KonsortSWD
Konsortium für die
Sozial-, Verhaltens-, Bildungs- und
Wirtschaftswissenschaften

RDCnet

Teilnahmeprozess am RDCnet Pilotnetzwerk

Jan Goebel,[1] Neil Murray,[1] Kenny Pedrique,[1] Ingo Sieber[1]

April 2023

[1] SOEP am DIW Berlin

Abstract

Im folgenden Dokument wird der Aufbau und der Prozess zur Umsetzung des Pilotnetzwerk des RDCnet dargestellt. Ziel des RDCnet ist die multilaterale Vernetzung von Gastwissenschaftler*innen Arbeitsplätze verschiedener im KonsortSWD akkreditierter Forschungsdatenzentren (FDZ). Somit können Forschende auf sensible Daten zugreifen – unabhängig davon, an welchem GWAP sie arbeiten. Bevor das RDCnet in den Produktivbetrieb übergehen kann, werden im Rahmen des Pilotnetzwerk die Verbindungen zwischen den teilnehmenden FDZ definiert und getestet. Hierfür wurde gemeinsam mit den Partner-FDZ ein Prozess erarbeitet, um den Aufbau des Pilotnetzwerk strukturiert und standardisiert durchführen zu können.

Keywords: Forschungsdateninfrastruktur, Remote Access, Gastwissenschaftler*innen Arbeitsplätze, Forschungsdatenzugang, Sensible Forschungsdaten

Ziel und Idee des Pilotnetzwerks

Bevor das RDCnet in den Produktivbetrieb übergehen kann, werden im Rahmen des Pilotnetzwerk die Verbindungen zwischen den teilnehmenden FDZ definiert und getestet. Ziel ist somit der multilaterale Verbindungsaufbau zwischen den FDZ, der mittels VMware Horizon durchgeführt werden soll.

Dies erfordert zum einen, dass jedes FDZ innerhalb ihrer VMware Horizon-Umgebung einen Testbenutzerkonto anlegt, damit der Remote Access durch die anderen FDZ erfolgen kann. Zum anderen muss jedes FDZ ein Endgerät (z.B. Thin Client) für das RDCnet bereitstellen, mit welchem die Verbindungen zu den anderen FDZ über den VMware Horizon Client implementiert und getestet werden können. Nach erfolgreicher Einrichtung des Pilotnetzwerks sollte also jedes FDZ ein Endgerät/Client so konfiguriert haben, dass der Remote Access zu den Verbindungsservern der anderen FDZ vordefiniert und mittels des Testbenutzerkontos geprüft worden ist.

