KonsortSWD

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

RDCnet

TA2.M2 RDCnet

2. Workshop

Technische Umsetzung

Neil Murray (nmurray@diw.de)
Jan Goebel (jgoebel@diw.de)
Kenny Pedrique (kpedrique@diw.de)

Berlin, 11.08.2022

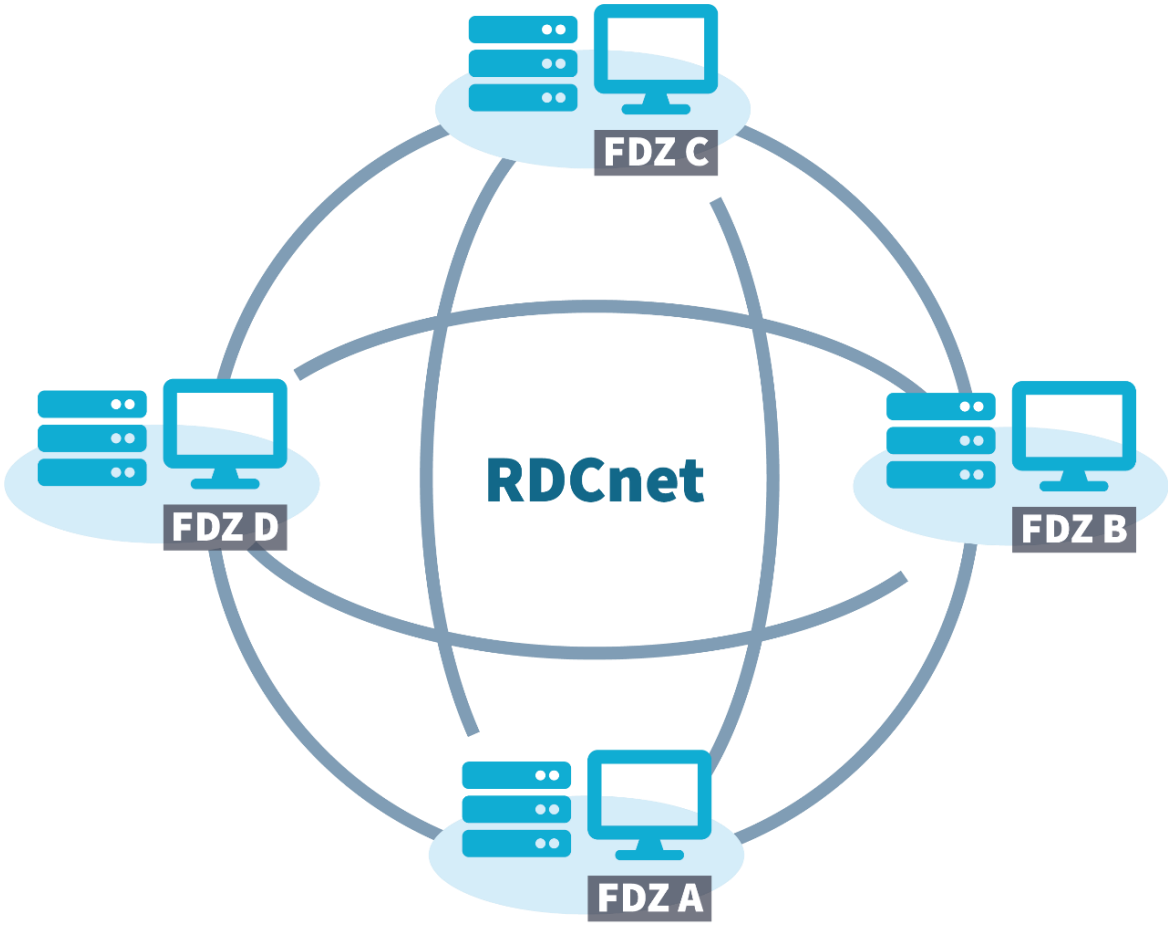
Konzept des RDCnet

Zugang zu sensiblen Daten unabhängig davon, von welchem GWAP aus gearbeitet wird

Jedes FDZ hat die Rolle als „Datenempfänger“und „Datengeber“

Dezentrales System: Daten verlassen zu keinem Zeitpunkt den Server des datenanbietenden FDZ

RDCnet schafft die Vertrauensbasis durch sicherere GWAP und definiert Vorgaben für ein kompatibles Netzwerk



Vertragliche Grundlagen

Kooperationsvereinbarung

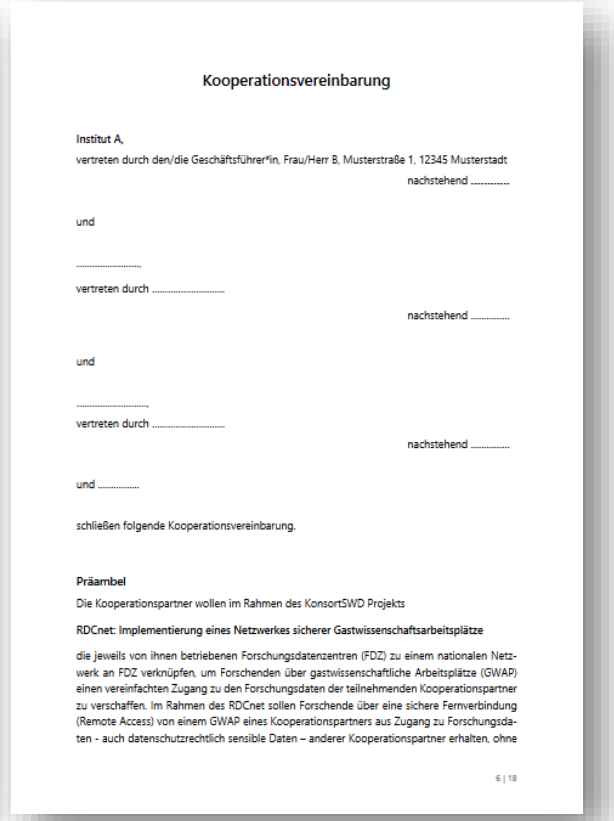
Technische und organisatorische Maßnahmen zum Schutz der GWAP

