch separate VPN-Verbindungen oder Proxy-Server entfallen. Dies vereinfacht insbesondere die Konfiguration der Zugänge von den einzelnen GWAP erheblich. Ein weiterer Vorteil ist, dass Omnissa Horizon bereits von der Mehrheit der im RDCnet beteiligten FDZ eingesetzt wird. Dadurch reduziert sich der Aufwand für den Aufbau einer kompatiblen Serverstruktur, und der Zugriff kann einheitlich über den Horizon Client erfolgen.

Allerdings hat die Übernahme von VMware Horizon durch Broadcom und Omnissa im Jahr 2023 und die damit einhergehenden Konzernumstrukturierungen, einschließlich deutlich gestiegener Lizenzkosten, gezeigt, dass die ausschließliche Standardisierung auf eine einzelne Lösung langfristig problematisch sein kann.

Aus diesem Grund haben sich die Kooperationspartner des RDCnet darauf verständigt, dass Omnissa Horizon zwar weiterhin die bevorzugte Standardlösung bleibt, es jedoch zulässig ist, auch andere Remote-Desktop-Lösungen zu verwenden – vorausgesetzt, diese können ohne größeren Zusatzaufwand[4] von den IT-Abteilungen an den jeweiligen GWAP eingerichtet werden und die beteiligten FDZ stimmen der Nutzung zu.

2.2. Umsetzung

Die Umsetzung eines Remote-Desktop-Systems betrifft nur die Forschungsdatenzentren, die ihre Daten im RDCnet remote verfügbar machen wollen und im Folgenden als Datenpartei bezeichnet werden. Grundsätzlich steht es jeder Daten-Partei im RDCnet frei, wie das Remote-Desktop-System im Detail umgesetzt wird. Jede Daten-Partei entscheidet eigenverantwortlich darüber, welche Rechenressourcen den Nutzenden auf den virtuellen Desktops zur Verfügung stehen und welche Analysesoftware eingesetzt wird. Ebenso ist jede Daten Partei selbst dafür

[2] FDZ-DZHW, EBDC, FDZ GESIS, FDZ IDSC am IZA, FDZ-LIfBi, FDZ Ruhr am RWI, FDZ SOEP, FDZ ZEW

[3] Horizon gehörte ursprünglich zur Produktpalette von VMware, das im Jahr 2023 von Broadcom übernommen wurde. Die Remote-Desktop-Lösung Horizon wurde anschließend von Broadcom an das Unternehmen Omnissa verkauft, das heute der Anbieter ist. Es ist darauf hinzuweisen, dass an manchen Stellen im Dokument noch der Name VMware verwendet wird.

[4] Beispielsweise ist für die Einrichtung der Remote-Desktop-Verbindung über Horizon 8 auf dem GWAP lediglich die Installation einer Client-Software erforderlich, in der anschließend die Verbindungsparameter konfiguriert werden. Auch andere Remote-Desktop-Lösungen sollten mit einem vergleichbar geringen Aufwand umsetzbar sein.

verantwortlich, den Forschenden klare Anleitungen zur Durchführung von Datenanalysen innerhalb der bereitgestellten virtuellen Desktops bereitzustellen. Darüber hinaus obliegt es den jeweiligen Daten Partien, den Analyse-Output zu prüfen sowie den Import von Datensätzen oder Auswertungsskripten zu verwalten und zu kontrollieren.

Kurz gesagt: Die einzige grundlegende Voraussetzung für eine Daten-Partei im RDCnet besteht darin, ein Remote-Desktop-System bereitzustellen, das für Nutzende an den externen GWAP ausführbar ist und deren Anbindung von den IT-Abteilungen der GWAP Partei ohne größeren Aufwand eingerichtet werden kann.

Die von Omnissa Horizon bereitgestellte Lösung zur Bereitstellung einer Remote-Desktop-Infrastruktur (VDI) kann auf verschiedene Weise konfiguriert und genutzt werden. Eine bedarfsgerechte Ausgestaltung hängt dabei von verschiedenen Faktoren ab, etwa der Anzahl simultaner Nutzender oder der benötigten Rechenleistung der virtuellen Maschinen. Diese Abhängigkeit erschwert die Definition einer einheitlichen „One-fits-all"-Lösung.

Aus diesem Grund wird in diesem Dokument ein Referenzsystem vorgestellt, in dem die VDI als sogenannter „Jump Host" fungiert. In diesem Szenario stellt die Daten-Partei eine virtuelle Maschine bereit, auf die von den externen GWAP aus über gesicherte und verschlüsselte Verbindungen zugegriffen wird. Diese VM dient als vermittelnde Instanz, über die Nutzende Zugang zu einem nachgelagerten Rechenserver erhalten, auf dem die eigentliche Datenanalyse erfolgt.

Der Vorteil dieses Ansatzes besteht darin, dass der Rechenserver unabhängig von der VDI konfiguriert, betrieben und gewartet werden kann. Die VDI lässt sich zudem nahtlos in bestehende lokale Recheninfrastrukturen integrieren. Ein weiterer Vorteil ist, dass die virtuellen Desktops, die als Jump-Host fungieren, nur mit minimaler Hardwareausstattung betrieben werden müssen. Da sie ausschließlich eine SSH-Verbindung[5] zum eigentlichen Rechenserver herstellen und selbst keine rechenintensiven Aufgaben übernehmen, bleiben die Anforderungen an die VDI-Ressourcen gering.

3. Omnissa Horizon

Im folgenden Kapitel wird die durch Omnissa bereitgestellte Remote-Desktop-Lösung Horizon im Detail erläutert und ihre erforderlichen Komponenten beschrieben. Diese

[5] Eine SSH-Verbindung ist eine gesicherte, verschlüsselte Netzwerkverbindung zwischen zwei Computern, die über das Protokoll Secure Shell (SSH) aufgebaut wird.

Darstellung ist notwendig, um die Funktionsweise und Einbindung der Lösung in die Gesamtarchitektur des Netzwerks (Kapitel 5) nachzuvollziehen.

3.1. Virtuelle Desktop-Infrastruktur (VDI)

Die virtuelle Desktop-Infrastruktur (VDI) umfasst die Verwendung virtueller Maschinen zur Bereitstellung und Verwaltung virtueller Desktops. Eine VDI stellt Desktop-Umgebungen auf einem zentralen Server bereit und ermöglicht Nutzenden den Zugriff auf diese Arbeitsumgebungen von entfernten Standorten aus- beispielsweise von