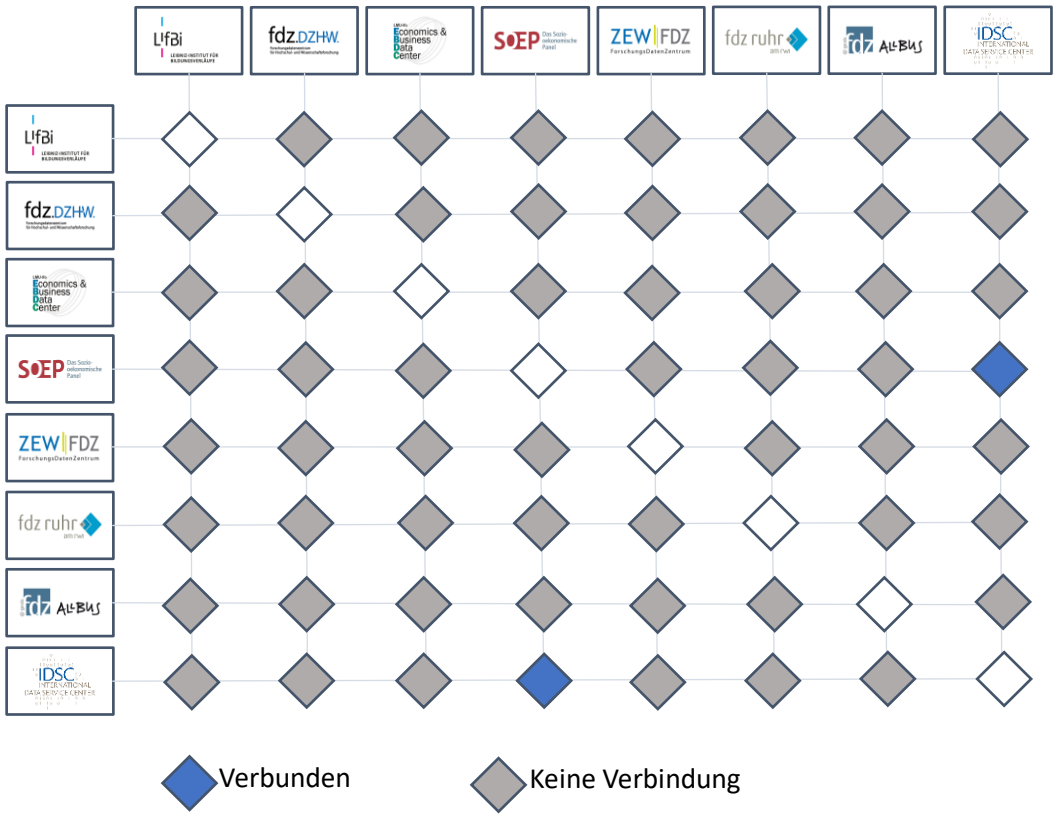


Abbildung 1: Verbindungsmatrix teilnehmender FDZ- Ziel des Pilotnetzwerks ist der multilaterale Verbindungsaufbau zwischen den FDZ.

Prozess zur Teilnahme am Pilotnetzwerk

In einem ersten bilateralen Verbindungsaufbau zwischen dem FDZ SOEP und FDZ IZA wurde der Prozess für die Teilnahme am Pilotnetzwerk erarbeitet und anschließend in einem gemeinsamen Workshop mit allen Partner FDZ evaluiert. Der Prozess lässt sich dabei in vier Stufen zusammenfassen:

1. Erstellung eines Testbenutzerkontos innerhalb der eigenen VMware Umgebung
2. Austausch der Verbindungsparameter durch das bereitgestellte Teilnahmeformular

3. Implementierung der Verbindungsparameter anderer FDZ via VMware Horizon Client
4. Verbindungsaufbau zum jeweiligen Testbenutzerkonto der anderen FDZ

Das Pilotnetzwerk soll sukzessive ausgebaut werden, da sich die Verfügbarkeit der erforderlichen Ressourcen (insbesondere der IT-Aufwand) zur Durchführung der oben genannten Schritte zwischen den FDZ unterscheiden. Besondere Priorität hat jedoch die Einrichtung des Testbenutzerkontos und der Austausch der Verbindungsparameter, was nun so zeitnah wie möglich umgesetzt werden sollte. Die im Teilnahmeformular angegebenen Verbindungsparameter werden vom FDZ SOEP gesammelt und dann für eine vom SOEP ausgehende Testverbindung herangezogen. Ist die Verbindung erfolgreich, werden die gesammelten und geprüften Verbindungsparameter gebündelt und an die Partner FDZ übermittelt.

Im Folgenden werden die einzelnen Schritte des Teilnahmeprozess näher erläutert und insbesondere technische Kriterien definiert.

1. Erstellung des Testbenutzerkontos

Wie auch im späteren Produktivbetrieb des RDCnet, obliegt die Entscheidung, wie das Benutzerkonto eingerichtet ist (Betriebssystem, Software- und Hardwareausstattung), jedem datengebenden FDZ selbst. Hierbei werden keine Vorgaben durch das RDCnet gemacht. Innerhalb des Pilotnetzwerks sollten jedoch noch keine sensible Daten auf dem Konto abgelegt oder der Zugang zu anderen internen Ressourcen erlaubt werden. Das Testbenutzerkonto sollte nach erfolgreichen Verbindungen durch die anderen FDZ wieder gelöscht werden und kann somit sehr minimal konfiguriert werden. **Wichtig ist jedoch, dass sich das Konto bzw. die virtuelle Maschine, die dem Konto zugewiesen wird, auf dem Horizon Verbindungsserver befindet, der auch im späteren Produktivbetrieb verwendet wird.**

Grundsätzlich kann für das Testbenutzerkonto auf eine Multi-Faktor-Authentifizierung verzichtet werden, um den Verbindungsaufbau für die verschiedenen FDZ zu erleichtern. Falls jedoch eine Multi-Faktor-Authentifizierung eingerichtet sein sollte, ist es zwingend notwendig, die entsprechenden Authentifizierungsinformationen im Teilnahmeformular anzugeben, wie beispielsweise die Benutzerkennung für OTP oder TAN-Liste.