Prozessbeschreibung zur Nutzung des RDCnet

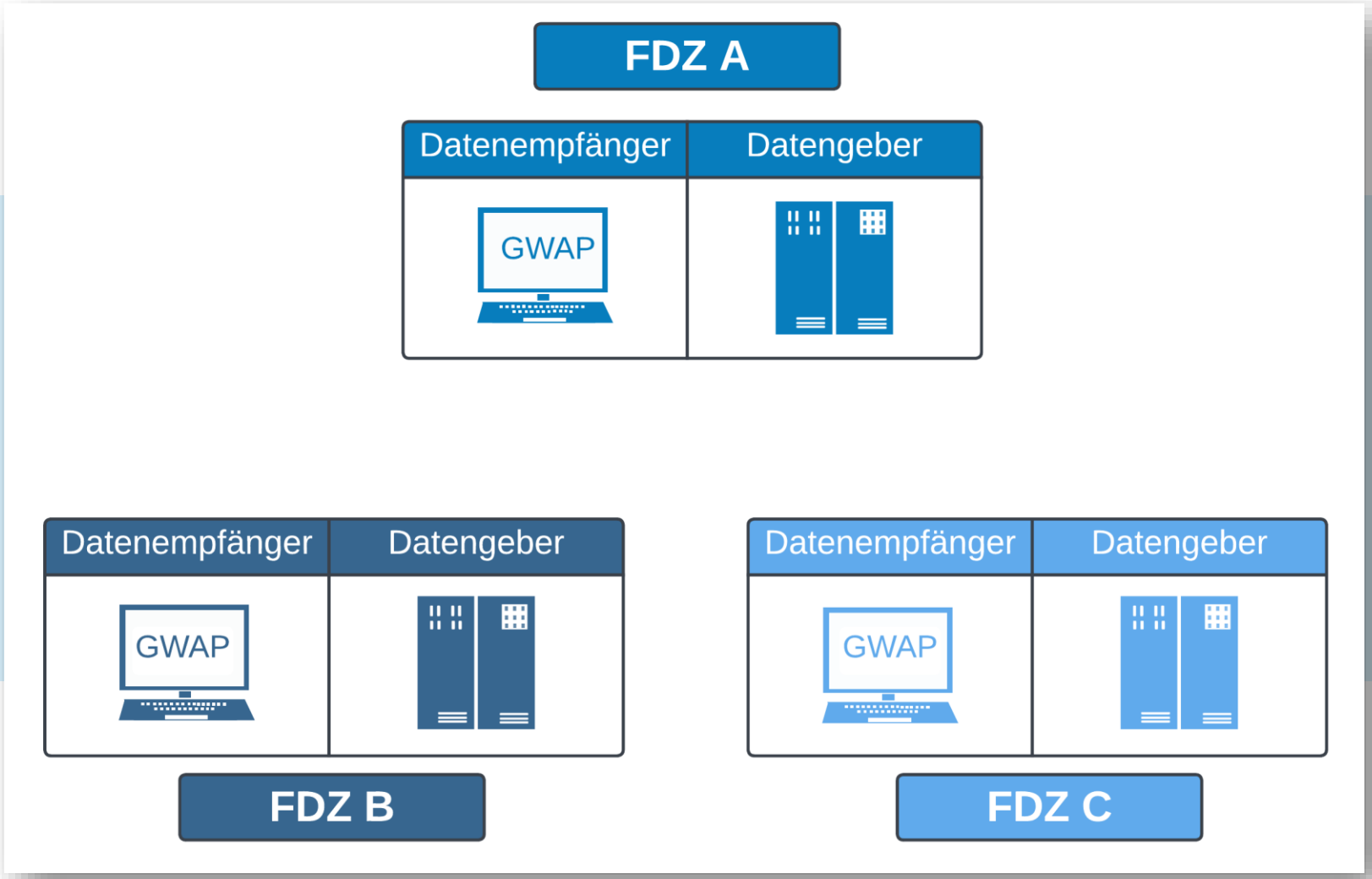
Vertragliche Grundlagen werden erst mit Veröffentlichung des RDCnet bindend

Veröffentlicht als Working Paper:

https://zenodo.org/record/6358334

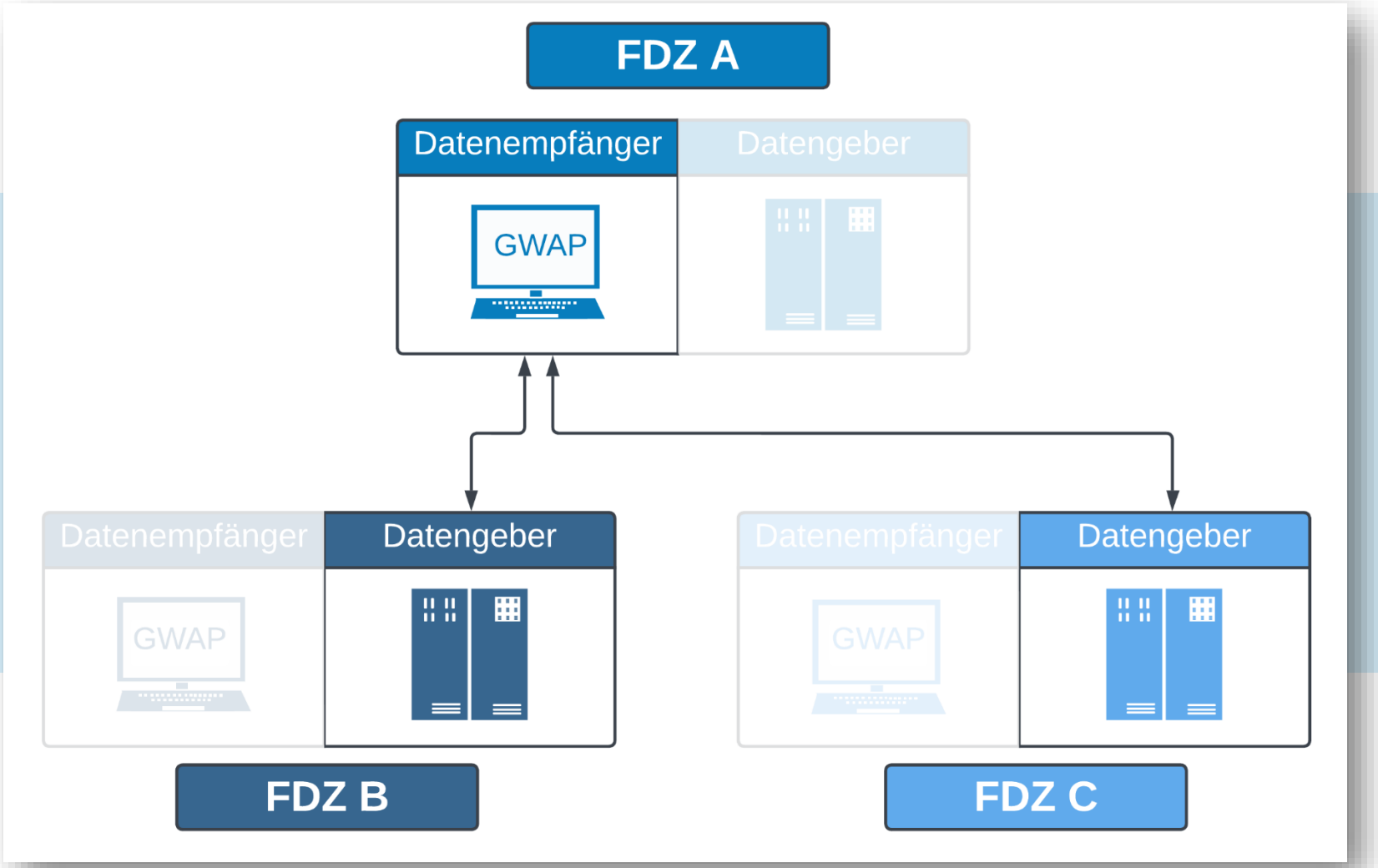


Netzwerk-Struktur



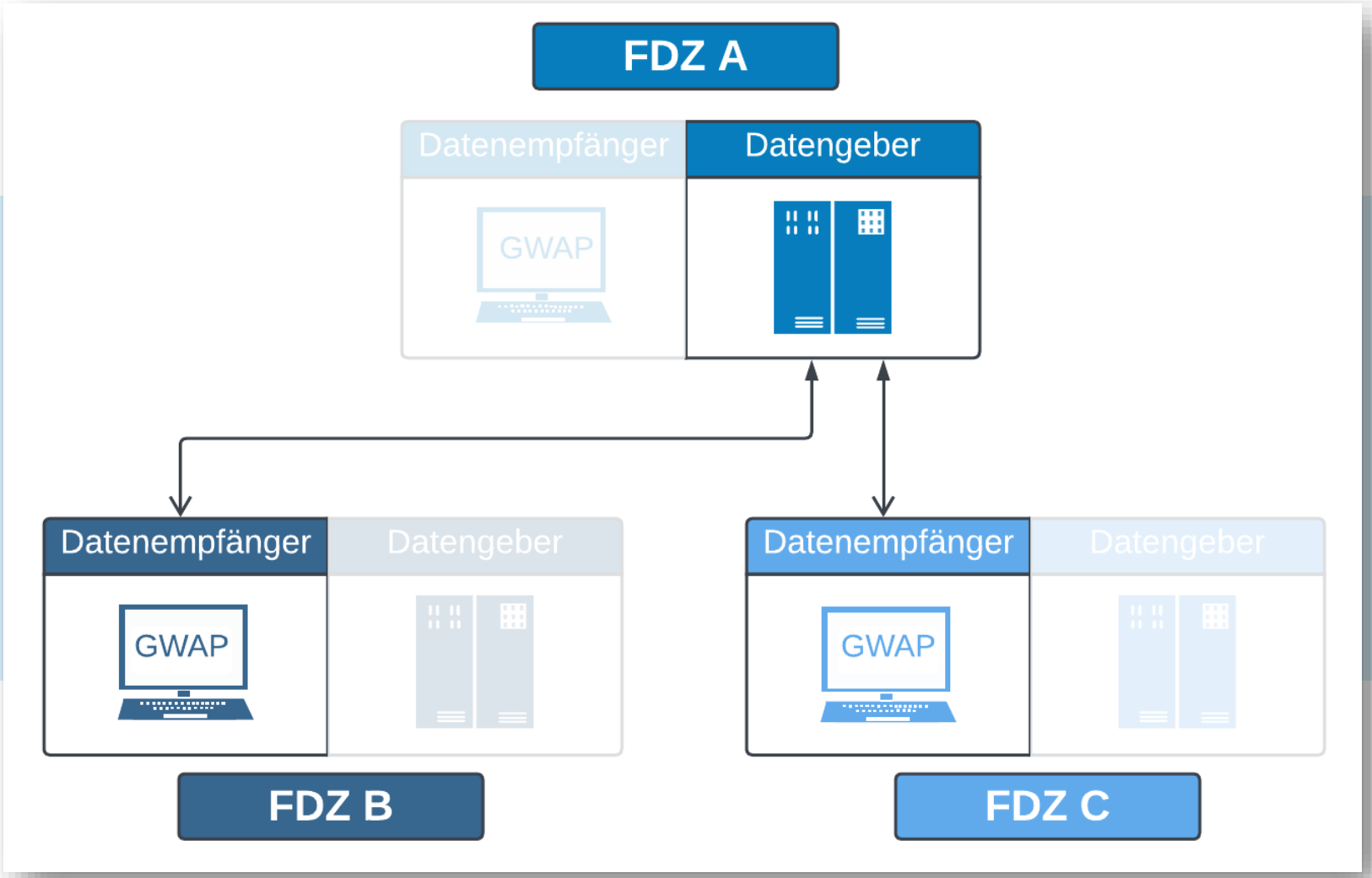
Grafik 1: Netzwerkstruktur RDCnet: Allgemein
Quelle: Eigene Darstellung

Netzwerk-Struktur



Grafik 2: Netzwerkstruktur RDCnet: FDZ A -> FDZ B & FDZ C
Quelle: Eigene Darstellung

Netzwerk-Struktur



Grafik 3: Netzwerkstruktur RDCnet: FDZ B -> FDZ A & FDZ C
Quelle: Eigene Darstellung

Aufgaben & Herausforderungen

Datenempfänger

- Umsetzung TOM
- Konfiguration Thin Client
- Konfiguration VPN Tunnel
- Remote Desktop Software (Client)

Datengeber

- Remote Desktop Software (Server)
- Konfiguration VPN Tunnel
- Bereitstellung Software
- Bereitstellung Hardware

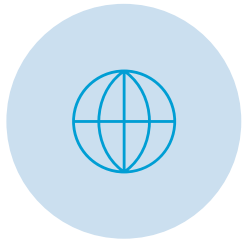
Vereinheitlichung
vs.
Freie Umsetzung

Einheitliche Remote Desktop Software:
VMware Horizon 8 oder Citrix

VMware Horizon & Citrix

- FDZ wählen zur Umsetzung einer Remote Desktop Infrastruktur entweder VMware Horizon oder Citrix

- RDCnet bietet Guide und Support nur für die Umsetzung von **VMware Horizon** da:



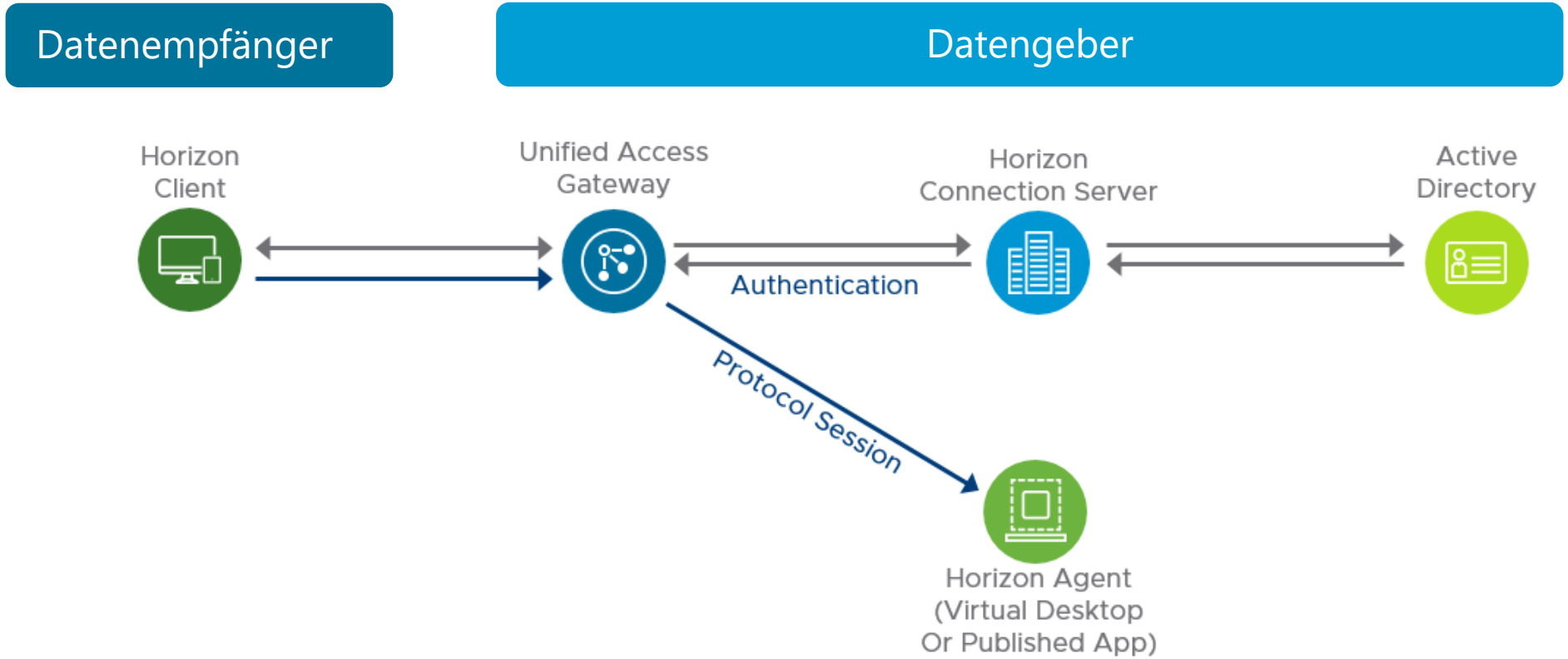
Weit verbreitet: VMware Horizon wird bereits von einer Vielzahl an FDZ genutzt (EcoSoc Workshop „Remote Access“ 17.02.2022)

Kosten: Langfristig geringere Kosten (Keine zusätzliche Lizenzen für Komponenten oder Fachpersonal)

Umsetzbarkeit: Geringere Komplexität und einfachere Umsetzung gegenüber Citrix z.B. UAG vs. Citrix Gateway

Robust: Weniger Fehleranfällig und leichtere Wartung

VMware Horizon: Kernkomponenten



Grafik 4: Core Components VMware Horizon for external access
Quelle: https://techzone.vmware.com/resource/horizon-architecture#architectural-overview (fig 2)

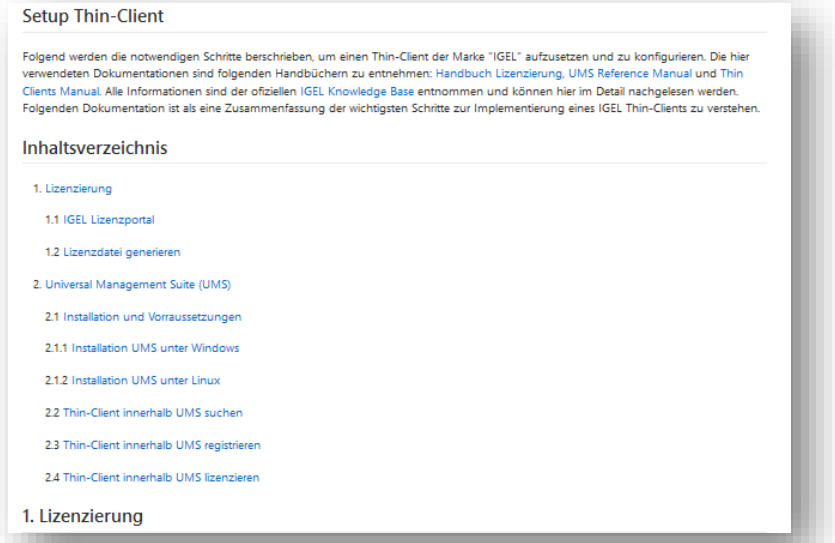
Datenempfänger: Übersicht Aufgaben

1. Jedes FDZ setzt die vertraglich definierten TOM's der GWAP selbstständig um

2. Die Wahl und Konfiguration des Thin-Clients obliegt jedem FDZ selbst. **Voraussetzung: Kompatibilität mit VMware Horizon Client / Citrix Workspace**

3. Verbindung zu anderen FDZ definieren

Falls keine Expertise mit Thin Clients/GWAP: **Bereitstellung eines Guides zur Implementierung von IGEL Thin Clients**


Setup Thin-Client

Folgend werden die notwendigen Schritte berschrieben, um einen Thin-Client der Marke "IGEL" aufzusetzen und zu konfigurieren. Die hier verwendeten Dokumentationen sind folgenden Handbüchern zu entnehmen: Handbuch Lizenzierung, UMS Reference Manual und Thin Clients Manual. Alle Informationen sind der oficiellen IGEL Knowledge Base entnommen und können hier im Detail nachgelesen werden. Folgenden Dokumentation ist als eine Zusammenfassung der wichtigsten Schritte zur Implementierung eines IGEL Thin-Clients zu verstehen.

