

15. Identity & Cloud Summit 2024



Zeit	Thema	Speaker
09:00 – 09:30	Begrüßung, Vorstellung der Partner, Keynotes IDABUS nur in der Cloud? – Mögliche Hybride und onPrem Architekturen (Ausblick)	OCG: Rüdiger / Rike , Partner
09:30 – 10:30	▪ Interessante Lösungen mit IDABUS (Sync zwischen Umgebungen, PAM V2 über HC, Migrationserfahrungen)	OCG: Rike / Rüdiger
10:30 – 11:00	Fragen / Feedback / Pause / Networking an den Messeständen	OG Panorama Tagungsraum
11:00 – 12:00	▪ Direkte und Interaktive Workflows in IDABUS ▪ Attestierungen leicht gemacht – neue integrierte IDABUS Funktionen (z.B. SoD Verletzungen)	OCG: Rike / Rüdiger
12:00 – 13:30	Mittagspause / Networking an den Messeständen	Restaurant Empire EG
13:30 – 14:15	▪ Kundenvortrag – Erfahrungen mit IDABUS	IPG: Sven Spiess , TIMETOACT: Thomas Overbeck
14:15 – 15:15	▪ Mastering Access Governance: A deep dive into NEXIS 4	NEXIS: Benedikt Bruckner
15:15 – 15:45	Fragen / Feedback / Pause / Networking an den Messeständen	OG Panorama Tagungsraum
15:45 – 16:15	▪ Vermeidung von Risiken bei der Rechtevergabe im Vorhinein (SoD Simulationen)	OCG: Philipp
bis ca.16:45	MEET THE EXPERTS! – Offene Fragerunde an die Experten von Microsoft, IPG, NEXIS und OCG	
17:30	Abfahrt Bus zur Abendveranstaltung Erdinger Herbstfest - Geme in Tracht!	Treffpunkt Hotelvorfahrt!

Zeit	Thema	Speaker
09:00 – 10:00	Gemeinsames Weißwurst Frühstück	OG Panorama Tagungsraum
10:00 - 10:30	▪ Cloud First with Identity Management	OCG Worldwide: James Cowling
10:30 – 11:00	▪ IPGCORE – Erweiterungen und Services für IDABUS	IPG: Mario Bader
11:00 – 11:30	Fragen / Feedback / Pause / Networking an den Messeständen	OG Panorama Tagungsraum
11:30 – 12:15	▪ NEWS von Microsoft – Was bringt die Microsoft Entra Suite?	Microsoft: Markus Wilhelm-Köstner
Bis 12:30	Zusammenfassung Summit 2024	
12:30 – 13:30	Mittagessen und Abreise	

Änderungen der Themen und Zeiten vorbehalten.

15. IDENTITY & CLOUD SUMMIT 2024 von 5.-6.September,
Anmeldeschluss ist der **15.08.2024**

Zur Anmeldung

15. Identity & Cloud Summit 2024

IDABUS nur in der Cloud? – Mögliche hybride und onPrem Architekturen



Microsoft



IDABUS®



EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.



NEXIS

IDABUS Deployment Optionen im Überblick

- Installation im eigenen Azure Tenant
 - ✓ Cloud only
 - ✓ Hybrid
 - ✓ Hybrid mit „lokalem“ Netzwerk



- Installation im eigenen „Behörden Tenant“



- Installation im Azure Stack HCI



- Installation auf lokalem Windows Server



Cloud / Hybrid Variante



HR (Cloud)
(Successfactors/SAP
Hana/Workday / ...)



Function App
Cloud HR Inbound Connectors
(Employees, Companies, Departments,
Costcenters, Business structures)



Service Desk
(e.g. Service Now / Remedy / ...)

Sync API for Tickets
Tasks, Companies, Costcenters,...



IDABUS
IDENTITY Solution
Business Logic, Enterprise Roles,
central processes

NGS
(Unique Names)



Function Apps

- User & Group Provisioning Entra ID
- Teams Management
- PIM f. Entra ID
- Service Desk Task Sync, ...



IDABUS TEAMS APP

- Self Services
- Approval Interface



ENTRA ID CLOUD SYNC
(Users / Groups)



Azure

On premises

Services (opt)
Azure Hybrid

Inbound provisioning
For existing MIM Customers



HR (onPrem)
(SAP HR / other
Systems)

Extended HR Inbound Connectors
(Employees, Companies, Departments,
Costcenters, Business structures)

onPrem Services

- PAM f. AD
- PWD Reset
- Signed E-Mail
- HR Inbound

MIM Sync (optional)



Active Directory

DB

Oracle



1. Installation im eigenen Azure Tenant

Vorteile:

- ✓ Eigene Security Policies möglich
- ✓ Private Endpunkte möglich
 - Integration ins lokale Netzwerk
 - Zugriff von „außen“ kann komplett unterbunden bzw. gesteuert werden
- ✓ Partieller Zugriff aus dem Internet möglich, wenn gewünscht
- ✓ Keine Anpassungen in IDABUS notwendig
- ✓ Günstiger Preis, schnelle automatische Installation
- ✓ Hohe Performance, dynamisch/online skalierbar



Nachteile (in Bezug auf Datensicherheit):

