Seminar Microsoft Azure Design

DZ-Bank Hamburg, 23. -26. Februar 2026

https://github.com/www42/Hamburg

Tag 1 Einführung

- Einführung Azure
- Einführung Künstliche Intelligenz

Tag 2 Architektur

- Azure Well-Architected Framework
- Cloud Adoption Framework

Tag 3 Azure Services

- Compute, Applications, Network, Migrations
- Storage,Databases, Data Integration

Tag 4 Deep Dive

- Governance, Authentication, Authorization, Monitoring
- Backup, Disaster Recovery, High Availability

Thomas Jäkel

brainymotion

Lead Trainer Cloud Infrastructure

Microsoft Certified Trainer since 1999

https://github.com/www42/Hamburg

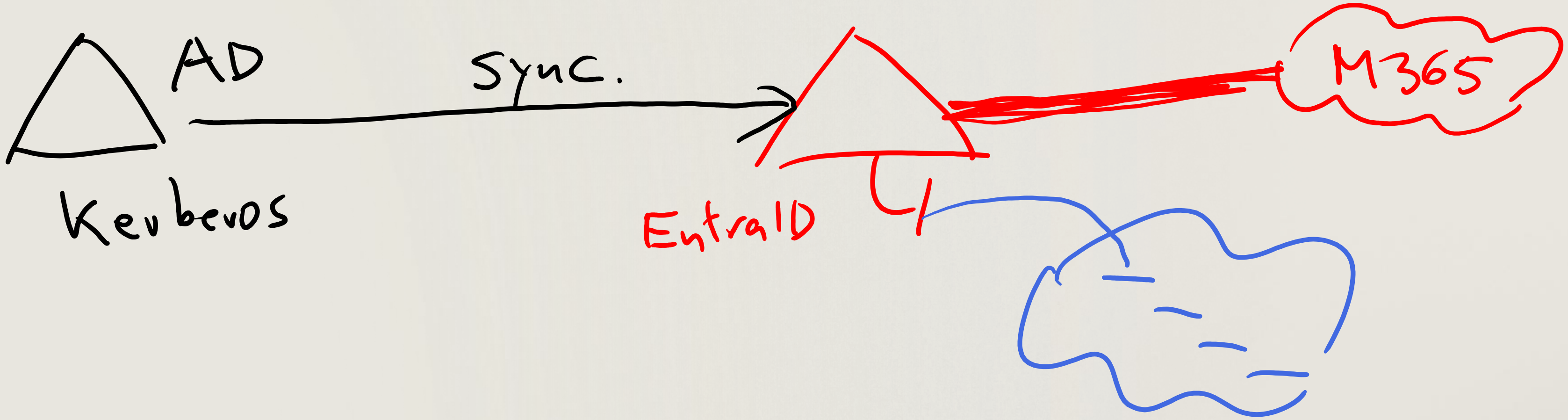
Let's have a great time together

We all contribute to a great class

9^{00} – 17^{00}

12^{00} – 12^{45}

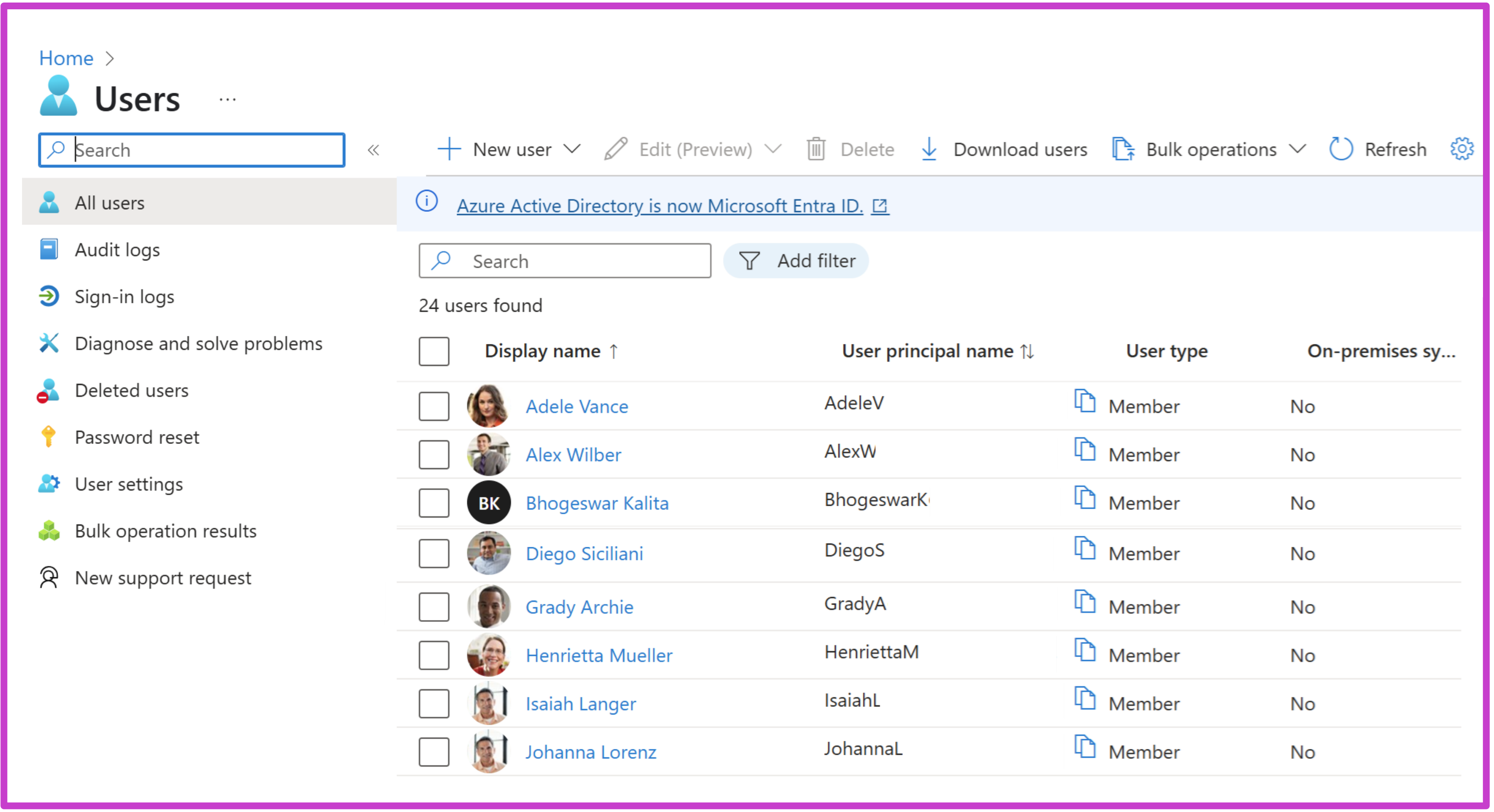
What you should know about our facilities



Create, configure, and manage identities

Create, configure, and manage users

- A user account contains all the information needed to authenticate the user during the sign-on process
- You use the **Identity – All users** dashboard in the Microsoft Entra admin center to work with user objects
- Three kinds of users:
  - Cloud identities
  - Directory-synchronized identities
  - External users



Azure Active Directory is now Microsoft Entra ID.

24 users found

□	Display name ↑	User principal name ↑↓	User type	On-premises sy...
□	Adele Vance	AdeleV	Member	No
□	Alex Wilber	AlexW	Member	No
□	Bhogeswar Kalita	BhogeswarK	Member	No
□	Diego Siciliani	DiegoS	Member	No
□	Grady Archie	GradyA	Member	No
□	Henrietta Mueller	HenriettaM	Member	No
□	Isaiah Langer	IsaiahL	Member	No
□	Johanna Lorenz	JohannaL	Member	No

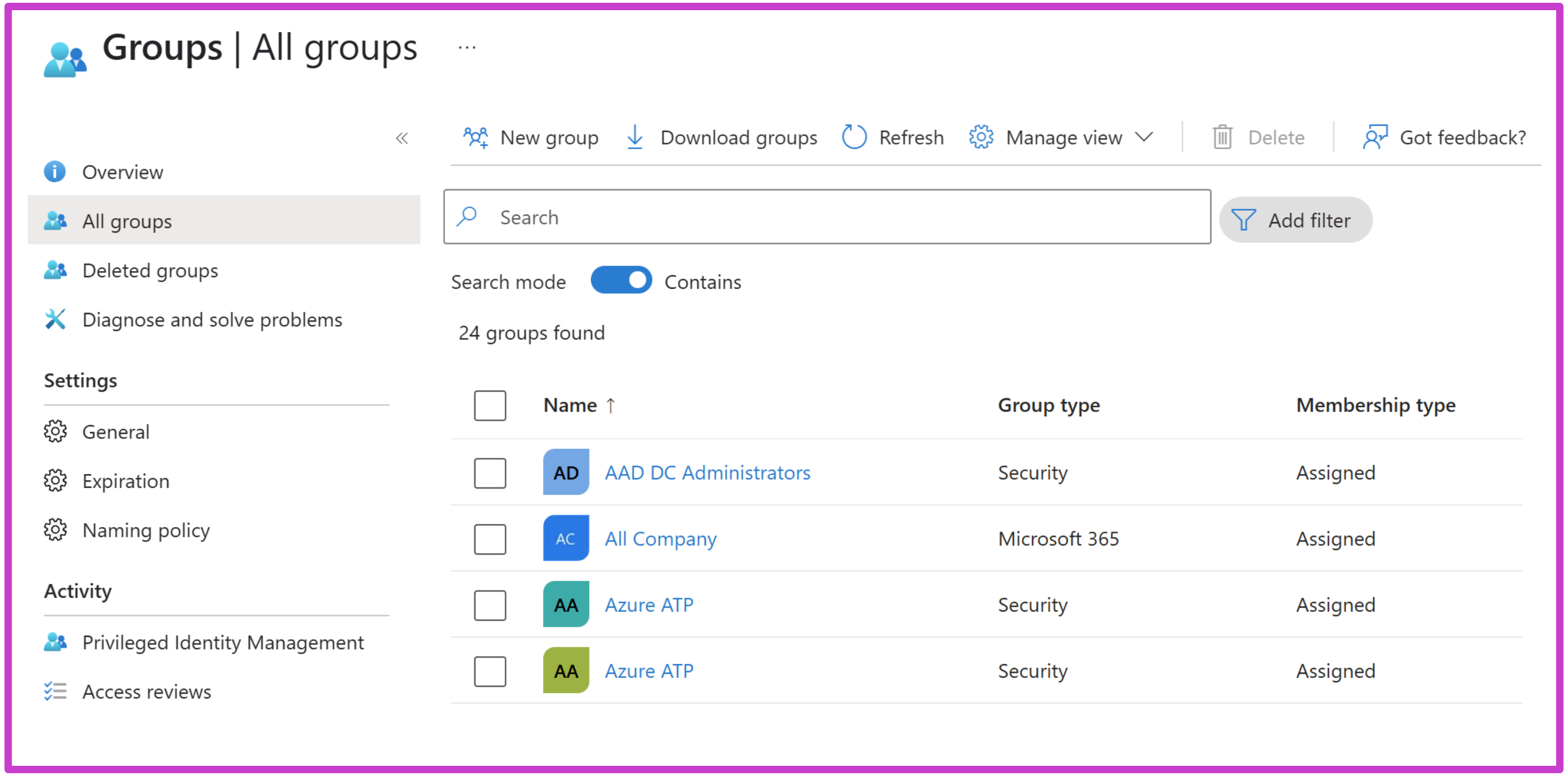
Create, configure, and manage groups

Security groups:

- Most common
- Manage access to shared resources for a group
- Can be nested groups

Microsoft 365 groups:

- Access shared mailbox, calendar, SharePoint, and more
- Give access to external people
- Unable to nest within groups



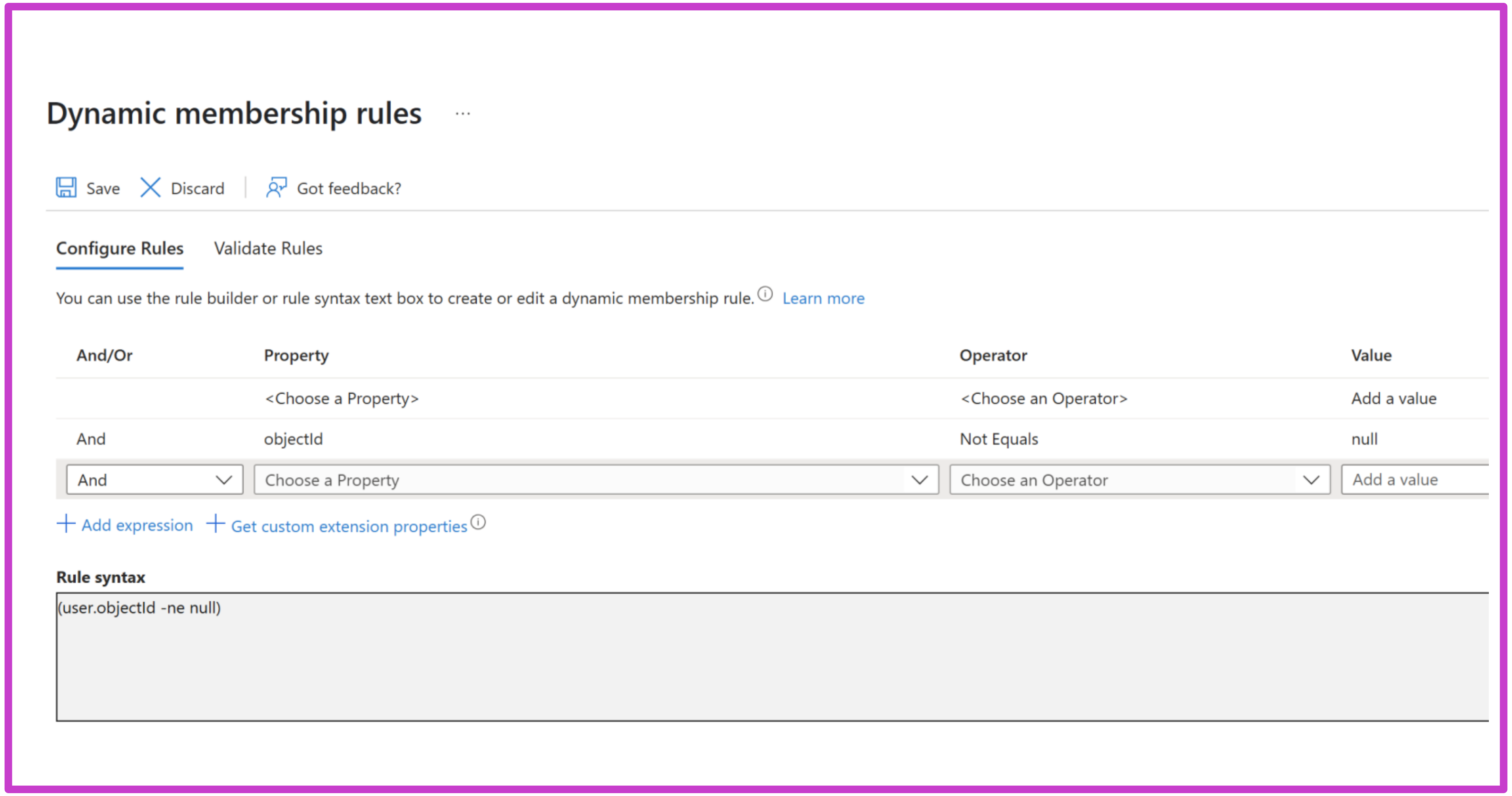
Search mode: Contains

24 groups found

□	Name ↑	Group type	Membership type
□	AD AAD DC Administrators	Security	Assigned
□	AC All Company	Microsoft 365	Assigned
□	AA Azure ATP	Security	Assigned
□	AA Azure ATP	Security	Assigned

Dynamic groups

- Special type of security group
- Membership dynamically generated via membership rule
  - Property -- example = department, region, and other items



Dynamic membership rules ···

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ⓘ Learn more

And/Or	Property	Operator	Value
	<Choose a Property>	<Choose an Operator>	Add a value
And	objectId	Not Equals	null
And	Choose a Property	Choose an Operator	Add a value

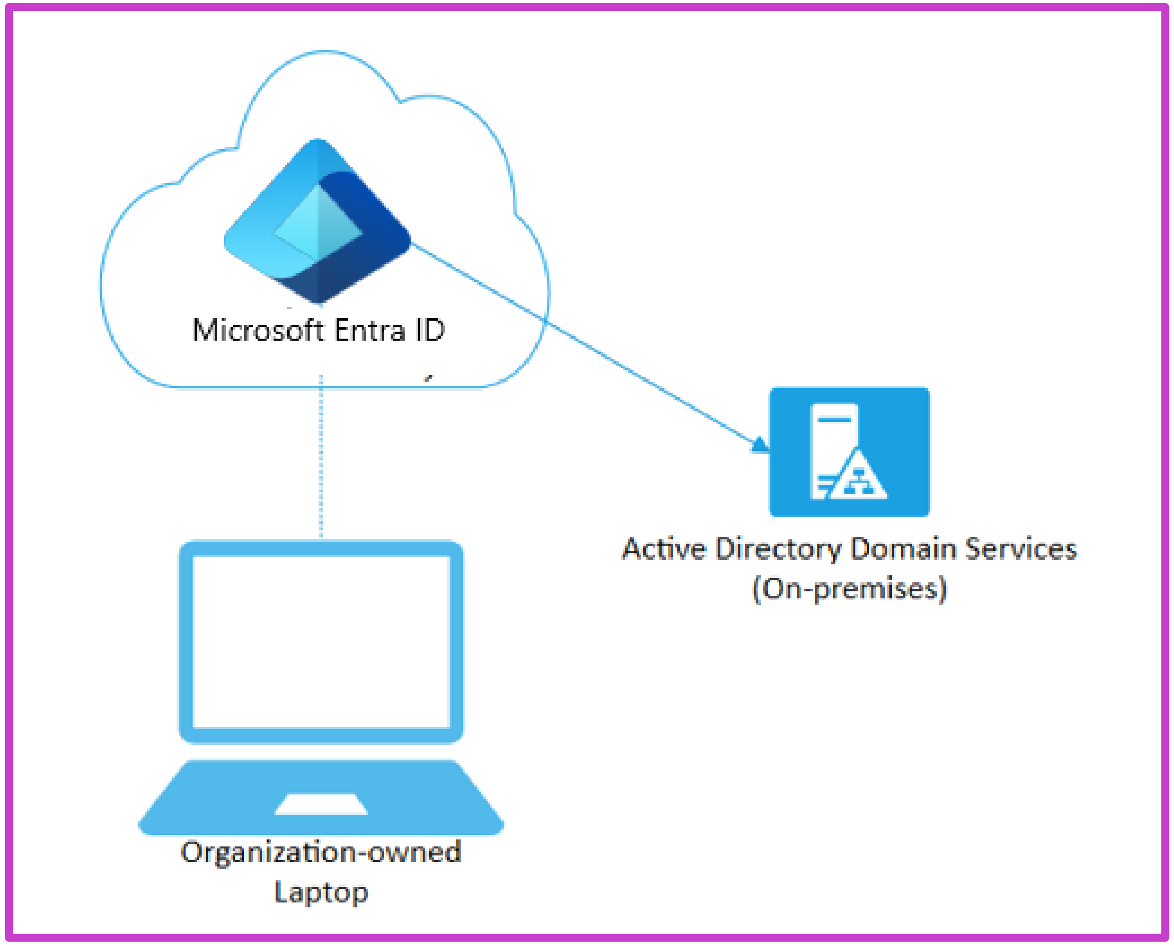
Rule syntax

```
(user.objectId -ne null)
```

Microsoft Entra ID joined devices

- Intended for cloud-first or cloud-only organizations
- Organization-owned devices
- Joined only to Microsoft Entra ID; organizational account required to sign in
- Easy to sign in with an Entra ID account
- Conditional Access policies can be applied to the device identity

OS: Windows 10/11 devices (not Home)