Ergänzung 1: Multifaktor-Authentifizierung im späteren Produktivbetrieb

Gemäß der multilateralen Kooperationsvereinbarung ist jedes FDZ verpflichtet, die Identität von Nutzenden vor Ort zu überprüfen, indem ein Lichtbildausweis kontrolliert wird, bevor diese im Datensicherheitsraum an den GWAP des RDCnet arbeiten können. Diese physische Identitätskontrolle bildet den ersten Sicherheitsfaktor. Nach dieser Kontrolle müssen die Nutzenden innerhalb des VMware Horizon Clients ihren Benutzernamen und ihr Passwort eingeben, die sie vom datengebenden FDZ erhalten haben - dies bildet den zweiten Sicherheitsfaktor. Darüber hinaus kann jedes FDZ selbst entscheiden, ob es dem Nutzer einen zusätzlichen Authentifizierungsprozess einrichtet, wie beispielsweise OTP. Für diesen Faktor werden im RDCnet jedoch keine Vorgaben gemacht, da ausschließlich das datengebende FDZ dafür verantwortlich ist und hierzu keine Informationen mit dem GWAP-stellenden FDZ ausgetauscht werden müssen.

Wenn ein FDZ die Notwendigkeit sieht, einen weiteren Faktor einzurichten, der durch das FDZ-Personal des GWAP-stellenden FDZ getätigt werden muss, wie beispielsweise ein Mitarbeiterpasswort, ist darauf zu achten, dass dem GWAP-stellenden FDZ dadurch kein zusätzlicher Aufwand entsteht, außer der Eingabe des Passworts am Endgerät. Eine Möglichkeit wäre beispielsweise die Nutzung von Token-Generatoren, die durch die datengebenden FDZ eingerichtet und jedem GWAP-stellenden FDZ ausgegeben werden. Auf diese Weise müsste das Personal des GWAP-stellenden FDZ lediglich das am Generator angezeigte Passwort eingeben, ohne dass für dieses FDZ weiterer Aufwand entsteht.

2. Austausch der Verbindungsparameter

Nachdem ein Testbenutzerkonto erstellt wurde, müssen die erforderlichen Verbindungsparameter für den Remote-Access mithilfe des bereitgestellten Teilnahmeformulars dokumentiert werden. Dadurch wird sichergestellt, dass der Austausch dieser Verbindungsparameter standardisiert und gebündelt durchgeführt werden kann.

Das Formular umfasst einen ersten Block (Abb. 2) mit allgemeinen Informationen zum FDZ, die für die Organisation und Kommunikation relevant sind. Darüber hinaus enthält es Angaben, die für die Buchungsplattform erforderlich sind, wie zum Beispiel die Adresse des FDZ, Öffnungszeiten und Dauer der buchbaren Zeitslots. Falls es im Rahmen des Pilotnetzwerks noch nicht möglich ist, den Ansprechpartner für Buchungsbestätigungen und Terminnotation zu benennen, können diese Angaben zu einem späteren Zeitpunkt nachgereicht werden.

