

Kapitel 4:

Zugriffskonzept

Einleitung

Dieses Kapitel beschreibt das Zugriffskonzept zum digitalen Zwilling. Ziel ist es, einen klar strukturierten Überblick über mögliche Zugriffsszenarien zu geben und Verantwortlichkeiten eindeutig darzustellen.

Motivation und Bedarf

Die zunehmende Vernetzung im Industrial Metaverse erfordert klare Regelungen zum Zugriff auf digitale Ressourcen

Unterschiedliche Rollen benötigen differenzierte Rechte. Von vollständiger Administration über Partnerzugriffe bis hin zu reinen Visualisierungen für externe Interessierte. Dieses Kapitel beschreibt die technischen und organisatorischen Maßnahmen, die diesen Bedarf abdecken.

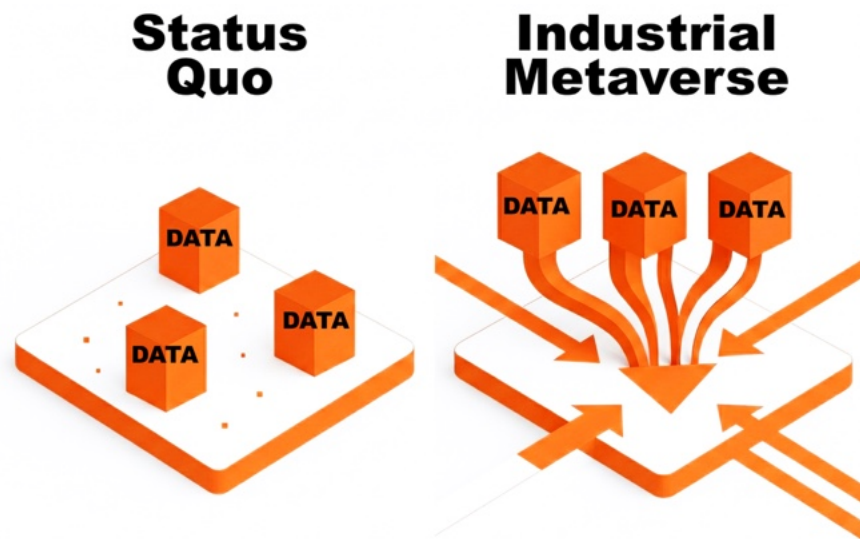


ABBILDUNG 5 HERAUSFORDERUNGEN BEI DER DATENVERWALTUNG

Zugriffsszenarien

Use Case 1: Direkter Zugriff (Remote-Desktop und Vor-Ort-Server)

Dieser Anwendungsfall betrifft **den direkten Zugriff auf einen Server oder eine Workstation über Remote-Desktop oder direkt vor Ort**. Dies ist die höchste Zugriffsebene und wird nur Personen mit umfassender technischer Verantwortung gewährt. Dazu zählen Aufgaben wie das Erstellen neuer Assets für das gesamte digitale Zwillingmodell (z. B. Rhino-Lizenzen auf der Workstation) sowie die Konfiguration und Verwaltung zentraler Nucleus-Tools, Backups und Wartung.

- **Technik:** Nutzer auf dieser Ebene haben vollen Zugriff auf Management- und Infrastrukturwerkzeuge. Der Zugriff wird einem kleinen Kreis von Personen zugewiesen, die Konfigurationen und Wartungsaufgaben durchführen, Checkpoints erstellen und sicherstellen, dass zentrale Elemente des digitalen Zwillings für andere Partner zugänglich bleiben.
- **Zugriff für:** Administratoren und zentrale technische Manager.
- **Vorteile:** Volle Kontrolle und direkte Administration.
- **Zugangsverantwortliche:** IT-Administrationsteam.