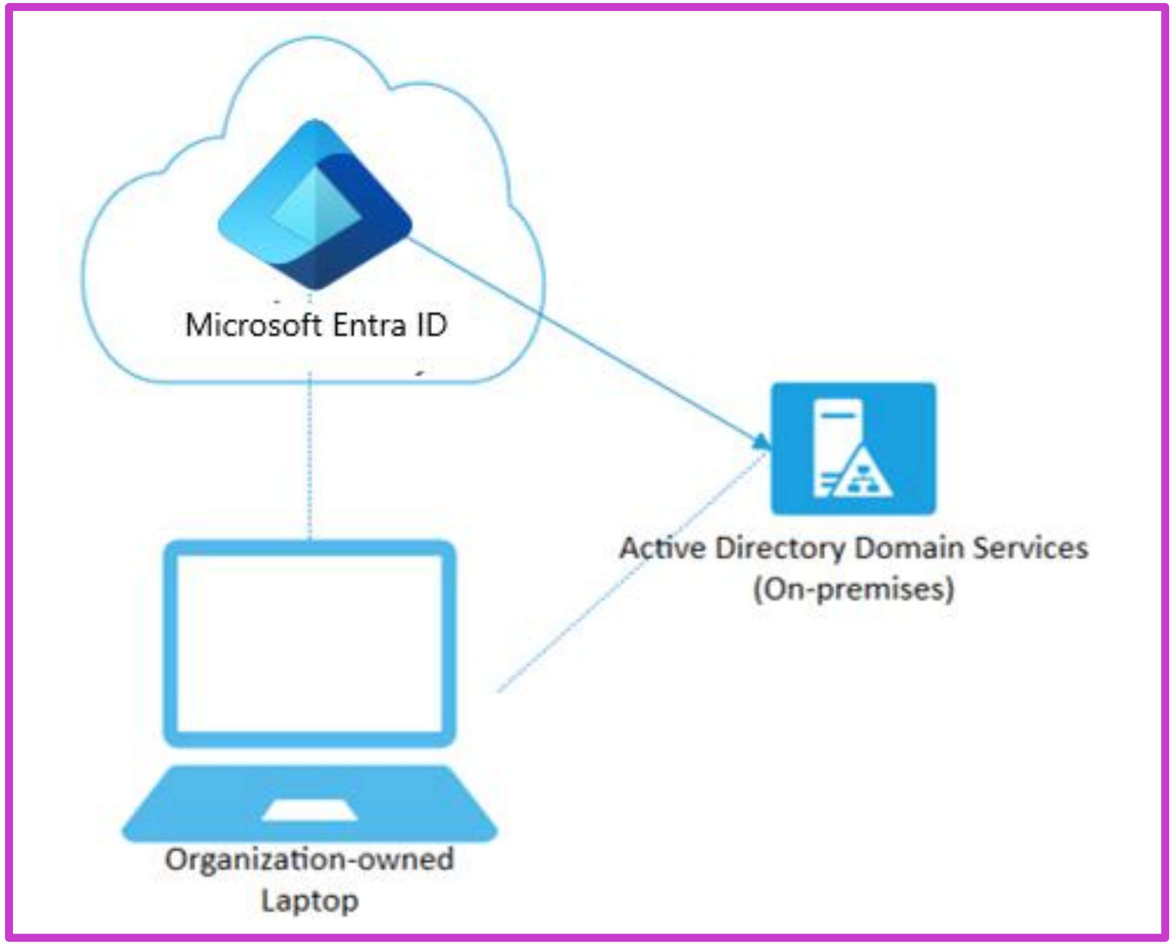

Microsoft Entra ID
Active Directory Domain Services (On-premises)
Organization-owned Laptop

Microsoft Entra hybrid joined devices

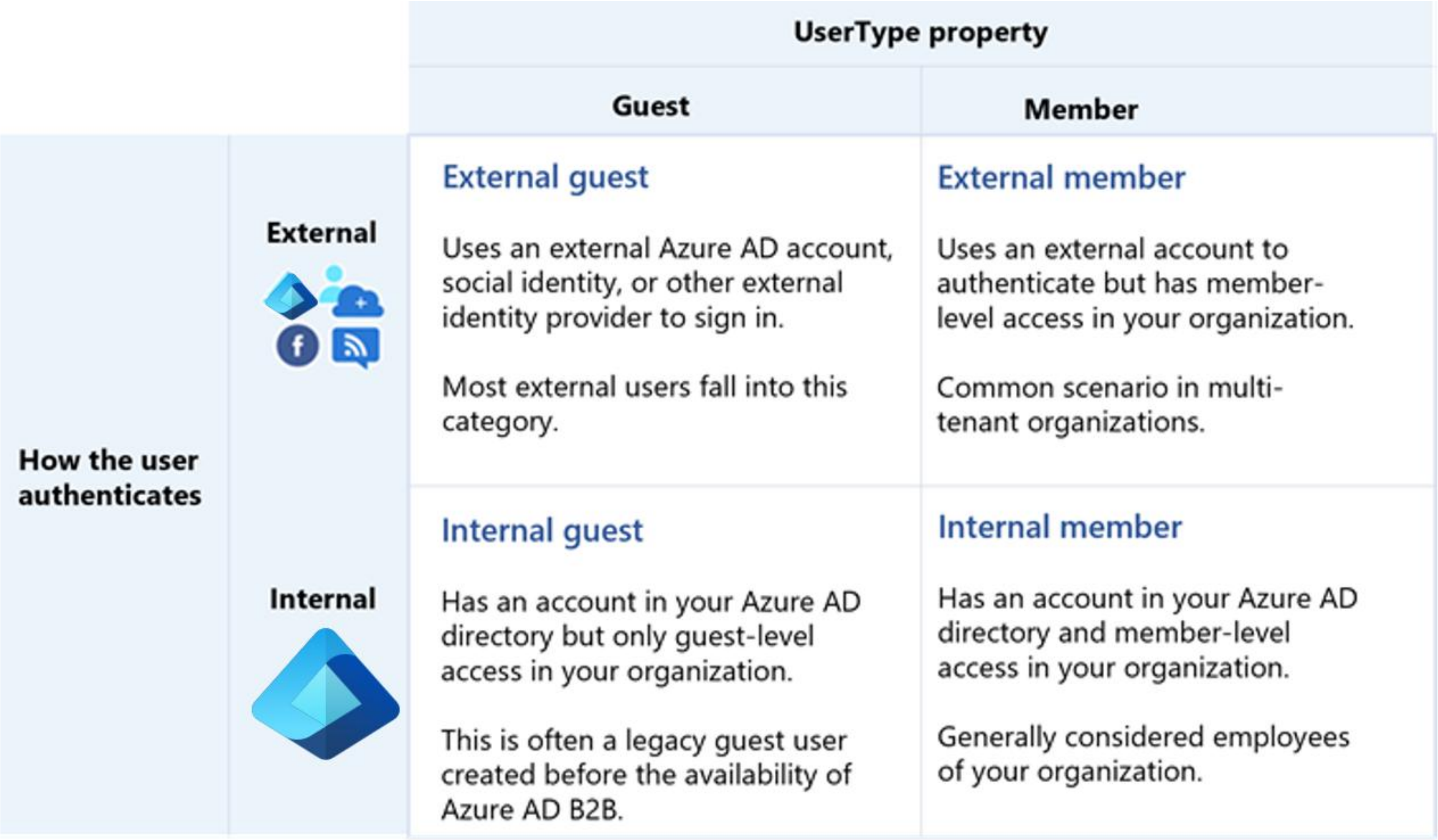
Use Microsoft Entra hybrid joined devices if:

- You have Win32 apps deployed to these devices using Microsoft Entra ID machine authentication.
- You want to continue to use group policy to manage the device.
- You want to use existing image solutions to deploy devices.

OS: Windows 8.1 devices in addition to Windows 10/11, plus later Windows Server versions.

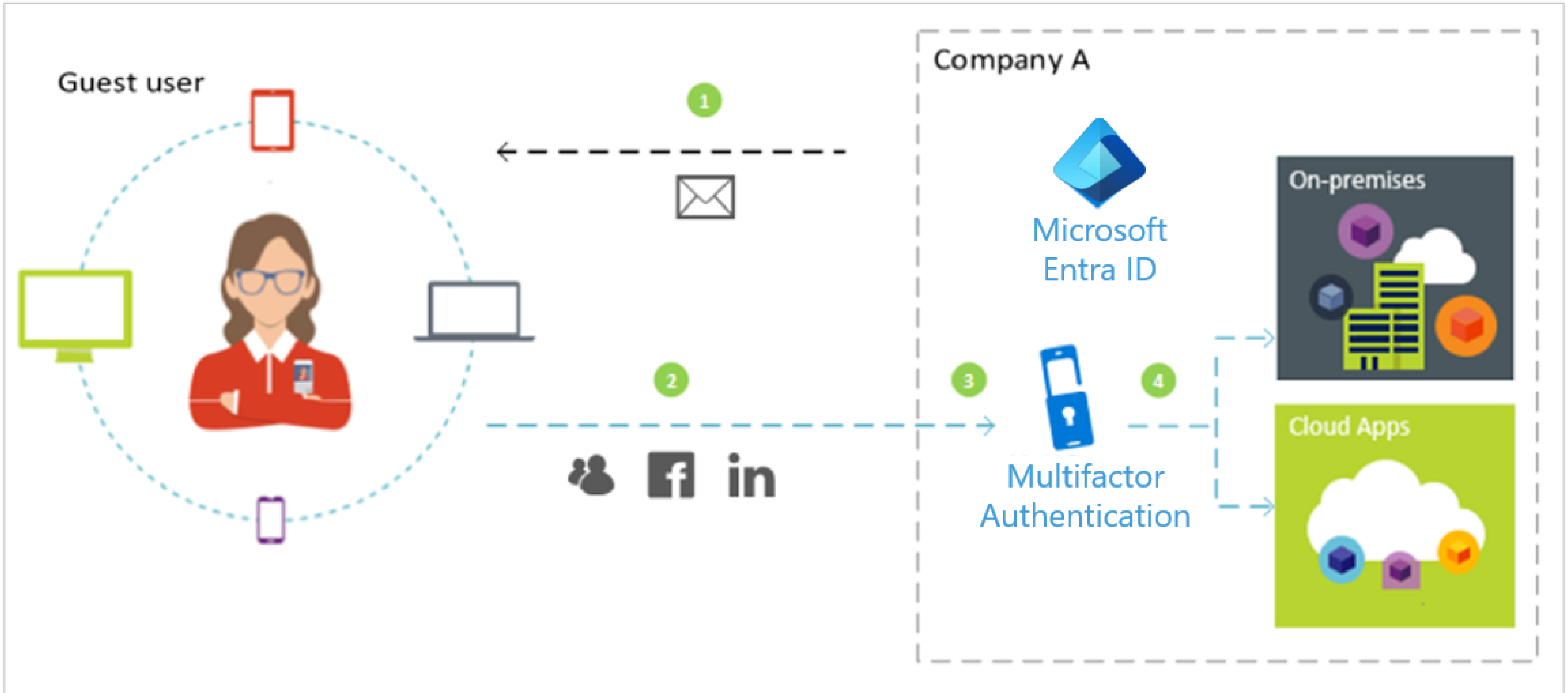


Relationship between external and member users



		UserType property	
		Guest	Member
How the user authenticates	External	External guest Uses an external Azure AD account, social identity, or other external identity provider to sign in. Most external users fall into this category.	External member Uses an external account to authenticate but has member-level access in your organization. Common scenario in multi-tenant organizations.
	Internal	Internal guest Has an account in your Azure AD directory but only guest-level access in your organization. This is often a legacy guest user created before the availability of Azure AD B2B.	Internal member Has an account in your Azure AD directory and member-level access in your organization. Generally considered employees of your organization.

Microsoft Entra B2B



Guest user—a user invited to join your corporate Microsoft Entra ID.

Sourced from another directory, social media, partners, and other services.

Secure B2B collaboration projects enabled.

