Microsoft

AZ-900T00 Lernpfad 02: Azure-Architektur und -Dienste

Gliederung des Lernpfads

Lernpfad 02: Azure-Architektur und -Dienste

Die folgenden Konzepte werden behandelt:

1. **Komponenten der Azure-Architektur**
   - Regionen und Verfügbarkeitszonen
   - Abonnements und Ressourcengruppen
2. **Compute und Netzwerk**
   - Computetypen
   - Anwendungshosting
   - Virtuelle Netzwerke
3. **Speicher**
   - Speicherdienste
   - Redundanzoptionen
   - Dateiverwaltung und -migration
4. **Identität, Zugriff und Sicherheit**
   - Verzeichnisdienste
   - Authentifizierungsmethoden
   - Sicherheitsmodelle

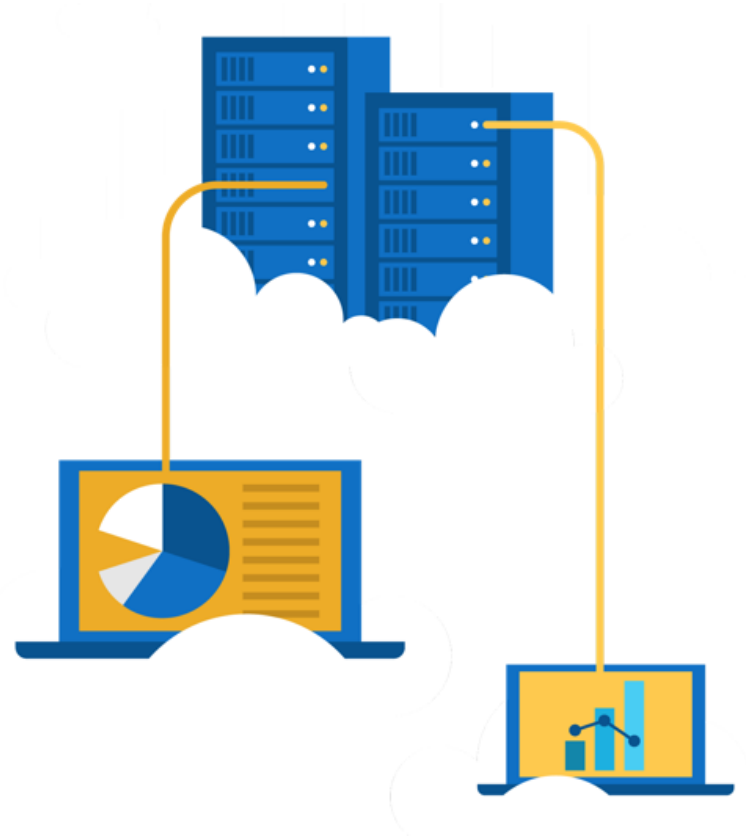
Azure-Konten

- Azure-Konto
- Kostenloses Azure-Konto
- Kostenloses Azure-Konto für Studierende
- Microsoft Learn-Sandbox

Übung: Erstellen eines Azure-Kontos

Erstellen eines kostenlosen Azure-Kontos

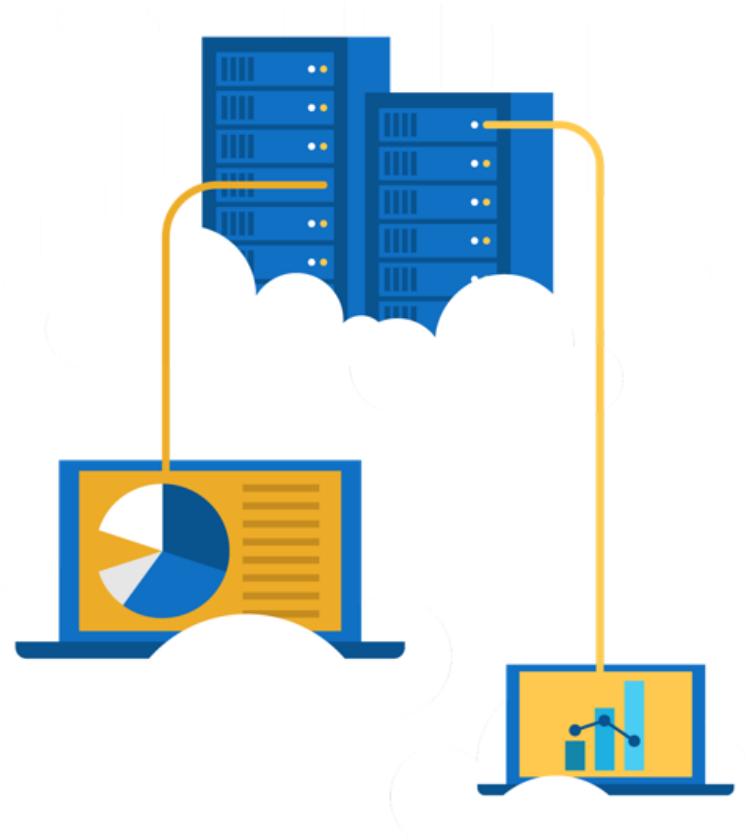
1. Erstellen eines kostenlosen Azure-Kontos



Übung: Erkunden der Sandbox in MS Learn

Erkunden der Sandbox in Learn

1. Aktivieren der Sandbox
2. Verwenden von PowerShell
3. Wechseln zu BASH
4. Wechseln zum interaktiven Azure-Modus
5. Navigieren im Portal



Komponenten der Azure-Architektur

Wichtige Komponenten der Azure-Architektur

Lernziele

- Beschreiben von Azure-Regionen, Regionspaaren und unabhängigen Regionen
- Beschreiben von Verfügbarkeitszonen
- Beschreiben von Azure-Rechenzentren
- Beschreiben von Azure-Ressourcen und -Ressourcengruppen
- Beschreiben von Abonnements
- Beschreiben von Verwaltungsgruppen
- Beschreiben der Hierarchie von Ressourcengruppen, Abonnements und Verwaltungsgruppen

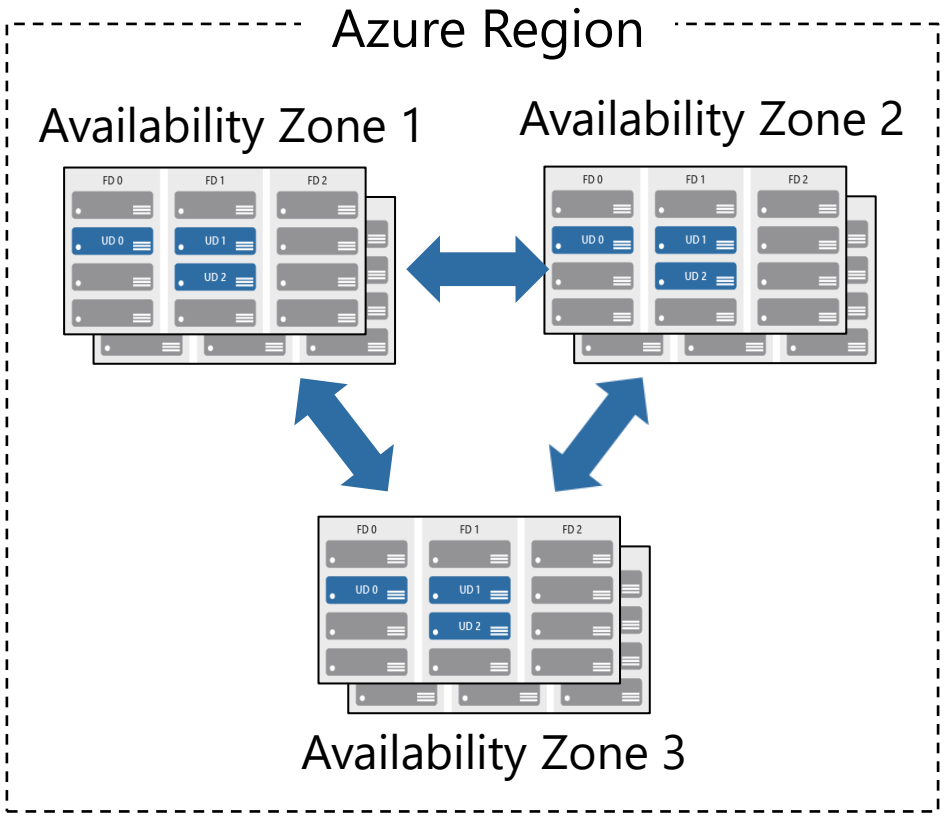
Regionen

Mit mehr als 60 Regionen, die über 140 Länder repräsentieren, bietet Azure mehr globale Regionen an als alle anderen Cloudanbieter

- Regionen bestehen aus einem oder mehreren Rechenzentren, die nahe beieinander liegen.
- Bieten Sie Flexibilität und Skalierbarkeit, um die Wartezeit für Kunden zu reduzieren.
- Schützen Sie Ihre Data Residency mit einem umfassenden Compliance-Angebot.

Verfügbarkeitszonen (Availability Zones)

- Bieten Schutz vor Ausfällen aufgrund von Störungen im Rechenzentrum.
- Physisch getrennte Rechenzentren innerhalb derselben Region.
- Jedes Rechenzentrum ist mit unabhängiger Stromversorgu Kühlung und unabhängigem Netzwerk ausgestattet.
- Die Rechenzentren sind über private Glasfasernetze miteinander verbunden.



Regionspaare

- Mindestens 480 km (300 Meilen) zwischen Regionspaaren.
- Automatische Replikation für bestimmte Dienste.
- Vorrang bei der Regionswiederherstellung nach einem Ausfall.
- Updates werden nacheinander installiert, um Ausfallzeiten zu minimieren.
- Web link: https://aka.ms/PairedRegions-ger

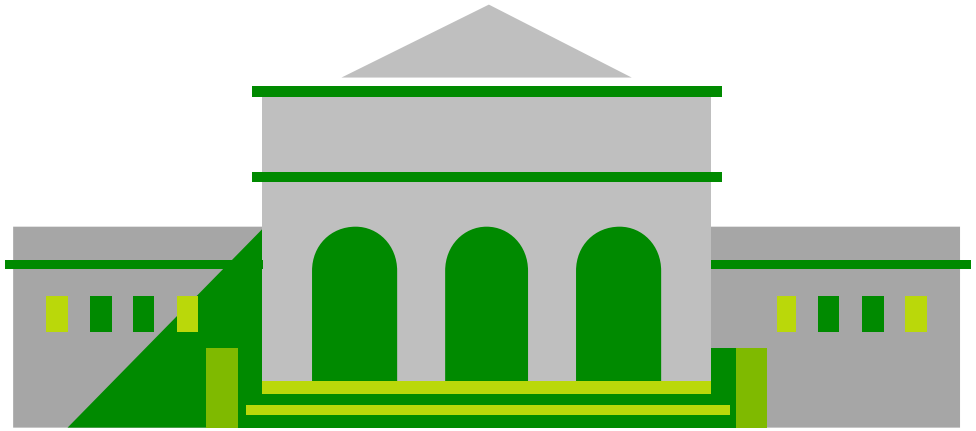
Region	Region
North Central US	South Central US
East US	West US
West US 2	West Central US
US East 2	Central US
Canada Central	Canada East
North Europe	West Europe
UK West	UK South
Germany Central	Germany Northeast
South East Asia	East Asia
East China	North China
Japan East	Japan West
Australia Southeast	Australia East
India South	India Central
Brazil South (Primary)	South Central US

Azure Sovereign Regions (Dienste für US-Regierungsbehörden)

Erfüllt die Sicherheits- und Compliance-Anforderungen von US-Bundesbehörden, Bundesstaaten und Kommunen sowie deren Lösungsanbietern.

Azure Government:

- Separate Instanz von Azure.
- Physisch isoliert von Bereitstellungen außerhalb der US-Regierung.
- Nur für abgeschirmtes, autorisiertes Personal zugänglic



Azure Sovereign Regions (Azure China)

Microsoft is China's first foreign public cloud service provider, in compliance with government regulations.