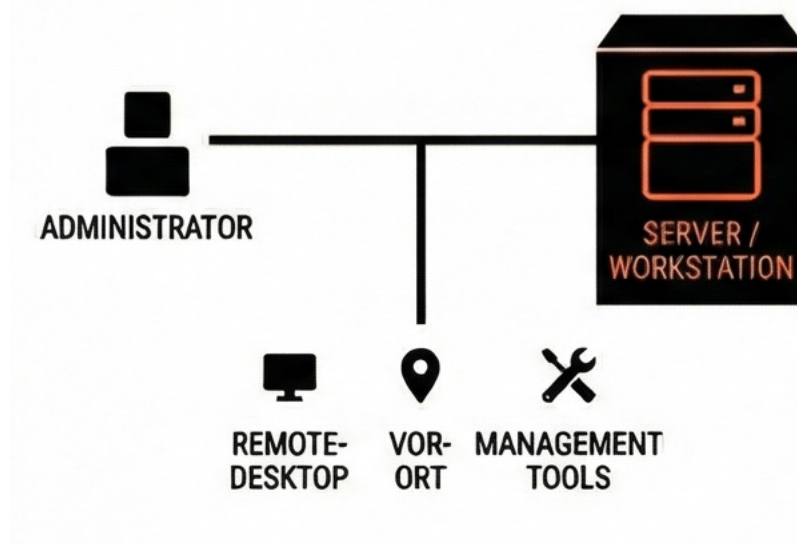


ABBILDUNG 6 DIREKTER ZUGRIFF

Use Case 2: Partnerzugriff (VPN oder lokales Netzwerk)

Dieser Anwendungsfall beschreibt den **Zugriff über VPN oder lokales Netzwerk**, der für Partnerorganisationen bereits eingerichtet wurde. Im VPN-Szenario erfolgt die Verbindung verschlüsselt über einen Tunnel. Im lokalen Netzwerk sind direkte interne Zugriffe auf Server oder Workstations möglich. In beiden Fällen sind Portfreigaben auf den beteiligten Servern notwendig.

- **Technik:** Der Zugriff erfolgt über VPN-Konfigurationen oder über das lokale Netzwerk mit entsprechenden Portfreigaben auf den Servern. Damit können Partner auf die benötigten Ressourcen zugreifen.
- **Zugriff für:** Partnerorganisationen mit VPN- oder LAN-Zugang
- **Zugangsverantwortliche:** IT-Administrationsteam

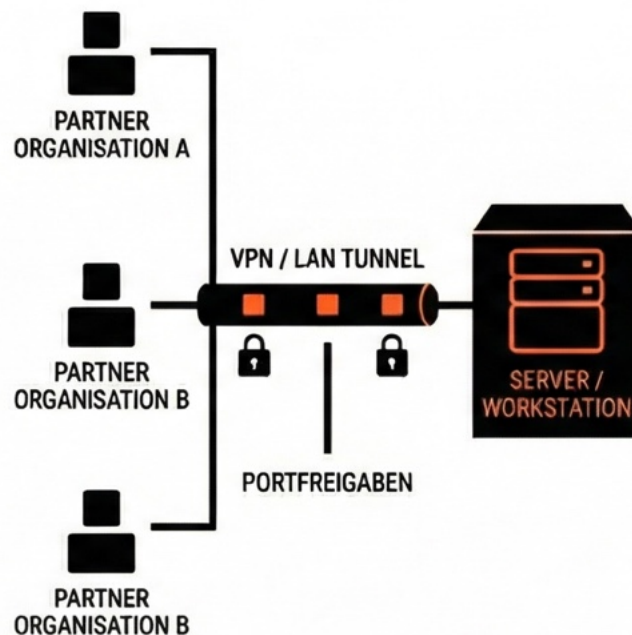


ABBILDUNG 7 PARTNERZUGRIFF

Use Case 3: Öffentlicher Zugriff als Nucleus-Cloud-Instanz

In diesem Szenario wird eine Instanz von Nucleus so betrieben, **als ob sie in der Cloud wäre**. Externe Nutzer können wie im Use Case 2 mit denselben Rollen auf die Plattform zugreifen, jedoch ohne die Einschränkungen einer Doppel-VPN-Struktur. Zusätzlich können bestimmte Zonen als Read-Only Bereiche für Demo-Nutzer freigegeben werden. Der restliche Teil der Umgebung bleibt weiterhin rollenbasiert eingeschränkt. So können Inhalte für Präsentationen oder Tests zugänglich gemacht werden, ohne die Integrität des Gesamtsystems zu gefährden.