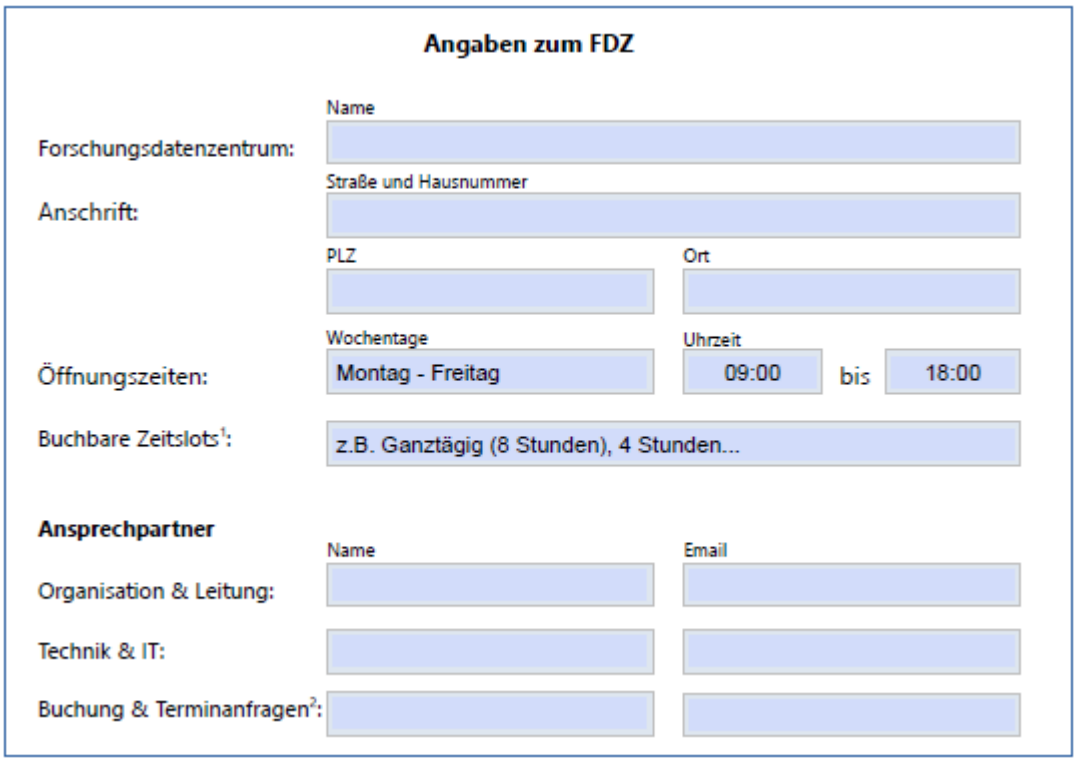


Abbildung 2: Auszug Teilnahmeformular RDCnet

Im zweiten Abschnitt (Abb. 3) des Formulars werden die Informationen zum Horizon Verbindungsserver aufgeführt. Hier ist der Host-Name oder die Host-IP sowie die Ports anzugeben, die bei einer Filterung ausgehender Verbindungen freigegeben werden müssen, damit der Remote Access durchgeführt werden kann. Darüber hinaus ist anzugeben, auf welcher Active Directory-Domäne die Kennungen der Nutzenden hinterlegt sind, falls innerhalb des entsprechenden Horizon Connection Servers mehr als eine Domäne verwendet wird.

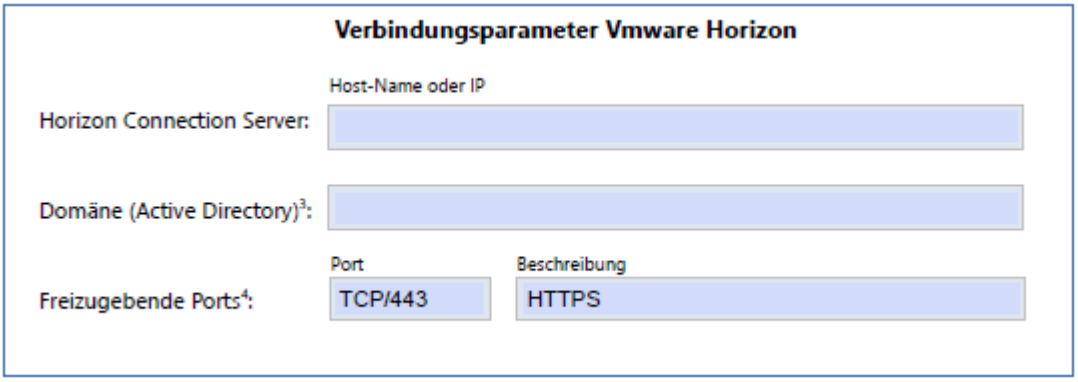


Abbildung 3: Auszug Teilnahmeformular RDCnet

Im dritten Block (Abb. 4) werden Angaben zum Testbenutzer-Konto gemacht, wie zum Beispiel der Benutzername und das Passwort. Falls eine Multi-Faktor-Authentifikation implementiert wurde, müssen die relevanten Informationen hierzu angegeben werden.