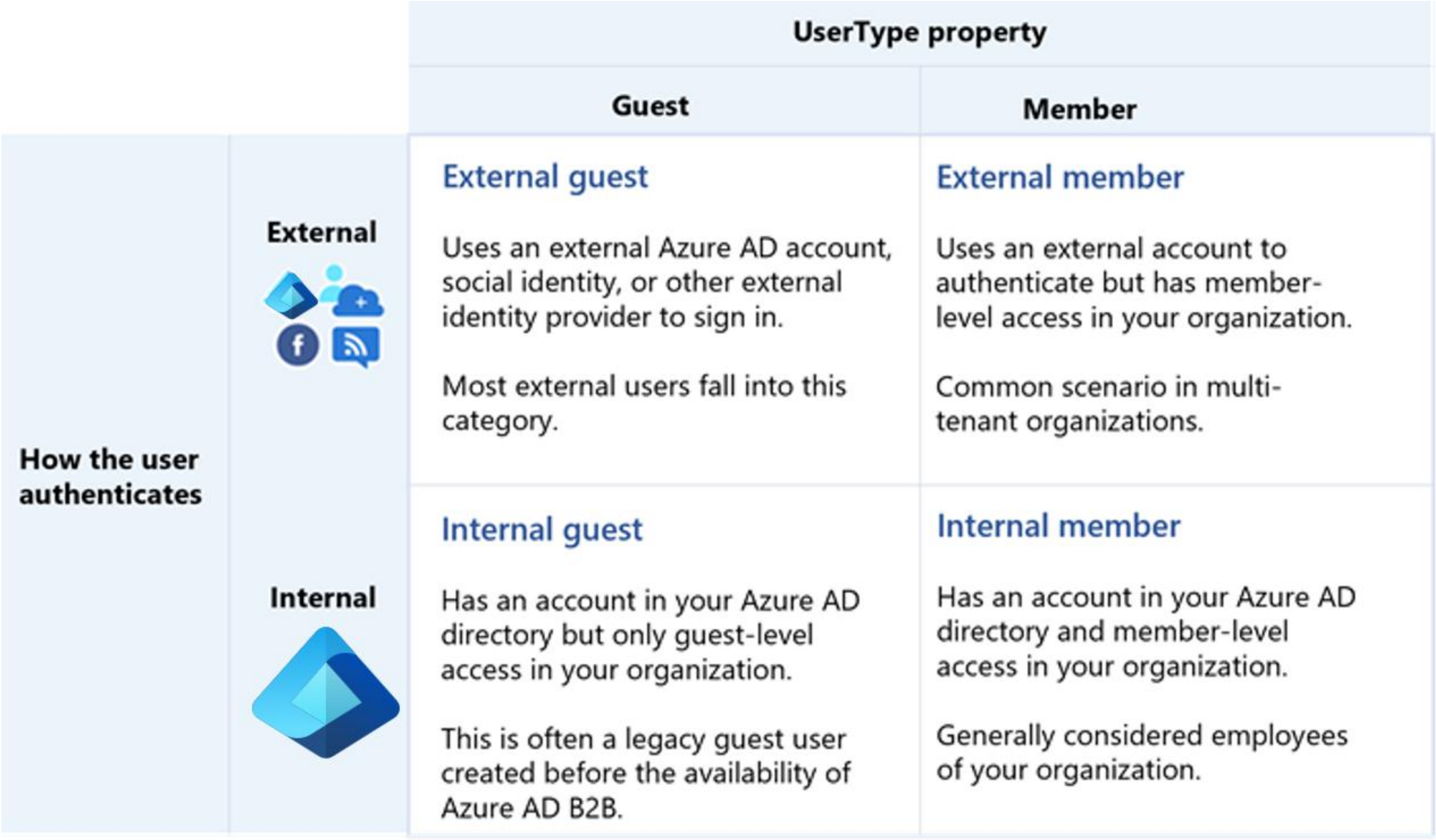
Collaborating with external users

CA Policies

Access Review

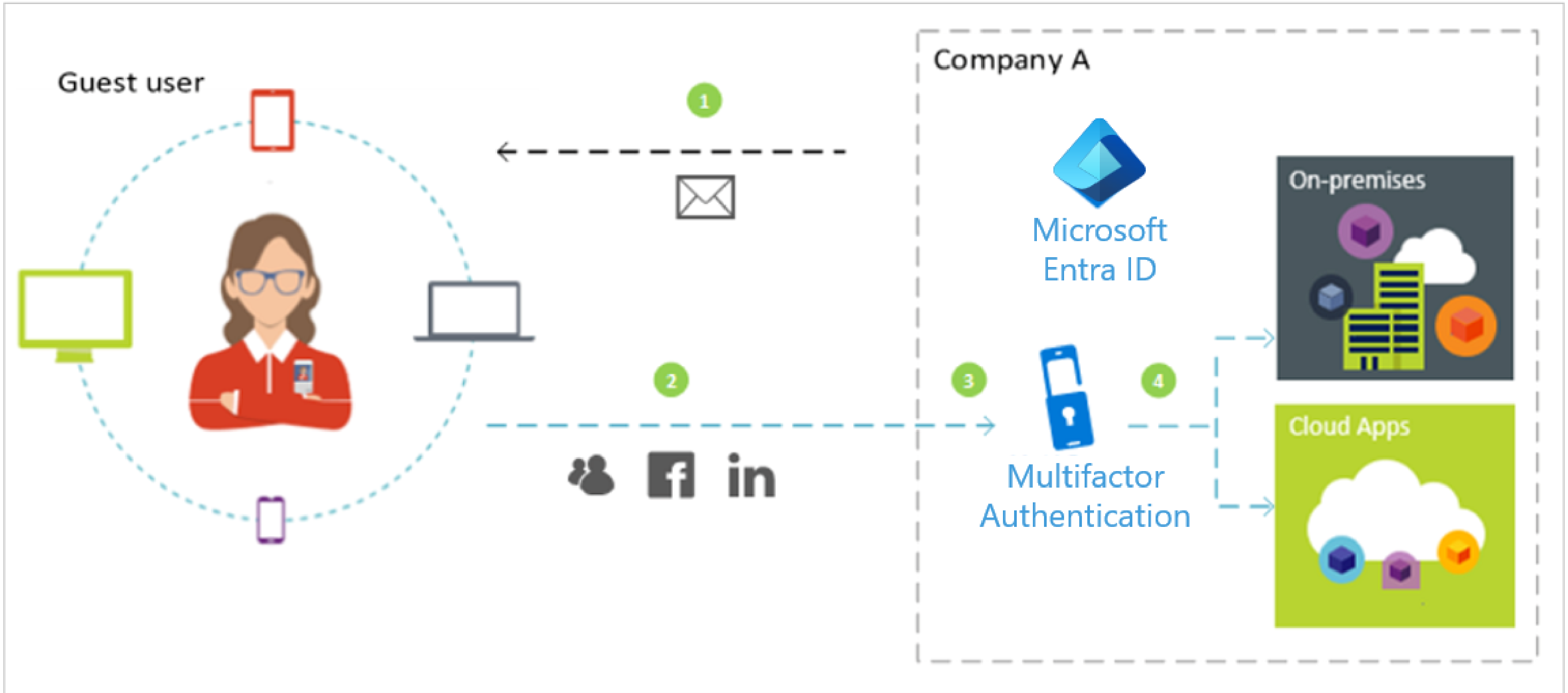
- Invite external users into your tenant typically as guests
- External users use their existing credentials for authentication
- They are assigned permissions for authorization
- You can restrict what external users can see and do

Relationship between external and member users



		UserType property	
		Guest	Member
How the user authenticates	External	**External guest** Uses an external Azure AD account, social identity, or other external identity provider to sign in. Most external users fall into this category.	**External member** Uses an external account to authenticate but has member-level access in your organization. Common scenario in multi-tenant organizations.
	Internal	**Internal guest** Has an account in your Azure AD directory but only guest-level access in your organization. This is often a legacy guest user created before the availability of Azure AD B2B.	**Internal member** Has an account in your Azure AD directory and member-level access in your organization. Generally considered employees of your organization.

Microsoft Entra B2B



Guest user—a user invited to join your corporate Microsoft Entra ID.

Sourced from another directory, social media, partners, and other services.

Secure B2B collaboration projects enabled.

Collaborating with external users

CA Policies

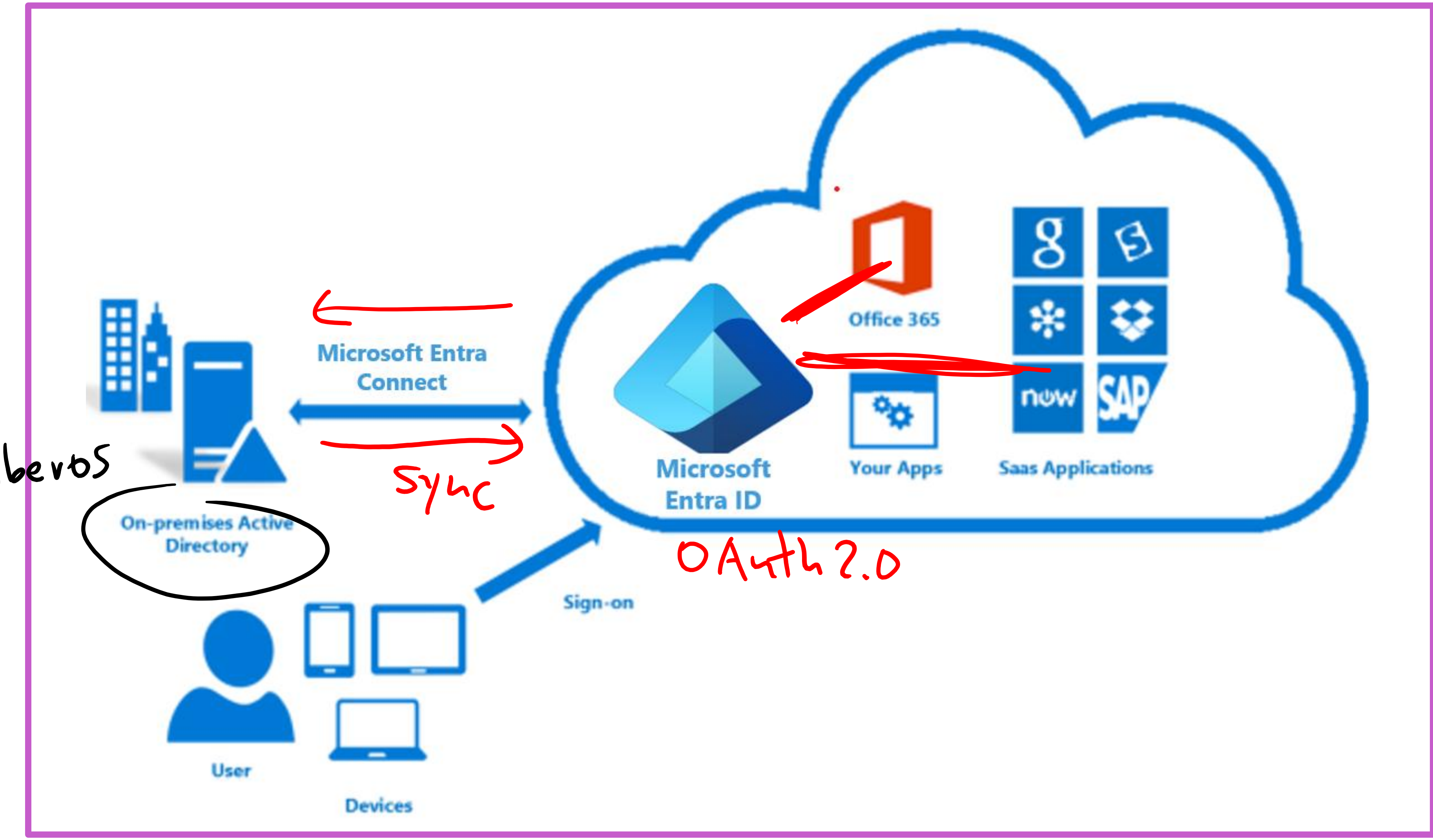
Access Review

- Invite external users into your tenant typically as guests
- External users use their existing credentials for authentication
- They are assigned permissions for authorization
- You can restrict what external users can see and do

What is Microsoft Entra Connect?

