beta systems

Garancy®

Data Sheet – Azure Connect

Überblick

Azure Connect wurde entwickelt, um Benutzer und Konten in Microsoft Azure Active Directory (Azure AD) zu verwalten, die nicht in der lokalen Active Directory-Umgebung (AD) enthalten sind. Es bietet eine effiziente Möglichkeit, Cloud-Only-Konten und Benutzerobjekte unabhängig von lokalen Verzeichnisdiensten zu verwalten.

Für Szenarien, die eine Synchronisierung zwischen lokalem AD und Azure AD erfordern, empfiehlt Microsoft die Verwendung von Windows Connect oder Azure AD Connect, die Benutzerdaten und Anmeldeinformationen zwischen beiden Umgebungen synchronisieren. Dies gewährleistet konsistentes Identity Management über hybride Infrastrukturen hinweg.

Azure-Konzepte

Azure Connect basiert auf der Microsoft Graph API, die eine zentrale Verwaltung von Azure AD-Ressourcen und Microsoft 365-Diensten ermöglicht. Über diese API können Administratoren Benutzer, Gruppen und Berechtigungen programmbasiert steuern und so eine sichere und konsistente Zugriffskontrolle gewährleisten.

Die Graph API ermöglicht eine nahtlose Integration mit Microsoft Azure AD, Microsoft 365-Diensten (einschließlich Exchange Online und Teams) sowie anderen Azure-Ressourcen, die Identity & Access Governance unterstützen.