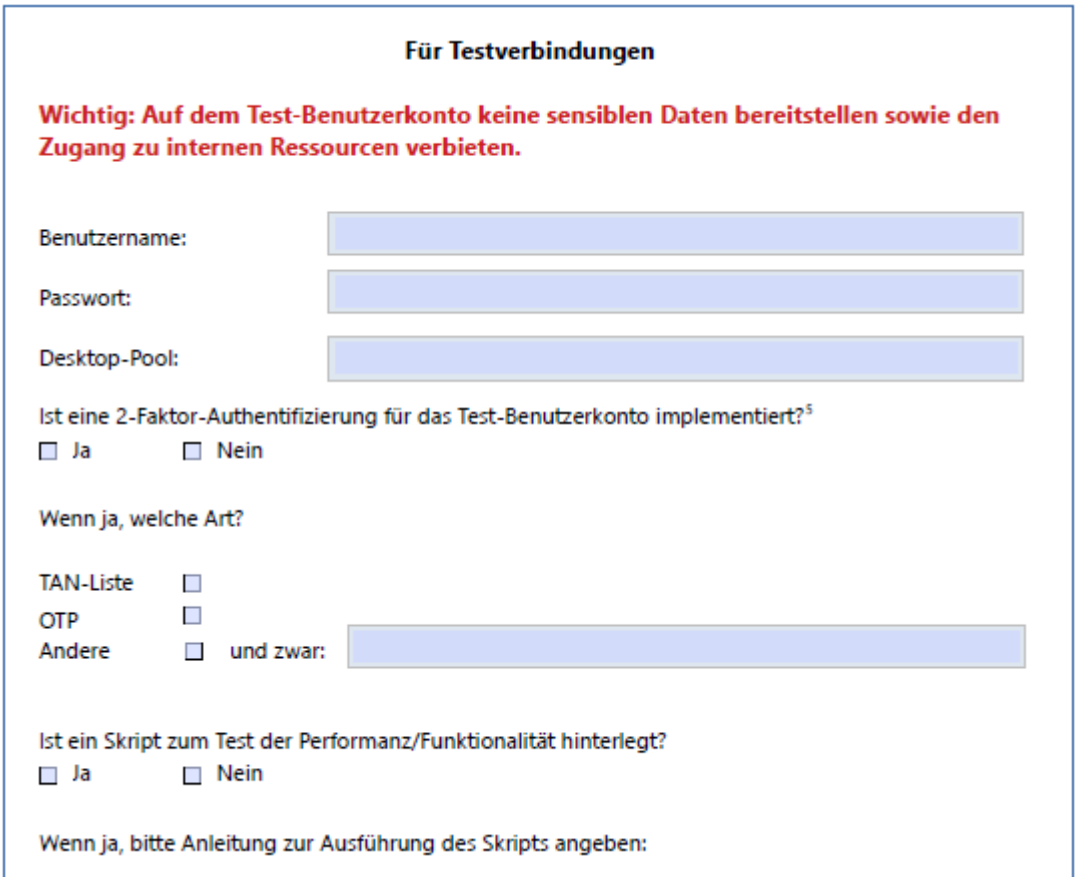


Abbildung 4: Auszug Teilnahmeformular RDCnet

Zuletzt kann der vierte Block (Abb. 5) genutzt werden, um Ergänzungen zu dokumentieren, für die es kein separates Eingabefeld gibt. Dies kann beispielsweise Informationen über eine Multi-Faktor-Authentifizierung durch FDZ-Personal des GWAP-stellenden FDZ betreffen (Siehe „Ergänzung 1“).