- ❖ Zugriff durch Microsoft ist begrenzt möglich (z.B. im Supportfall)
- ❖ Backup Rechenzentren können außerhalb des Datenstandortes liegen

2. Installation im Behörden-Tenant

Vorteile:

- ✓ Speziell für die Nutzung von Behörden entwickelt
- ✓ Integration ins lokale Netzwerk
- ✓ Keine/ev. wenige Anpassungen in IDABUS notwendig



Nachteile (in Bezug auf Datensicherheit):

- ❖ Zugriff durch den jeweiligen Betreiber ist möglich (z.B. im Supportfall)
- ❖ Abgeschottete Umgebung
 - Zugriff auf lokale Dienste ggf. begrenzt

3. Installation in Azure Stack HCI (z.B. HP/Dell)

Vorteile:

- ✓ Läuft auf lokalen Servern im eigenen Rechenzentrum im lokalen Netzwerk
- ✓ Nur wenige bis keine Anpassungen in IDABUS notwendig

Nachteile:

- ❖ Höherer Preis für die Azure Stack HCI Hardware im Vergleich zum Betrieb in der Azure Cloud
- ❖ Anpassungen im Monitoring nötig



➤ **Wahrscheinlich verfügbar ab Ende 2025!**

4. Installation im Windows Server 2022

Vorteile:

- ✓ Analog zu bestehenden MIM Systemen installierbar
- ✓ Vollständige on premises Architektur

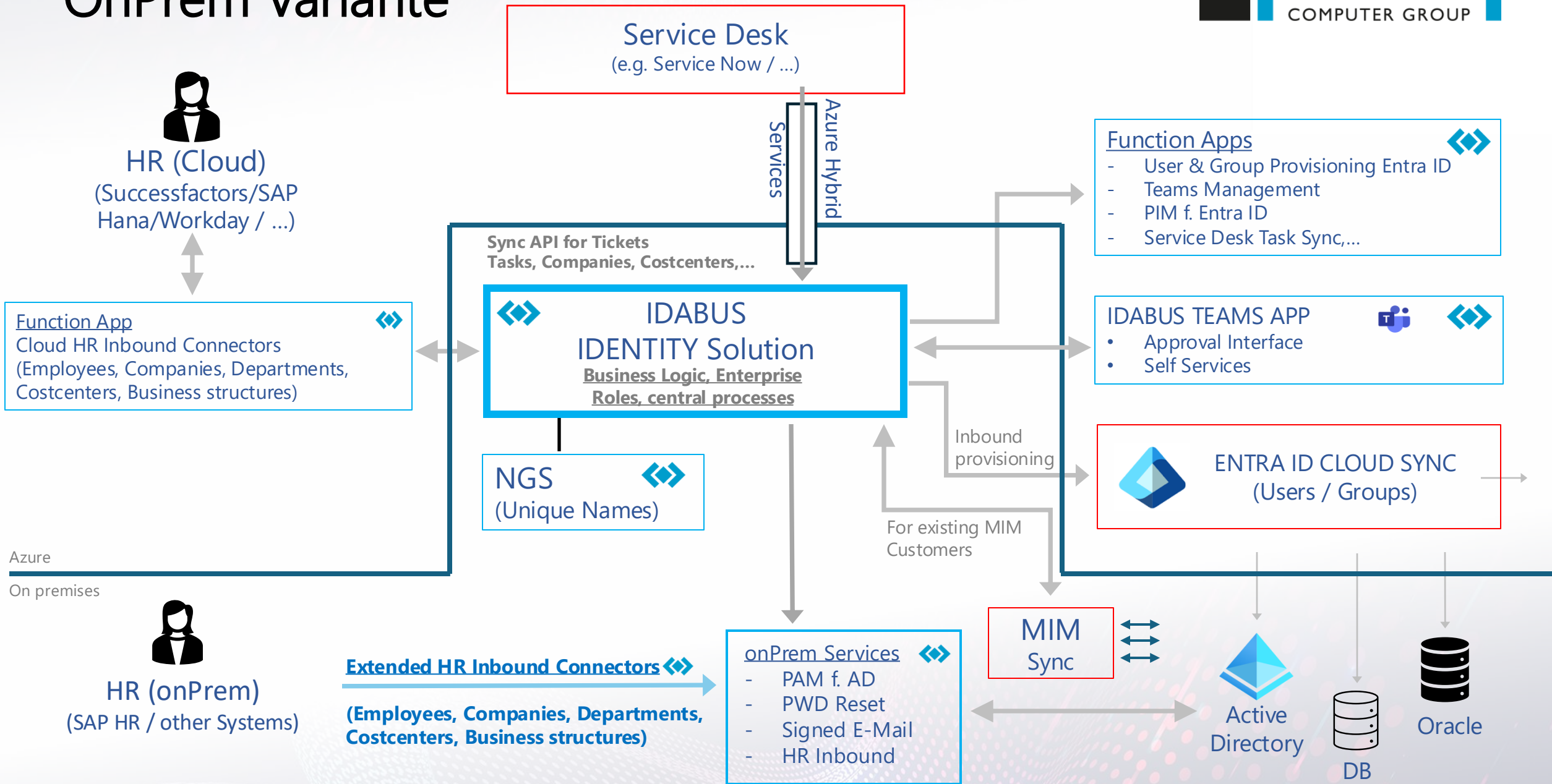
Nachteile:

- ❖ Performance Anpassungen nur durch klassische Verfahren möglich
- ❖ Hochverfügbarkeitsoptionen der Datenbank noch offen
- ❖ „Inbound“ Verbindungen aus der Cloud erfordern ggf. Hybrid Connector
- ❖ Auth Verfahren entweder Kerberos oder OAUTH (Entra ID)



➤ **Wahrscheinlich verfügbar ab Ende 2025!**

OnPrem Variante



15. Identity & Cloud Summit 2024

Aktuelle Lösungen mit IDABUS



Microsoft



IDABUS®



EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.