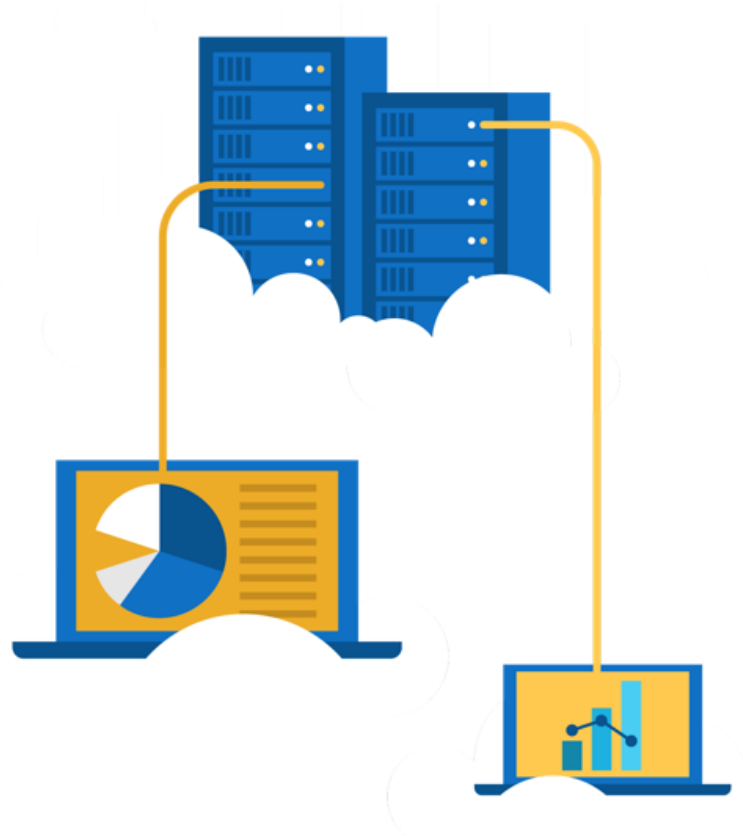
Features von Azure China:

- Physisch getrennte Instanz von Azure-Clouddiensten, betrieben von 21Vianet
- Die Daten bleiben in China, um die Complianceanforderungen zu erfüllen

Übung:
Erkunden der globalen Azure-Infrastruktur

Erkunden der globalen Azure-Infrastruktur

1. Wählen Sie **Explore the Globe** (nach der Einführung) aus.
2. Beachten Sie die verschiedenen Symbole (Geografie, Regionen, Points of Presence (PoPs) und so weiter).
3. Suchen Sie Ihre Position auf der Weltkarte, und suchen Sie dann nächsten PoP und die nächste Region für Ihren Standort.



Azure-Ressourcen

Azure-**Ressourcen** sind Komponenten wie Speicher, virtuelle Computer und Netzwerke, die zur Erstellung von Cloudlösungen verwendet werden.

Virtuelle Maschinen

Speicherkonten

Virtuelle Netzwerke

App Services

SQL-Datenbanken

Funktionen

Ressourcengruppen

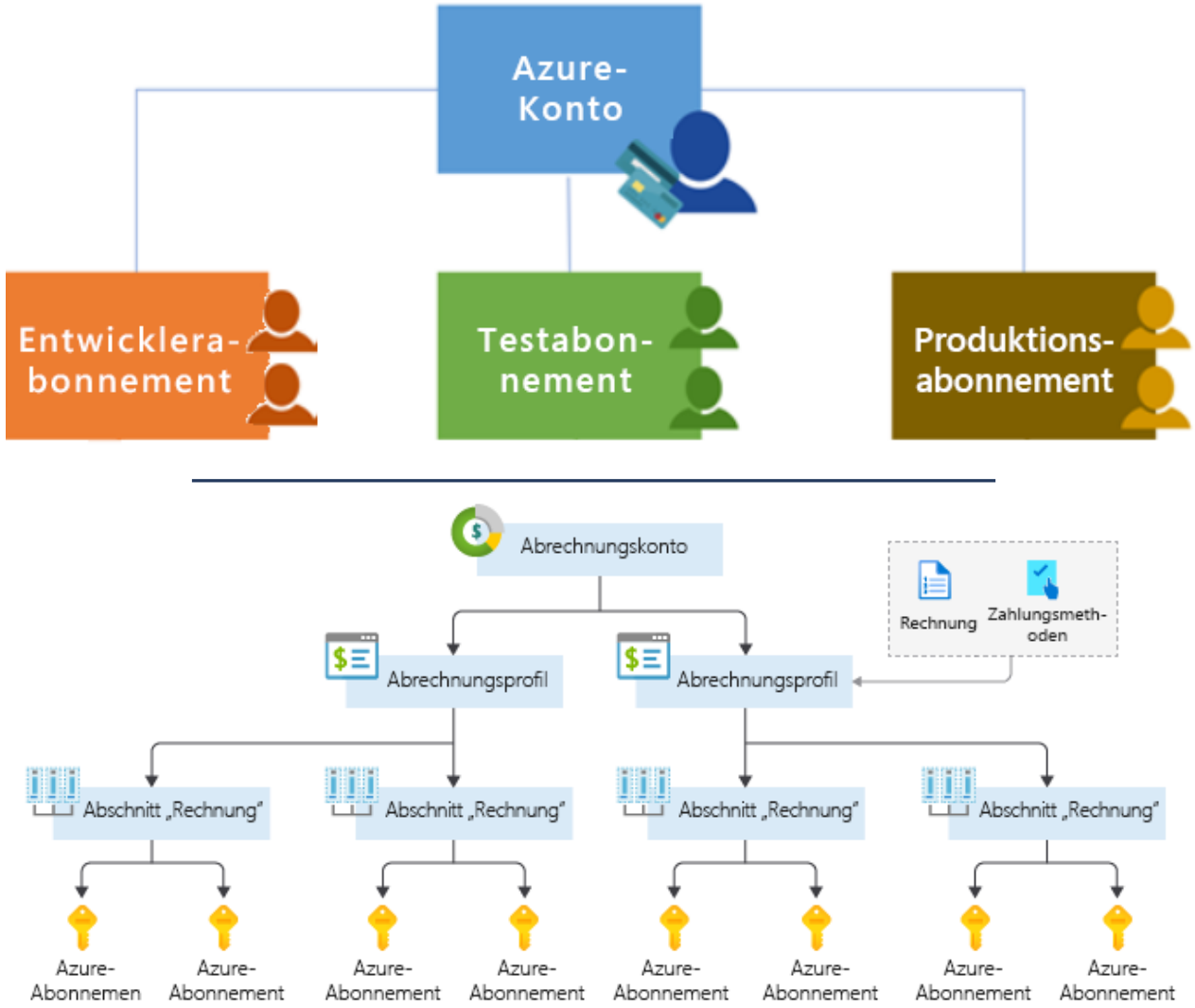
Eine **Ressourcengruppe** ist ein Container, mit dem Ressourcen als eine einzige Einheit verwaltet und aggregiert werden.

- Ressourcen können nur in einer Ressourcengruppe vorhanden sein.
- Ressourcen können sich in verschiedenen Regionen befinden.
- Ressourcen können in andere Ressourcengruppen verschoben werden.
- Anwendungen können mehrere Ressourcengruppen verwenden.

Azure Subscription (Abonnement)

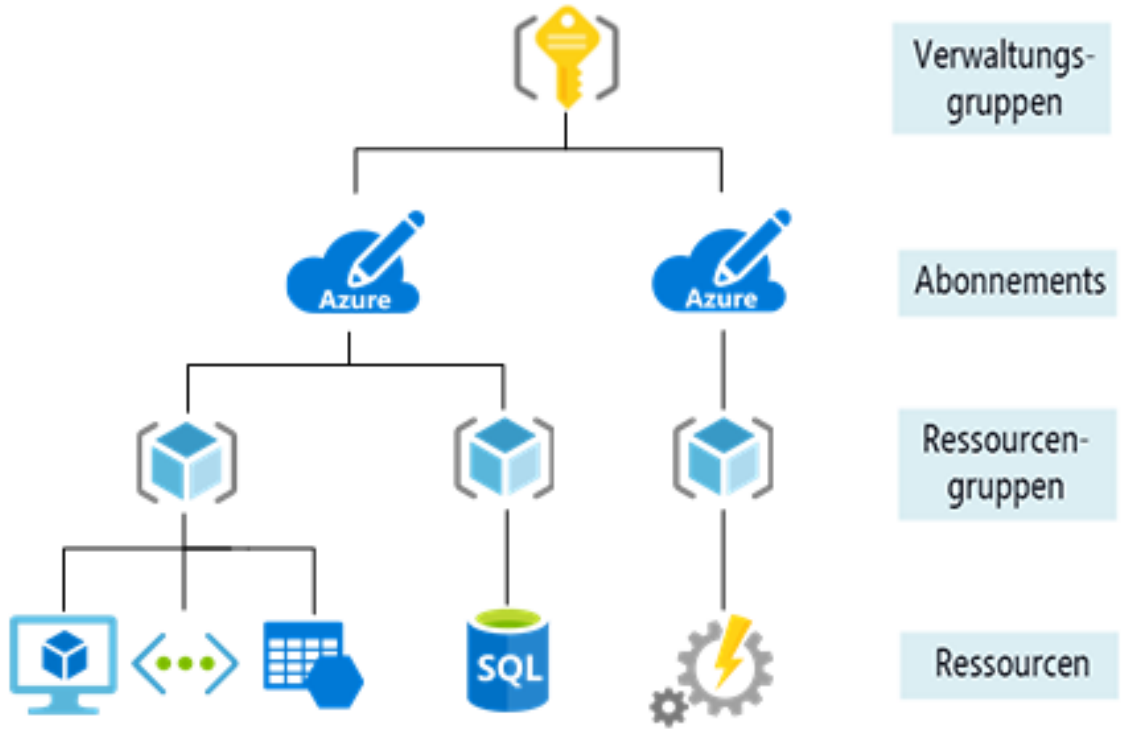
Mit einem Azure-Abonnement erhalten Sie authentifizierten und autorisierten Zugriff auf Azure-Konten.

- **Abrechnungsgrenze:** Generieren separater Abrechnungsberichte und Rechnungen für jedes Abonnement
- **Zugriffssteuerungsgrenze:** Verwalten und Steuern des Zugriffs auf die Ressourcen, die Benutzer*innen mit bestimmten Abonnements bereitstellen können



Verwaltungsgruppen (Management Groups)

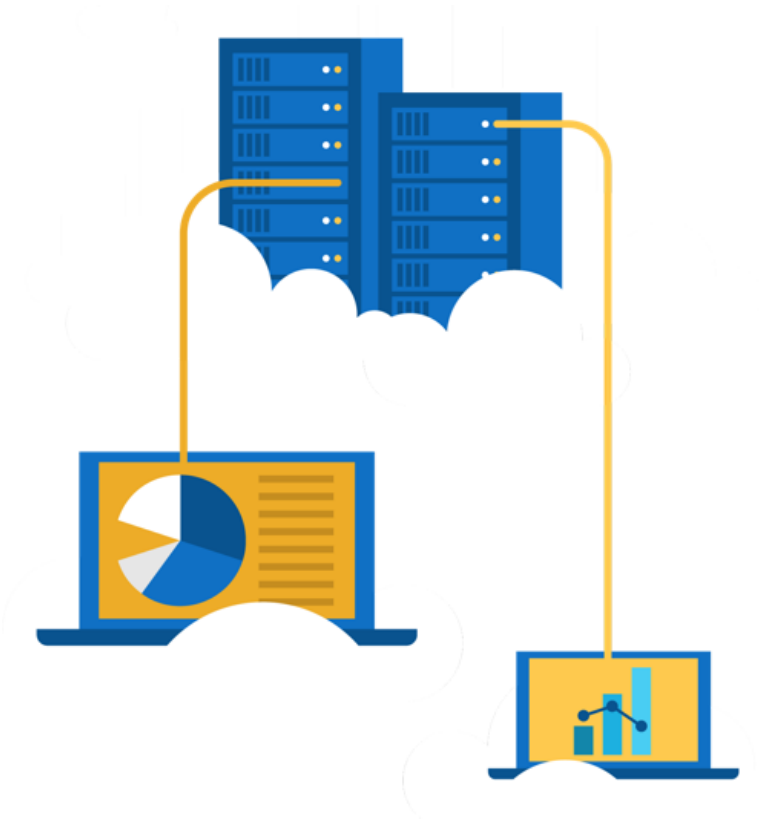
- Verwaltungsgruppen können mehrere Azure-Abonnements enthalten.
- Abonnements erben Bedingungen, die auf die Verwaltungsgruppe angewendet werden.
- 10.000 Verwaltungsgruppen können in einem einzigen Verzeichnis unterstützt werden.
- Eine Verwaltungsgruppenstruktur kann bis zu sechs Tiefenebenen unterstützen.