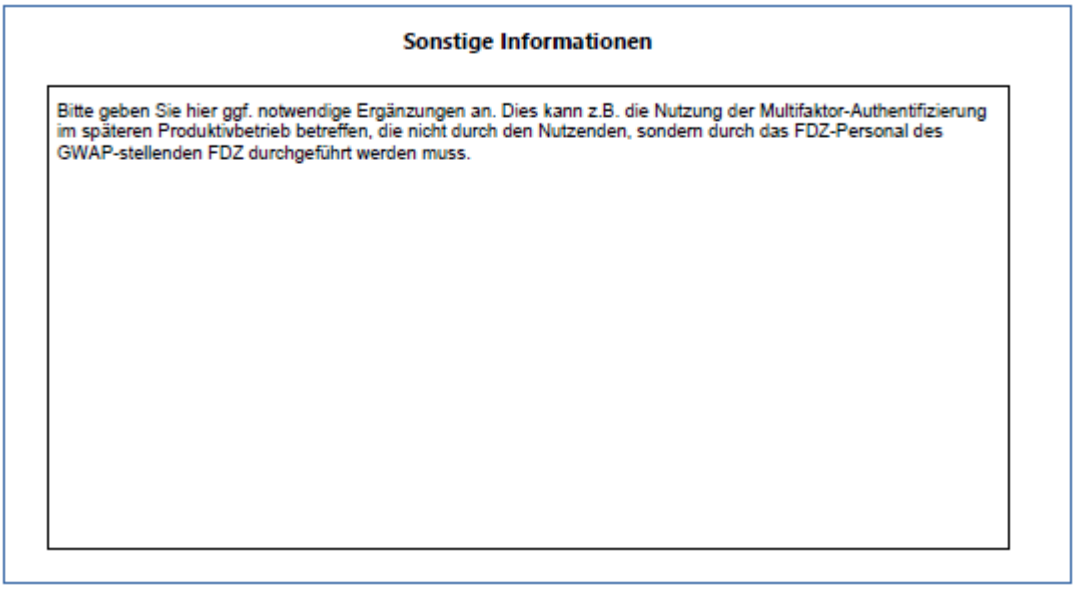


Abbildung 5: Auszug Teilnahmeformular RDCnet

3. Implementierung der Verbindung via VMware Horizon Client

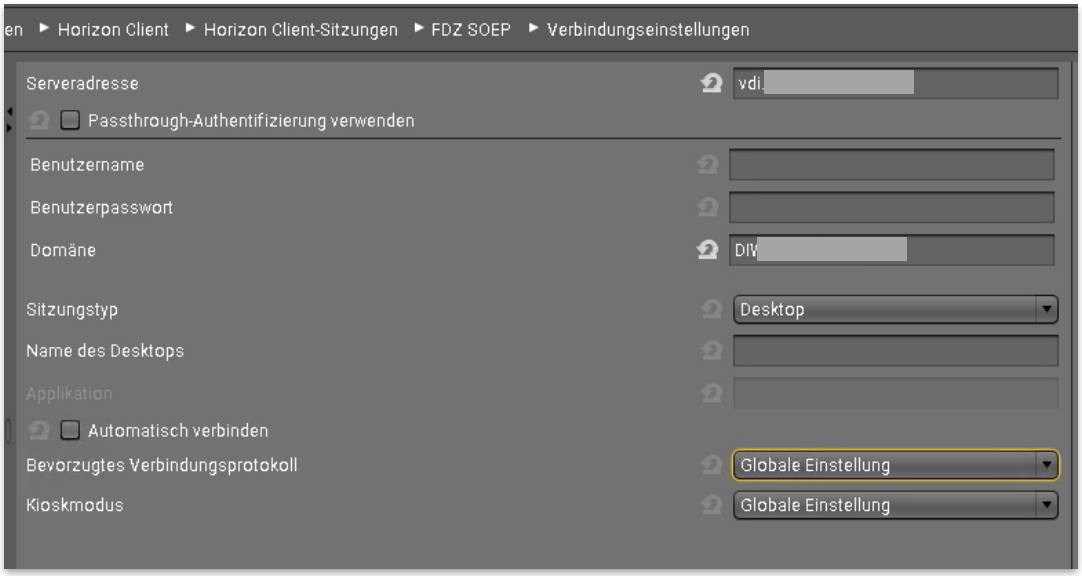
Nachdem einem FDZ die Verbindungsparameter der anderen FDZ auf Basis der Teilnahmeformulare übermittelt wurden, müssen die Verbindungen zu den Connection-Servern an einem Endgerät, z.B. einem Thin-Client, mithilfe des "VMware Horizon Clients" eingerichtet werden. Die Entscheidung bezüglich des genutzten Endgeräts obliegt jedem FDZ selbst, jedoch ist darauf zu achten, dass im späteren Produktivbetrieb des RDCnet die entsprechenden technischen und organisatorischen Maßnahmen (TOM), die in der multilateralen Kooperationsvereinbarung definiert wurden, umgesetzt sind (z.B. Gerät befindet sich in einem Datensicherheitsraum, keine Möglichkeit der lokalen Speicherung, kein Zugang zum Internet, Deaktivierung von USB-Schnittstellen für Speichermedien...). Es empfiehlt sich daher für die FDZ, bereits im Pilotnetzwerk das Endgerät zu nutzen, das auch für das RDCnet im späteren Produktivbetrieb als GWAP reserviert ist.