NEXIS

Übersicht Szenarien

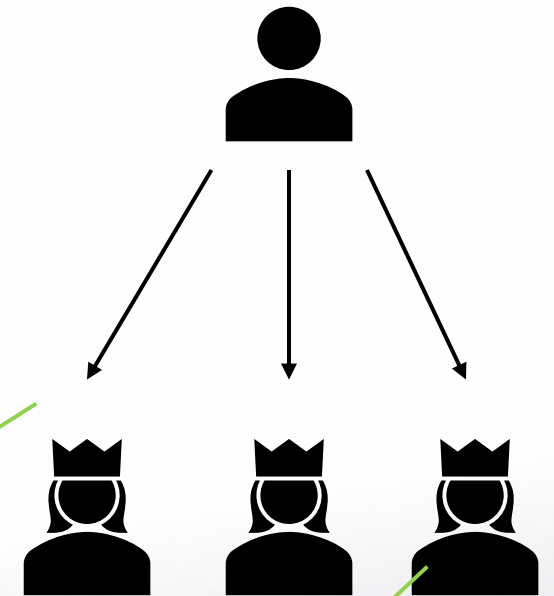
1. Erhöhung der Sicherheit von Admin Accounts
2. Erstellung eindeutiger Attribute beim Entra ID Inbound Sync
3. Regelbasierte Synchronisation mehrerer IDABUS Instanzen
4. Integration von Service Desk Anwendungen
5. Weitere Szenarien
6. Migration von MIM Portal zu IDABUS

Szenarien

1. **Erhöhung der Sicherheit von Admin Accounts**
2. Erstellung eindeutiger Attribute beim Entra ID Inbound Sync
3. Regelbasierte Synchronisation mehrerer IDABUS Instanzen
4. Integration von Service Desk Anwendungen
5. Weitere Szenarien
6. Migration von MIM Portal zu IDABUS

Erhöhung der Sicherheit von Admin Accounts

1. Informationen über den „normalen“ User Account im Admin Account hinterlegen
 - Direkte Verlinkung als „Owner“ oder „Manager“
 - Alternativ Eingabe Accountname in einem zusätzlichen Attribut
2. Über DataFlow Rule – Vererbung von Benutzereigenschaften auf den Admin Account – z.B.
3. Beantragung von zeitlich begrenzten Admin Berechtigungen (PAM für AD, PIM für Entra ID)



Vererbung vom User:

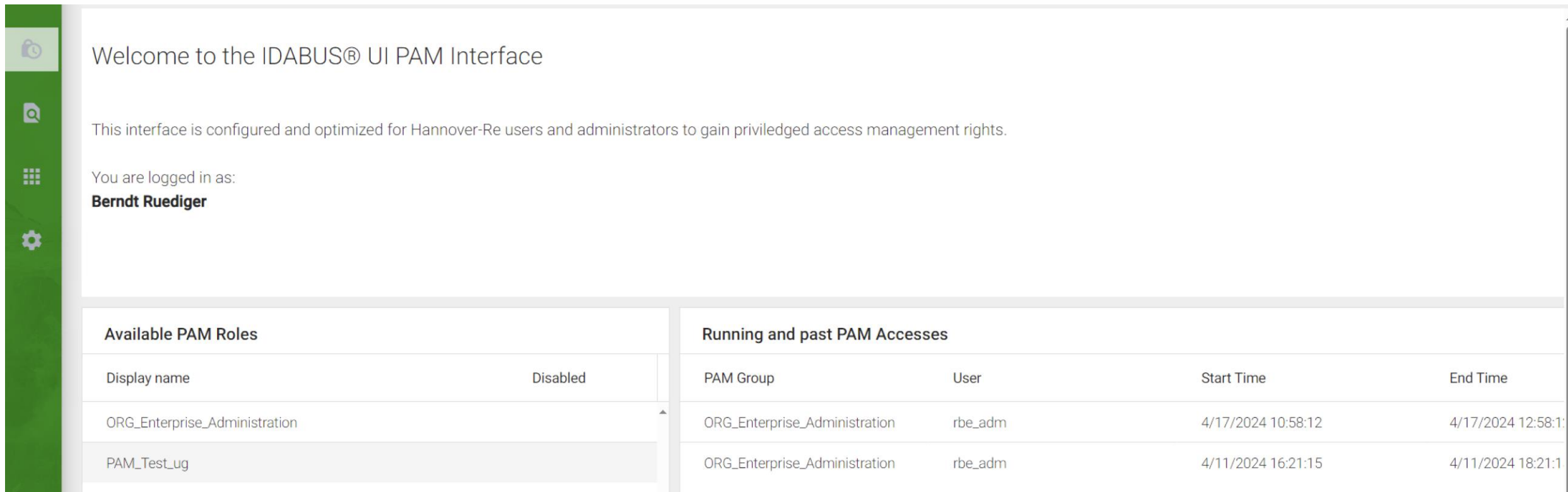
- ✓ Austrittsdatum
- ✓ Enable / Disable Status
- ✓ Name + "Admin"