Übung: Erstellen einer Azure-Ressource

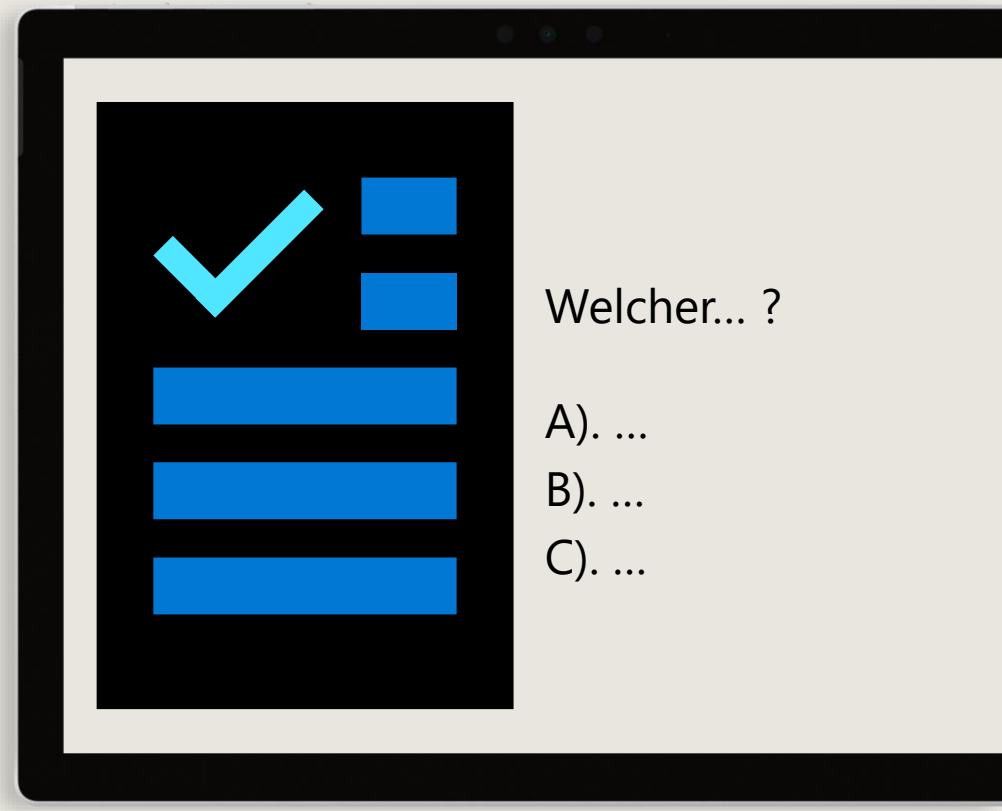
Erstellen einer Azure-Ressource und Überwachen der Ressourcengruppe auf erforderliche Ressourcen, die in derselben Gruppe erstellt werden

1. Erstellen Sie eine VM.
2. Überwachen Sie die Ressourcengruppe.



Quiz

Lernpfad 2:
Komponenten der Azure-Architektur



Compute und Netzwerk

Compute und Netzwerk

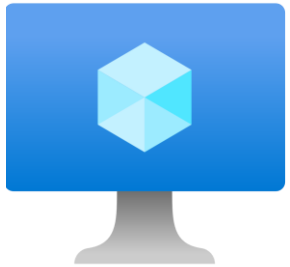
Lernziele

Beschreiben der Vorteile und der Nutzung von:

- Vergleichen von Computetypen, einschließlich Containerinstanzen, VMs und Funktionen.
- Beschreiben der VM-Optionen, einschließlich VMs, VM-Skalierungsgruppen, VM-Verfügbarkeitsgruppen und Azure Virtual Desktop
- Beschreiben der für VMs erforderlichen Ressourcen
- Beschreiben der Optionen für das Anwendungshosting, einschließlich Azure Web-Apps, Container und VMs.
- Beschreiben von virtuellen Netzwerken, einschließlich des Zwecks von Azure Virtual Networks, virtuellen Azure-Subnetzen, Peering, Azure DNS, VPN Gateway und ExpressRoute
- Definieren von öffentlichen und privaten Endpunkten

Azure-Compute-Dienste

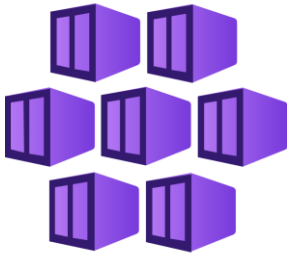
Azure **Compute** ist ein On-Demand-Computing-Dienst und stellt bei Bedarf Computing-Ressourcen wie Datenträger, Prozessoren, Speicher, Netzwerk und Betriebssysteme bereit.



Virtual Machines

App Services

Container Instances



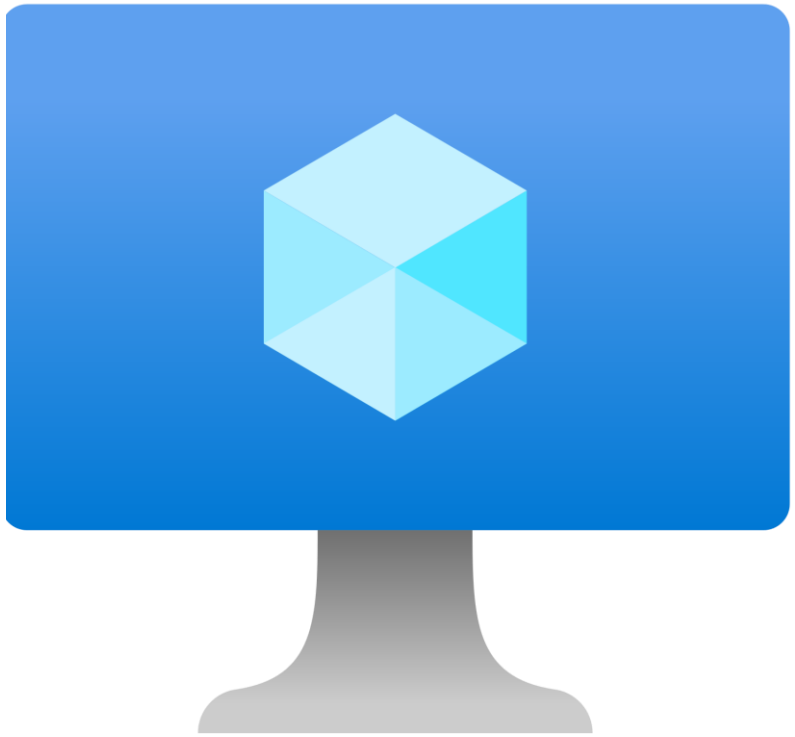
Azure Kubernetes Services (AKS)

Azure Virtual Desktop

Azure-VMs

Azure **Virtual Machines (VM)** stellen virtuelle Maschinen in der Cloud zur Verfügung.

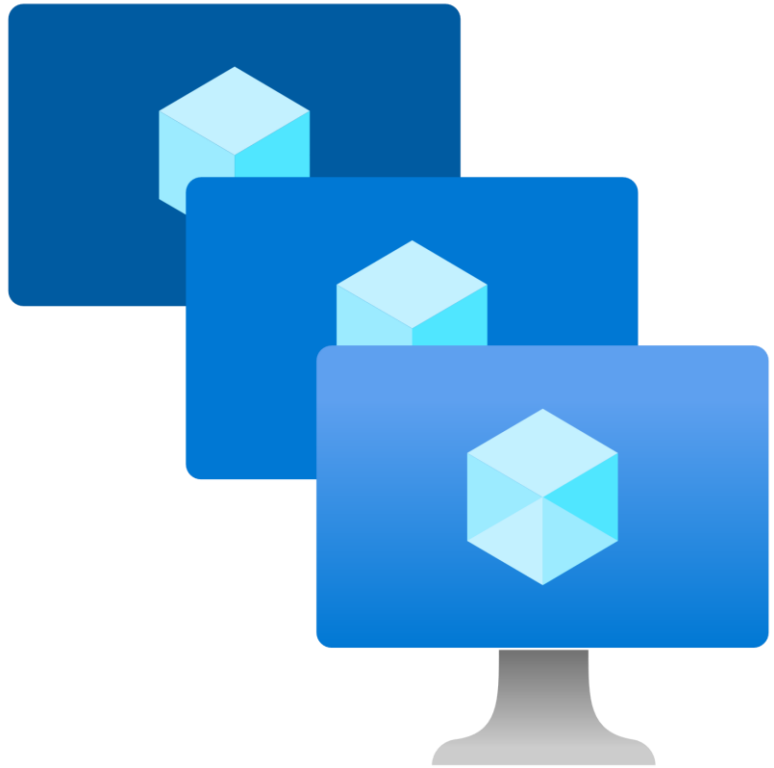
- Sie bestehen aus virtuellen Prozessoren, Arbeitsspeicher, Speicher und Netzwerkressourcen.
- IaaS-Angebot für volle Kontrolle und maximale Anpassungsmöglichkeiten.



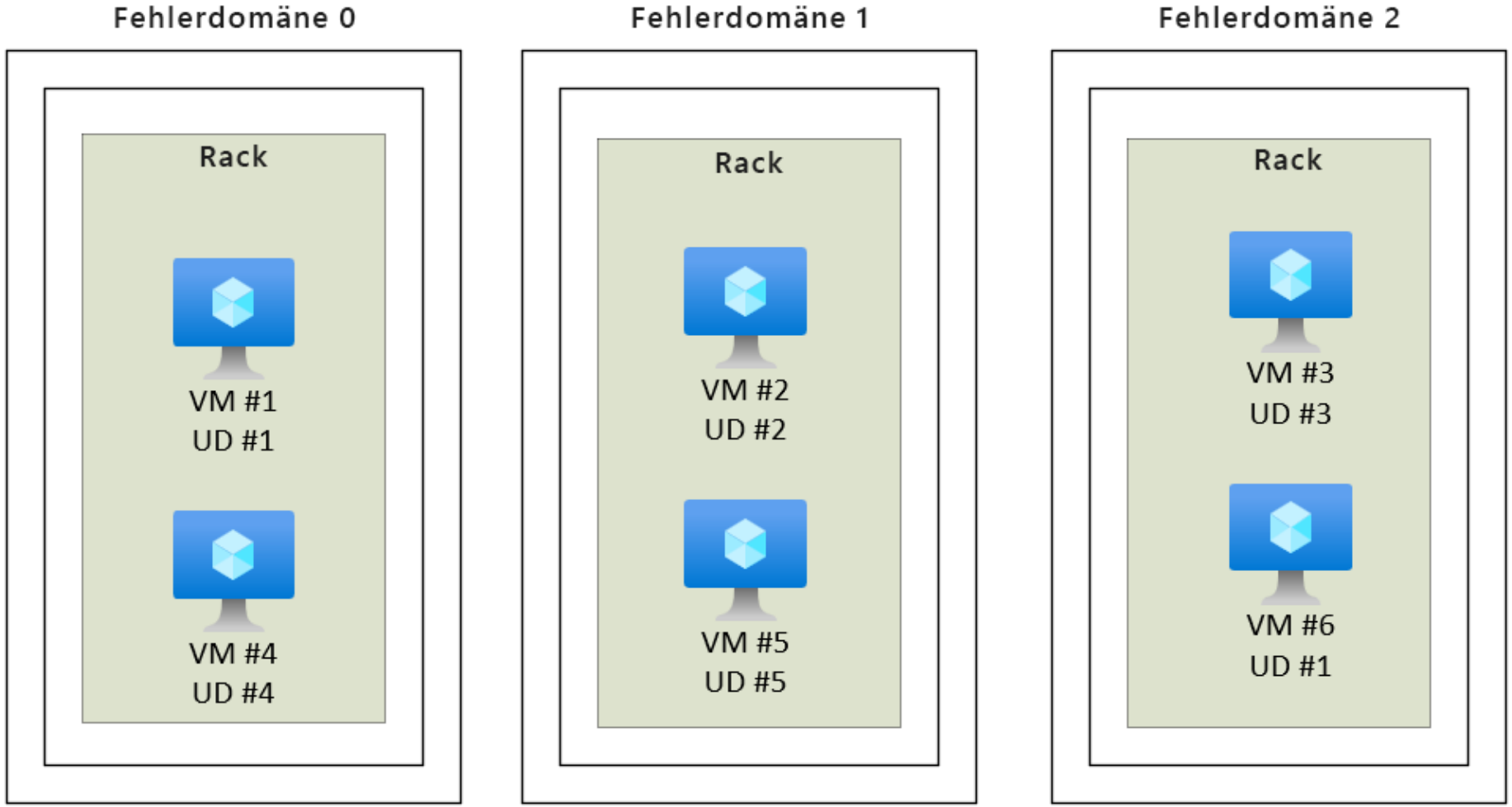
VM-Skalierungsgruppen

Mit Hilfe von Skalierungsgruppen kann ein Lastenausgleich vorgenommen werden, um Ressourcen automatisch zu skalieren.