Ergänzung 2: Verbindungsrestriktion durch IP-Whitelist im Produktivbetrieb

Im Produktivbetrieb des RDCnet sollen nur die von den teilnehmenden FDZ bereitgestellten Endgeräte/GWAP in den Datensicherheitsräumen einen Zugang auf die Connection Server der datengebenden FDZ erhalten. Hierfür muss jedes datengebende FDZ innerhalb ihrer VMware UAG / Firewall eine IP-Whitelist implementieren, die nur die IP-Adressen der zugelassenen Endgeräte beinhaltet. Im Rückschluss bedeutet dies, dass jedes GWAP-stellende FDZ ihrem Endgerät eine statische öffentliche IP-Adresse zuweist, die für den späteren produktivbetrieb des RDCnet mit den Partner FDZ geteilt wird. Da im Rahmen des Pilotnetzwerk noch keine sensiblen Daten verwendet werden und der Fokus darin besteht die Verbindung zu den Horizon Connection-Server zu testen, muss eine solche Restriktion noch nicht umgesetzt werden. Für den Übergang zum Produktivbetrieb ist dieser Faktor jedoch von essentieller Bedeutung und muss im weiteren Verlauf des Projekts noch klarer diskutiert und definiert werden.

Je nach verwendetem Endgerät kann sich die Einrichtung und die Benutzeroberfläche natürlich unterscheiden. Im Folgenden wird am Beispiel eines Thin-Clients der Marke IGEL beispielhaft gezeigt, wie eine Implementierung der entsprechenden Connection Server anderer FDZ aussehen kann.

Abbildung 5: Beispiel Konfiguration von Horizon Sitzungen an einem IGEL Thin-Client



Beispiel: Eine Möglichkeit, diese Verbindungen nutzerfreundlich einzurichten, besteht darin, vorkonfigurierte Sitzungen für jede datengebende FDZ bereitzustellen. Dazu ist es zunächst notwendig, den Hostnamen des Connection Servers, die Domäne (Active Directory Domäne) und den Sitzungstyp anzugeben (Abb. 5).

Daraufhin wird für jede vorkonfigurierte Sitzung ein Icon auf dem Desktop erstellt (Abb. 6). Der spätere Nutzende hat auf dem Thin-Client nur die Möglichkeit, die vordefinierten Sitzungen auszuwählen und sich mit den entsprechenden Anmeldedaten zu authentifizieren. Neben diesen Horizon-Sitzungen hat der Nutzende keine Möglichkeit, andere Software oder Anwendungen auf dem Thin-Client zu starten.