Beim Adm Account:

- ✓ Owner / Manager festlegen (automatisch / manuell)

Erhöhung der Sicherheit von Admin Accounts

1. Anzeige aller zur Verfügung stehender Admin Gruppen für alle verlinkten ADM Accounts



Welcome to the IDABUS® UI PAM Interface

This interface is configured and optimized for Hannover-Re users and administrators to gain privileged access management rights.

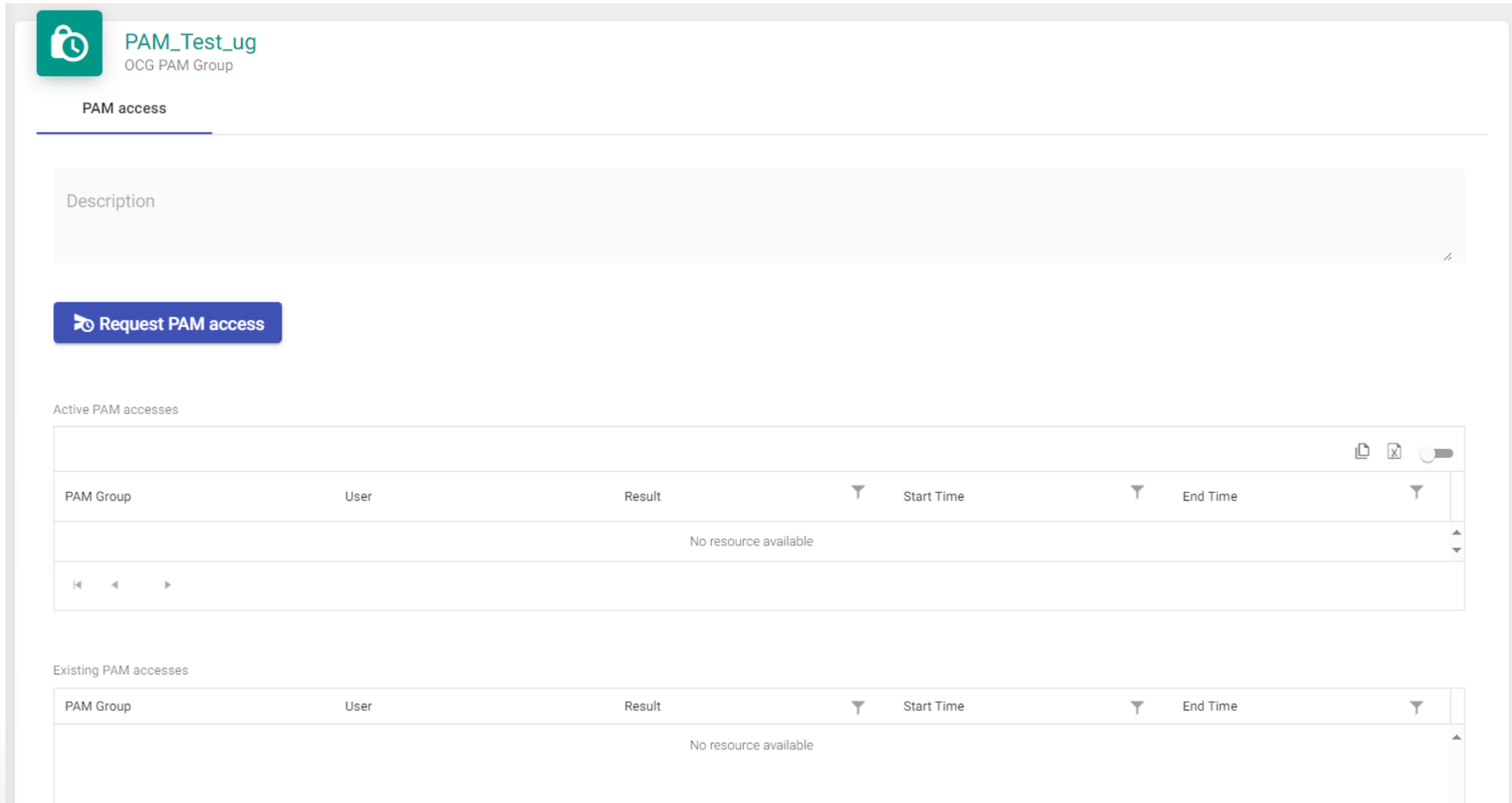
You are logged in as:
Berndt Ruediger

Available PAM Roles	
Display name	Disabled
ORG_Enterprise_Administration	
PAM_Test_ug	

Running and past PAM Accesses			
PAM Group	User	Start Time	End Time
ORG_Enterprise_Administration	rbe_adm	4/17/2024 10:58:12	4/17/2024 12:58:12
ORG_Enterprise_Administration	rbe_adm	4/11/2024 16:21:15	4/11/2024 18:21:15