- Skalieren Sie auf, wenn der Ressourcenbedarf steigt.
- Skalieren Sie ab, wenn der Ressourcenbedarf sinkt.



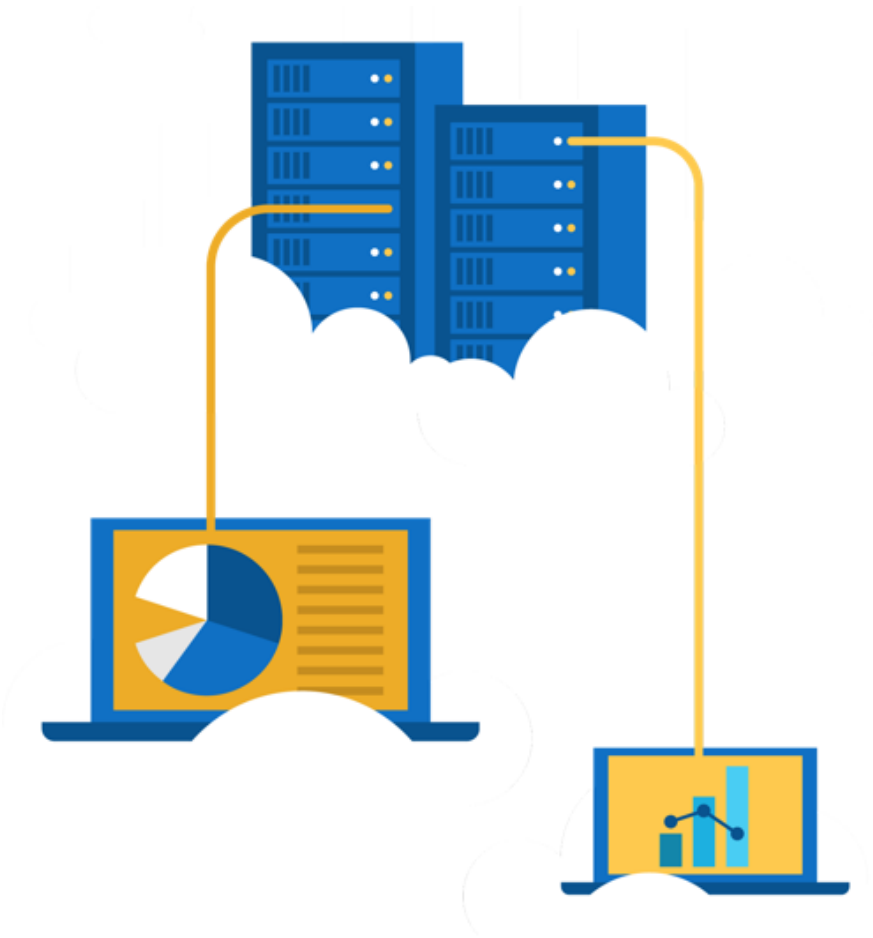
VM-Verfügbarkeitsgruppen (Availability Sets)



Übung: Erstellen einer VM

Erstellen Sie einen virtuellen Computer (VM) im Azure-Portal, stellen Sie eine Verbindung mit dem virtuellen Computer her, installieren Sie die Webserverrolle, und testen Sie.

1. Erstellen Sie die virtuelle Maschine.
2. Installieren Sie das Webserverpaket.



Azure Virtual Desktop

Bei **Azure Virtual Desktop** handelt es sich um einen in der Cloud ausgeführten Dienst für die Desktop- und App-Virtualisierung.

- Erstellen Sie eine komplette Desktopvirtualisierungsumgebung ohne zusätzliche Gatewayserver.
- Geringeres Risiko von zurückgelassenen Ressourcen
- Echte Multisessionbereitstellungen

Azure container services

Container sind eine ressourcenschonende, virtualisierte Umgebung, die keine Betriebssystemverwaltung erfordert und die bedarfsgesteuert auf Änderungen reagieren kann.

Azure Container Instances: Ein PaaS-Angebot (Platform-as-a-Service), das einen Container oder einen Pod von Containern in Azure ausführt.

Azure Container Apps: Ein PaaS-Angebot wie Containerinstanzen, mit dem ein Lastausgleich und Skalierungen vorgenommen werden können.

Azure Kubernetes Service: Ein Orchestrierungsdienst für Container mit verteilten Architekturen und großen Containervolumes.

Azure Functions

Azure Functions: Hierbei handelt es sich um ein PaaS-Angebot, das serverlose Computingvorgänge unterstützt. Ereignisbasierter Code wird ausgeführt, wenn dieser während inaktiver Phasen aufgerufen wird, ohne dass dafür Serverinfrastruktur benötigt wird.

Vergleich von Azure Compute-Optionen

Virtual machines

- Cloudbasierter Server, der Windows- oder Linux-Umgebungen unterstützt.
- Hilfreich bei Migrationen in die Cloud per Lift & Shift.
- Vollständiges Betriebssystempaket, einschließlich des Hostbetriebssystems.

Virtual Desktop

- Stellt eine cloudbasierte Windows-PC-Desktopumgebung bereit.
- Dedizierte Anwendungen zur Verbindung und Nutzung oder zugänglich über jeden modernen Browser.
- Die Möglichkeit zur Anmeldung mehrerer Clients ermöglicht es mehreren Benutzern, sich gleichzeitig auf demselben Computer anzumelden.

Containers

- Leichte Miniaturumgebung, die gut für die Ausführung von Microservices geeignet ist.
- Entwickelt für Skalierbarkeit und Resilienz durch Orchestrierung.
- Anwendungen und Dienste sind in einem Container enthalten, der auf dem Hostbetriebssystem basiert. Auf einem Hostbetriebssystem können mehrere Container basieren.

Azure App Services

Azure **App Services** ist eine vollständig verwaltete Plattform zum schnellen Erstellen, Bereitstellen und Skalieren von Web-Apps und APIs.

- Der Dienst funktioniert mit .NET, .NET Core, Node.js, Java, Python oder php.
- PaaS-Angebot mit Leistung, Sicherheit und Compliance-Anforderungen auf Enterprise-Level.

Azure-Netzwerkdienste

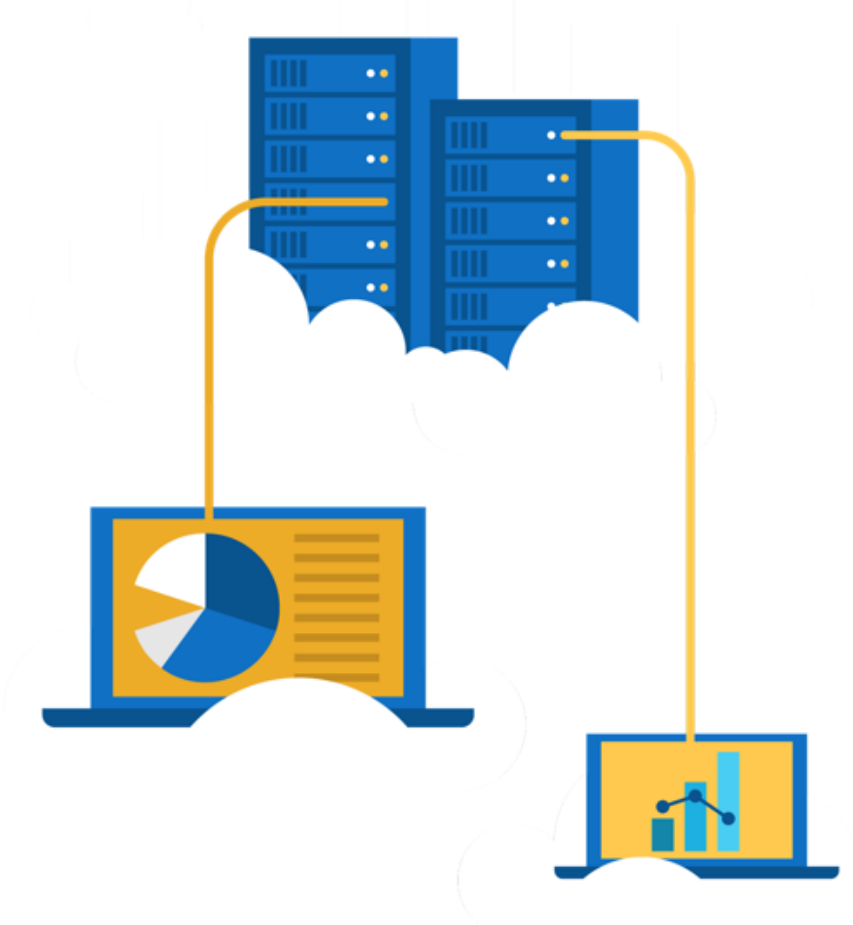
Über **Azure Virtual Network (VNet)** können verschiedene Azure-Ressourcen miteinander, mit dem Internet und mit lokalen Netzwerken kommunizieren.

- Öffentliche Endpunkte, zugänglich von überall im Internet
- Private Endpunkte, auf die nur innerhalb Ihres Netzwerks zugegriffen werden kann
- Virtuelle Subnetze zum Unterteilen Ihres Netzwerks für Ihre Anforderungen
- Netzwerk-Peering, zum direkten Verknüpfen Ihrer privaten Netzwerke

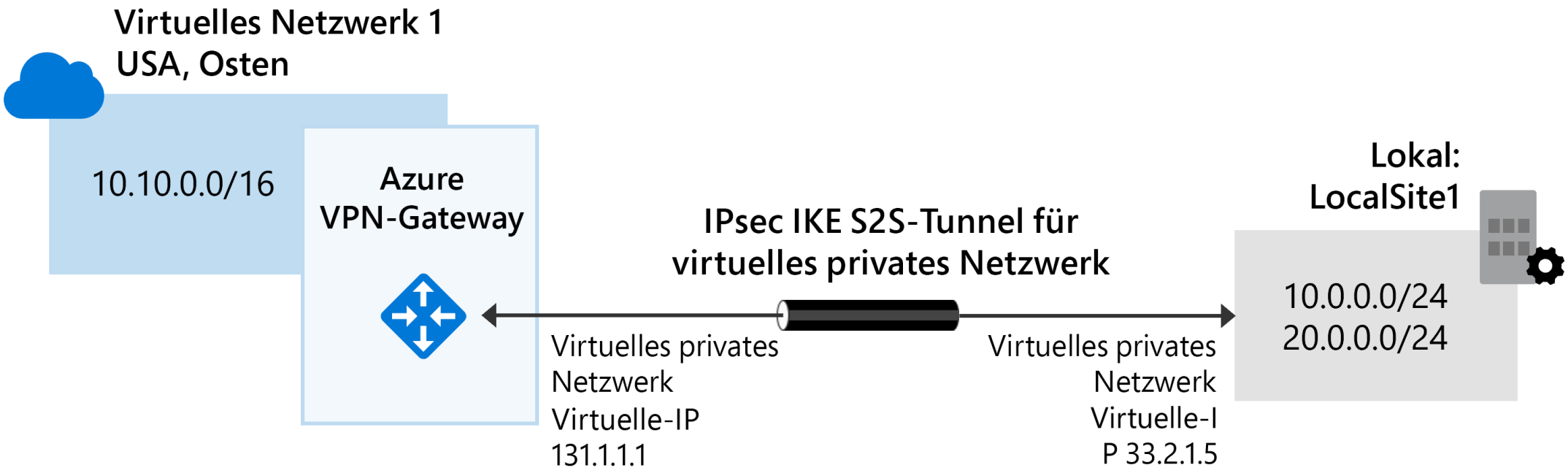
Übung: Konfigurieren des Netzwerkzugriffs

Konfigurieren des öffentlichen Zugriffs auf die zuvor erstellte VM

1. Überprüfen der derzeit geöffnete Ports
2. Erstellen einer Netzwerksicherheitsgruppe
3. Konfigurieren des HTTP-Zugriffs (Port 80)
4. Testen der Verbindung.