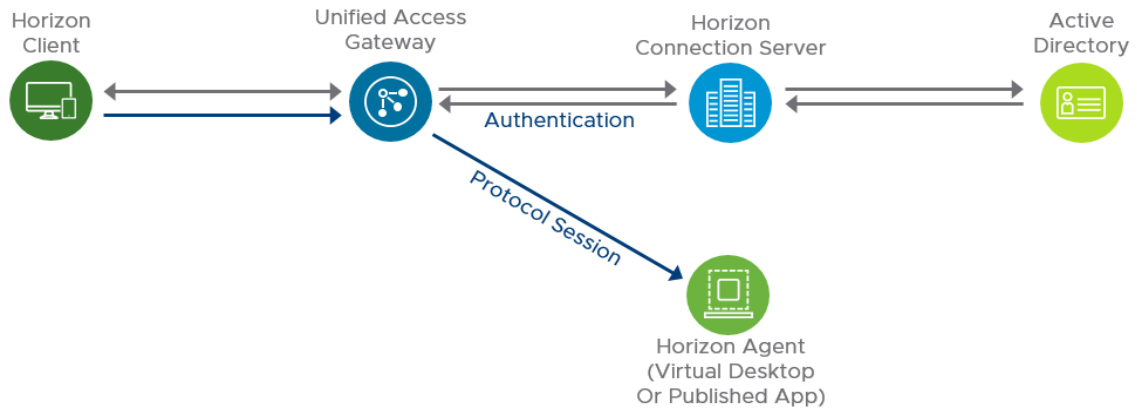


Abbildung 3: Kernkomponenten VMware Horizon. Quelle: VMware Techzone [1], 2023

einem externem GWAP an einem am RDCnet teilnehmenden FDZ. Eine solche Umgebung erlaubt Nutzenden die Fernverarbeitung von Daten, ohne dass diese zu irgendeinem Zeitpunkt physisch die Server des Hosts verlassen. In Verbindung mit technischen und organisatorischen Maßnahmen (TOMs) der GWAP kann so sichergestellt werden, dass Nutzende keine sensiblen Daten unbefugt übertragen können. Zu den Kernkomponenten von Omnissa Horizon gehört der Horizon Client (Zugangssoftware beispielsweise installiert auf einem Thin-Client) der sich über den Unified Access Gateway (UAG) bei einem Connection Server authentifiziert (Prüfung der Benutzerkennung über die Active Directory), welcher daraufhin eine gesicherte Verbindung zu virtuellen Desktops und Anwendungen herstellt (Siehe Abbildung 3).

3.2. Horizon Komponenten

Grundsätzlich bietet Horizon eine Vielzahl von Tools und Komponenten an, die der übergeordneten Virtualisierungsplattform „vSphere“ zugeordnet werden können (siehe Abbildung 2). Für den Zweck des sicheren Remote Access, wie er in RDCnet vorgesehen ist, sind einige der verfügbaren Komponenten jedoch optional und nicht zwingend erforderlich. Daher werden im Folgenden nur die Komponenten erläutert, die für die Einrichtung einer entsprechenden VDI-Umgebung wesentlich sind.

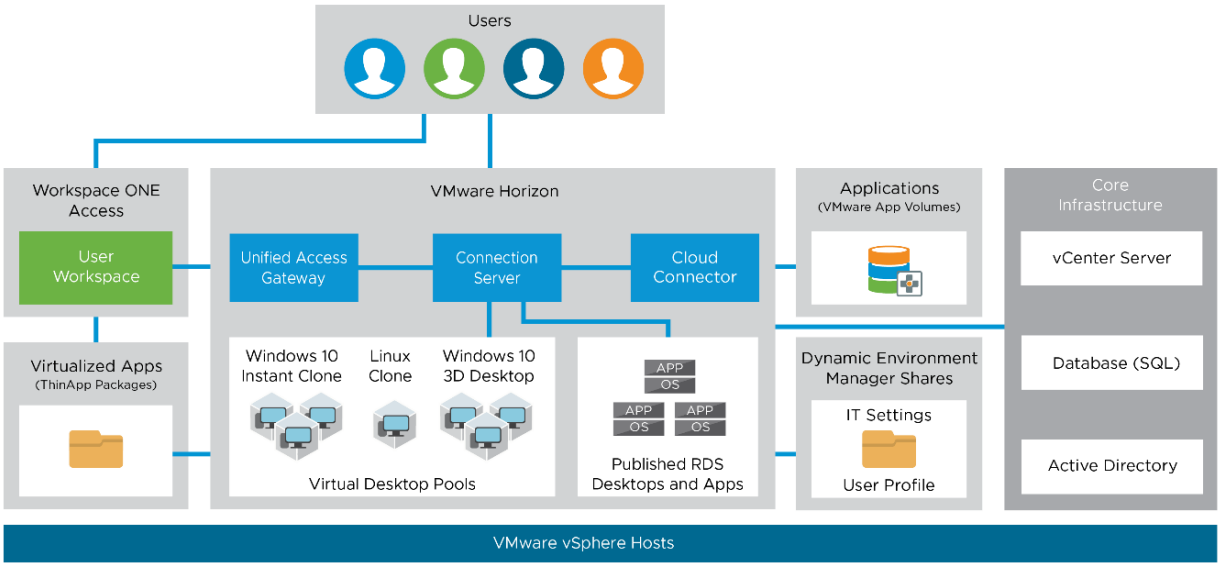


Abbildung 4: Logische Architektur und Komponenten. Quelle: VMware Techzone [2], 2023

3.2.1. Horizon Client

Der Horizon Client ist eine Anwendungssoftware, die es Nutzenden ermöglicht, auf virtuellen Desktops und Anwendungen von einem entfernten Endgerät aus zuzugreifen. In der Praxis wird Horizon Client von jeder GWAP Partei auf einem Thin-Client installiert, der für das RDCnet vorgesehen ist. Innerhalb der Software werden die Horizon Connection-Server der teilnehmenden GWAP Partein hinzugefügt, womit Forschende bei einer Nutzung des übersichtlich auswählen können, zu welchem FDZ sie eine Verbindung herstellen möchten (vorausgesetzt, sie verfügen über die entsprechenden Benutzerkennung).

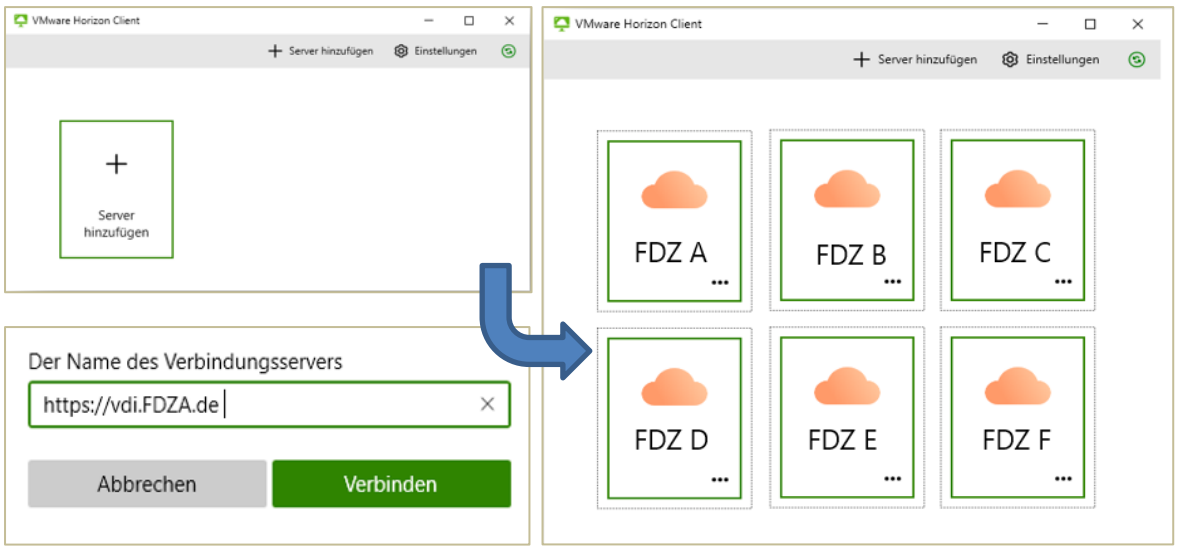


Abbildung 5: Horizon Client. Quelle: Eigene Darstellung

3.2.2. Connection Server

Der Horizon Connection Server ist ein grundlegender Bestandteil der Omnissa Horizon-Lösung für virtuelle Desktops. Es handelt sich hierbei um eine zentralisierte Serverkomponente, welche die Verbindung zwischen den virtuellen Desktops und den Endbenutzern verwaltet. Der Horizon Connection Server agiert als Schnittstelle für Client-Verbindungen, indem er eingehende Benutzeranfragen authentifiziert und sie dann an die entsprechenden Remote-Desktops bzw. virtuelle Maschinen weiterleitet. Die Adresse des Connection Servers bildet den zentralen Verbindungsparameter, um über den Horizon Client auf einen Remote-Desktop zuzugreifen.

