



# Microsoft Azure from Zero to Hero

Michael Petersen, Microsoft Cloud Solution Architect

# In this workshops

## 1 Introduction into Azure

## 2 Azure AD for Azure

- Tenants and Auditing
- Roles in AD and in Azure
- Identities and external Collaboration

## 3 Cloud Security and Governance

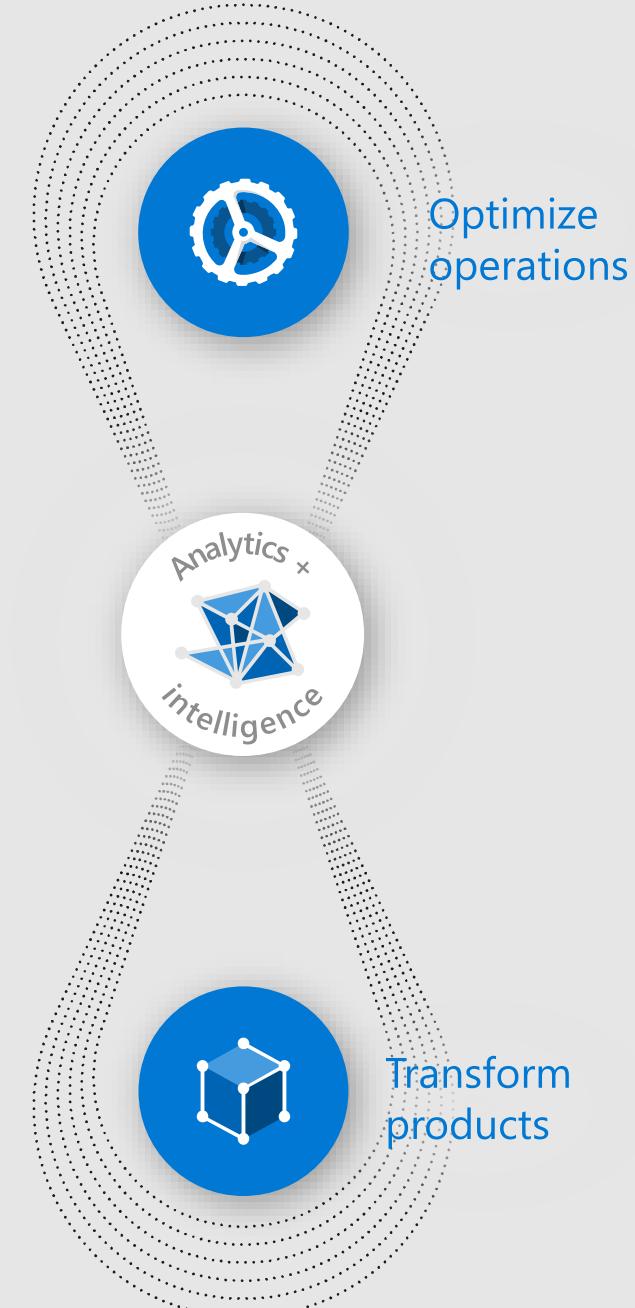
- Organize your Enrollment
- Enforce Governance and Security