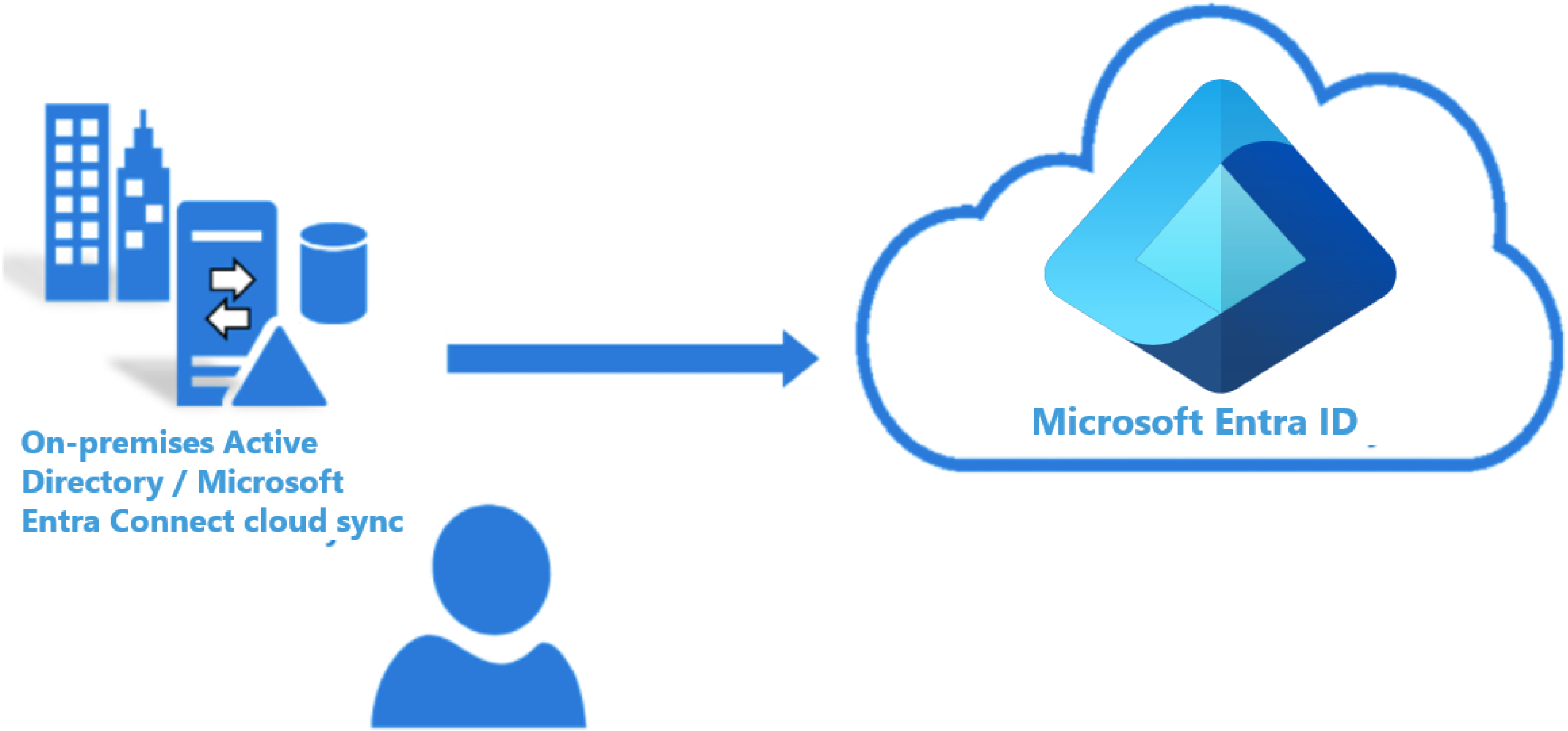
- Microsoft Entra Connect is a solution that bridges an organization’s on-premises Active Directory with your cloud-based Microsoft Entra ID
- Microsoft Entra Connect provides:
  - Synchronization
  - Password hash synchronization PHS
  - Pass-through authentication
  - Federation integration
  - Health monitoring

Kerberos



Microsoft Entra cloud sync

- Microsoft Entra cloud sync is a solution that syncs your on-premises AD with Microsoft Entra ID
- Lightweight provisioning agent required on the on-premises AD
- All sync configuration is managed in the cloud
- Can be used in conjunction with Microsoft Entra Connect


On-premises Active Directory / Microsoft Entra Connect cloud sync
Microsoft Entra ID

Authentication methods

Cloud authentication

Microsoft Entra password hash synchronization (PHS)

- Users can use the same username and password that they use on-premises

Microsoft Entra pass-through authentication (PTA)

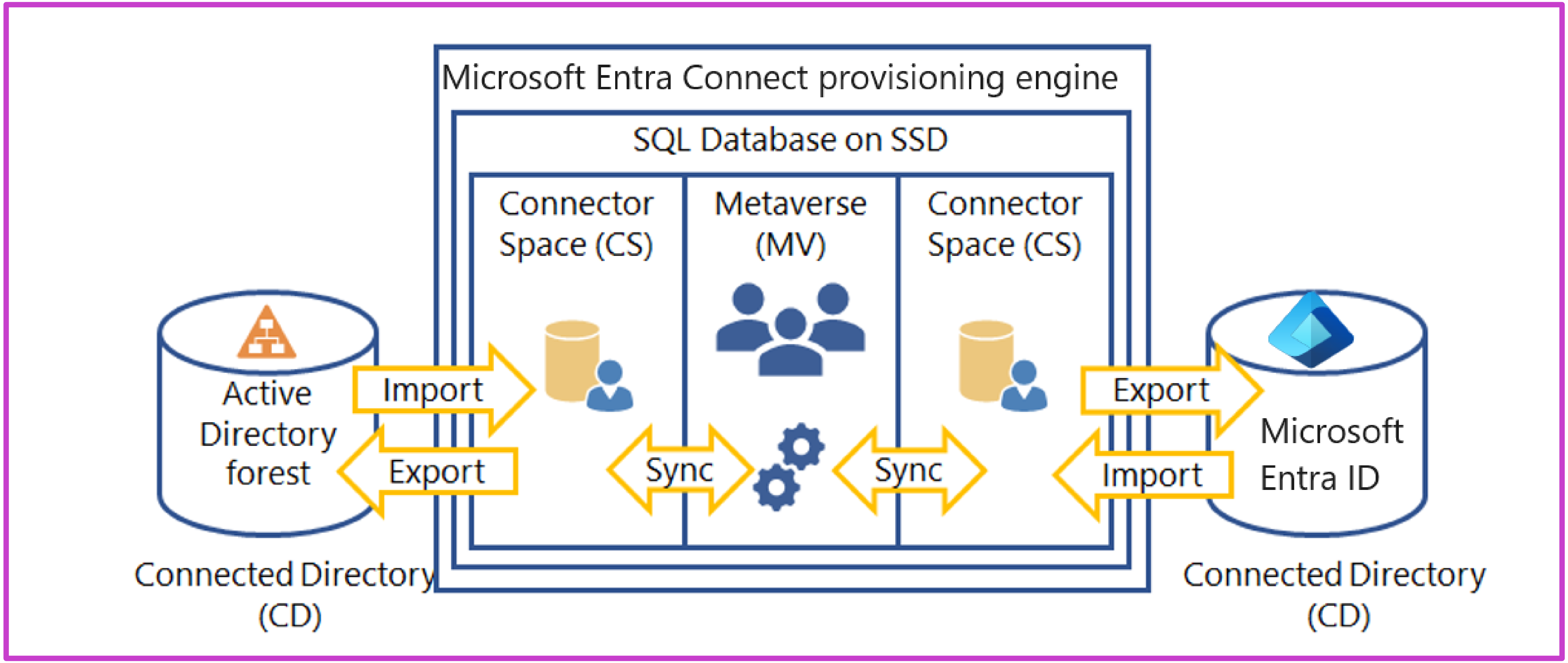
- Simple password validation for Microsoft Entra ID authentication services using a software agent that runs on one or more on-premises servers

Federated authentication

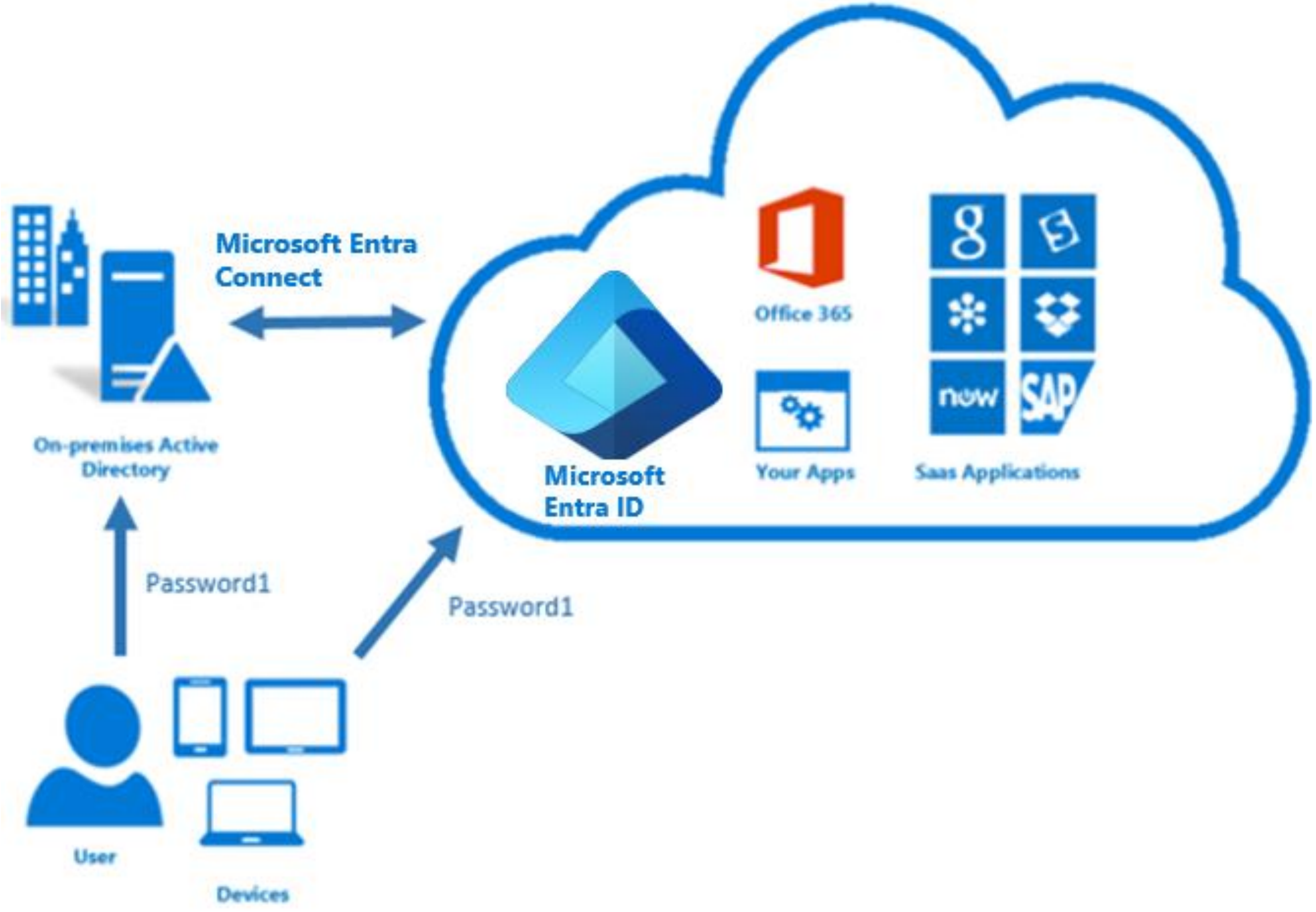
Handoff to trusted authentication system