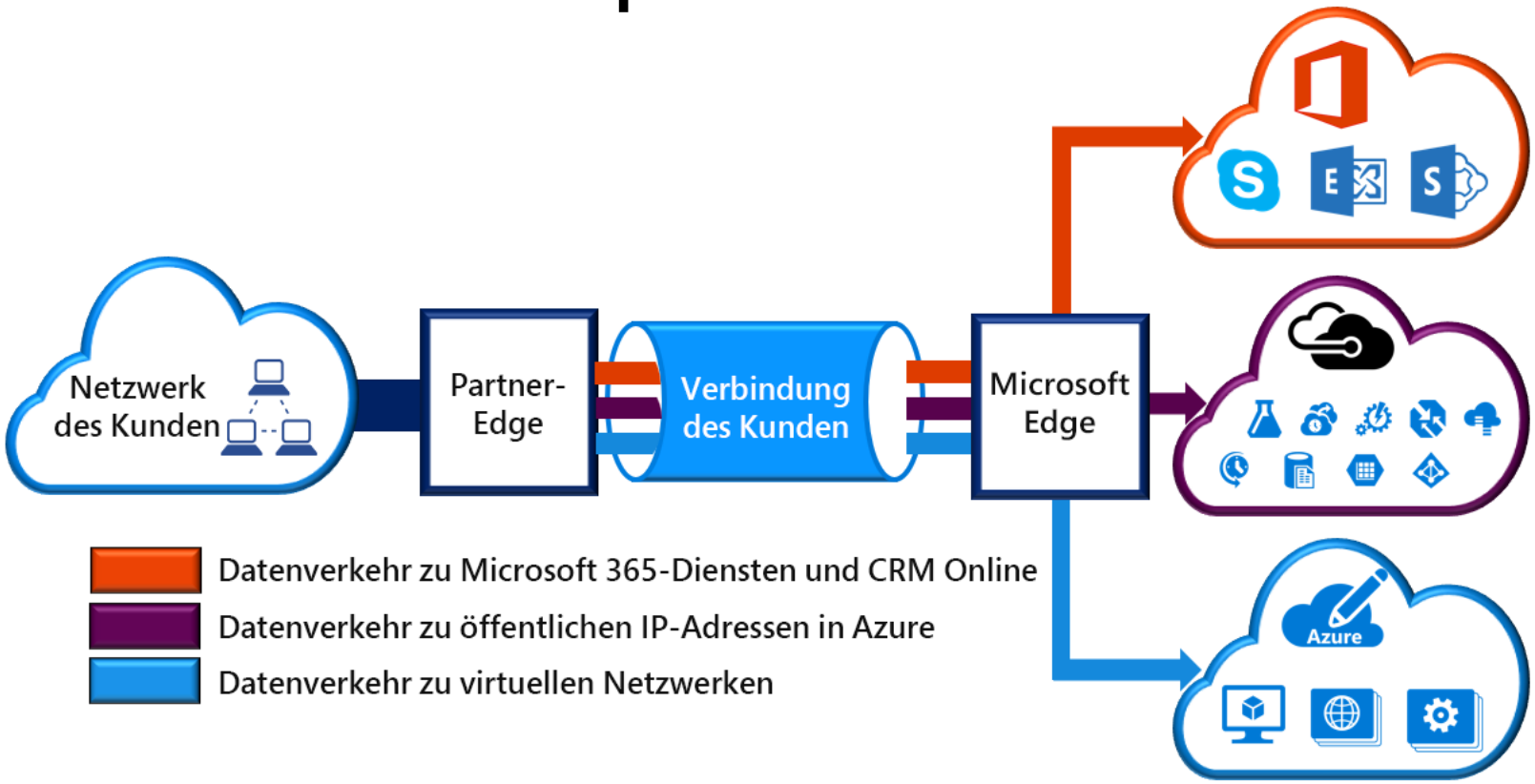


Azure-Netzwerkdienste: VPN Gateway



VPN Gateway wird verwendet, um verschlüsselten Datenverkehr zwischen einem virtuellen Azure-Netzwerk und einem lokalen Standort über das öffentliche Internet zu senden.

Azure-Netzwerkdienste: Express Route



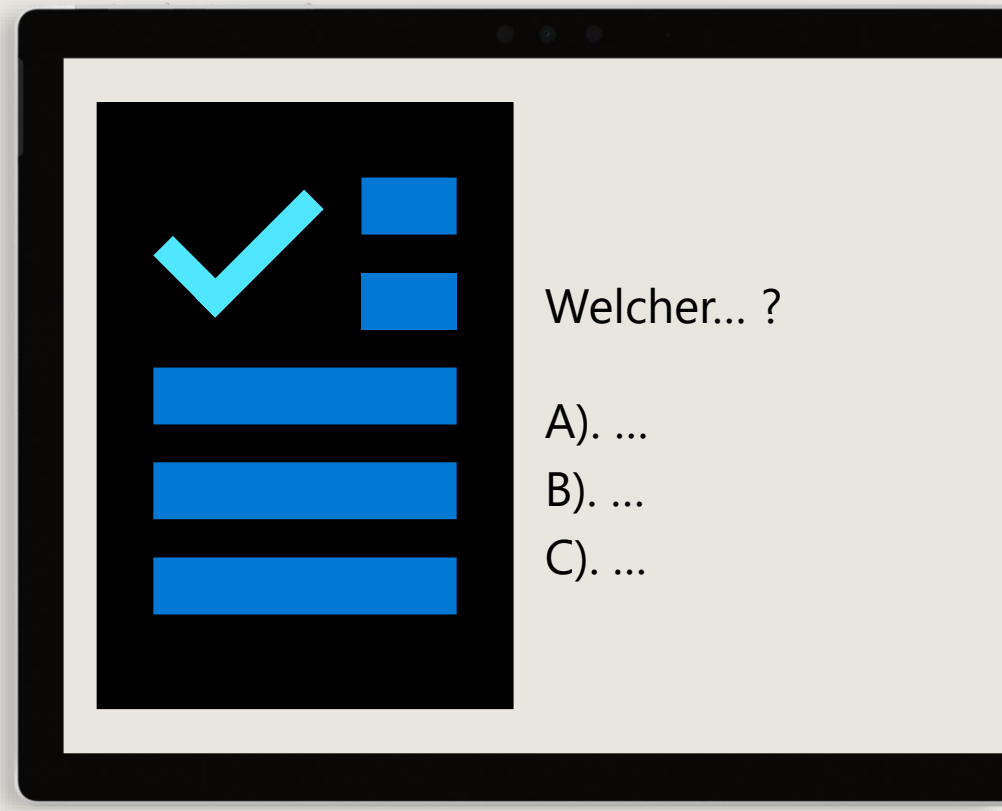
ExpressRoute erweitert lokale Netzwerke in Azure über eine private Verbindung, die durch einen Konnektivitätsanbieter ermöglicht wird.

Azure DNS

- Zuverlässigkeit und Leistung durch Nutzung eines globalen Netzwerks von DNS-Servern mithilfe von Anycast-Netzwerken.
- Die Azure DNS-Sicherheit basiert auf dem Azure-Ressourcen-Manager und aktiviert die rollenbasierte Zugriffssteuerung, -überwachung und -protokollierung.
- Benutzerfreundlichkeit für die Verwaltung Ihrer Azure- und externen Ressourcen mit einem einzigen DNS-Dienst.
- Durch anpassbare virtuelle Netzwerke können Sie private, vollständig angepasste Domänennamen in privaten virtuellen Netzwerken verwenden.
- Aliasdatensätze unterstützen Aliasdatensatzgruppen beim unmittelbaren Verweisen auf eine Azure-Ressource.

Quiz

Lernpfad 2:
Compute und Netzwerk



Speicher

Speicher

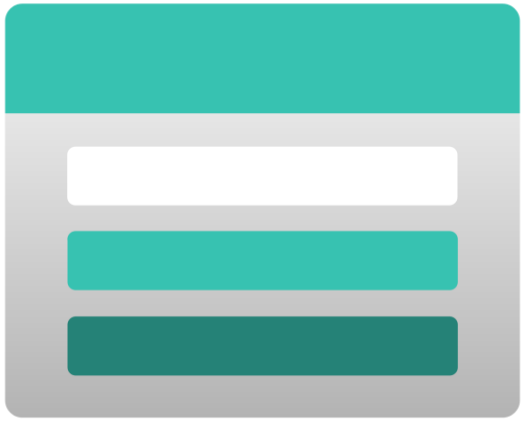
Lernziele

Beschreiben der Vorteile und der Nutzung von:

- Vergleichen der Azure-Speicherdienste
- Beschreiben von Speicherebenen
- Beschreiben von Redundanzoptionen
- Speicherkontooptionen und Speichertypen
- Optionen für die Verschiebung von Dateien, einschließlich AzCopy, Azure Storage-Explorer und Azure-Dateisynchronisierung.
- Beschreiben von Migrationsoptionen wie Azure Migrate und Azure Data Box

Speicherkonten

- Müssen einen global eindeutigen Namen aufweisen
- Stellen weltweiten Zugriff über das Internet bereit
- Bestimmen Speicherdienste und Redundanzoptionen



Speicherredundanz

Redundanzkonfiguration	Bereitstellung	Dauerhaftigkeit
Lokal redundanter Speicher (LRS)	Einzelnes Rechenzentrum in der primären Region	11 Neunen
Zonenredundanter Speicher (ZRS)	Drei Verfügbarkeitszonen in der primären Region	12 Neunen
Georedundanter Speicher (GRS)	Einzelnes Rechenzentrum in der primären und sekundären Region	16 Neunen
Geozonenredundanter Speicher (GZRS)	Drei Verfügbarkeitszonen in der primären Region und ein einzelnes Rechenzentrum in sekundärer Region	16 Neunen

Azure-Speicherdienste

Azure Blob: Für die Speicherung großer Mengen unstrukturierter Daten wie Text oder Binärdaten optimiert.

Azure Disk: Stellt Datenträger für VMs, Anwendungen und andere Dienste zur Verfügung.

Azure Queue: Nachrichtenspeicherdienst, der das Speichern und Abrufen für große Mengen von Nachrichten ermöglicht, jeweils bis zu 64 KB.

Azure Files: Richtet die hochverfügbare Netzwerkdateifreigabe ein, die über das SMB-Protokoll (Server Message Block) erreichbar ist.

Azure Tables: Bietet eine Schlüssel-/Attributoption für strukturierten, nichtrelationalen Datenspeicher mit schemalosem Entwurf.