## 4 Operations and Automation

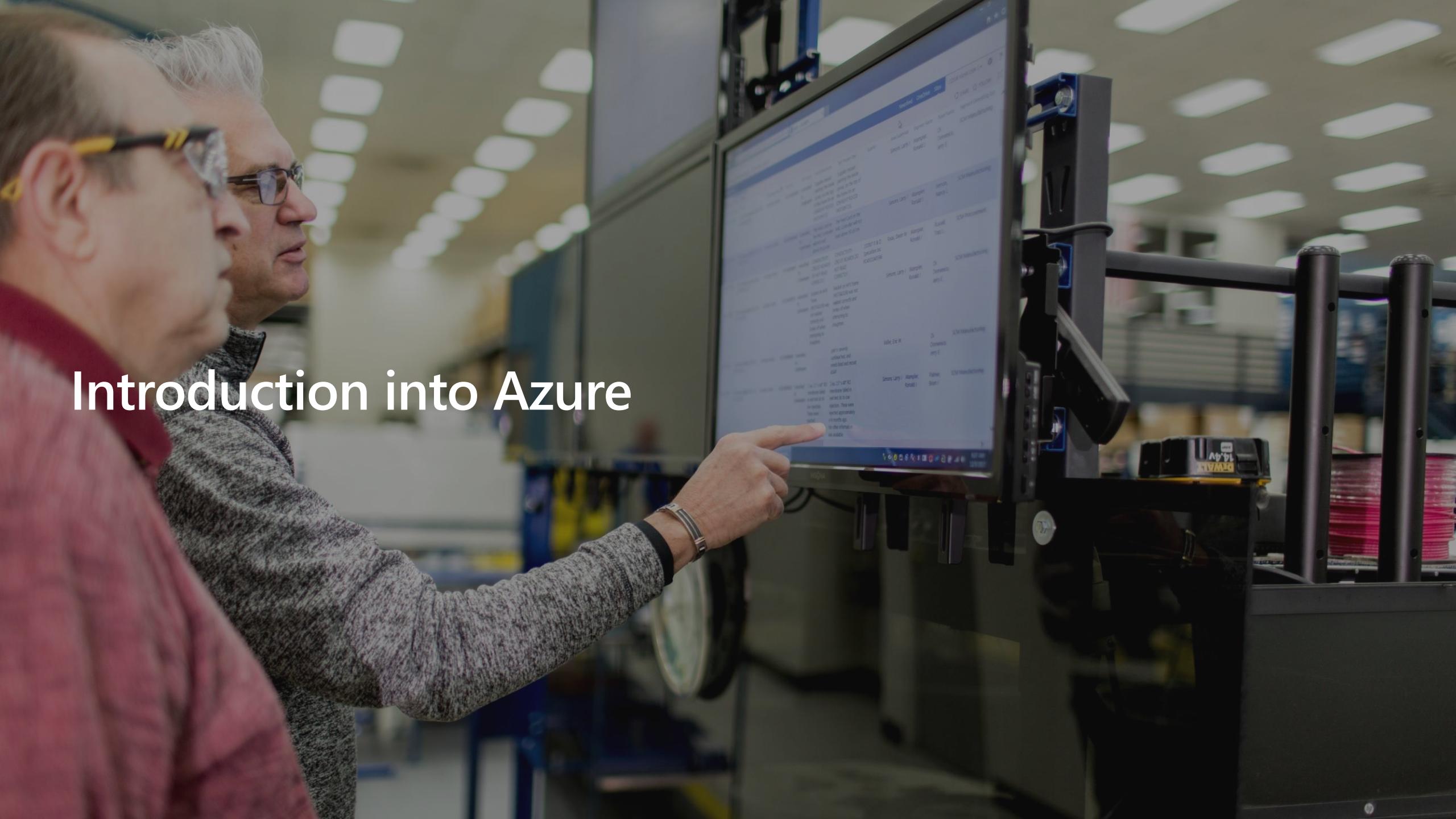
- High Availability and Resiliency
- Monitoring and Alerting
- Automate Hybrid Operations
- Automate Builds and Deployments
- Encryption and Keys