- **Technik:** Der Zugriff erfolgt über WAN über einen Cloud-Endpoint. Nutzer authentifizieren sich über einen zentralen Authentifizierungsdienst. Demozonen werden mit Leserechten konfiguriert, während produktive Bereiche nur mit den zugewiesenen Rollen bearbeitet werden können.
- **Zugriff für:** Externe Partner und Demonutzer (Read-Only) sowie autorisierte Rollen mit erweiterten Rechten.
- **Vorteile:** Geeignet für Unternehmensumgebungen. Erlaubt Demonstrationen und externe Visualisierungen ohne zusätzliche Clientinstallation. Gleiche Rollenlogik wie beim Partnerzugriff, jedoch ohne Einschränkungen durch Doppel-VPN
- **Limitierungen:** Erfordert WAN-Portforwarding, wie im nächsten Kapitel beschrieben
- **Zugangsverantwortlicher:** das IT-Administrationsteam in Abstimmung mit der Universitäts-IT.

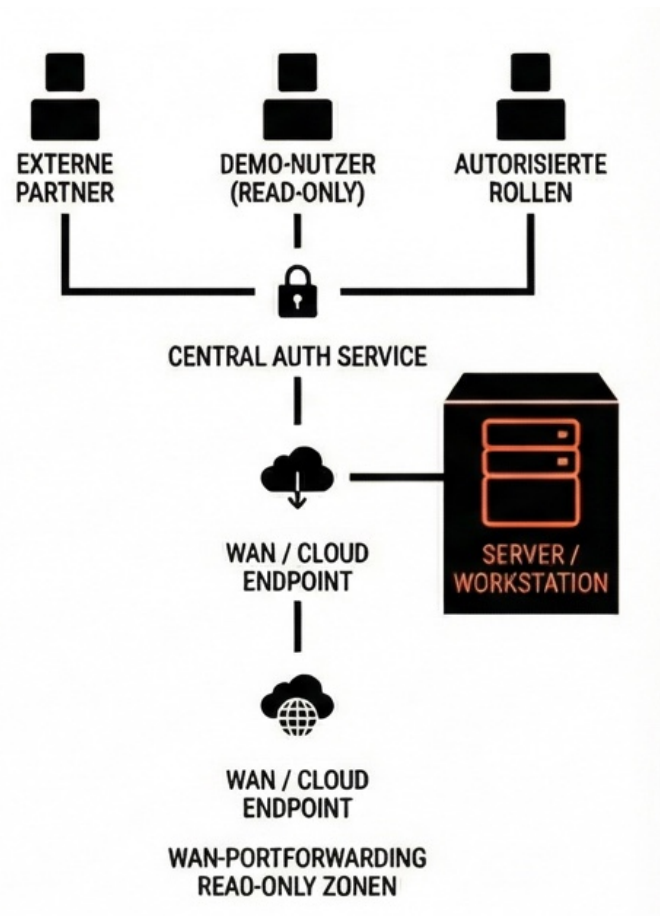


ABBILDUNG 8 CLOUD-INSTANZ

Portfreigaben und Protokolle

Die folgende Übersicht listet die relevanten Ports aus der Omniverse Nucleus Dokumentation. Für Use Case 2 (Partnerzugriff via VPN) gelten diese Anforderungen am Server und Workstation. Für Use Case 3 (Cloud/Öffentlich) gelten die gleichen Anforderungen plus zusätzliches Port Forwarding auf WAN-Ebene.

Quelle: https://docs.omniverse.nvidia.com/nucleus/latest/ports_connectivity.html

Nucleus Workstation (Tarox – Windows Rechner)

Zweck	TCP Port
Nucleus Core und Discovery API	3001, 3009, 3333
Prometheus Metrics	3010
Nucleus Tagging Service	3020
Nucleus System Monitor	3080, 3085
Authentication Service	3100
Authentication Web	3180
Search Service	3400
Cache Service	8891
Cache API	8892
Nucleus Navigator (Launcher)	34080

Enterprise Nucleus Server (Linux Server)

Zweck	TCP Port
Web Port*	8080 (oder 80 ohne TLS)
API Ports	3009, 3019
Prometheus Metrics	3010
Tagging Service	3020
Large File Transfer	3030
Authentication Services	3100, 3180
Discovery	3333
Search Service	3400
Service API	3006
Meta Dump	5555