Öffentliche Endpunkte des Speicherdiensts

Speicherdienst	Öffentlicher Endpunkt
Blob Storage	https://<storage-account-name>.blob.core.windows.net
Data Lake Storage Gen2	https://<storage-account-name>.dfs.core.windows.net
Azure Files	https://<storage-account-name>.file.core.windows.net
Queue Storage	https://<storage-account-name>.queue.core.windows.net
Table Storage	https://<storage-account-name>.table.core.windows.net

Azure storage access tiers

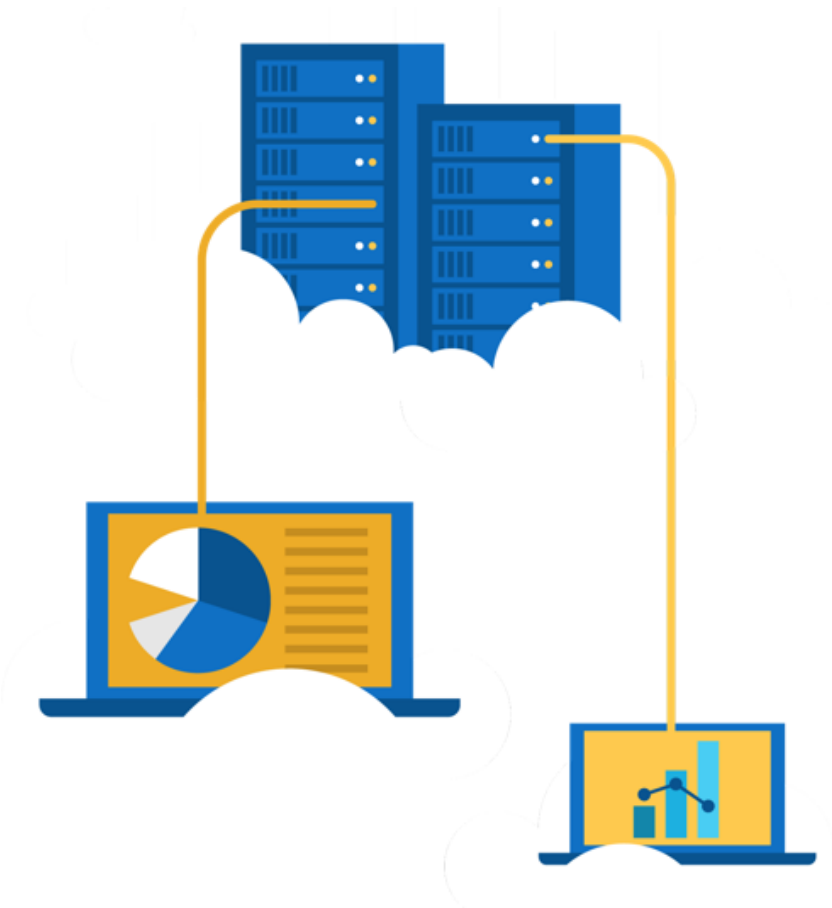
Hot	Cool	Cold	Archive
Optimiert für Daten, auf die häufig zugegriffen wird.	Optimiert für Daten, auf die weniger häufig zugegriffen wird und die mindestens 30 Tage lang aufbewahrt werden.	Optimiert für Daten, auf die weniger häufig zugegriffen wird und die mindestens 90 Tage lang aufbewahrt werden.	Optimiert für Daten, auf die selten zugegriffen wird und die mindestens 180 Tage lang mit flexiblen Wartezeit-anforderungen aufbewahrt werden.

Sie können jederzeit zwischen den Zugriffsebenen wechseln.

Übung: Erstellen eines Speicherblobs

Erstellen Sie ein Speicherkonto mit einem Blobspeichercontainer. Arbeiten Sie mit Blobdateien.

1. Erstellen Sie ein Speicherkonto.
2. Erstellen Sie einen Blobcontainer.
3. Laden Sie einen Blob hoch, und greifen Sie darauf zu.



Azure Migrate

- Einheitliche Migrationsplattform
- Verschiedene integrierte und eigenständige Tools
- Bewertung und Migration

Azure Data Box

- Speichern Sie bis zu 80 Terabytes an Daten.
- Verschieben Sie Ihre Sicherungen für die Notfallwiederherstellung in Azure.
- Schützen Sie Ihre Daten während des Transports in einem Schutzbehälter.
- Migrieren Sie Daten aus Azure, um die Einhaltung von Vorschriften oder gesetzlichen Bestimmungen zu gewährleisten.
- Migrieren Sie Daten von Remotestandorten mit eingeschränkter oder fehlender Konnektivität in Azure.

Dateiverwaltungsoptionen

AzCopy

- Befehlszeilen-Hilfsprogramm
- Kopieren von Blobs oder Dateien in oder aus Ihrem Speicherkonto
- Unidirektionale Synchronisierung

Azure Storage Explorer

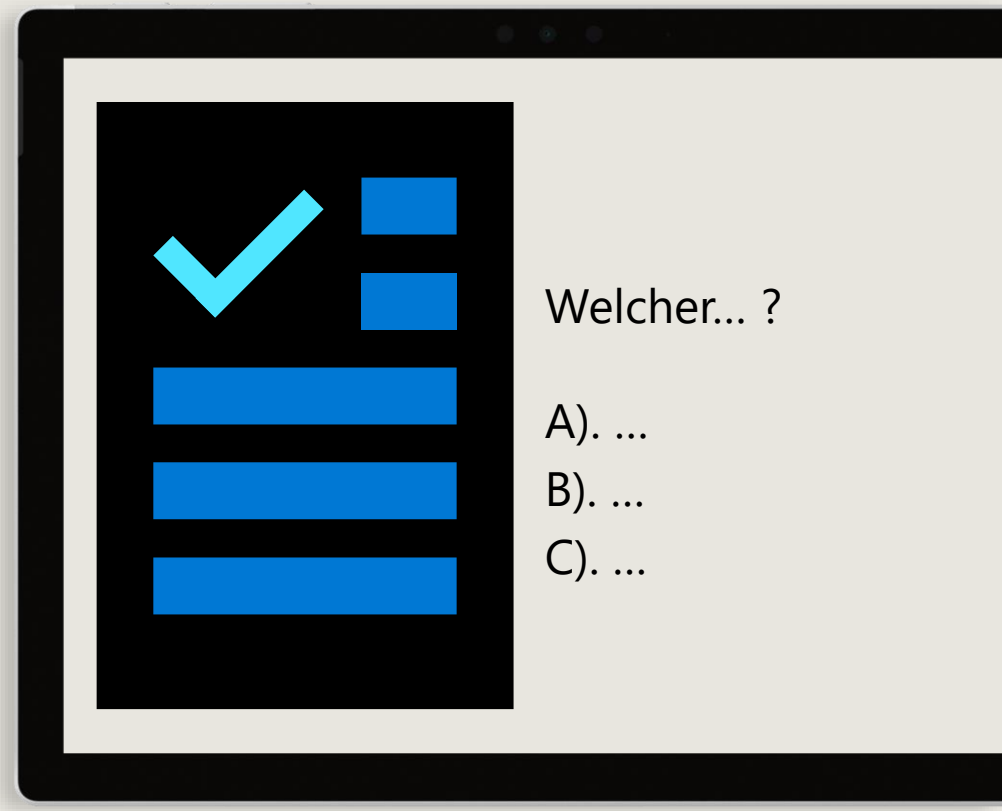
- Grafische Benutzeroberfläche (ähnlich wie der Windows-Explorer)
- Kompatibel mit Windows, macOS und Linux
- Verwendet AzCopy zum Verarbeiten von Dateivorgängen

Azure File Sync

- Synchronisiert Azure und lokale Dateien auf bidirektionale Weise
- Mit Cloudtiering bleiben häufig aufgerufene Dateien lokal, während Speicherplatz freigegeben wird
- Schnelle Neubereitstellung von fehlgeschlagenen lokalen Servern (Installation und Neusynchronisierung)

Quiz

Lernpfad 2: Speicher



Identität, Zugriff und Sicherheit

Identität, Zugriff und Sicherheit:

Lernziele

Beschreiben der Vorteile und der Nutzung von:

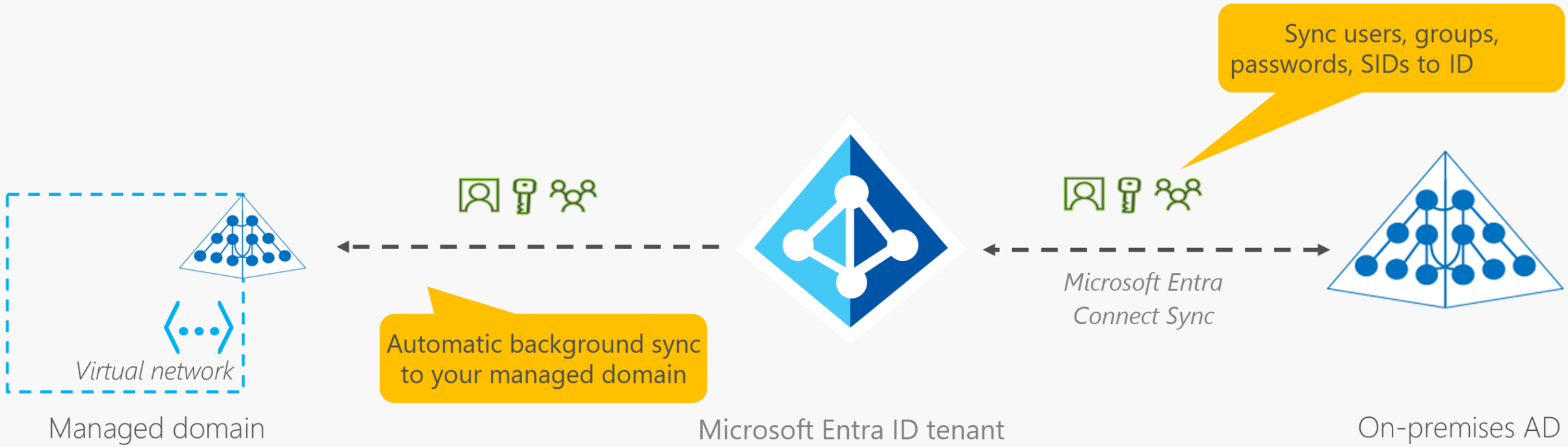
- Verzeichnisdienste in Azure, einschließlich Azure Active Directory (Azure AD) und Azure AD DS (Azure Active Directory Domain Services), ein Teil von Microsoft Entra.
- Authentifizierungsmethoden in Azure, einschließlich einmaligem Anmelden (Single Sign-On, SSO), Multi-Faktor-Authentifizierung (MFA) und kennwortloser Authentifizierung.
- Externe Identitäten und Gastzugriff in Azure
- Bedingter Zugriff von Azure AD
- Rollenbasierte Zugriffssteuerung in Azure (Role Based Access Control, RBAC)
- Zero Trust-Konzept.
- Zweck des Defense-in-Depth-Modells
- Zweck von Microsoft Defender für Cloud

Microsoft Entra ID (ehemals Azure Active Directory)

Microsoft Entra ID ist der cloudbasierte Identitäts- und Zugriffsverwaltungsdienst von Microsoft Azure.

- Authentifizierung (Mitarbeiter melden sich an, um auf Ressourcen zuzugreifen).
- Einmaliges Anmelden (Single Sign-On, SSO).
- Anwendungsverwaltung.
- Business-to-Business (B2B).
- Business-to-Customer-Identitätsdienste (B2C).
- Geräteverwaltung.

Microsoft Entra Domain Services



- Nutzen von cloudbasierten Domänendiensten ohne Verwaltung von Domänencontrollern
- Ausführen von Legacyanwendungen (die keine modernen Auth-Standards verwenden können) in der Cloud
- Automatische Synchronisierung von Azure AD

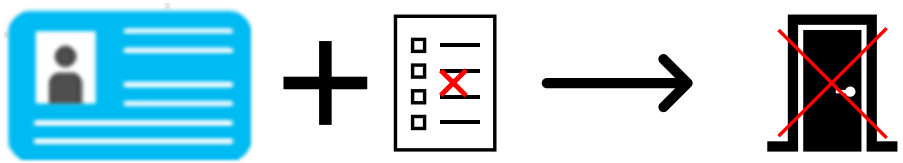
Authentifizierung und Autorisierung im Vergleich

Authentifizierung

- Identifiziert die Person oder den Dienst, die Zugriff auf eine Ressource anfordert.
- Fordert legitime Anmeldeinformationen an.
- Grundlage für die Schaffung sicherer Identitäts- und Zugriffssteuerungsprinzipien.

Autorisierung

- Bestimmt die Zugriffsebene einer authentifizierten Person oder eines authentifizierten Diensts.
- Definiert, auf welche Daten sie zugreifen können und was sie mit diesen tun können.