Erhöhung der Sicherheit von Admin Accounts

2. Nach Auswahl einer ADM Gruppe – Anzeige der laufenden Requests / Mitgliedschaften



The screenshot displays the interface for the PAM Test Group. At the top left, there is a green lock icon and the text "PAM_Test_ug" and "OCG PAM Group". Below this, the text "PAM access" is underlined. A large, empty text area labeled "Description" is present. A blue button with a play icon and the text "Request PAM access" is located below the description. The interface is divided into two sections: "Active PAM accesses" and "Existing PAM accesses". Each section contains a table with columns for "PAM Group", "User", "Result", "Start Time", and "End Time". Both tables currently display "No resource available".

Active PAM accesses

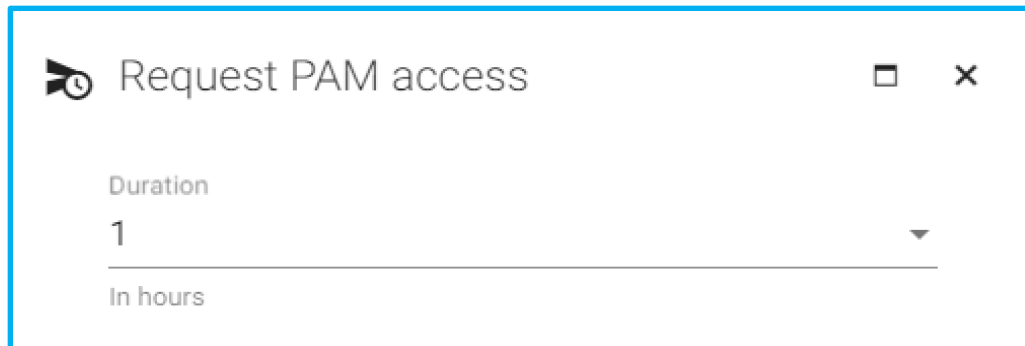
PAM Group	User	Result	Start Time	End Time
No resource available				

Existing PAM accesses

PAM Group	User	Result	Start Time	End Time
No resource available				

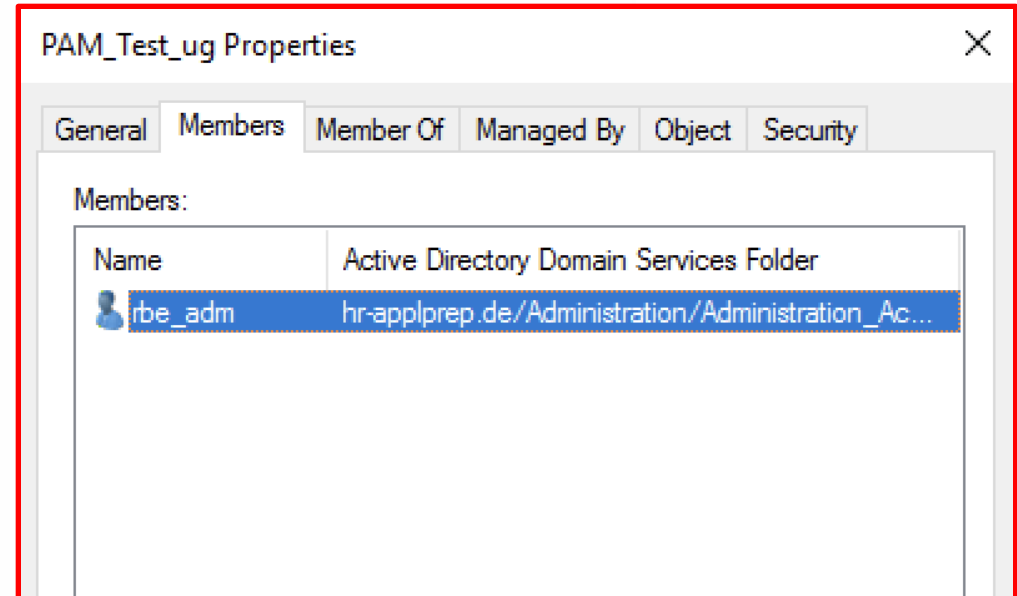
Erhöhung der Sicherheit von Admin Accounts

3. Request starten und Formular ausfüllen
4. Gruppenmitgliedschaft wird im AD aktualisiert
5. Ergebnis wird dokumentiert



Request PAM access

Duration
1
In hours



PAM_Test_ug Properties

General Members Member Of Managed By Object Security

Members:

Name	Active Directory Domain Services Folder
rbe_admin	hr-applprep.de/Administration/Administration_Ac...