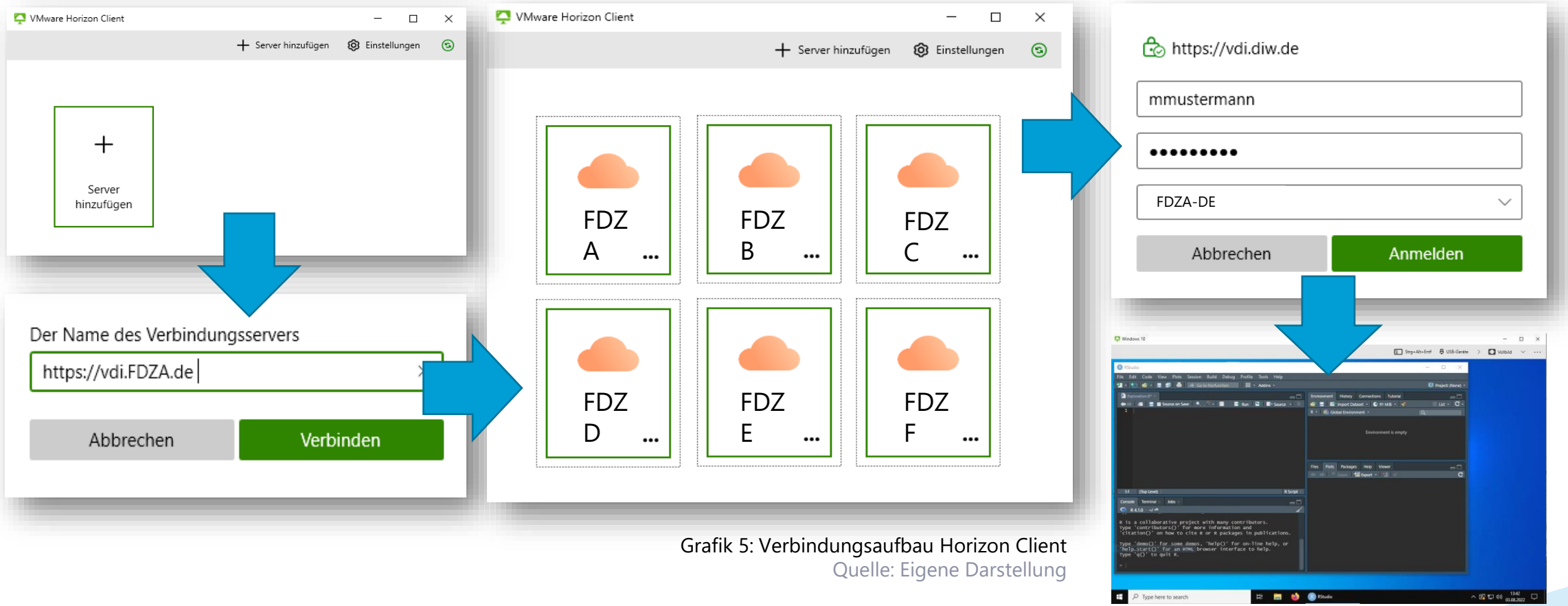
Inhaltsverzeichnis

1. Lizenzierung

Grafik 4: Guide zur Implementierung von IGEL Thin-Clients
Quelle: Eigene Darstellung

Datenempfänger: Horizon Client

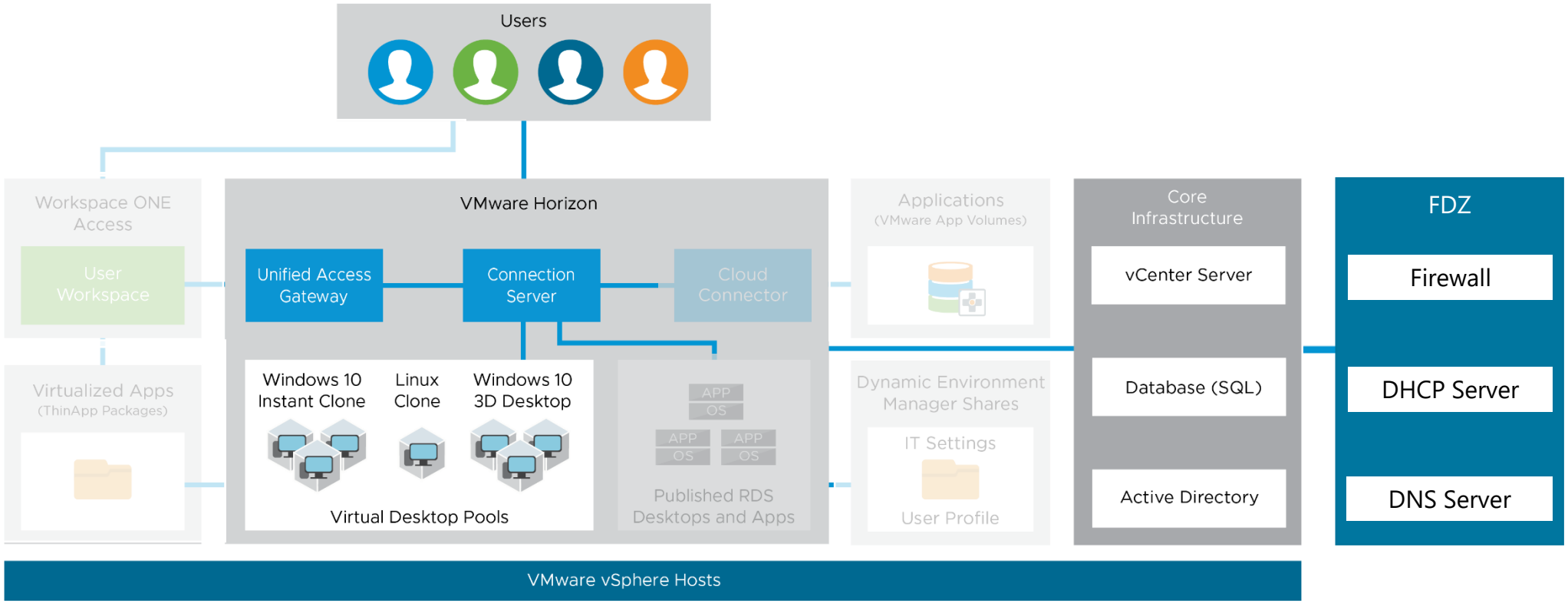
Verbindung zu anderen FDZ definieren:



Grafik 5: Verbindungsaufbau Horizon Client
Quelle: Eigene Darstellung

Datengeber: Anforderung

Implementierung der VMware Horizon Infrastruktur:



Grafik 6: Logical Architecture Horizon
Quelle: https://techzone.vmware.com/resource/horizon-architecture#architectural-overview (fig 3)

Datengeber: Anforderung

Implementierung der VMware Horizon Infrastruktur:

Connection Server

- Authentifiziert Nutzende via Active Directory
- Leitet Anfrage an passende VM (Virtual Machine) weiter und stellt Verbindung her
- Installation auf Windows Server

Unified Access Gateway

- Fungiert als Sicherheitsgateway und ermöglicht den sicheren Fernzugriff von einem externen Netzwerk auf interne Ressourcen
- Virtuelle Applikation die über vCenter implementiert wird.

vCenter Server

- Zentrale Administrationsplattform
- „All in one“
- Konfiguration Virtual Desktop Pool
- Installation UAG

Virtual Desktop Pool

- Virtuelle Maschinen, die den Nutzenden bereitgestellt werden
- Linux oder Windows Gast-OS
- Dynamische Hardwarezuweisung

Active Directory

- Windows Active Directory
- Usermanagement und Gruppen

Database SQL

- Microsoft SQL-Server
- Eventdatenbank

Datengeber: Hardware

Empfohlene Hardwareanforderung für VMware Horizon 8 Infrastruktur:

Komponente	Arbeitsspeicher	CPU (>2 Ghz)	Festplatte
Vcenter Server[1]	12 GB	2 Kerne	580 GB
VM Horizon Connection Server[2]	10 GB	4 Kerne	40 GB
UAG[3]	4 GB	2 Kerne	50 GB
ESXI	8 GB	4 Kerne	128 GB
Zwischensumme	**34 GB**	**12 Kerne**	**798 GB**
Virtuelle Maschinen[4]	92 GB	8 Kerne	1.500 GB
Active Directory/DNS	2 GB	4 Kerne	256 GB
Gesamt	**128 GB**	**24 Kerne**	**2.554 GB**

[1] Bis zu 10 Hosts oder 100 virtuelle Maschinen
[2] Bereitstellungen von 50 oder mehr Remote-Desktops
[3] Einsatz mit bis zu 2.000 Horizon-Verbindungen
[4] Abhängig von bereitgestellter Rechenleistung (für Nutzende)

Tabelle 1: Hardware Anforderungen
Quelle: Eigene Darstellung auf Basis https://docs.vmware.com/de/

Kostenkalkulation

Direkte Kosten bei nicht vorhandener Ausstattung:

Produkt	Fixkosten	Jährliche Kosten	Kostenmodul
Igel UD3 M350C	524 €	-	**Thin Client**
IGEL Workspace Edt. OS 11	-	125 €	
IGEL Workspace Maintenance	-	27 €	
VMware Horizon 8[1]	-	1.436€ – 3.445 €	**VMware**
Windows Server 2022 Standard Edition[2]	1.308€	-	**Windows**
Server Hardware[3]	8.625 €	-	**Server**
Summe	**10.832 €**	**1.588-3.597€**	

[1] Lizenzen für 10 Concurrent Users (CCU):
- Horizon Standard (Linux) – 1.436,94 €
- Horizon Standard (Windows) – 1.610,25 €
- Horizon Enterprise – 3.445,59 €

[2] Bis zu 2 VM und 24 Core Lizenzierung
[3] Dell Rack Server, 128GB Arbeitsspeicher, 24 CPU-Kerne, 2,4 TB Festplatte

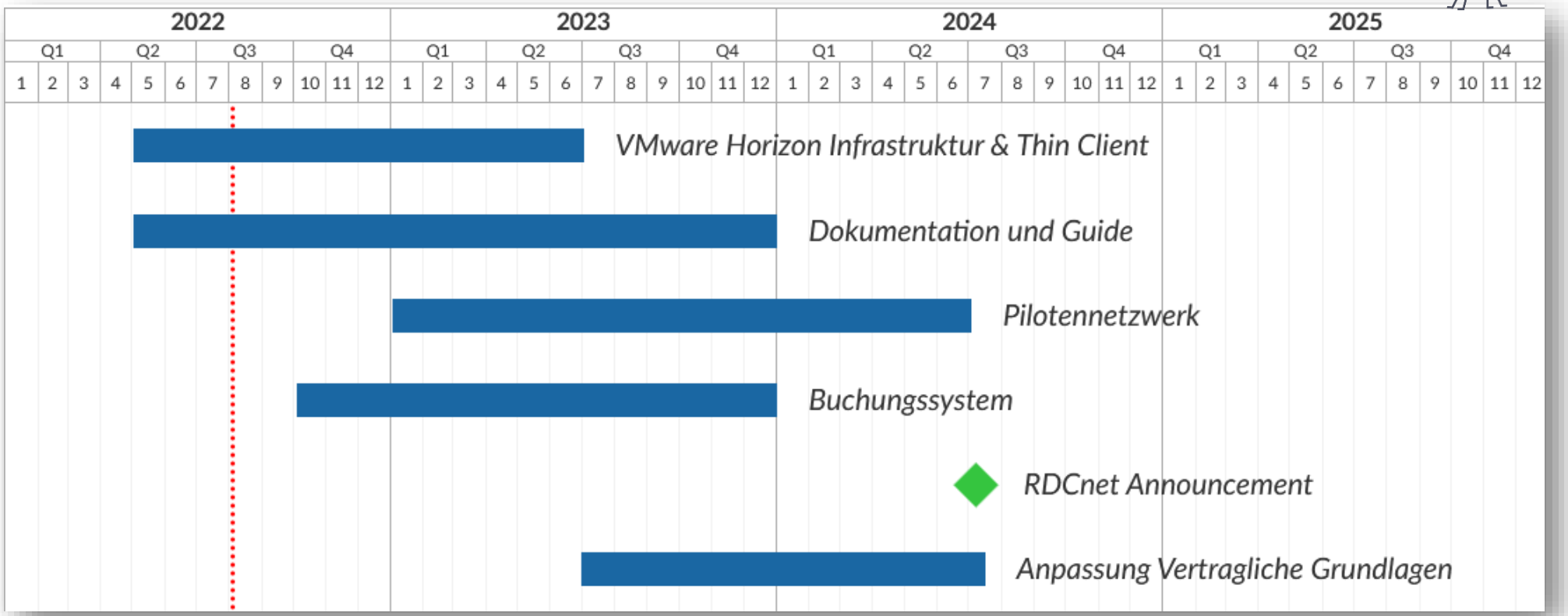
Tabelle 2: Kostenkalkulation
Quelle: Eigene Darstellung auf Basis von:
https://www.software-express.de/hersteller/vmware/horizon/ (02.08.2022)
https://www.bechtle.com/shop/igel-ud3-lx-m350c-4-8-gb-os11--4448220--p (02.08.2022)
https://www.software-express.de/hersteller/microsoft/windows-server/standard-2022/ (04.08.2022)
https://www.dell.com/de-de/shop (09.08.2022)