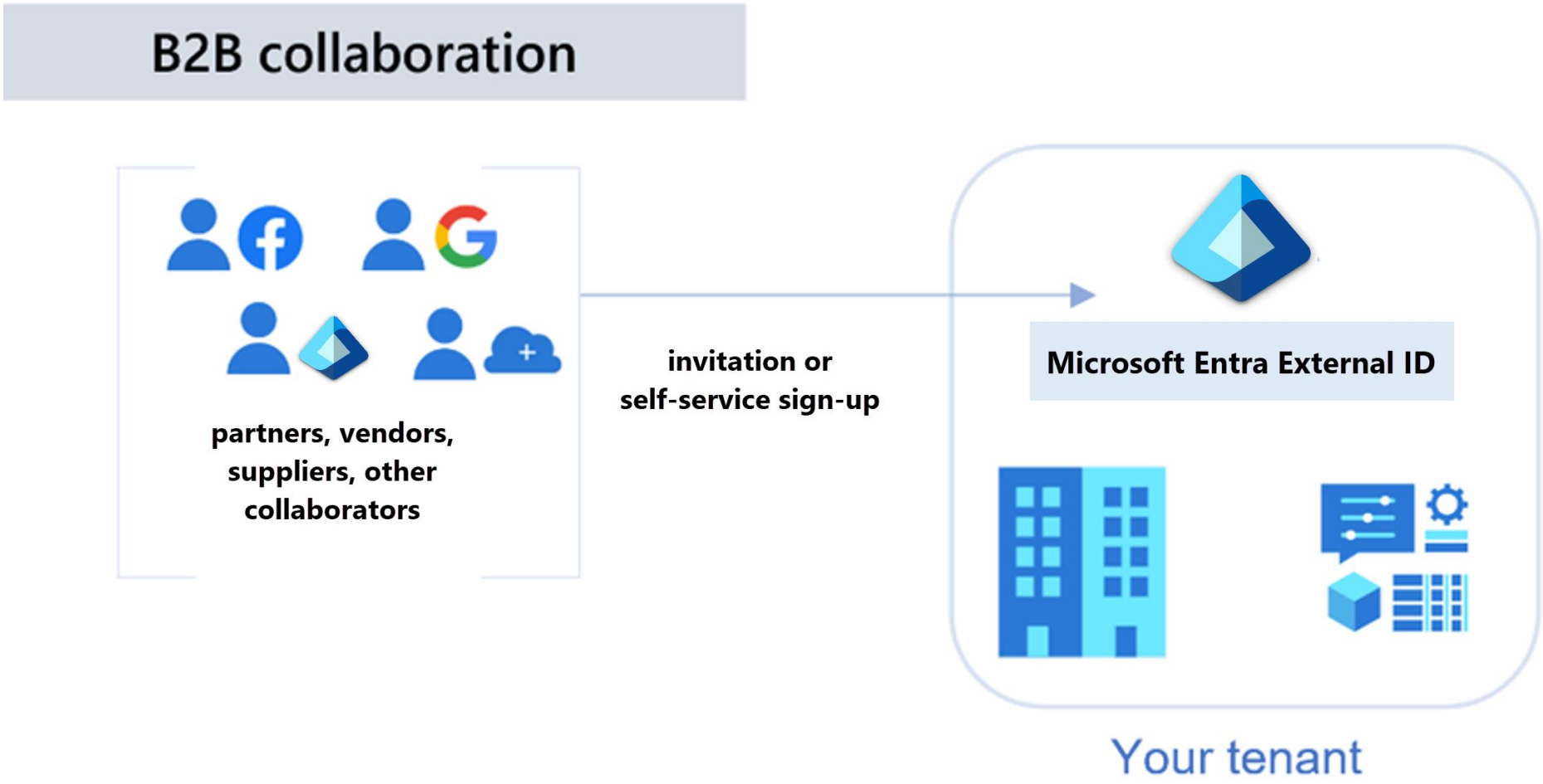


Mehrstufige Authentifizierung in Azure

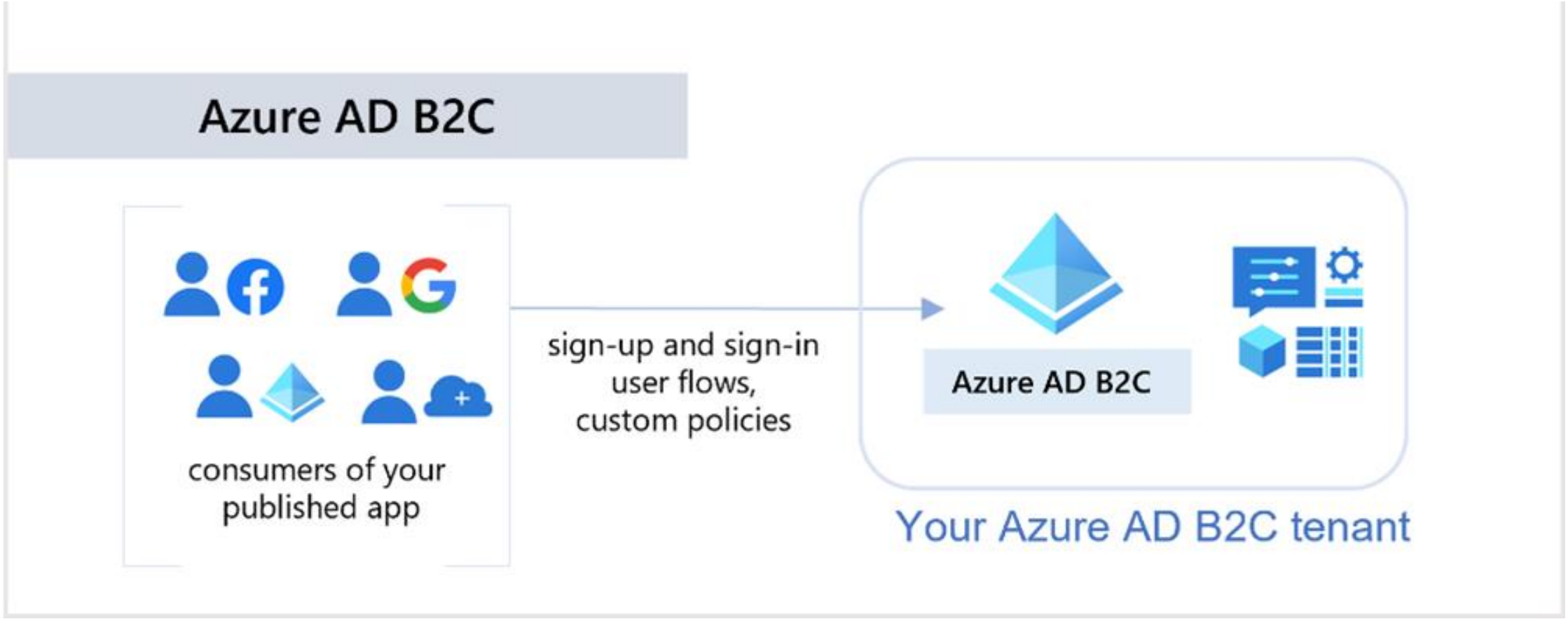
Bietet zusätzliche Sicherheit für Ihre Identität, indem mindestens zwei Komponenten für die vollständige Authentifizierung erforderlich sind.

- Etwas, das Sie wissen ←→ Etwas, das Sie besitzen ←→ Etwas, das Sie sind

Microsoft Entra External ID B2B



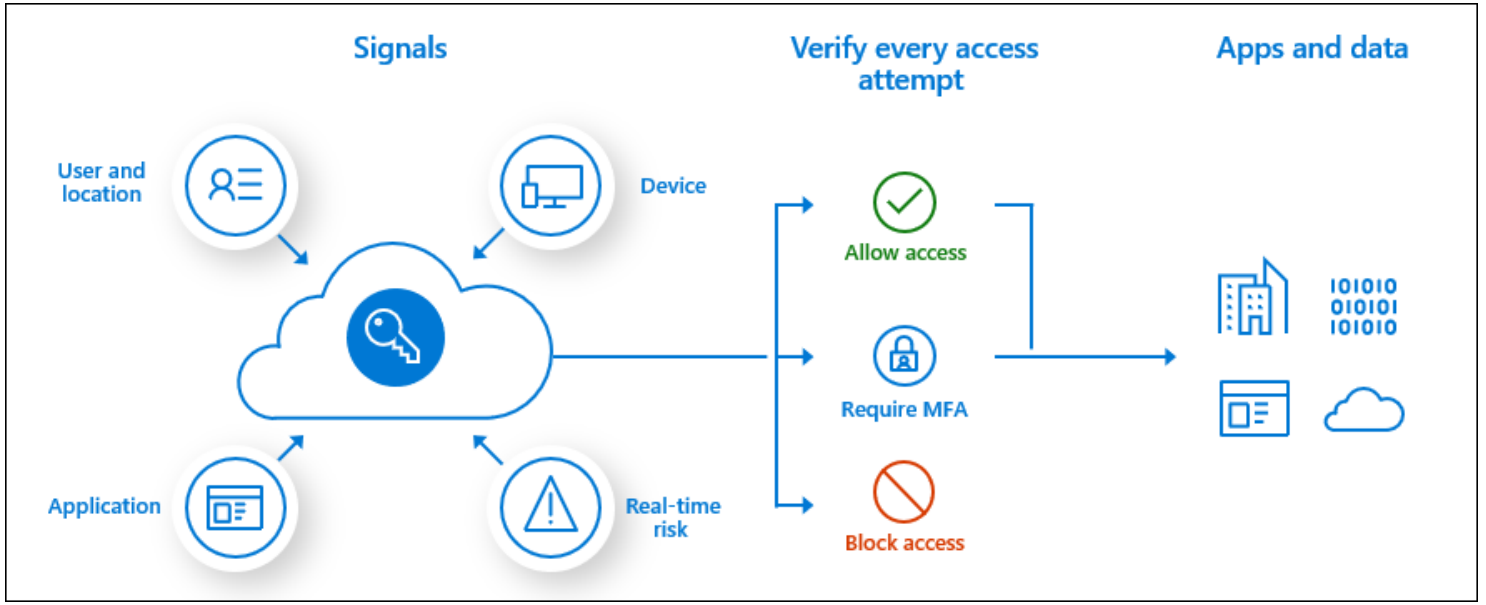
Azure AD External Identities B2C



Bedingter Zugriff

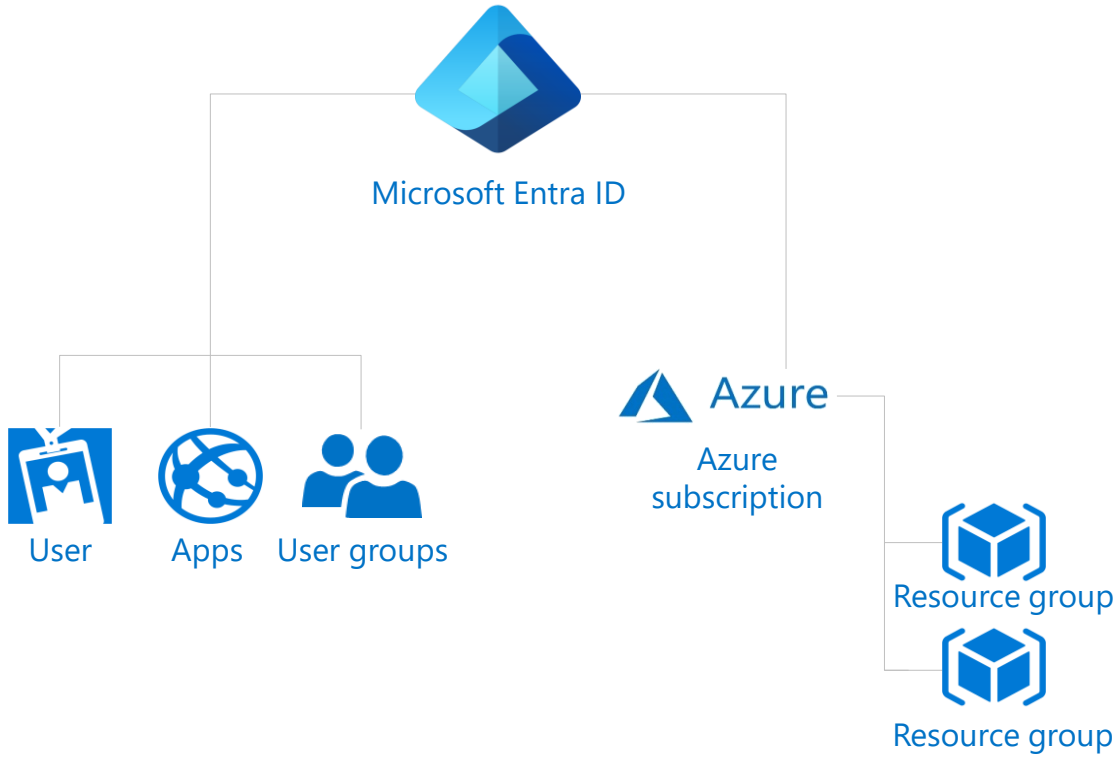
Conditional Access wird von Azure Active Directory verwendet, um Signale zusammenzuführen, Entscheidungen zu treffen und Unternehmensrichtlinien umzusetzen.