3.2.3. vCenter Server

Der Horizon vCenter Server bildet die zentrale Verwaltungsoberfläche der gesamten vSphere Infrastruktur, darunter fällt beispielsweise die Erstellung und Konfiguration virtueller Maschinen, die für die entsprechenden Desktop-Pools bereitgestellt werden. Der vCenter Server wird mithilfe der vCenter Server Appliance (VCSA) bereitgestellt.

3.2.4. Virtual Desktop Pools

Ein virtueller Desktop-Pool definiert sich als eine Gruppe von virtuellen Desktops, die auf identisch konfigurierten virtuellen Maschinen gehostet werden. Durch das Bündeln von virtuellen Desktops können Administratoren die Desktop-Verwaltung zentralisieren und die Konfiguration vereinfachen. Der maßgebliche Vorteil von virtuellen Desktop-Pools liegt in der Zuweisung identischer Anwendungen, Rechenleistung und Berechtigungen für bestimmte Benutzergruppen sowie der automatisierten Bereitstellung von virtuellen Desktops.

In der Praxis können Daten Partien für die Benutzergruppe von externen bzw. RDCnet Nutzende einen virtuellen Desktop Pool mit beispielsweise zehn identisch konfigurieren virtuellen Maschinen erstellen. Die Konfiguration umfasst dabei die für Nutzende bereitgestellte Rechenleistung, Festplattenspeicher, implementierte Software und restrktiere Funktionen. Wenn sich Nutzende über den Horizon Client verbinden, wird ihnen jeweils automatisch ein virtueller Desktop auf Basis der virtuellen Maschinen zur Verfügung gestellt, wobei sich in diesem Beispiel bis zu zehn Nutzende gleichzeitig verbinden können.

Um die Erstellung und Konfiguration der virtuellen Maschinen zu vereinfachen, bietet Horizon die Nutzung von „Instant Clones“. Diese Methode ermöglicht die Erstellung mehrerer virtueller Desktops indem entsprechende Klone auf Grundlage einer einzigen übergeordneten virtuellen Maschine erzeugt werden. Auf diese Weise ist es nicht erforderlich, eine Vielzahl von virtuellen Maschinen zu konfigurieren, sondern nur ein einziges "Master-Image". Dies verringert nicht nur den Zeitaufwand für die Erstellung

der VMs, sondern auch für die Wartung und Updates, da die Klone dasselbe Betriebssystem (Windows oder Linux) wie das Master-Image nutzen.

3.2.5. ESXi

VMware ESXi ist ein „Bare-Metal-Hypervisor", der direkt auf einem physischen Server (oder einem Cluster mehrerer physischer Server) ausgeführt wird. Er bildet eine Abstraktionsebene zwischen der physischen Hardware und den virtuellen Maschinen, so dass mehrere VMs dieselben zugrunde liegenden physischen Ressourcen gemeinsam nutzen können, ohne ein zusätzliches Betriebssystem auf den Servern aufspielen zu müssen.

3.2.6. Unified Access Gateway (UAG)

Der Unified Access Gateway bildet die maßgebliche Sicherheitskomponente der VDI und kann verwendet werden, um den sicheren Remote-Access auf Anwendungen und Desktops bereitzustellen, die innerhalb einer Omnissa Horizon Umgebung gehostet werden. Dabei fungiert der UAG als Instanz zwischen den Remotenutzenden und den internen Netzwerkressourcen. Nutzende bauen über den Horizon Client eine sichere Verbindung mit der UAG auf und authentifizieren (Methoden: Benutzername/Passwort, Smartcards oder Zwei-Faktor-Authentifizierung) sich daraufhin mit ihren entsprechenden Anmelde-informationen. Der UAG leitet die Nutzenden dann über den Connection Server zu einem für sie vorgesehenen virtuellen Desktop weiter. Ein maßgeblicher Vorteil der UAG liegt darin, dass keine umfangreiche Konfiguration von zusätzlichen VPN-Tunneln vorgenommen werden muss, um eine sichere Verbindung zwischen externen Nutzenden und internen Ressourcen zu gewährleisten. Insbesondere im multilateralen Kontext des RDCnet bedeutet dies eine erhebliche Arbeitsersparnis für alle beteiligten FDZ.

(Quelle zu Komponenten: VMware Docs [10], 2023)

4. Netzwerkkonzept

4.1. VDI als Jumphost

Im hier vorgestellten System sind die bereitgestellten virtuellen Maschinen nicht dafür vorgesehen, dass Nutzende ihre Analysen direkt auf ihnen durchführen. Stattdessen dienen sie ausschließlich dazu, eine SSH-Verbindung zu einem Rechenserver herzustellen, auf dem die eigentlichen Analysen erfolgen. Die VDI fungiert in diesem Szenario also primär als Tunnel (bzw. Jumphost), der den Zugriff auf den Rechenserver ermöglicht.

Das bedeutet: Die Rechenleistung für die Analyse der Forschungsdaten wird vollständig auf dem angebundenen Rechenserver bereitgestellt und nicht auf den virtuellen Maschinen der VDI. Entsprechend sind diese virtuellen Maschinen lediglich mit der minimalen Rechenkapazität ausgestattet, die zur Herstellung und Aufrechterhaltung der SSH-Verbindung erforderlich ist.

Bei der Erstellung der virtuellen Maschinen ist darauf zu achten, dass diesen eine statische IP-Adresse zugewiesen wird. Diese ist erforderlich, um die für die SSH-Verbindung zum Rechenserver notwendigen Zertifikate installieren zu können. Aus diesem Grund wird in diesem Szenario nicht mit Instant Clones gearbeitet. Bei diesem Verfahren erhalten die virtuellen Maschinen erst bei der Erstellung (z. B. beim Login von Nutzenden) eine dynamische IP-Adresse, was eine gezielte Konfiguration im Vorfeld erschwert. Stattdessen wird für jede virtuelle Maschine ein sogenannter Full Clone erstellt. Ähnlich wie bei Instant Clones basiert auch dieses Verfahren auf einer Parent VM, in der alle relevanten Konfigurationen und Eigenschaften definiert werden. Anschließend werden vollständige Kopien dieser Parent VM erstellt. Diese Full Clones sind eigenständig, teilen keine Ressourcen mit der Parent VM und können dauerhaft mit einer festen MAC- und IP-Adresse konfiguriert werden.

Ein wesentlicher Vorteil der Nutzung der VDI als Jump-Host besteht darin, dass bestehende Rechenserverstrukturen weiterverwendet werden können. Im Gegensatz zu einem Szenario, in dem der Zugriff ausschließlich von lokalen Clients aus möglich ist, erlaubt die VDI auch externen Nutzenden einen sicheren Remote-Zugang zum Rechenserver.

Zudem steht den Nutzenden die Rechenleistung des Servers als aggregierte Ressource zur Verfügung. So kann beispielsweise festgelegt werden, dass jedem Nutzenden mindestens 16 GB Arbeitsspeicher zugewiesen werden. Falls darüber hinaus weitere Ressourcen verfügbar sind, können diese dynamisch genutzt werden. Dieses System eignet sich daher besonders für FDZ, deren Nutzende heterogene oder besonders hohe Rechenanforderungen an ihre Analysen stellen.

Ein Nachteil dieses Ansatzes besteht jedoch in dem zusätzlichen Administrationsaufwand für den Rechenserver. Neben der grundlegenden Systemkonfiguration müssen etwa Benutzerkonten sowohl für die VDI als auch für den Rechenserver angelegt und verwaltet werden, insbesondere dann, wenn nicht dieselbe Active Directory-Instanz für beide Systeme verwendet wird.