Running and past PAM Accesses

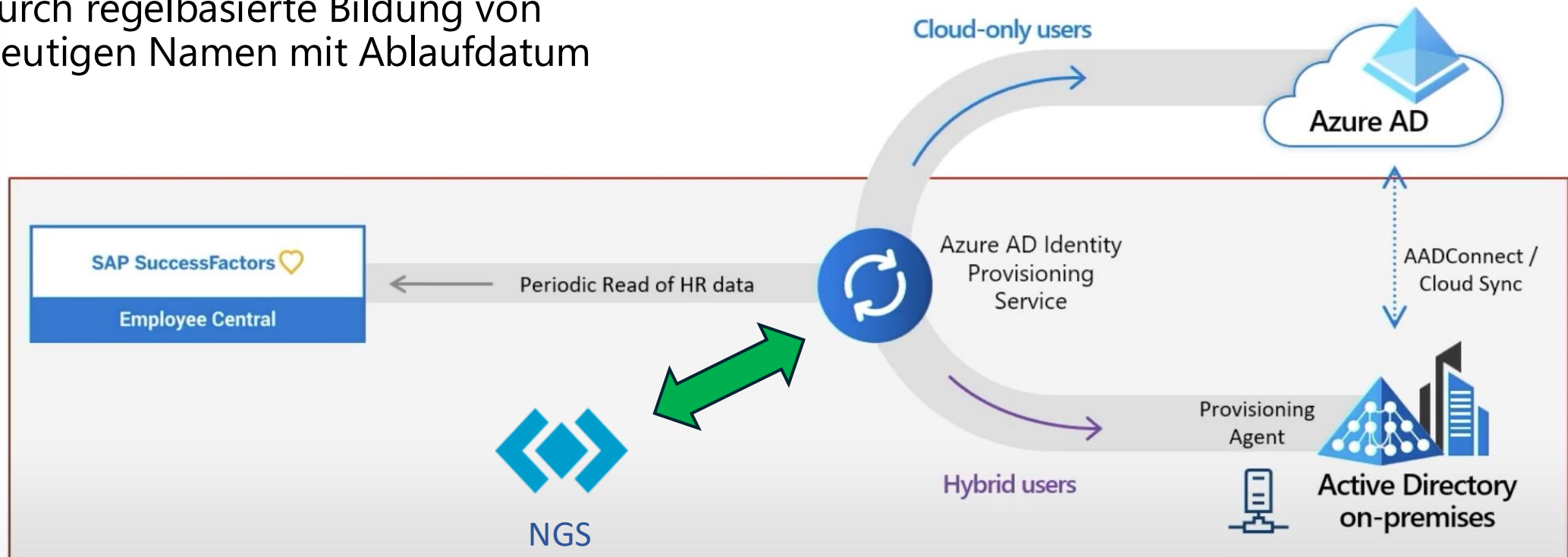
PAM Group	User	Start Time	End Time
PAM_Test_ug	rbe_admin	8/30/2024 16:42:22	8/30/2024 17:42:22
ORG_Enterprise_Administration	rbe_admin	4/17/2024 10:58:12	4/17/2024 12:58:12
ORG_Enterprise_Administration	rbe_admin	4/11/2024 16:21:15	4/11/2024 18:21:15

Szenarien

1. Erhöhung der Sicherheit von Admin Accounts
- 2. Erstellung eindeutiger Attribute beim Entra ID Inbound Sync**
3. Regelbasierte Synchronisation mehrerer IDABUS Instanzen
4. Integration von Service Desk Anwendungen
5. Weitere Szenarien
6. Migration von MIM Portal zu IDABUS

Erstellung eindeutiger Attribute beim Entra ID Inbound Sync

- IDABUS NGS als Standardlösung für Inbound Entra ID Cloud Sync
- Einbindung in den Inbound Connector via Code Injection (Standard Feature)
- ✓ Dadurch regelbasierte Bildung von eindeutigen Namen mit Ablaufdatum