- Microsoft Entra ID hands off the authentication process to a separate trusted authentication system to validate the user's password
- The authentication system can provide additional advanced authentication requirements, such as a smartcard or third-party multifactor authentication

Microsoft Entra Connect component factors



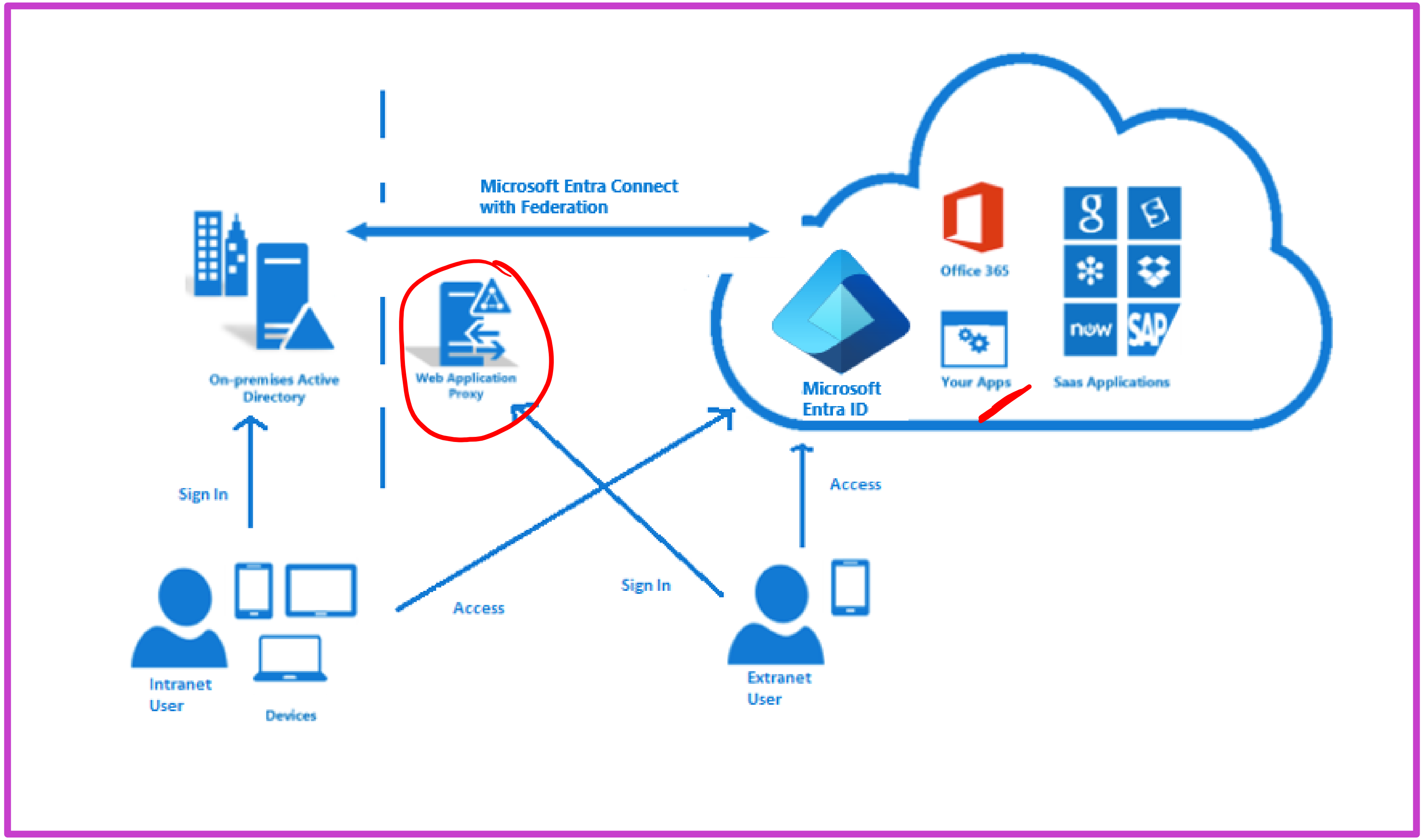
How password hash synchronization works



What is federation?

Federation uses a new or existing farm with AD FS in Windows Server 2012 R2 and later

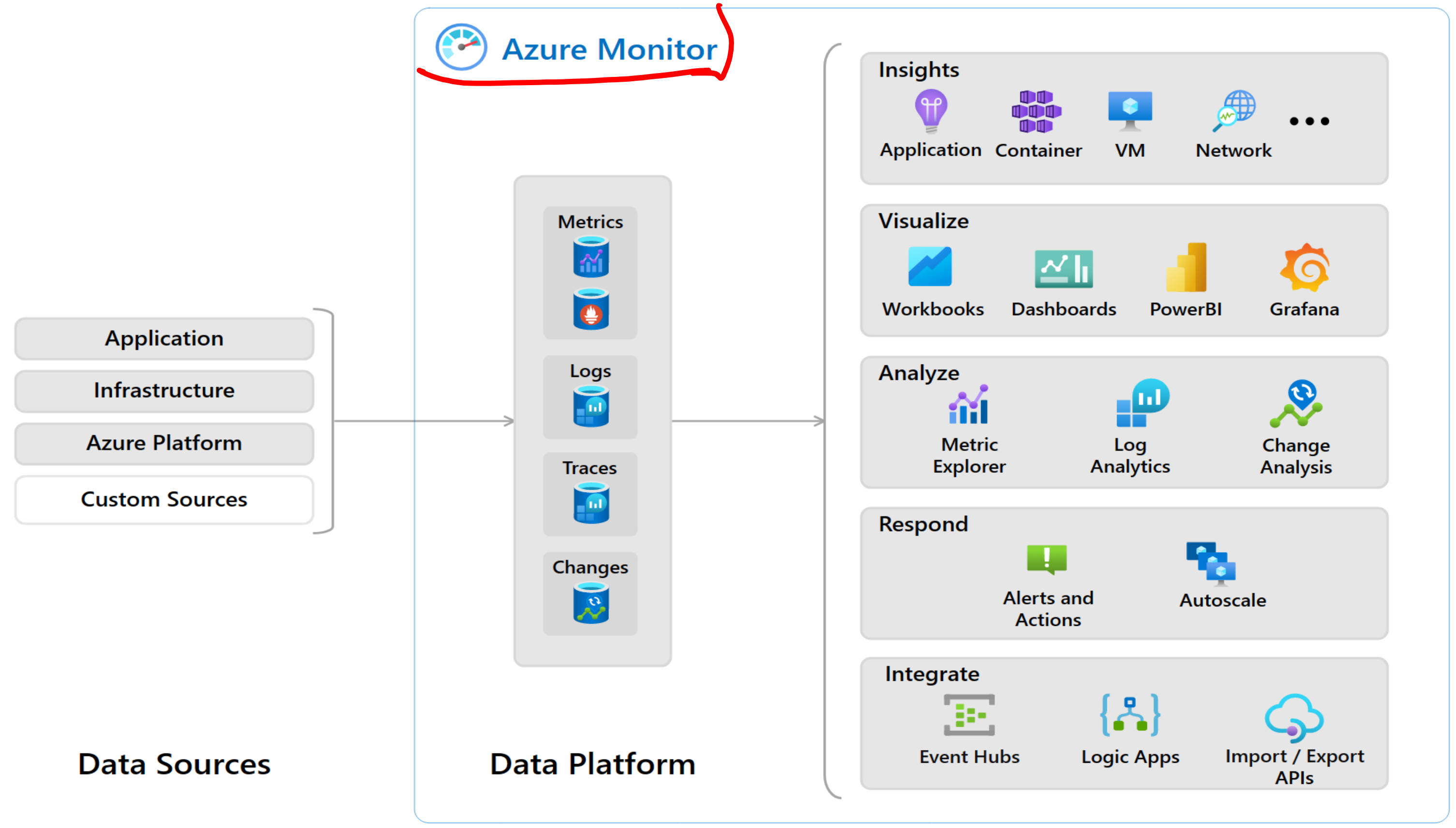
- Users sign in to Microsoft Entra ID services using their on-premises passwords
- Microsoft Entra Connect configures the trust between Microsoft Entra ID and the on-premises farm