Kostenkalkulation

Weitere Kosten

- Kosten für Räumlichkeit (Datensicherheitsraum mit GWAP)
- Personalkosten für IT-Setup, Nutzermanagement und Support
- Lizenzkosten: Gast OS, Software für Nutzende, Firewall
- Sonstiges: Tastatur, Bildschirm, Maus, Headset….

Roadmap



Grafik 7: Gantt Chart RDCnet Roadmap
Quelle: Eigene Darstellung mit OpenProject

Fazit

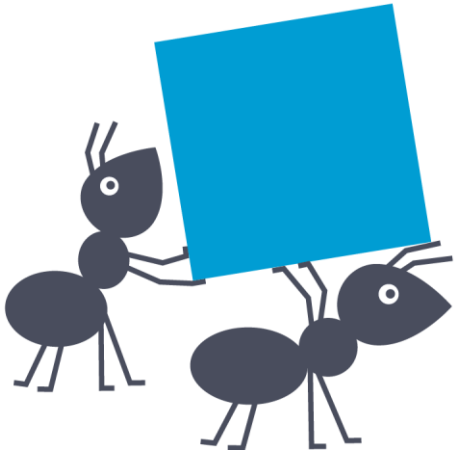
Datenempfänger

- Setzen TOM selbstständig um
- Konfigurieren Thin-Client selbständig (Guide für die Implementierung eines IGEL Thin-Clients wird innerhalb des RDCnet bereitgestellt)
- Voraussetzung Thin-Client: Kompatibilität mit „VMware Horizon Client“ und „Citrix Workspace“
- Definiert Verbindungen zu anderen FDZ innerhalb der Remote Desktop Software

Datengeber

- Implementiert Infrastruktur zum hosten von Remote Desktops im eigenen FDZ
- Nutzung von:
  - VMware Horizon 8 (Guide und Support wird innerhalb des RDCnet bereitgestellt), oder
  - Citrix

Vielen Dank für Ihre Aufmerksamkeit



Gute Zusammenarbeit startet im Kleinen

KonsortSWD wird Rahmen der NFDI durch die Deutsche Forschungsgemeinschaft (DFG) gefördert - Projektnummer: **442494171**

Appendix: Alternative VDI Lösungen

VMware:

- VMware Horizon View ist die verbreitetste Lösung für eine virtuelle Infrastruktur
- Idealer Mittelweg aus Benutzerfreundlichkeit und Performance
- Dafür ist das System weniger flexibel
- VMware bietet eine **bessere Storage-Verwaltung**, was Performance-Flaschenhälsen vorbeugt, wenn gleichzeitig viele Nutzer anspruchsvolle Anwendungen ausführen.

Sonstige: Es gibt **kostenlose Lösungen**, die allerdings weder technisch noch rechtlich den Anforderungen eines mittelständischen Unternehmens entsprechen. Entweder sind sie **zu unflexibel, zu unsicher oder einfach nicht stabil und ausgereift** genug.

Quelle: 1) https://sentinel-it.de/desktop-virtualisierung-mit-citrix-und-vmware-horizon-was-ist-besser-fuer-ihr-unternehmen/
2) https://wire19.com/vdi-options-compared-vmware-horizon-vs-citrix/
3) https://www.cbtnuggets.com/blog/technology/system-admin/vdi-infrastructure-citrix-vs-vmware
4) https://www.appsanywhere.com/resource-centre/vdi/citrix-vdi-vs-vmware-vdi-what-are-the-differences-and-benefits-of-each

Appendix: Alternative VDI Lösungen

Citrix

- Mehr Funktionen und Verwaltungsoptionen
- Detailliertere Anpassungen der Desktop-Umgebung
- Kompliziertere Bereitstellung (Bsp. Citrix Gateway vs. UAG: benötigt eigene Lizenzen und spezifisches Personal)
- Langfristig teurer in der Wartung
- „Für mittelständische Unternehmen ist dieses VDI-Programm (Citrix) etwas überdimensioniert und Sie brauchen Fachpersonal, um die ganze Bandbreite der Funktionen sinnvoll zu nutzen.“

Quelle: 1) https://sentinel-it.de/desktop-virtualisierung-mit-citrix-und-vmware-horizon-was-ist-besser-fuer-ihr-unternehmen/
2) https://wire19.com/vdi-options-compared-vmware-horizon-vs-citrix/
3) https://www.cbtnuggets.com/blog/technology/system-admin/vdi-infrastructure-citrix-vs-vmware
4) https://www.appsanywhere.com/resource-centre/vdi/citrix-vdi-vs-vmware-vdi-what-are-the-differences-and-benefits-of-each

Appendix

- Core Components VMware Horizon:

Component	Description
Connection Server	The Horizon Connection Server securely brokers and connects users to the Horizon Agent that has been installed in the desktops and RDS Hosts. The Connection Server authenticates users through Active Directory and directs the request to the appropriate and entitled resource.
Horizon Agent	The Horizon Agent is installed on the guest OS of target VM or system. This agent allows the machine to be managed by Connection Servers and allows a Horizon Client to form a protocol session to the machine. Machines can be virtual desktops, Remote Desktop Session Hosts (RDS Host), physical desktops PCs.
Horizon Client	The Horizon Client is installed on a client device to access a Horizon-managed system that has the Horizon Agent installed. You can optionally use a web browser as an HTML client for devices on which installing client software is not possible.