- Benutzer oder Gruppenmitgliedschaft
- IP-Standort
- Gerät
- Anwendung
- Risikoerkennung



Role-based access control

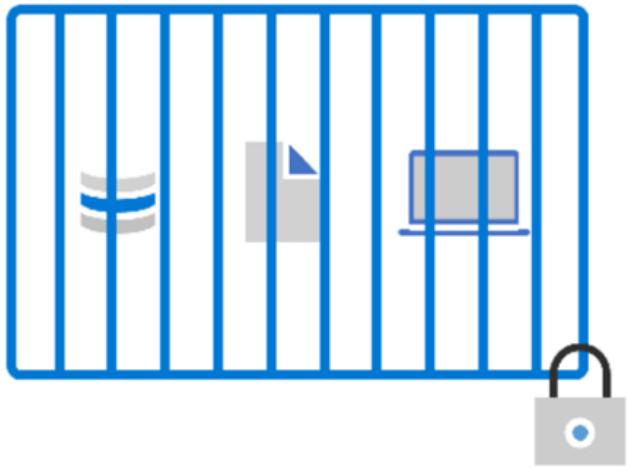
- Fein abgestimmte Zugriffsverwaltung.
- Trennen Sie Aufgaben innerhalb Ihres Teams, und gewähren Sie Benutzern nur die Zugriffsberechtigungen, die sie für die Ausführung ihrer Aufgaben benötigen.
- Ermöglicht den Zugriff auf das Azure-Portal und bietet Zugriffskontrollen für Ressourcen.



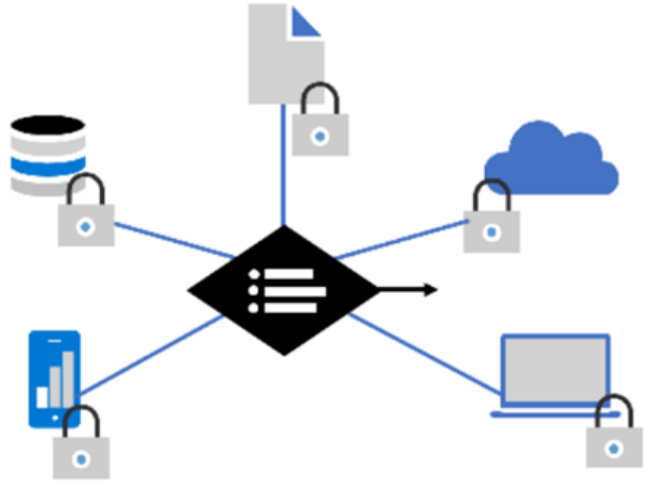
Zero Trust

Objekte dort, wo sie sich befinden, mit Zero Trust sichern

Sicherheit vereinfachen und effektiver umsetzen



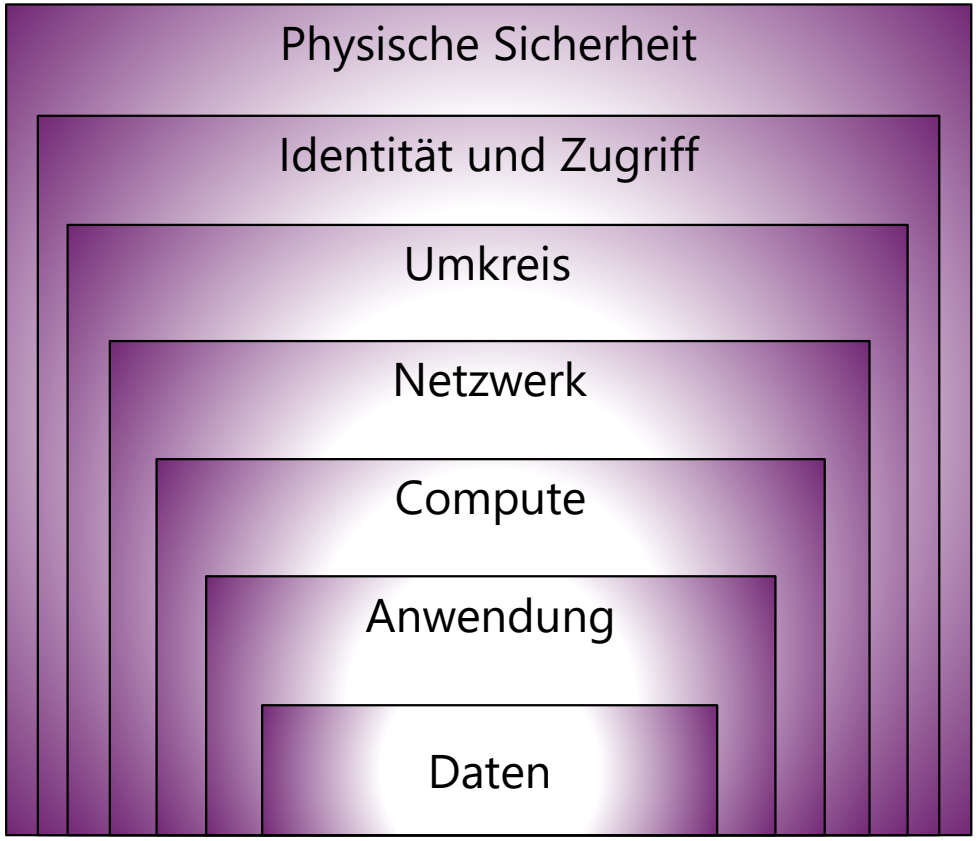
Klassischer Ansatz
Alles auf ein 'sicheres' Netzwerk beschränken



Zero Trust
Objekte überall durch eine zentrale Richtlinie schützen

Defense in depth

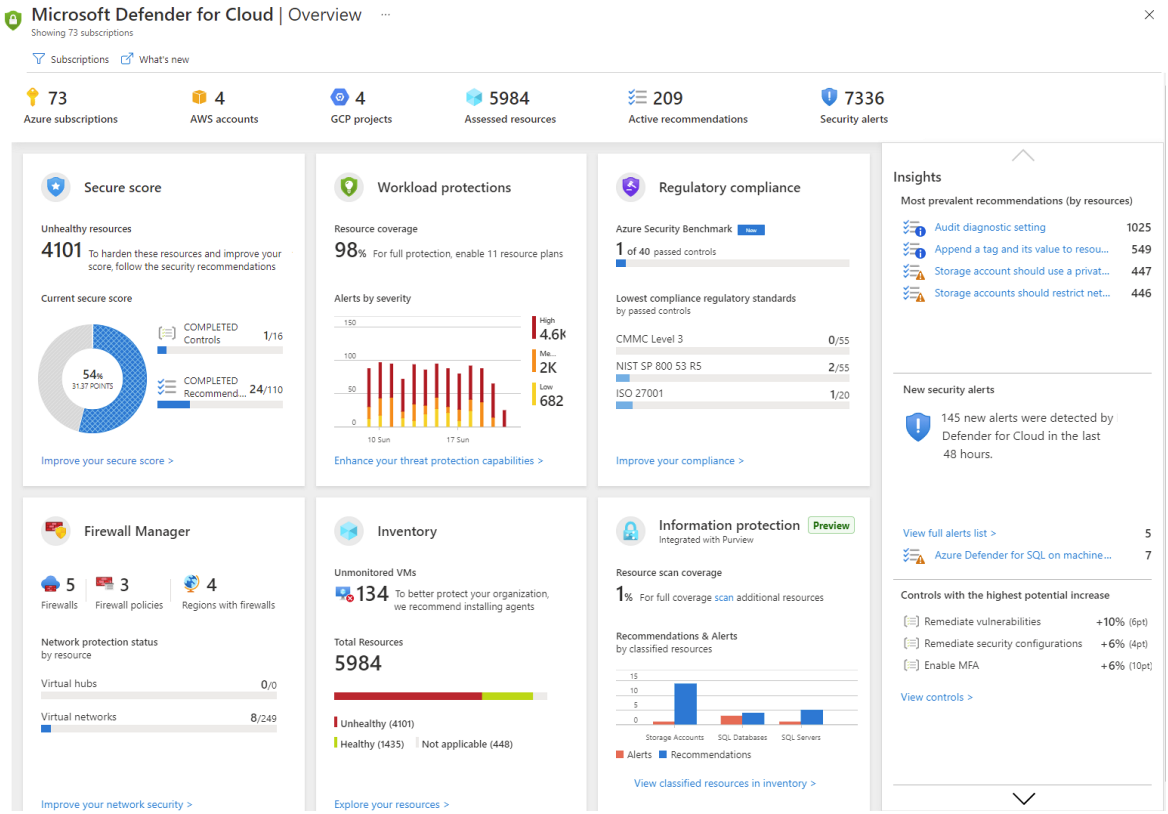
- Ein mehrstufiger Ansatz zur Sicherung von Computersystemen.
- Bietet mehrere Schutzebenen.
- Angriffe gegen eine Ebene sind von nachfolgenden Ebenen isoliert.



Microsoft Defender for Cloud

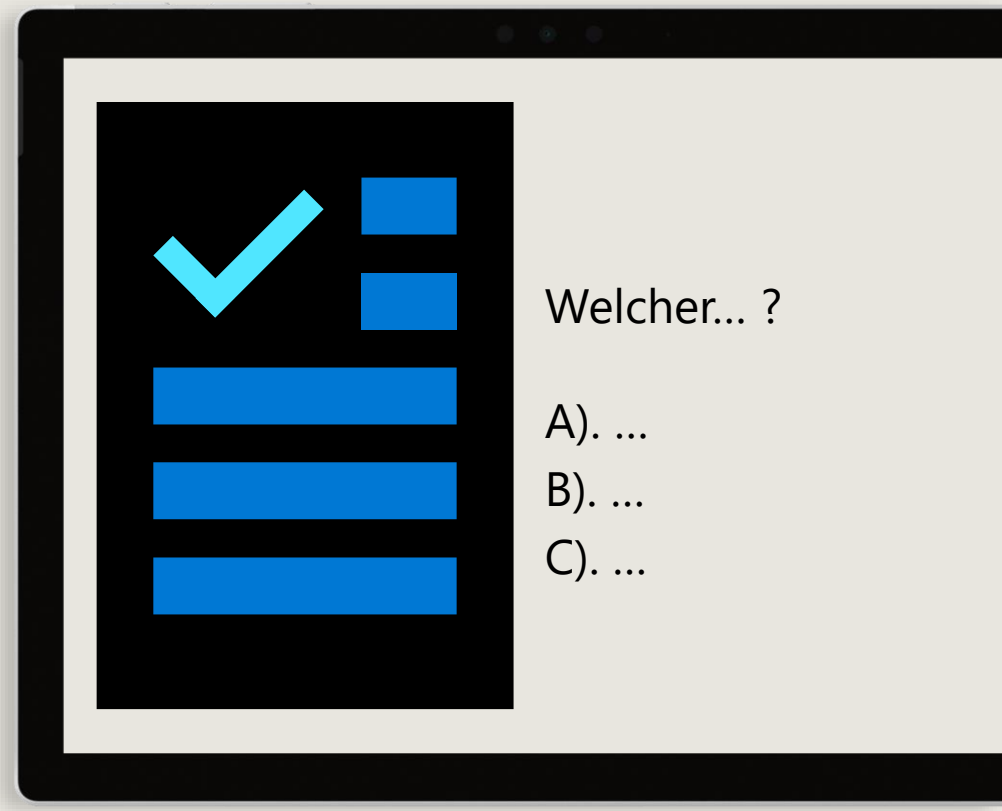
Microsoft Defender for Cloud ist ein Überwachungsdienst, de Schutz vor Bedrohungen für Ihr gesamten Dienste ermöglicht, sowohl in Azure als auch lokal.

- Sicherheitsempfehlungen liefern
- Schadsoftware erkennen und blockieren
- Potenzielle Angriffe analysieren und identifizieren
- Just-In-Time-Zugriffskontrolle für Ports

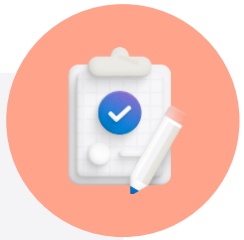


Quiz

Lernpfad 2:
Identität, Zugriff und Sicherheit



Lernpfad 2: Überprüfung



Microsoft Learn Modules (learn.microsoft.com/training)

- Physische Infrastruktur und Verwaltungsinfrastruktur von Microsoft Azure
- Compute- und Netzwerkdienste
- Speicherdienste
- Identität, Zugriff und Sicherheit