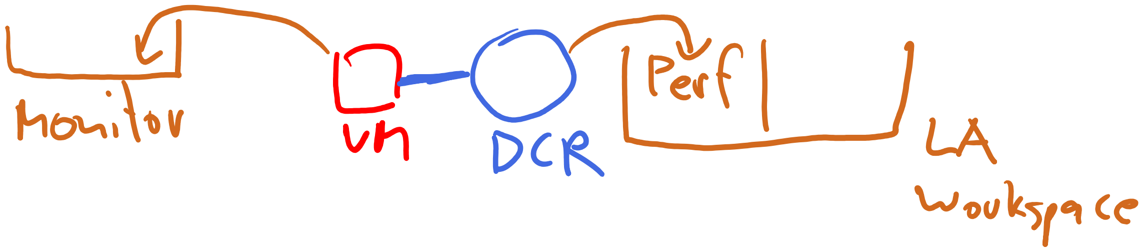
Introduction to Azure Monitor

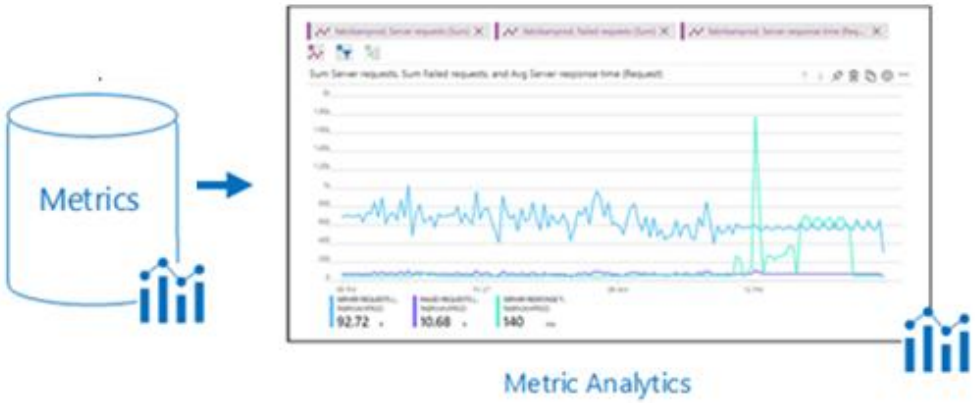
Understand Azure Monitor Components

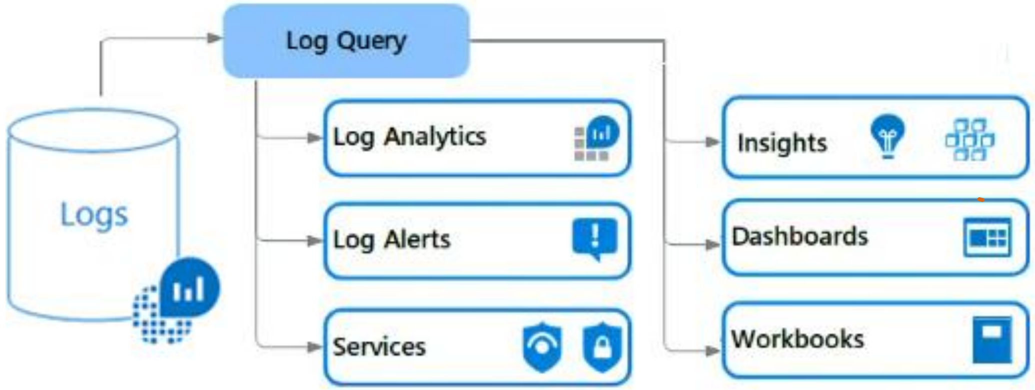
- Application monitoring data
- Guest OS monitoring
- Azure resource monitoring
- Azure subscription monitoring
- Azure tenant monitoring



Define Metrics and Logs



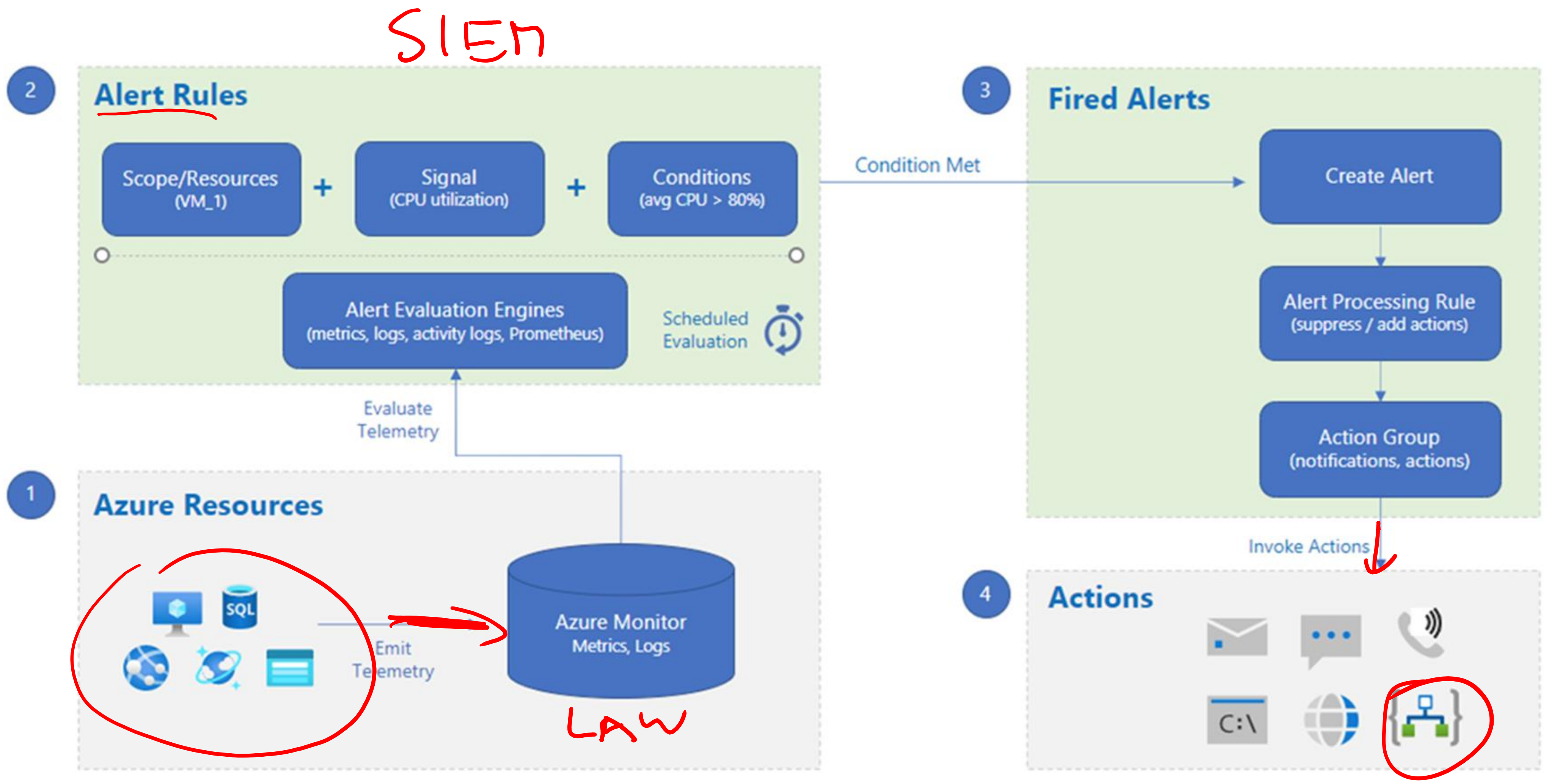




- Metrics are numerical values that describe some aspect of a system at a point in time
- They are lightweight and capable of supporting near real-time scenarios

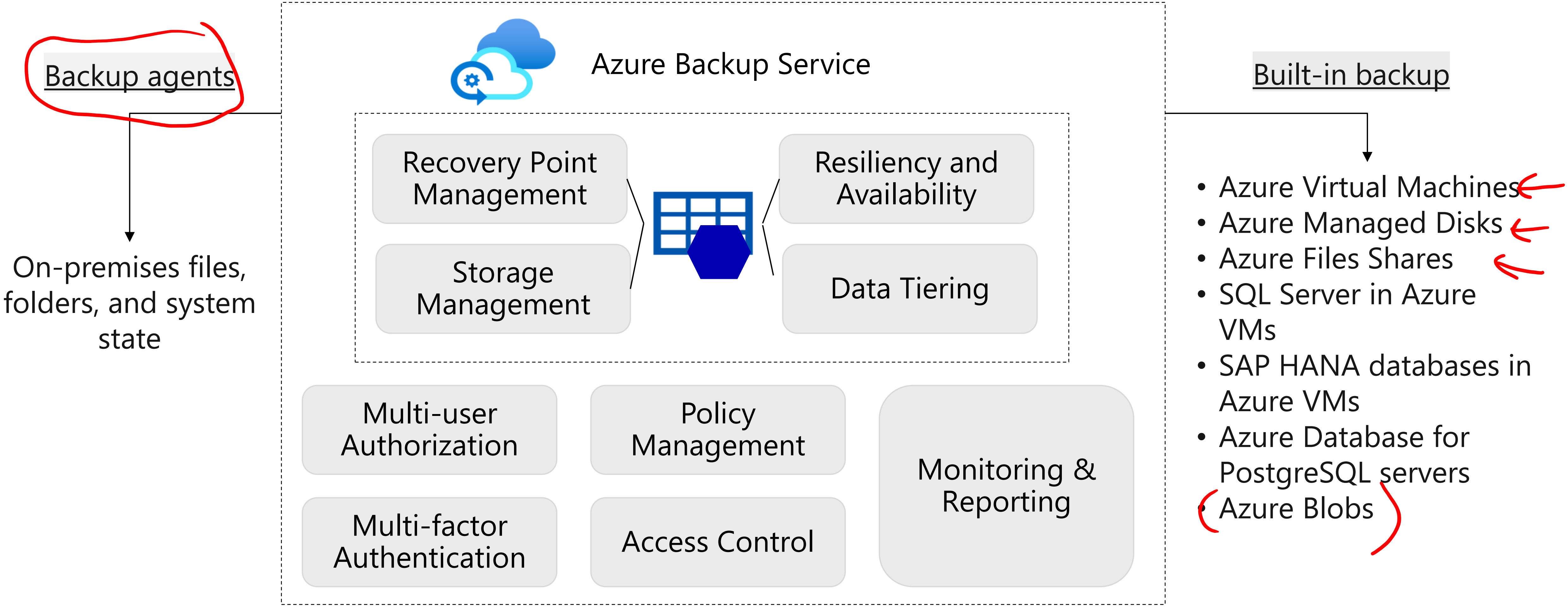
- Logs contain different kinds of data organized into records with different sets of properties for each type
- Telemetry (events, traces) and performance data can be combined for analysis

Manage Azure Monitor Alerts


SIEM
2
Alert Rules
Scope/Resources (VM_1)
+
Signal (CPU utilization)
+
Conditions (avg CPU > 80%)
Alert Evaluation Engines (metrics, logs, activity logs, Prometheus)
Scheduled Evaluation
Evaluate Telemetry
Condition Met
3
Fired Alerts
Create Alert
Alert Processing Rule (suppress / add actions)
Action Group (notifications, actions)
Invoke Actions
1
Azure Resources
SQL
Emit Telemetry
Azure Monitor Metrics, Logs
LAW
4
Actions
C:\

Introduction to Azure Backup

What is Azure Backup?