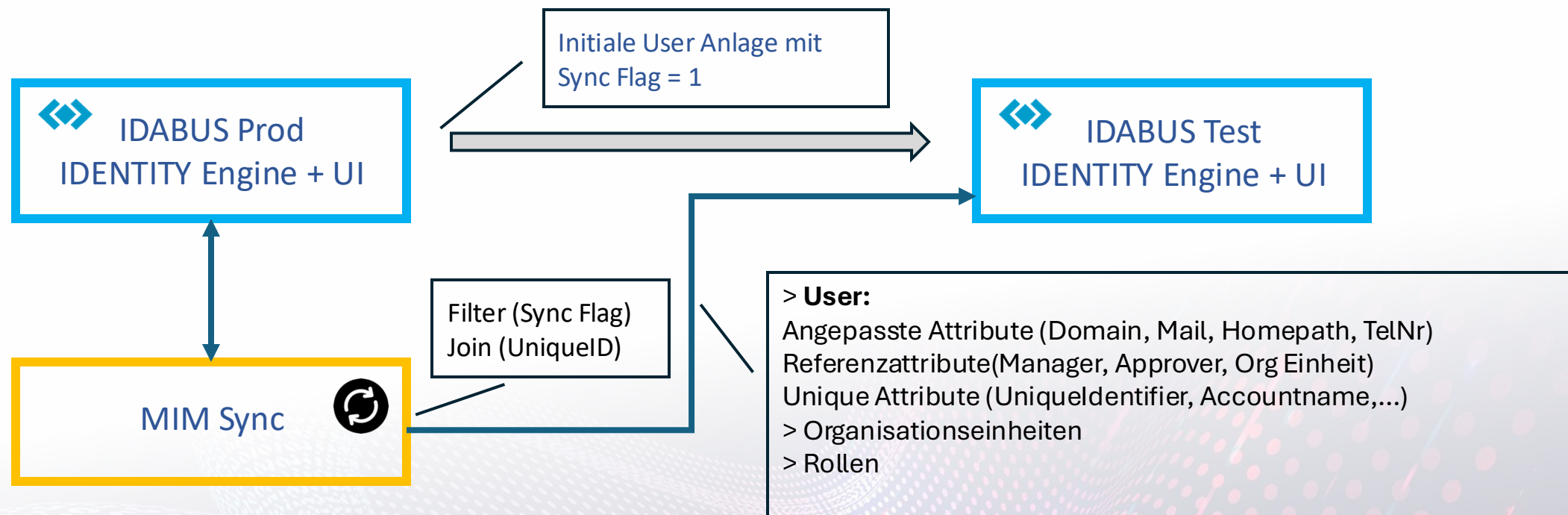


Szenarien

1. Erhöhung der Sicherheit von Admin Accounts
2. Erstellung eindeutiger Attribute beim Entra ID Inbound Sync
- 3. Regelbasierte Synchronisation mehrerer IDABUS Instanzen**
4. Integration von Service Desk Anwendungen
5. Weitere Szenarien
6. Migration von MIM Portal zu IDABUS

Regelbasierte Synchronisation mehrerer IDABUS Instanzen

- Bereitstellung eines zusätzlichen MAs für IDABUS aus der Prod Instanz
- Erstellung von Sync Workflows für das initiale Anlegen von (User) Objekten zwischen IDABUS Instanzen und für das Setzen der Sync Flags (z.B. Manager)

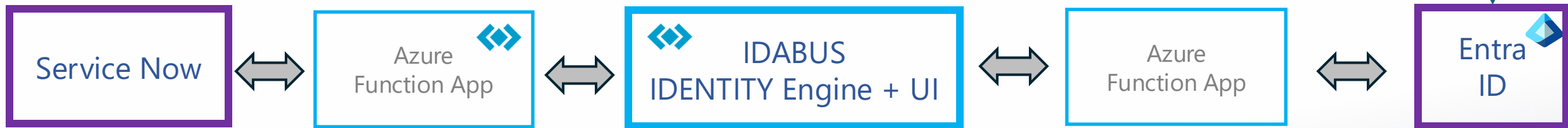


Szenarien

1. Erhöhung der Sicherheit von Admin Accounts
2. Erstellung eindeutiger Attribute beim Entra ID Inbound Sync
3. Regelbasierte Synchronisation mehrerer IDABUS Instanzen
- 4. Integration von Service Desk Anwendungen**
5. Weitere Szenarien
6. Migration von MIM Portal zu IDABUS

Integration von Service Desk Anwendungen

1. Function Apps für den Abgleich von Tasks (SN <> IDABUS)
2. FA für Anlage Group/Team/B2B User
3. Opt. MIM MA für stetigen Abgleich



- Request
- Role Request
 - Team
 - B2B Guest
 - App Permission

- ✓ Create Task
- ✓ Sync Tasks (Status / Result)

- ✓ Permission Rules
- ✓ UI Forms
- ✓ Workflows for Group/Team Creation, Guest invitation, Role Assignments

- ✓ Create Group / Team / (B2B Request)
- ✓ Sync Properties
- ✓ Sync Membership

Weitere Szenarien - 1

- Verwaltung von Zugangskarten / Tokens (Studierende)
- Verwaltung von Softwarepaketen auf Clientcomputern
- IDABUS UI Dashboard als Einstiegspunkt für weitere Anwendungen
- Telefonverzeichnis

Weitere Szenarien - 2

- Lizenzverwaltung
- Veröffentlichung / Steuerung von Citrix Anwendungen
- Vergabe von vergünstigten Tickets für Studierende
- Accountmanagement für Google und AWS