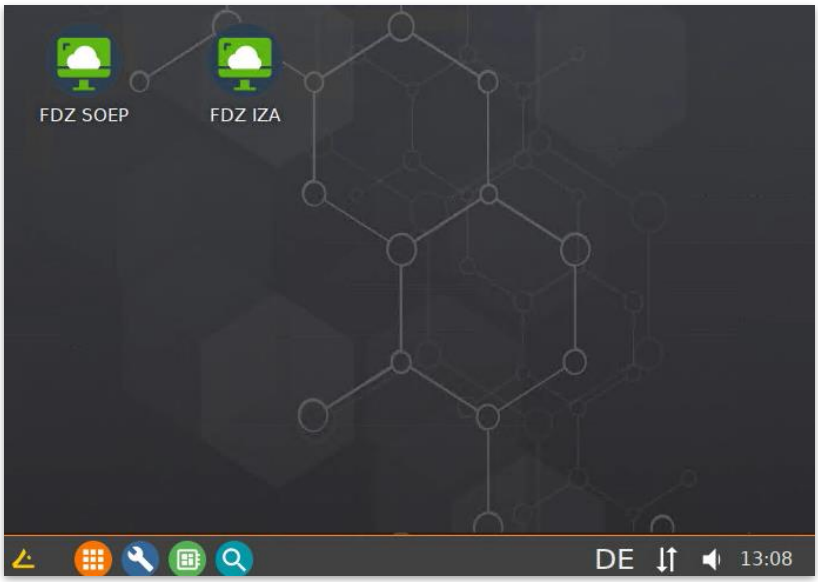


Abbildung 6: Thin-Client Desktop nach Konfiguration der Sitzungen

4. Verbindungsaufbau zu Testbenutzer-Konten

Der letzte notwendige Schritt besteht darin, die Verbindungen zu den Testbenutzerkonten der Partner-FDZ zu überprüfen. Auf Basis der in Schritt 3 definierten Horizon Client Sitzungen sollten nun Anmeldungen mit den im Teilnahmeformular bereitgestellten Benutzerkenndaten der anderen FDZ vorgenommen werden.

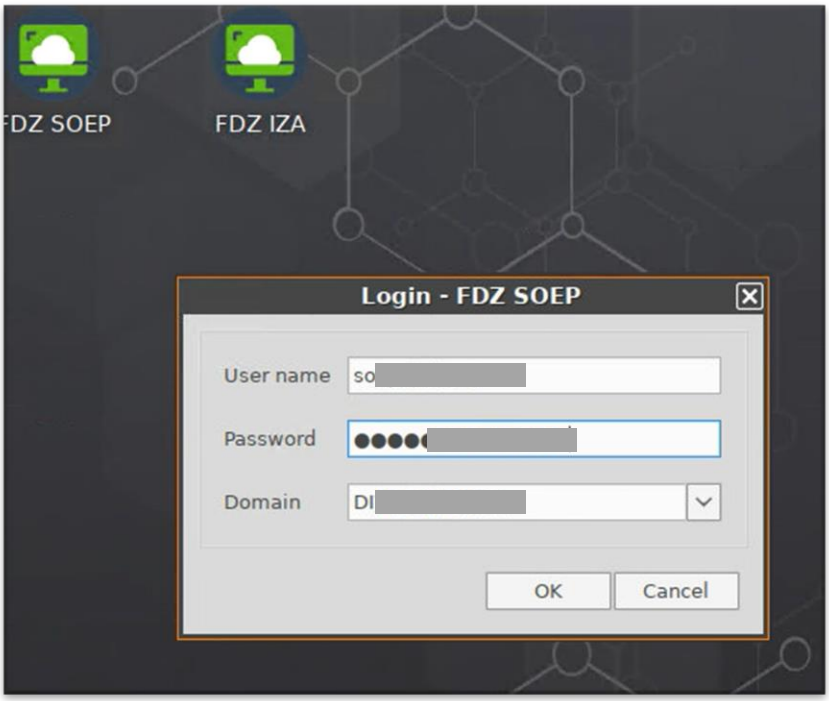


Abbildung 7: Beispiel Anmeldung Testbenutzerkonto via VMware Horizon Client

Da jedes datengebende FDZ selbst für die Performanz der entsprechenden virtuellen Maschinen der Nutzenden verantwortlich ist, wird nicht erwartet, dass die GWAP-stellenden/prüfenden FDZ umfangreiche Performance-Tests durchführen. Sollten allerdings schwerwiegende Probleme hinsichtlich Performanz oder Latenz auftreten, bitten wir darum, diese zu notieren. Nach Durchführung der Testverbindungen wird um Rückmeldung an nmurray@diw.de gebeten. Dabei sollte angegeben werden, ob die Verbindungen zu den einzelnen FDZ erfolgreich waren und falls nicht, welche Probleme aufgetreten sind.

Optional: Die datengebenden FDZ können bei Bedarf ein Testskript bereitstellen, um die Performanz der virtuellen Maschine durch die GWAP-stellenden FDZ prüfen zu lassen. In diesem Fall sollte eine klare Anleitung beigefügt werden, die beschreibt, wie das Skript ausgeführt werden soll, ohne dass die GWAP-stellenden/prüfenden FDZ größere Anpassungen vornehmen müssen. Das entsprechende Vorgehen für die Ausführung des Testskripts kann im Teilnahmeformular unter der Sektion "Testverbindung" angegeben werden.

Impressum

Kontakt:

Neil Murray
SOEP in DIW Berlin
Mohrenstraße 58
10117 Berlin
Webseite
nmurray@diw.de

Berlin, April 2023

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

DOI: 10.5281/zenodo.7895433