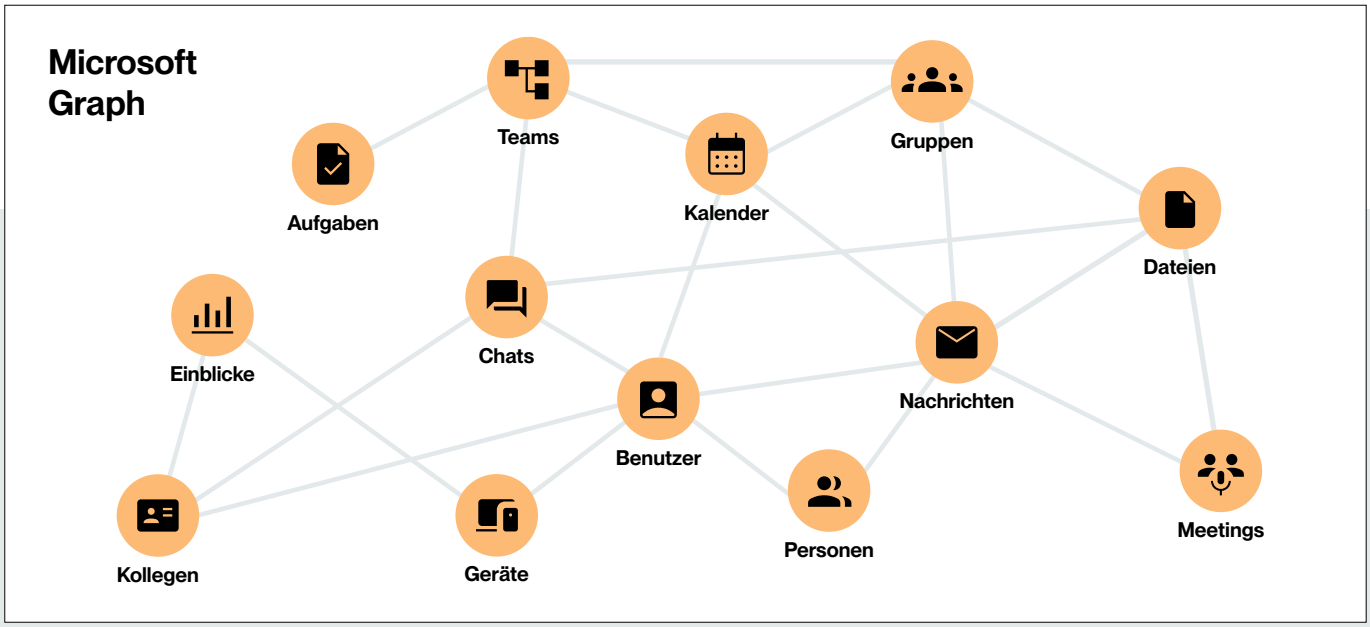
Überblick über Microsoft Graph

Die Microsoft Graph API stellt einen zentralen Endpunkt bereit, um auf Daten in der Microsoft Cloud zuzugreifen. Sie verbindet Millionen von Benutzern, Ressourcen und Verknüpfungen und ermöglicht Anwendungen eine reibungslose Integration mit Microsoft 365- und Azure-Diensten.

Microsoft Graph modelliert Daten über verknüpfte Ressourcen, z. B. durch die Verbindung von Benutzern mit Gruppen über *memberOf*-Beziehungen oder mit anderen Benutzern über *manager*-Beziehungen.

Anwendungen können über diese Verknüpfungen auf zugehörige Daten zugreifen und Aktionen ausführen.

Die API bietet zudem Analyse- und Intelligence-Features, z. B. zur Erkennung wichtiger Dateien oder relevanter Kontakte eines Benutzers. Dies unterstützt ein smartes Identity Access Management.



Grafik 1 – Zentrale Ressourcen und Verbindungen in Microsoft Graph

Unterstützte IDM-Funktionen

Der Garancy Identity Manager (IDM) integriert sich nahtlos in Azure AD. Der Konnektor unterstützt die folgenden Kernfunktionen:

- **Initialer Import von Azure in IDM**
  Während der initialen Synchronisierung werden folgende Objekte importiert:

Azure-Objekt	Abbildung in IDM als
License and service plan information	Target system data
Users with attributes	Accounts
Groups with attributes	Groups
Memberships of users in groups	Group connections

- **Bi-direktionale Synchronisierung**
  Der Konnektor unterstützt Live Balancing und ermöglicht einen vollständigen Rechteabgleich zwischen IDM und Azure AD. Dies umfasst das Aktualisieren von IDM und Azure sowie das Melden von Abweichungen zwischen beiden Systemen.
- **Zuweisung von User-Lizenzen**
- **Erstellung von User-Mailboxen für Exchange Online**

Beta Systems IAM Software AG
Ernst-Reuter-Platz 6, 10587 Berlin
Tel. +49 (0) 30 726 118-0
www.betasystems.com, info-iam@betasystems.com

Data Mapping zwischen IDM und Azure

Die folgenden User-Attribute werden in IDM zur Verwaltung von Azure AD-Konten verwendet.

Schreibgeschützte (Read-Only) Attribute werden während des Live Balancing aktualisiert, um aktuelle Azure-Werte anzuzeigen. Attribute mit mehreren Einträgen werden in IDM als neue Tabellen abgebildet, um eine vollständige Datenabdeckung aus Azure sicherzustellen.

Legende zum Data Mapping

A: Pflichtfeld in Azure

R: Read-Only in Azure (Verwaltung ausschließlich in Azure; IDM kann anzeigen und synchronisieren, aber nicht überschreiben)