Quelle: https://techzone.vmware.com/resource/horizon-architecture#components

Appendix

- Core Components VMware Horizon:

Unified Access Gateway	VMware Unified Access Gateway is a virtual appliance that enables secure remote access from an external network to a variety of internal resources, including Horizon-managed resources. When providing access to internal resources, Unified Access Gateway can be deployed within the corporate DMZ or internal network and acts as a reverse proxy host for connections to your company's resources. Unified Access Gateway directs authenticated requests to the appropriate resource and discards any unauthenticated requests. It also can perform the authentication itself, leveraging an additional layer of authentication when enabled. (See Unified Access Gateway Architecture for design and implementation details.)
Horizon Console	A web application that is part of the Connection Server, allowing administrators to configure the server, deploy and manage desktops, control user authentication, initiate and examine system and user events, carry out end-user support, and perform analytical activities.

Quelle: https://techzone.vmware.com/resource/horizon-architecture#components

Appendix

- Core Components VMware Horizon:

VMware Instant Clone Technology	VMware technology that provides single-image management with automation capabilities. You can rapidly create automated pools or farms of instant-clone desktops or RDSH servers from a golden image VM. The technology reduces storage costs and streamlines desktop management by enabling easy updating and patching of hundreds or thousands of images from the golden image VM. See the Instant Clone Smart Provisioning section for more information.
RDSH servers	Microsoft Windows Servers that provide published applications and session-based remote desktops to end users.
Enrollment Server	Server that delivers True SSO functionality by ensuring a user can single-sign-on to a Horizon resource when launched from Workspace ONE Access™, or through Unified Access Gateway, regardless of the authentication method. See the True SSO section for more information.

Quelle: https://techzone.vmware.com/resource/horizon-architecture#components

Appendix

- Core Components VMware Horizon:

Horizon Cloud Connector	The Horizon Cloud Connector is required to use with Horizon subscription licenses, services and management features hosted in the Horizon Control Plane Services. The Horizon Cloud Connector is a virtual appliance that connects a Connection Server in a pod with the Horizon Cloud Service. You must have an active VMware Customer Connect account to purchase a Horizon license from https://customerconnect.vmware.com/.
vSphere	The vSphere product family includes VMware ESXi™ and VMware vCenter Server®, and it is designed for building and managing virtual infrastructures. The vCenter Server system provides key administrative and operational functions, such as provisioning, cloning, and VM management features, which are essential for VDI.

Quelle: https://techzone.vmware.com/resource/horizon-architecture#components

Appendix

Optional Components VMware Horizon:

- **Workspace ONE Access** – Provides enterprise single sign-on (SSO), securing and simplifying access to apps with the included identity provider or by integrating with existing identity providers. It provides application provisioning, a self-service catalog, conditional access controls, and SSO for SaaS, web, cloud, and native mobile applications. See Workspace ONE Access Architecture for design and implementation details.
- **App Volumes Manager** – Orchestrates application delivery by managing assignments of application volumes (packages and writable volumes) to users, groups, and target computers. See App Volumes Architecture for design and implementation details.
- **Dynamic Environment Manager** – Provides profile management by capturing user settings for the operating system and applications. See Dynamic Environment Manager Architecture for design and implementation details.
- **VMware vSAN™ storage** – Delivers high-performance, flash-optimized, hyper-converged storage using server-attached flash devices or hard disks to provide a flash-optimized, highly resilient, shared datastore.
- **VMware NSX-T Data Center** – Provides network-based services such as security, virtualized networking, routing, and switching in a single platform. With micro-segmentation, you can set application-level security policies based on groupings of individual workloads, and you can isolate each virtual desktop from all other desktops as well as protecting the Horizon management servers.
- **Database Servers** – Microsoft SQL servers or PostgreSQL servers are used to host an event database used by the Connection Servers.

Quelle: https://techzone.vmware.com/resource/horizon-architecture#components

Appendix

UAG vs VPN:

Unified Access Gateway und generische VPN-Lösungen ähneln sich, da beide sicherstellen, dass Datenverkehr nur für sicher authentifizierte Benutzer in ein internes Netzwerk weitergeleitet wird.

Unified Access Gateway bietet im Vergleich zu einem generischen VPN die folgenden Vorteile.

• Access Control Manager Unified Access Gateway wendet Zugriffsregeln automatisch an. Unified Access Gateway erkennt die Berechtigungen der Benutzer und die zur internen Verbindung erforderliche Adressierung. Ein VPN erreicht dasselbe, da bei den meisten VPNs ein Administrator Netzwerkverbindungsregeln für jeden Benutzer oder jede Benutzergruppe einzeln konfigurieren kann. Dies funktioniert zwar zunächst recht gut mit einem VPN, die Verwaltung der erforderlichen Regeln bringt aber erheblichen administrativen Arbeitsaufwand mit sich.

• Benutzeroberfläche Unified Access Gateway nimmt keine Änderungen an der unkomplizierten Benutzeroberfläche von Horizon Client vor. Mit Unified Access Gateway befinden sich authentifizierte Benutzer beim Start des Horizon Clients in ihrer Horizon Connection Server-Umgebung und haben kontrollierten Zugriff auf ihre Desktops und Anwendungen. **Bei einem VPN müssen Sie zunächst die VPN-Software einrichten und dann separat die Authentifizierung durchführen, bevor der Horizon Client gestartet wird.**

Quelle: https://docs.vmware.com/de/Unified-Access-Gateway/3.3.1/com.vmware.uag-331-deploy-config.doc/GUID-56BBCAD6-F0CE-4DD9-9750-16158E134C52.html

Appendix

UAG vs VPN:

• Leistung Unified Access Gateway ist für maximale Sicherheit und Leistung konzipiert. Mit Unified Access Gateway sind PCoIP-, HTML Access- und WebSocket-Protokolle ohne zusätzliche Kapselung gesichert. VPNs werden als SSL-VPNs implementiert. Diese Implementierung entspricht den Sicherheitsanforderungen und gilt bei aktiviertem TLS (Transport Layer Security) als sicher, aber das zugrunde liegende Protokoll bei SSL/TLS ist lediglich TCP-basiert. Da moderne Video-Remoting-Protokolle verbindungslose UDP-basierte Transporte nutzen, können die Leistungsvorteile bei Durchsetzen eines TCP-basierten Transports erheblich gemindert werden. Dies gilt nicht für alle VPN-Technologien, da diejenigen, die mit DTLS oder IPsec anstelle von SSL/TLS betrieben werden können, gut mit Horizon Connection Server-Desktop-Protokollen funktionieren können.

Quelle: https://docs.vmware.com/de/Unified-Access-Gateway/3.3.1/com.vmware.uag-331-deploy-config.doc/GUID-56BBCAD6-F0CE-4DD9-9750-16158E134C52.html