4.2. Netzwerkarchitektur

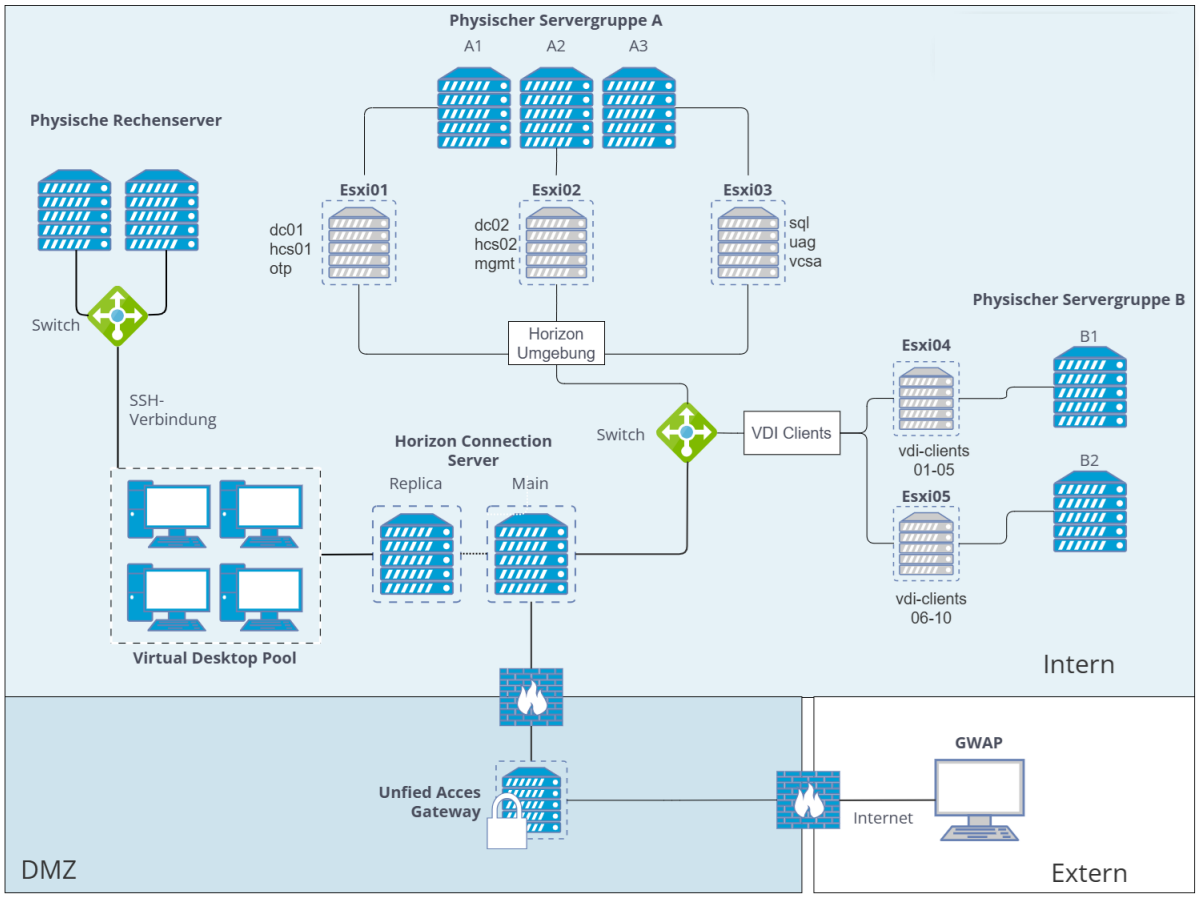


Abbildung 6: Netzwerkarchitektur des Remote-Desktop-Systems

4.3. Komponenten

Im Folgenden wird die Netzwerkarchitektur des vorgestellten Referenzsystems beschrieben. Dabei wird dargestellt, wie die einzelnen Komponenten, sowohl die physische Hardware als auch die virtuellen Maschinen, in Beziehung zueinanderstehen.

Die Systemumgebung basiert auf insgesamt fünf physischen Servern (ESXi-Hosts), die in zwei Gruppen unterteilt sind: Physische Servergruppe A und Physische Servergruppe B.

Physische Servergruppe A (Esxi01, Esxi02, Esxi03) stellt die Ressourcen für die zentrale VDI-Infrastruktur und die Management-Komponenten bereit. Auf diesen Hosts werden folgende virtuelle Maschinen betrieben:

1. **Esxi01:**
    I. **dc01:** Primärer Domain Controller für die Active Directory Domäne. Stellt die Dienste Active Directory und DNS (Domain Name System) bereit. Die Active

Directory dient der zentralen Verwaltung von Benutzerkonten, Computern und Ressourcen im Netzwerk. Das DNS ist für die Namensauflösung im Netzwerk zuständig.

II. **hcs01:** Horizon Connection Server (Main). Zentrale Komponente der Omnissa Horizon-Infrastruktur. Verwaltet die Verbindungen der Clients zur VDI-Umgebung. Er authentifiziert die Benutzer und leitet sie an die korrekten virtuellen Desktops weiter.

III. **otp:** Dieser Server stellt einen OTP-Service (One-Time Password) für die Multifaktor-Authentifizierung bereit.

2. **Esxi02:**

   I. **dc02**: Dient als Replikat des Domain Controllers dc01. Stellt ebenfalls Active Directory und DNS bereit und sorgt für Redundanz und Ausfallsicherheit dieser kritischen Dienste.

   II. **soep-hcs02**: Dient als Replikat des Horizon Connection Servers hcs01. Bietet Redundanz und Lastverteilung für die Verbindungen zur VDI-Umgebung.

   III. **mgmt**: Management-Server, der als Jumphost für administrative Aufgaben dient. Verfügt über eine zusätzliche Netzwerkkarte für den Zugriff auf die DMZ und ermöglicht so die sichere Verwaltung aller Komponenten.

3. **Esxi03:**

   I. **vcsa:** vCenter Server Appliance. Dies ist die zentrale Verwaltungsplattform für die gesamte Omnissa vSphere-Umgebung. Über den vCenter Server werden die ESXi-Hosts, die virtuellen Maschinen und andere Ressourcen der VDI-Umgebung verwaltet.

   II. **sql:** SQL-Server, der die Datenbanken für die VDI-Umgebung und möglicherweise für andere Anwendungen hostet.

   III. **uag:** Unified Access Gateway. Diese VM befindet sich in der DMZ und ermöglicht den sicheren Zugriff von externen Benutzern auf die VDI-Umgebung über das Internet.

Physische Servergruppe B (Esxi04, Esxi05) stellt die Ressourcen für die virtuellen Desktops (VDI-Clients) der Benutzer bereit.

1. **Esxi04: vdi01 bis vdi05 (VDI-Clients)**: Virtuelle Desktops für die Nutzenden.
2. **Esxi05: vdi06 bis vdi10 (VDI-Clients):** Virtuelle Desktops für die Nutzenden.

Die VDI-Clients (vdi01 bis vdi10) sind restriktiv konfigurierte virtuelle Maschinen auf Basis von Debian GNU/Linux 12 (64-bit). Sie dienen als gesicherte Zugangspunkte zur Datenanalyseumgebung und sind technisch so konfiguriert, dass ausschließlich ein einzelner, fest definierter Workflow erlaubt ist.

Die Nutzenden können dabei:

- keine Internetverbindung nutzen,
- keine zusätzlichen Programme öffnen,
- kein Terminal oder Dateimanager starten,
- nicht mit Rechtsklick interagieren,
- nicht auf Systemdateien zugreifen,
- und keine Systemkonfigurationen einsehen oder ändern.