O: Optional in Azure

I: Pflichtfeld in IDM

Azure User-Attribut	Data Mapping	IDM-Feld	IDM-Label
userPrincipalName	A / I	OBOXUS_TKID	Account ID
accountEnabled	A	OBOXUS_STATUS	Status
displayName	A	OBOXUS_NAME	Display Name
mailNickname	A	OBOXUS_C_00_07L	Mail Nick Name
passwordProfile	A	OBOXUS_C_01_01L/ OBOXUS_PASSWORD	Force Change Pwd Next Sign In / Password
assignedPlans	R	**New Table**	
Id	R	OBOXUS_C_256_02L	Azure-ID
Mail	R	OBOXUS_C_256_01L	Mail
provisionedPlans	R	**New Table**	
assignedLicenses	O	**New Table**	Assigned License
businessPhones	O	OBOXUS_C_00_01L	Phone
City	O	ADDRESS.OBOXUSS_C_00_05L	City
companyName	O	ADDRESS.OBOXUSS_C_00_01L	Company Name
country	O	ADDRESS.OBOXUSS_C_00_07L	Country
department	O	ADDRESS.OBOXUSS_C_00_02L	Organizational Unit
givenName	O	OBOXUS_C_00_06L	First Name
jobTitle	O	OBOXUS_C_00_02L	Job Title
mailboxSettings	O	**New Table**	
mobilePhone	O	OBOXUS_C_00_03L	Mobile
officeLocation	O	ADDRESS.OBOXUSS_C_00_03L	Office Location
passwordPolicies	O	OBOXUS_C_01_02L/ OBOXUS_C_01_03L"	Disable Strong Password / Disable Password Expiration
postalCode	O	ADDRESS.OBOXUSS_C_16_01L	Postal Code
preferredLanguage	O	OBOXUS_C_08_02L	Preferred Language
state	O	ADDRESS.OBOXUSS_C_00_04L	State
streetAddress	O	ADDRESS.OBOXUSS_C_00_06L	Street
surname	O	OBOXUS_C_00_04L	Last Name
usageLocation	O	OBOXUS_C_08_01L	Usage Location
userType	O	OBOXUS_C_16_01L	User Type

Nicht unterstützte User-Attribute

Azure User-Attribut	Data Mapping	Erklärung
AboutMe		Not relevant for access management
imAddresses		Not relevant for access management
interests		Not relevant for access management
mySite		Not relevant for access management
onPremisesImmutableId	R	Only for on-premises AD accounts, not in scope
onPremisesLastSyncDateTime	R	Only for on-premises AD accounts, not in scope
onPremisesSecurityIdentifier	R	Only for on-premises AD accounts, not in scope
onPremisesSyncEnabled	R	Only for on-premises AD accounts, not in scope
pastProjects		Not relevant for access management
proxyAddresses	R	Not relevant for access management
responsibilities		Not relevant for access management
Schools		Not relevant for access management
Skills		Not relevant for access management
birthday	O	These three attributes are not related to Azure AD but to SharePoint online. So these fields are currently not in scope
hireDate	O	
preferredName	O	

Group-Attribute

Azure Group-Attribut	Data Mapping	IDM-Feld	IDM-Label
allowExternalSenders	O	OBOXUG_C_01_01L	External Mails allowed
autoSubscribeNewMembers	O	OBOXUG_C_01_02L	Notification Autosubscription
classification	R	OBOXUG_C_08_01L	Classification
createdDateTime	R	OBOXUG_T_04_01	Creation Date
description	O	OBOXUG_C_512_01L	Description
displayName	A / I	OBOXUG_TKID	Group ID (Display Name)
groupTypes	O	OBOXUG_C_16_01L	Group Types*
mailNickname	A	OBOXUG_NAME	Mail Nickname
Id	R	OBOXUG_C_256_01L	Azure ID
isSubscribedByMail	O	OBOXUG_C_01_04L	Subscribed by Mail
Mail	R	OBOXUG_C_256_02L	Group Mail
mailEnabled	O	OBOXUG_C_01_03L	Mail enabled
securityEnabled	O	OBOXUG_C_01_04L	Security Group
visibility	O	OBOXUG_C_08_02L	Visibility

*Es wird nur der Gruppentyp „Unified“ unterstützt. Dynamische Membership-Gruppen werden vom Zielsystem automatisch verarbeitet.

Nicht unterstützte Group-Attribute

Azure Group-Attribut	Data Mapping	Erklärung
onPremisesLastSyncDateTime	R	Only for on-premises AD accounts, not in scope
onPremisesSecurityIdentifier	R	Only for on-premises AD accounts, not in scope
onPremisesSyncEnabled	R	Only for on-premises AD accounts, not in scope
proxyAddresses	R	Not relevant for access management
unseenCount	O	Not relevant for access management

Weitere Optionen für die Anbindung von Azure an IDM

Die Integration von Azure AD und IDM kann über zwei Konnektor-Typen erfolgen:

- AD oder Windows Connect
- Azure Connect

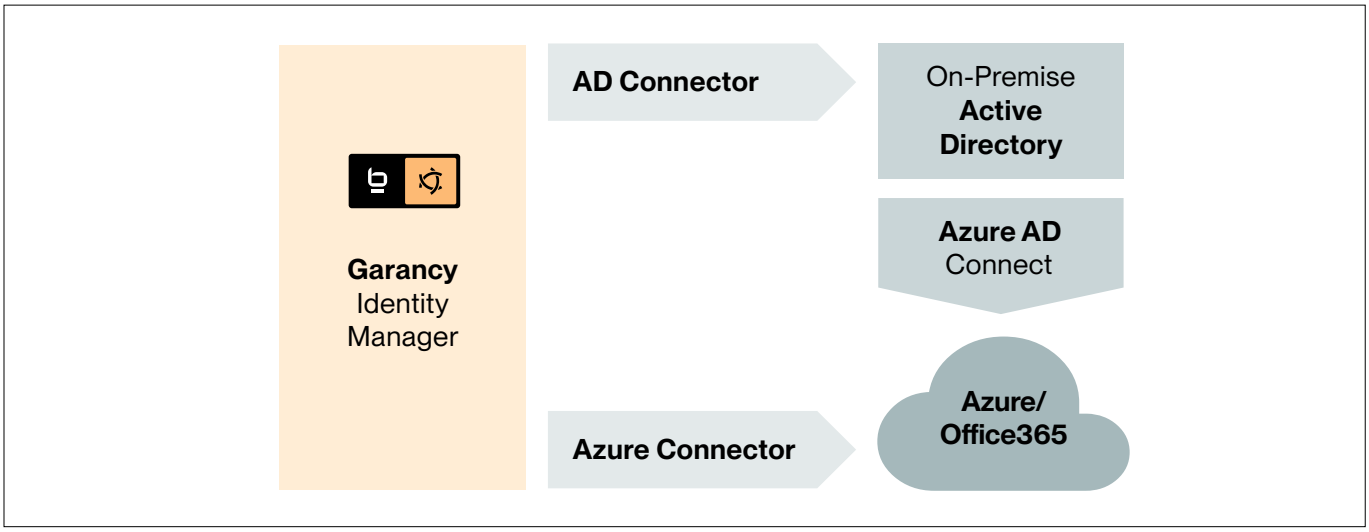
Die Wahl des Konnektors hängt von der Systemarchitektur und den Verwaltungsanforderungen ab.

Nutzen Sie Azure Connect, wenn Sie Azure-Benutzer unabhängig vom lokalen Active Directory verwalten möchten. Diese Option ist ideal, wenn Azure-Konten getrennt erstellt und gepflegt werden, beispielsweise aufgrund von AD-Lizenzbeschränkungen. Azure Connect ermöglicht außerdem die direkte Lizenzverwaltung für Azure-Benutzer innerhalb des IDM-Systems.

Hinweis: Azure Connect unterstützt keine Verwaltung lokaler AD-Konten, die mit Azure AD synchronisiert werden.

Nutzen Sie AD/ Windows Connect, wenn Sie lokale AD-Konten verwalten, die mit Azure AD synchronisiert sind. In dieser Konfiguration läuft die Benutzer- und Gruppenverwaltung über IDM für das lokale AD, während die Lizenz-verwaltung direkt in Azure AD erfolgen muss.

Wenn Sie **beide Konnektor-Optionen verwenden** möchten, beachten Sie bitte, dass die Lizenzübersicht ausschließlich über die Azure-Connect-Schnittstelle verfügbar ist.



Grafik 2 – Konnektor-Optionen zur Integration von IDM mit AD und Azure AD

Bereit für den nächsten Schritt?

Kontaktieren Sie uns, um mehr über unsere IAM-Lösung zu erfahren – wir freuen uns auf Ihre Anfrage.

Schreiben Sie uns eine E-Mail an **info-iam@betasystems.com** oder melden Sie sich telefonisch unter **+49 (0) 30 726 118-0**.

www.betasystems.com/de/produkte/garancy