Weitere Szenarien - 3

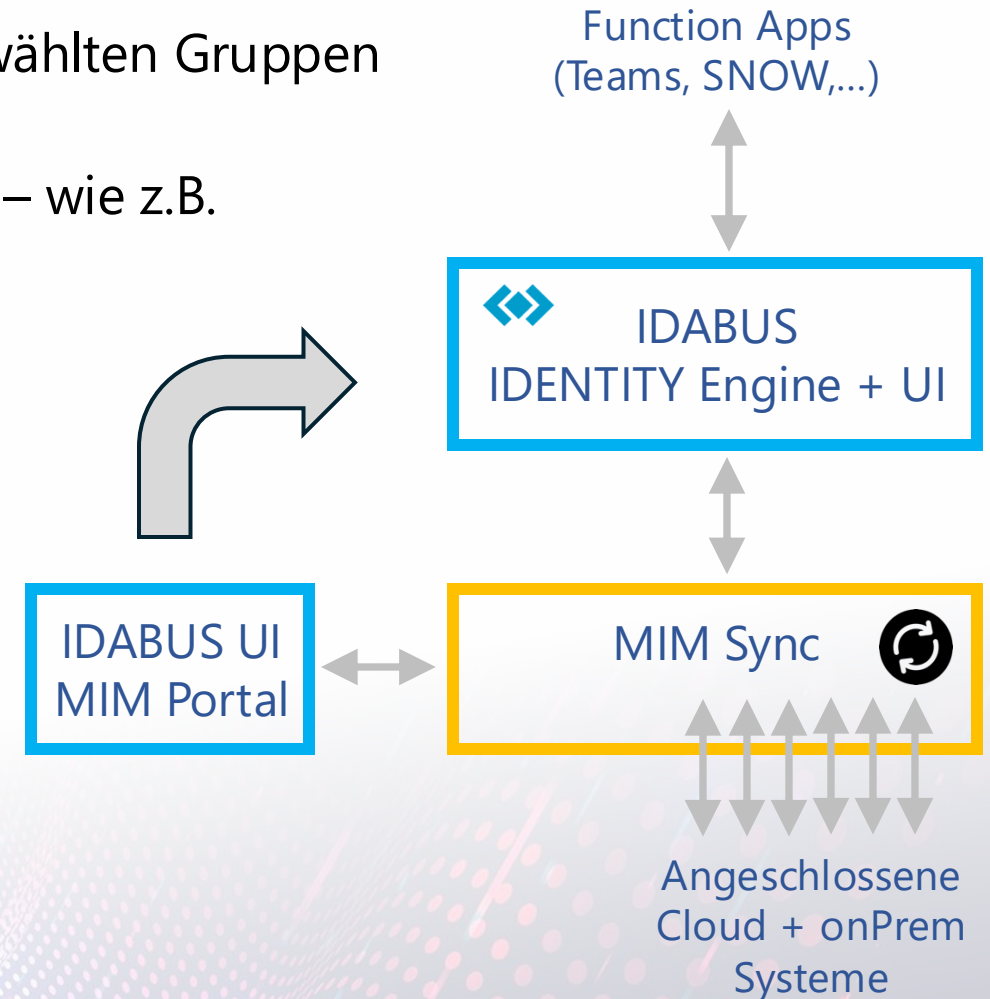
- Freigabe von sozialen Netzwerkdiensten (Facebook, X, Instagram,...)
- Integration von Webanwendungen IDABUS < > andere Web Apps
- Online Abruf von freien Teams Telefonnummern

Szenarien

1. Erhöhung der Sicherheit von Admin Accounts
2. Erstellung eindeutiger Attribute beim Entra ID Inbound Sync
3. Regelbasierte Synchronisation mehrerer IDABUS Instanzen
4. Integration von Service Desk Anwendungen
5. Weitere Szenarien
6. **Migration von MIM Portal zu IDABUS**

MIM Portal > IDABUS – Step by Step

- Zyklische Synchronisation von Benutzern und ausgewählten Gruppen nach IDABUS
- Neue Funktionalitäten werden in IDABUS abgebildet – wie z.B.
 - Verwaltung von Teams
 - Verwaltung von Shares
 - Verwaltung von Gästen
- IDABUS hat nur die Hoheit über ausgewählte Gruppen / Rollen und ausgewählte Attribute vom Benutzer oder anderen Objekten
- Schrittweise Migration der MIM Portal Prozesse nach IDABUS



MIM Portal > IDABUS – Step by Step

Vorteile:

- ✓ Beide IAM Systeme können parallel über Monate betrieben werden
- ✓ Kein Zeitdruck bei der Umstellung
- ✓ Neue Prozesse können sofort den erweiterten Funktionsumfang nutzen (z.B. Dataflow Rules, erweiterte XPATH Syntax, Simulationen, ...)



IDABUS
IDENTITY Engine + UI

Nachteile:

- ❖ Zusätzlicher Aufwand für den Betrieb
 - Neue Attribute müssen ggf. in 2 Umgebungen konfiguriert werden
- ❖ Genaue Abgrenzung nötig, was wird wo verwaltet
- ❖ Unterschiedliche Anmeldungen (Kerberos / Entra ID) falls kein SSO
- ❖ Höhere Umlaufzeiten für Sync Zyklus



Microsoft
Identity Manager

MIM Portal > IDABUS – sofortige Umschaltung



- Nutzung des Migrationstools für Übernahme
- Zyklische Synchronisation aller MIM Daten in IDABUS bis zur Umschaltung
- Tests der Datendifferenzen zwischen IDABUS und MIM Portal (Scriptgesteuert)
- Umschalten der Datenhoheit zu einem Stichtag
- Backup Szenario > Aktivieren der bisherigen Schnittstelle zu MIM Portal

MIM Portal > IDABUS – sofortige Umschaltung

Vorteile:

- ✓ Nahtlose Umstellung mit voller Funktionalität
- ✓ Vollständige Prüfung der neuen führenden Source (IDABUS) möglich
- ✓ Längere Testphase möglich (aber besser eher Wochen als Monate!)
- ✓ Kosteneinsparungen, da sofort kein MIM Portal und Sharepoint mehr nötig ist
- ✓ Performance Verbesserungen in MIM Sync, UI und Workflows

Nachteile:

- ❖ Anmeldung an UI über Entra ID Account bei Umstellung auf IDABUS UI
- ❖ Aufwand für Tests / Optimierungen nötig
 - XPATH Filter bei Sets und Gruppen
 - Workflow Optimierungen zu DataFlow Rules
 - Time based Trigger überprüfen