Die grafische Oberfläche wird so angepasst, dass nur ein einziges Element sichtbar und nutzbar ist: Ein nicht veränderbarer Desktop-Link zu einem vorinstallierten SSH-Skript, das automatisch eine Verbindung zum zentralen Rechenserver aufbaut. Die Nutzenden haben keine Möglichkeit, mit dem System außerhalb dieses Skripts zu interagieren.

Komponente	**Spezifikation**
Betriebssystem	Debian GNU/Linux 12 (64-bit)
CPU	2 vCPUs
RAM	4 GB
Festplatte	40 GB Thin Provision
Netzwerk	VM Network, keine Internetverbindung
Benutzerrechte	Stark eingeschränkt (kein Terminal, kein Menü, kein Zugriff)
Zugriff	Nur über vorinstalliertes SSH-Skript (Desktop-Link)

4.4. Kommunikation und Zugriff

Der Zugriff auf die virtuellen Desktops erfolgt über zwei redundante Horizon Connection Server (hcs01 und hcs02). Diese sorgen für eine hohe Verfügbarkeit und Lastverteilung der Verbindungen. Die Verbindung wird vom Horizon Client initiiert, der sich mit einem Unified Access Gateway (uag) verbindet, das sich in einem dedizierten DMZ-Netzwerk befindet. Dadurch ist ein sicherer Zugriff von außerhalb des internen Netzwerks ohne VPN erforderlich.

Sämtlicher externer Zugriff auf die VDI-Infrastruktur erfolgt über eine vorgeschaltete Firewall, die den Zugang zur DMZ reguliert. Nach erfolgreicher Authentifizierung über das UAG wird die Sitzung an einen verfügbaren Connection Server weitergeleitet, der dann den Zugriff auf den entsprechenden virtuellen Desktop im konfigurierten Pool ermöglicht.

Der Management-Server (mgmt) dient als zentrale Verwaltungsstelle für die gesamte Infrastruktur. Dieser Server ist ebenfalls mit der DMZ verbunden, was eine sichere Verwaltung aller Komponenten ermöglicht, einschließlich der Connection Server, Active Directory-Dienste, DNS und der zentralen Datenbank.

Für die Netzwerkkommunikation und -verfügbarkeit ist die gesamte ESXi-Server-Infrastruktur (esxi01 bis esxi05) redundant über zwei 10-Gbps-Glasfaser-Netzwerkschnittstellen verbunden. Sollte eine Schnittstelle ausfallen, wird der Datenverkehr automatisch über die zweite Schnittstelle weitergeleitet, wodurch eine durchgängige Verbindung sichergestellt wird. Diese Netzwerktopologie bietet nicht nur Hochverfügbarkeit zwischen den Hosts, sondern auch hohe Geschwindigkeit und geringe Latenz für alle gehosteten virtuellen Maschinen.

Alle virtuellen Maschinen innerhalb der VDI-Infrastruktur erben diese Netzwerkkonfiguration von ihren Hosts und profitieren gleichermaßen von der hohen Bandbreite und Redundanz.

Zusätzlich existiert ein separates VLAN, das ausschließlich für Wartung und Updates vorgesehen ist. Dieses VLAN wird nur während geplanter Wartungsfenster aktiviert und ermöglicht es den Servern, sich mit dem Internet zu verbinden, um notwendige Updates und Sicherheitspatches zu erhalten. Beispielsweise ist der Server soep-esxi01 über eine iDRAC-IP sowie eine dedizierte Konfigurationsnetzwerk-IP mit diesem VLAN verbunden.

5. Hardware-Referenz

In diesem Kapitel wird exemplarisch die am FDZ des Sozio-oekonomischen Panels (SOEP) für das definierte Referenzsystem eingesetzte Hardware dargestellt. Dabei wird die Ausstattung der einzelnen Server aufgelistet und die Hardware-Allokation auf die jeweiligen virtuellen Maschinen beschrieben.

5.1 Physische Hardware

1. Server: **esxi01**

Komponente	**Ausstattung**
Modell des Servers	PowerEdge R650xs
CPU	Intel Xeon Silver 4314, 32 vCPUs (32 Kerne, 2400 MT/s)
Arbeitsspeicher	128 GB DDR4 (16 GB pro DIMM, Dual Rank 3200 MT/s)
Netzwerkadapter	Intel(R) Ethernet 10G 2P X710-T2L-t Adapter (10G Fibre-Optik)
Festplatte	2 x 446,63 GB SSDs konfiguriert im RAID-1 (Write Back)
RAID-Controller	PERC H755 Front (Embedded), 8192 MB Speicher
Gastmaschinen	-soep-dc01 (Domänencontroller) -soep-hcs01 (Horizon Connection Server 01) -soep-mgmt (Management Server) -soep-otp (MFA Authentication Server)

2. Server: **esxi02**

Komponente	**Ausstattung**
Modell des Servers	PowerEdge R650xs
CPU	Intel Xeon Silver 4314, 32 vCPUs (32 Kerne, 2400 MT/s)
Arbeitsspeicher	128 GB DDR4 (16 GB pro DIMM, Dual Rank 3200 MT/s)
Netzwerkadapter	Intel(R) Ethernet 10G 2P X710-T2L-t Adapter (10G Glassfasser)
Festplatte	2 x 446,63 GB SSDs konfiguriert im RAID-1 (Write Back)
RAID-Controller	PERC H755 Front (Embedded), 8192 MB Speicher
Gastmaschinen	dc02 (Domänencontroller) hcs02 (Horizon Connection Server 02)

3. Server: **esxi03**

Komponente	**Ausstattung**
Modell des Servers	PowerEdge R650xs
CPU	Intel Xeon Silver 4314, 32 vCPUs (32 Kerne, 2400 MT/s)
Arbeitsspeicher	128 GB DDR4 (16 GB pro DIMM, Dual Rank 3200 MT/s)
Netzwerkadapter	Intel(R) Ethernet 10G 2P X710-T2L-t Adapter (10G Glassfasser)
Festplatte	2 x 446,63 GB SSDs konfiguriert im RAID-1 (Write Back)
RAID-Controller	PERC H755 Front (Embedded), 8192 MB Speicher
Gastmaschinen	- vcsa (vCenter Server) - uag (Unified Access Gateway)

4. Server: **esxi04**

Komponente	**Ausstattung**
Modell des Servers	PowerEdge R650xs
CPU	Intel Xeon Silver 4314, 32 vCPUs (32 Kerne, 2400 MT/s)
Arbeitsspeicher	128 GB DDR4 (16 GB pro DIMM, Dual Rank 3200 MT/s)
Netzwerkadapter	Intel(R) Ethernet 10G 2P X710-T2L-t Adapter (10G Glassfasser)
Festplatte	2 x 446,63 GB SSDs konfiguriert im RAID-1 (Write Back)
RAID-Controller	PERC H755 Front (Embedded), 8192 MB Speicher
Gastmaschinen	VDI-Clients 01 bis 05 (VDI Clients)

5. Server: **esxi05**

Komponente	**Ausstattung**
Modell des Servers	PowerEdge R650xs
CPU	Intel Xeon Silver 4314, 32 vCPUs (32 Kerne, 2400 MT/s)
Arbeitsspeicher	128 GB DDR4 (16 GB pro DIMM, Dual Rank 3200 MT/s)
Netzwerkadapter	Intel(R) Ethernet 10G 2P X710-T2L-t Adapter (10G Glassfasser)
Festpaltte	2 x 446,63 GB SSDs konfiguriert im RAID-1 (Write Back)
RAID-Controller	PERC H755 Front (Embedded), 8192 MB Speicher
Gastmaschinen	VDI-Clients 06 bis 10 (VDI Clients)

5.2 Allokation auf virtuelle Maschinen

Die Hardwareleistung der fünf oben genannten physischen Server wird wie folgt auf die folgenden virtuellen Maschinen aufgeteilt.