Backup agents

On-premises files, folders, and system state

Azure Backup Service

Recovery Point Management

Storage Management

Resiliency and Availability

Data Tiering

Multi-user Authorization

Multi-factor Authentication

Policy Management

Access Control

Monitoring & Reporting

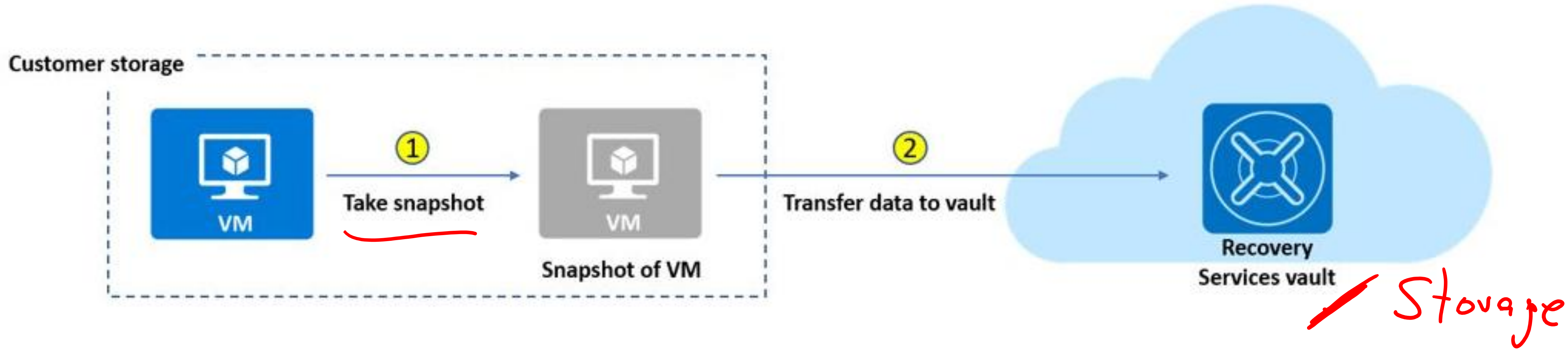
Built-in backup

- Azure Virtual Machines
- Azure Managed Disks
- Azure Files Shares
- SQL Server in Azure VMs
- SAP HANA databases in Azure VMs
- Azure Database for PostgreSQL servers
- Azure Blobs

Explore options to protect virtual machine data

Snapshots	Azure Backup	Azure Site Recovery
Managed snapshots provide a quick and simple option for backing up VMs that use Managed Disks	Azure Backup supports application-consistent backups for both Windows and Linux VMs	Azure Site Recovery protects your VMs from a major disaster scenario when a whole region experiences an outage

Create virtual machine snapshots in Azure Backup

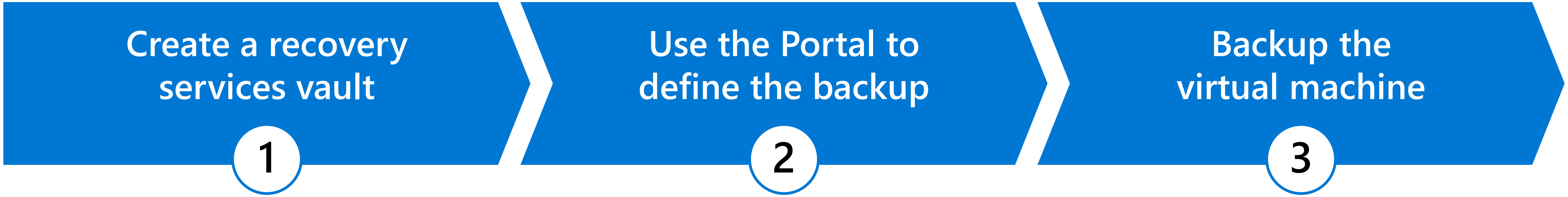


Use snapshots taken as part of a backup job

Reduces recovery wait times – don't wait for data transfer to the vault to finish

Configure Instant Restore retention (standard or enhanced)

Backup Virtual Machines



1. Create a recovery services vault

2. Use the Portal to define the backup

3. Backup the virtual machine

Use a Recovery Services Vault in the region where you are performing your Virtual Machine backups and choose a replication strategy for Vault

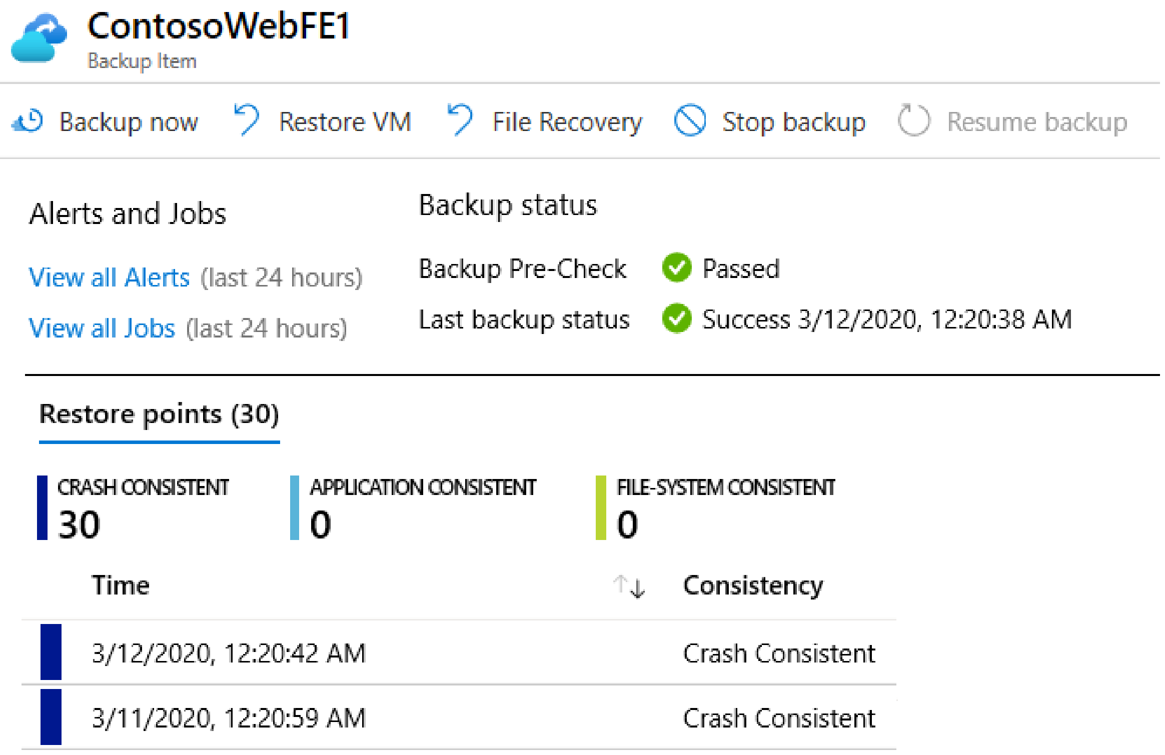
Take snapshots (recovery points) of your data at defined intervals. These snapshots are stored in recovery services vaults

For the Backup extension to work, the Azure VM Agent must be installed on the Azure virtual machine

Restore Virtual Machines

Once you trigger the restore operation, the Backup service creates a job for tracking the restore operation

The Backup service also creates and temporarily displays notifications, so you monitor how the backup is proceeding



ContosoWebFE1
Backup Item

Alerts and Jobs

View all Alerts (last 24 hours)

View all Jobs (last 24 hours)

Backup status

Backup Pre-Check	✓ Passed
Last backup status	✓ Success 3/12/2020, 12:20:38 AM

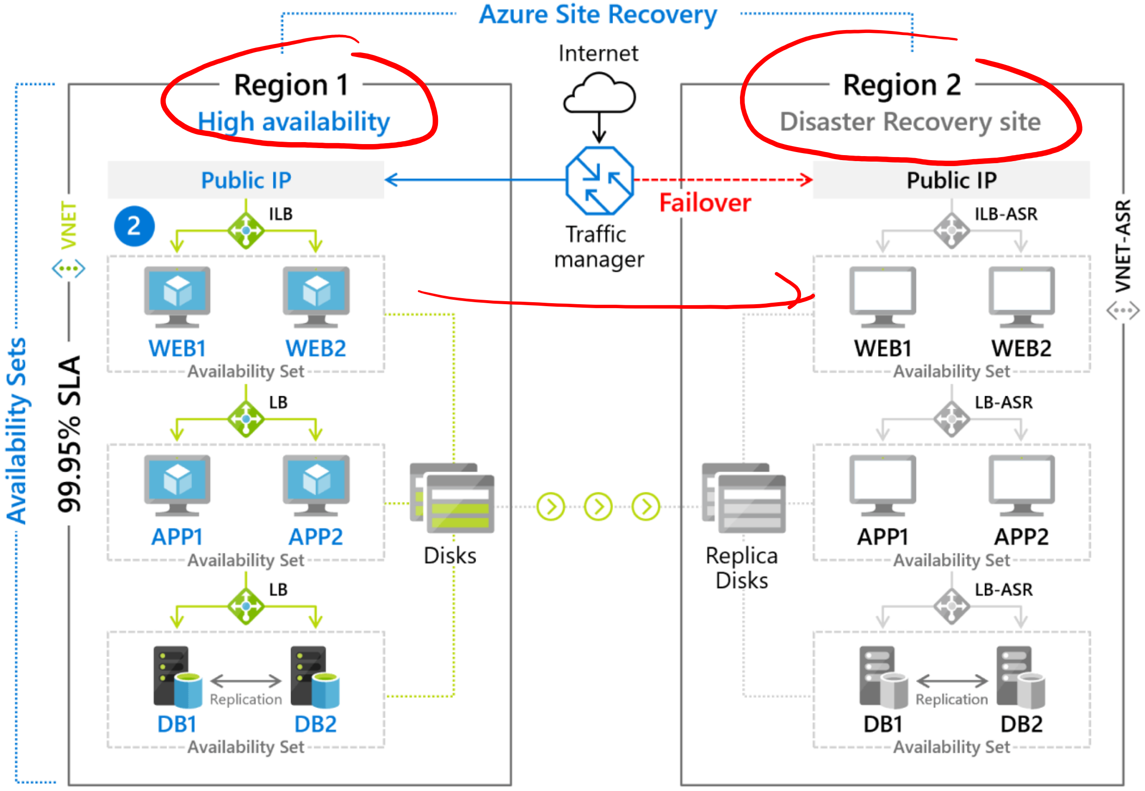
Restore points (30)

CRASH CONSISTENT	APPLICATION CONSISTENT	FILE-SYSTEM CONSISTENT
30	0	0

Time	Consistency
3/12/2020, 12:20:42 AM	Crash Consistent
3/11/2020, 12:20:59 AM	Crash Consistent

Implement Azure Site Recovery

- Manages the orchestration of disaster recovery
- Replicates workloads continuously from a primary location or region to a secondary location
- Failover to shift to the secondary location; failback to return to the primary location


Azure Site Recovery
Internet
Region 1
High availability
Public IP
ILB
2
VNET
Availability Sets
99.95% SLA
WEB1
WEB2
Availability Set
LB
APP1
APP2
Availability Set
LB
DB1
Replication
DB2
Availability Set
Disks
Traffic manager
Failover
Region 2
Disaster Recovery site
Public IP
ILB-ASR
WEB1
WEB2
Availability Set
LB-ASR
APP1
APP2
Availability Set
LB-ASR
DB1
Replication
DB2
Availability Set
Replica Disks
VNET-ASR