1. dc01 (Domänencontroller)

Komponente	**Ausstattung**
Betriebssystem	Microsoft Windows Server 2022 (64-bit)
CPU	2 vCPUs
Festplatte	90 GB Thin Provision
Arbeitsspeicher	6 GB
Host	esxi01
Netzwerkadapter	VM Netzwerk
Services	Active Directory, DNS

2. dc02 (Domänencontroller Replika)

Komponente	**Ausstattung**
Betriebssystem	Microsoft Windows Server 2022 (64-bit)
CPU	2 vCPUs
Festplatte	90 GB Thin Provision
Arbeitsspeicher	6 GB
Netzwerkadapter	VM Netzwerk
Host	soep-esxi02
Services	Active Directory Replika, DNS Replika

3. hcs01 (Horizon Connection Server 01)

Komponente	**Ausstattung**
Betriebssystem	Microsoft Windows Server 2022 (64-bit)
CPU	4 vCPUs
Festplatte	90 GB Thin Provision

Arbeitsspeicher	16 GB
Netzwerkadapter	VM Netzwerk
Host	esxi01
Services	Horizon Connection Server

4. hcs02 (Horizon Connection Server 02)

Komponente	**Ausstattung**
Betriebssystem	Microsoft Windows Server 2022 (64-bit)
CPU	4 vCPUs
Festplatte	90 GB Thin Provision
Arbeitsspeicher	16 GB
Netzwerkadapter	VM Netzwerk
Host	esxi02
Services	Active Directory, DNS

5. vcsa (vCenter Server)

Komponente	**Ausstattung**
Betriebssystem	Microsoft Windows Server 2022 (64-bit)
CPU	4 vCPUs
Festplatte	50 GB Thin Provision
Arbeitsspeicher	21 GB
Netzwerkadapter	VM Netzwerk
Host	esxi03
Services	vCenter Server

6. uag (Unified Access Gateway)

Komponente	**Ausstattung**
Betriebssystem	Microsoft Windows Server 2022 (64-bit)
CPU	2 vCPUs
Festplatte	20GB Thin Provision

Arbeitsspeicher	4 GB
Netzwerkadapter	DMZ (verbunden)
Host	esxi03
Services	vCenter Server

7. soep-vdi-client 01 bis 05 (VDI Clients)

Komponente	**Ausstattung**
Betriebssystem	Debian GNU/Linux 12 (64-bit)
CPU	2 vCPUs
Festplatte	20 GB Thin Provision
Arbeitsspeicher	4 GB
Netzwerkadapter	VM Netzwerk
Standort	esxi04
Services	VDI-Clients 01-05

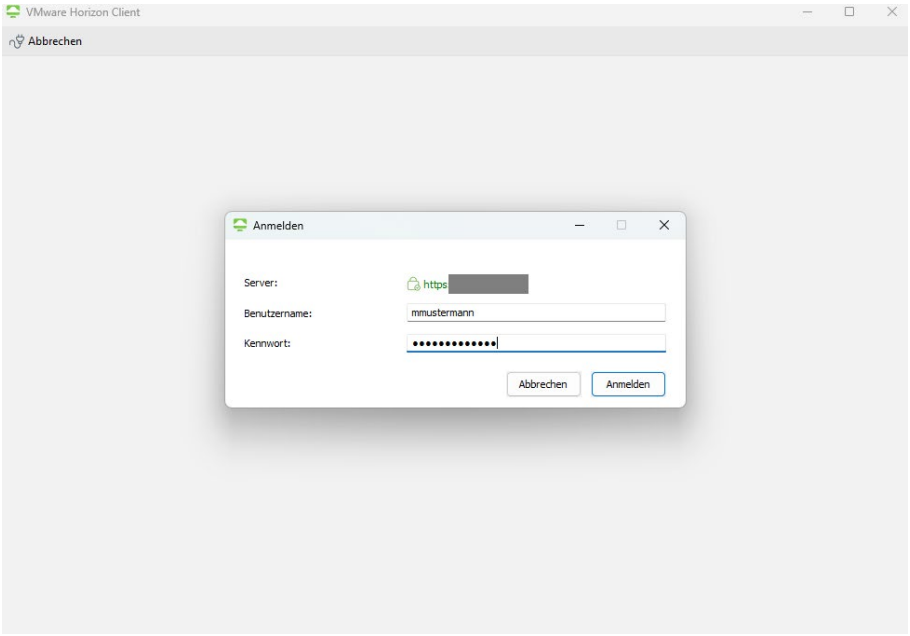
8. vdi-client 06 bis 10 (VDI Clients)

Komponente	**Ausstattung**
Betriebssystem	Debian GNU/Linux 12 (64-bit)
CPU	2 vCPUs
Festplatte	20 GB Thin Provision
Arbeitsspeicher	4 GB
Netzwerkadapter	VM Netzwerk
Host	esxi05
Services	VDI-Clients 06-10

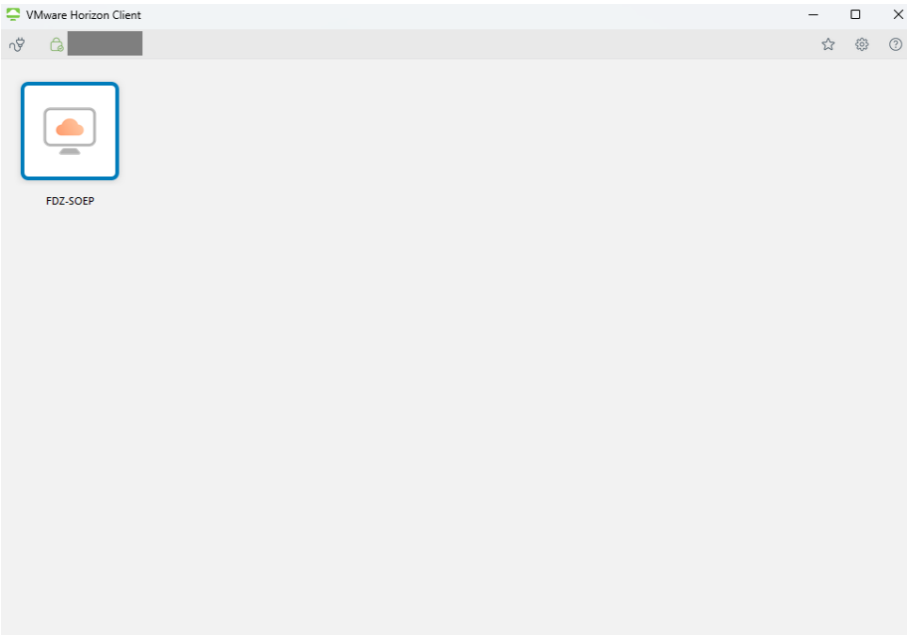
6. Prozessbeschreibung

Im Folgenden wird aufgezeigt, wie der Zugang von einem externen GWAP (Thin Client) über das Remote-Desktop-System auf den entsprechenden Rechenserver erfolgen kann.

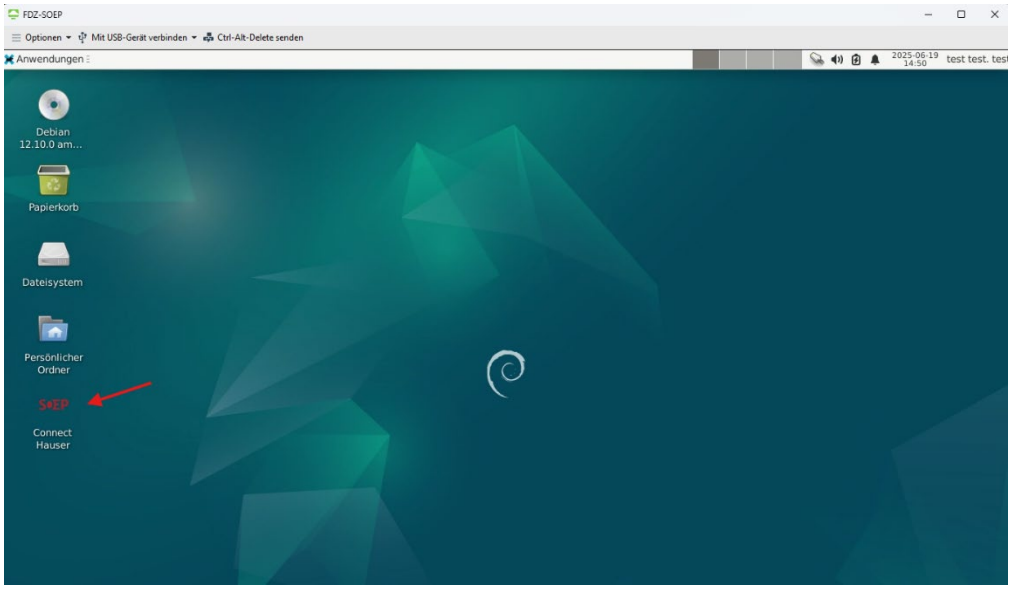
1. Verbindung auf Horizon Connection Server (via Horizon Client).



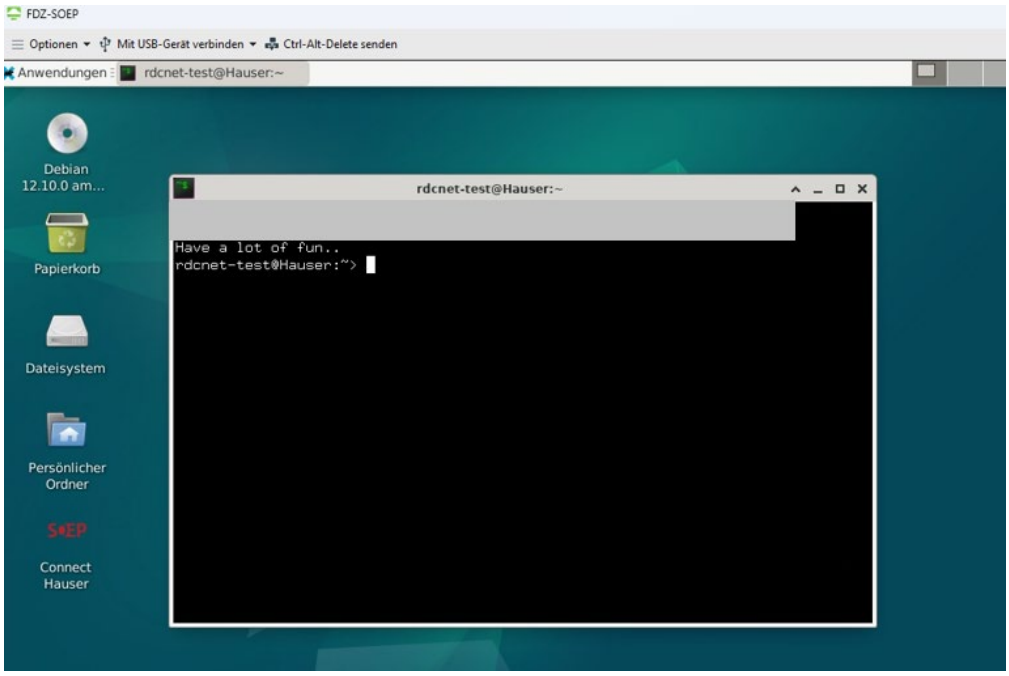
2. Auswahl Desktop-Pool.



3. SSH-Verbindung zu Rechenserver über Desktop-App aufbauen.



4. Verbindung zum Rechenserver erfolgreich aufgebaut. Software z.B. Stata oder R kann über die Konsole geöffnet werden.



7. Kosten

Die Kosten für die Umsetzung des beschriebenen Referenzsystems lassen sich wie folgt aufteilen:

Komponente	Kosten in € (brutto)	Kaufdatum
5x DELL PowerEdge R650xs – Server siehe Kapitel 5.1	20.006,30	01.2024
Aufrüstung Server: 5x 10Gbit Netzwerkkarte (Intel X710-T2L Dual Port 10GbE)	2.962,92	09.2024
Aufrüstung Server: 288 GB DDR4 3200MT Arbeitsspeicher (18x 16GB)	6.142,61	09.2024
Externe Dienstleistung: Initiale Installation und Konfiguration des Systems.	8.925,00	12.2024
Lizenz Omnissa: Horizon 8 Enterprise Term Edition- 10 Concurrent User Pack for 1 year term license	3.289,88	12.2024
Gesamtkosten	**41.326,71**	

Zusätzlich zu den in der Tabelle aufgeführten direkten Kosten entstehen weitere, schwer quantifizierbare Aufwände, da auf bereits vorhandene Ressourcen zurückgegriffen werden konnte.

Komponente
6x Windows 2022 Serverlizenz (64bit)
Serverrack
Netzwerkkabel Cat 7
Switch 10Gbit
Personal für Wartung und detaillierte Systemkonfiguration – 0,5 VZÄ Systemadministrator

8. Geplante Erweiterungen

Das in diesem Dokument beschriebene System ist grundsätzlich für den Produktivbetrieb geeignet und stellt eine gesicherte Möglichkeit dar, Remote-Zugriffe von definierten Standorten aus zu ermöglichen. Dennoch bestehen insbesondere in zwei Komponenten Erweiterungspotenziale, die zusätzliche Aspekte der Sicherheit und Ausfallsicherheit abdecken können. Zum Zeitpunkt der Erstellung dieses Dokuments waren diese Erweiterungen noch nicht implementiert. Ihre Umsetzung wird jedoch ausdrücklich empfohlen.

8.1. Zwei-Faktor-Authentifizierung (2FA)

Die Nutzung des beschriebenen Remote-Desktop-Systems erfolgt ausschließlich von vordefinierten, physischen Standorten, die über eine IP-Whitelist freigegeben sind. Dabei handelt es sich in der Regel um restriktiv konfigurierte Thin Clients, die sich in Datensicherheitsräumen der beteiligten GWAP-Parteien bzw. Forschungsdatenzentren befinden. Diese Umgebung stellt sicher, dass kein Remotezugriff von privaten oder unkontrollierten Endgeräten erfolgen kann. Bei der derzeitigen Nutzung erfolgen drei implementierte Sicherheit Prüfungen:

1. **Physische Identitätsprüfung vor Ort**
   Der erste Authentifizierungsschritt erfolgt physisch: Die Identität der Nutzenden wird durch autorisiertes FDZ-Personal am Standort überprüft. Erst nach erfolgreicher Prüfung und Validierung der Zugriffsberechtigung wird der Zugang zum Datensicherheitsraum sowie zur Nutzung des zugewiesenen GWAP freigegeben.

2. **Anmeldung am Remote Desktop System (Horizon Client)**
   Die Nutzenden melden sich anschließend mit persönlichen Zugangsdaten (Benutzername und Passwort) am Horizon Client an, um Zugriff auf eine virtuelle Maschine (Jump Host) zu erhalten.

3. **Zugriff auf Rechenserver per SSH**
   Vom Jump Host aus erfolgt der Zugriff auf die eigentlichen Rechenserver via SSH. Hierfür ist eine separate SSH-Nutzerkennung notwendig, die unabhängig von den Horizon-Zugangsdaten vergeben wird.

Insgesamt ergibt sich so ein dreistufiges Authentifizierungssystem, bestehend aus physischer Zutrittskontrolle und zwei digitalen Zugangsschritten.

Zur weiteren Absicherung der digitalen Authentifizierungsstufen wird die Einführung einer Zwei-Faktor-Authentifizierung (2FA) mittels One-Time Passwords (OTP) empfohlen. Dies würde die digitale Anmeldesicherheit erhöhen und einen zusätzlichen Schutz gegen Kompromittierung von Benutzerkonten bieten. Die Systemarchitektur sieht bereits eine entsprechende Erweiterung vor: Hierfür ist ein dedizierter virtueller Server für die OTP-Verwaltung eingeplant (siehe Kapitel 4.2.1 – Komponente esxi010-otp). Auf diesem Server kann eine OTP-Management-Lösung betrieben werden (z.B. PrivacyIDEA oder LinOTP).

Die Einrichtung erfolgt typischerweise durch das Versenden eines QR-Codes an die Nutzenden, welcher in einer Authenticator-App (z. B. FreeOTP, Google Authenticator) gescannt wird. Die App generiert anschließend zeitbasierte Einmalpasswörter (TOTP), die bei der Anmeldung zusätzlich eingegeben werden müssen.

8.2. Network Storage

Im aktuellen System werden die Benutzerdaten über das Active Directory auf dem virtuellen Server dc01 gespeichert (siehe Kapitel 4.2.1). Sollte dieser Server ausfallen, muss das System zunächst neu gestartet werden. Anschließend übernimmt der redundante Server esxi02-dc01 vorübergehend die Rolle des primären Verzeichnisdienstes.

Idealerweise sollte jedoch ein zentraler Netzwerkspeicher (z. B. ein NAS oder SAN), der unabhängig von den einzelnen Servern betrieben wird, zur Speicherung und Bereitstellung der Benutzerdaten verwendet werden. Dadurch könnte sichergestellt werden, dass im Falle eines Serverausfalls der Zugriff auf die Benutzerdaten ohne Verzögerung und ohne einen notwendigen Neustart der Infrastruktur weiterhin möglich ist. Dies würde die Ausfallsicherheit und Verfügbarkeit des Systems deutlich erhöhen.

Literaturverzeichnis

Bender, S., and Heining, J. (2011): The Research-Data-Centre in Research-Data-Centre Approach: A First Step Towards Decentralised International Data Sharing. IASSIST Quarterly 35 (3), 10-16.

Goebel, J., Murray, N., Pedrique, K., & Sieber, I. (2023). Implementierung eines Gastwissenschaftsarbeitsplatzes im RDCnet - Technische Anleitung zur Konfiguration eines Thin Clients. In KonsortSWD Working Paper (1.1, Bd. 6). https://doi.org/10.5281/zenodo.10040912

Murray, N., & Goebel, J. (2024). Vertragliche Grundlagen zur Teilnahme am RDCnet. In KonsortSWD Working Paper (Version v2, Bd. 1). https://doi.org/10.5281/zenodo.13827792

VMware Techzone [1]: Architectural Overview, Figure 1: Horizon Core Components. Zugriff am 13.02.2023. https://techzone.vmware.com/resource/horizon-architecture#introduction

VMware Techzone [2]: Architectural Overview, Figure 3: Horizon Logical Components. Zugriff am 13.02.2023. https://techzone.vmware.com/resource/horizon-architecture#introduction

VMware Docs [1]: Einführung in virtuelle Desktops. Zugriff am 28.06.2023. https://docs.vmware.com/de/VMware-Horizon-7/7.13/virtual-desktops/GUID-5973DBA5-15DF-425E-A362-9E23D12F22E1.html

VMware Docs [2]: Hardware requirements Horizon Connection Server. Zugriff am 28.06.2023. https://docs.vmware.com/en/VMware-Horizon/2303/horizon-installation/GUID-332CFB83-784A-4578-9354-888C0538909A.html#GUID-332CFB83-784A-4578-9354-888C0538909A

VMware Docs [3]: Hardware Requirements for vCenter Server and Platform Services Controller on Windows. Zugriff am 28.06.2023. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcenter.install.doc/GUID-D2121DC5-1FC8-48DC-A4BA-C3FD72D0BE77.html

VMware Docs [4]: Storage Requirements for vCenter Server and Platform Services Controller on Windows. Zugriff am 28.06.2023. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcenter.install.doc/GUID-FFC41E86-F949-4366-A111-C3A80410FB3D.html

VMware Docs [5]: Database Requirements for vCenter Server on Windows. Zugriff am 28.06.2023. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcenter.install.doc/GUID-2F1D0E79-52C4-4DC2-AF01-11564207FBE1.html

VMware Docs [6]: Unified Access Gateway Sizing Options. Zugriff am 28.06.2023. https://docs.vmware.com/en/Unified-Access-Gateway/2303/uag-deploy-config/GUID-3055F669-7CC3-4F12-8CBF-F144854C471A.html

VMware Docs [7]: Deploying Unified Access Gateway Appliance. Zugriff am 28.06.2023. https://docs.vmware.com/en/Unified-Access-Gateway/2303/uag-deploy-config/GUID-F1C1700C-EB06-4F59-8CE6-F155C9AD8555.html

VMware Docs [8]: Reduzieren der Speicheranforderungen mit Instant Clones. Zugriff am 28.06.2023. https://docs.vmware.com/de/VMware-Horizon-7/7.13/horizon-architecture-planning/GUID-4880340C-C80C-4CE1-95FA-8692A5BFA3BC.html

VMware Docs [9]: ESXi Hardware Requirements. Zugriff am 29.06.2023. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.upgrade.doc/GUID-DEB8086A-306B-4239-BF76-E354679202FC.html

VMware Docs [10]: Zusammenspiel der Komponenten. Zugriff am 29.06.2023. https://docs.vmware.com/de/VMware-Horizon/2203/horizon-architecture-planning/GUID-C6AD7E43-FC69-4D8C-AB97-423FC0DCDB3D.html

Impressum

Kontakt:
Deutsches Institut für Wirtschaftsforschung (DIW Berlin)
Abteilung SOEP
Anton-Wilhelm-Amo-Straße 58
10117 Berlin
nmurray@diw.de
https://www.diw.de

KonsortSWD Working Paper: KonsortSWD baut als Teil der Nationalen Forschungsdateninfrastruktur Angebote zur Unterstützung von Forschung mit Daten in den Sozial-, Verhaltens-, Bildungs- und Wirtschaftswissenschaften aus. Unsere Mission ist es, die Forschungsdateninfrastruktur zur Beforschung der Gesellschaft zu stärken, zu erweitern und zu vertiefen. Sie soll nutzungsorientiert ausgestaltet sein und die Bedürfnisse der Forschungscommunities berücksichtigen. Wichtiger Grundstein ist dabei das seit über zwei Jahrzehnten durch den Rat für Sozial- und Wirtschaftsdaten (RatSWD) aufgebaute Netzwerk von Forschungsdatenzentren.

In dieser Reihe erscheinen Beiträge rund um das Forschungsdatenmanagement, die im Kontext von KonsortSWD entstehen. Beiträge, die extern und doppelblind begutachtet wurden sind entsprechend gekennzeichnet.

KonsortSWD wird im Rahmen der NFDI durch die Deutsche Forschungsgemeinschaft (DFG) gefördert – Projektnummer: 442494171.

Berlin, September 2025

DOI: https://doi.org/10.5281/zenodo.17106418

Zitationsvorschlag:
Murray, N., & Pedrique, K. (2025). Remote-Desktop-Verarbeitung sensibler Forschungsdaten: Ein Referenzsystem. Zenodo. https://doi.org/10.5281/zenodo.17106418