Workshop 1

Workshop 2



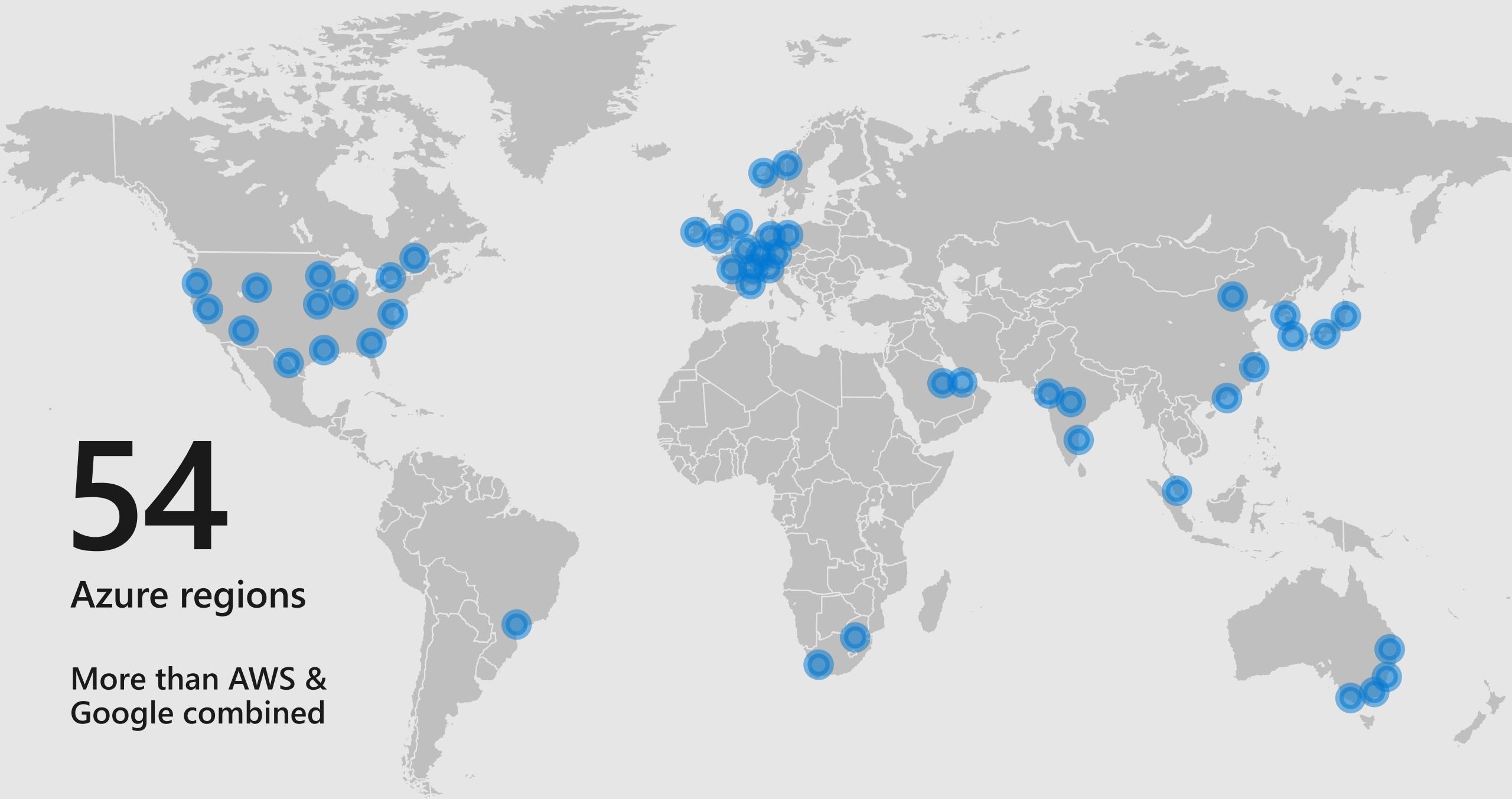
# Introduction into Azure



# 54

Azure regions

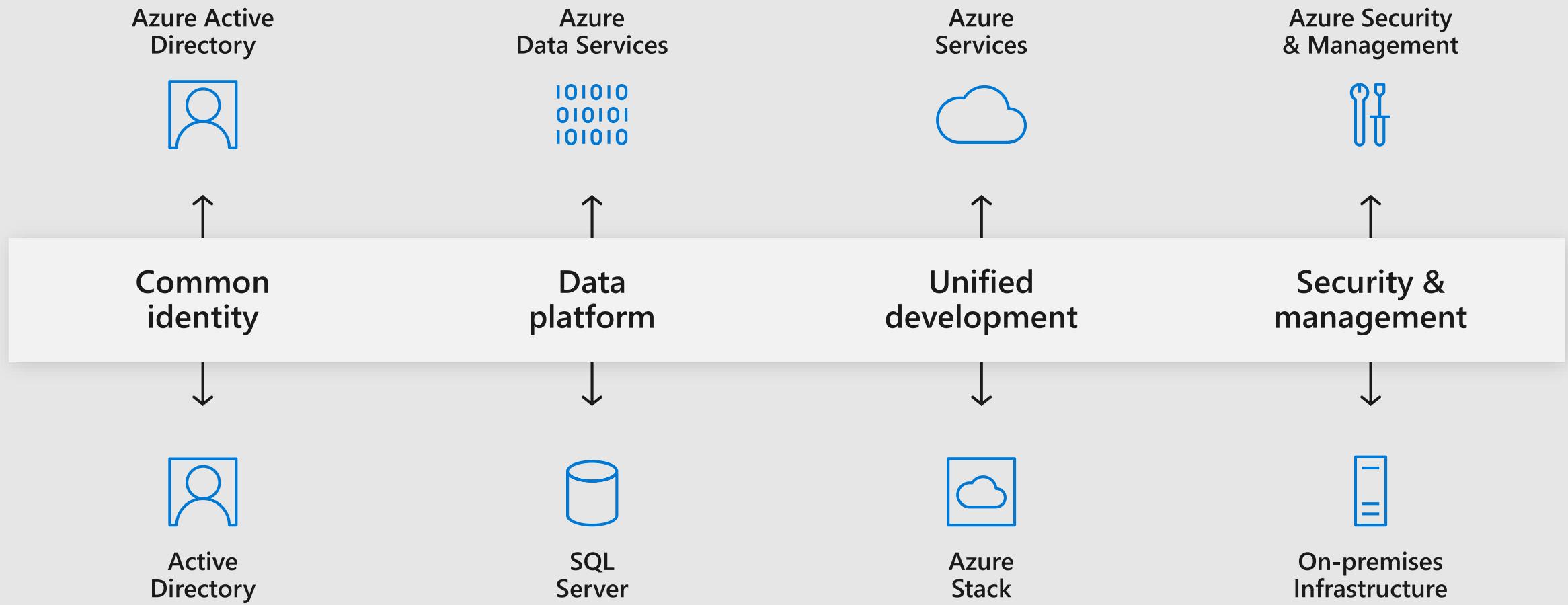
More than AWS &  
Google combined



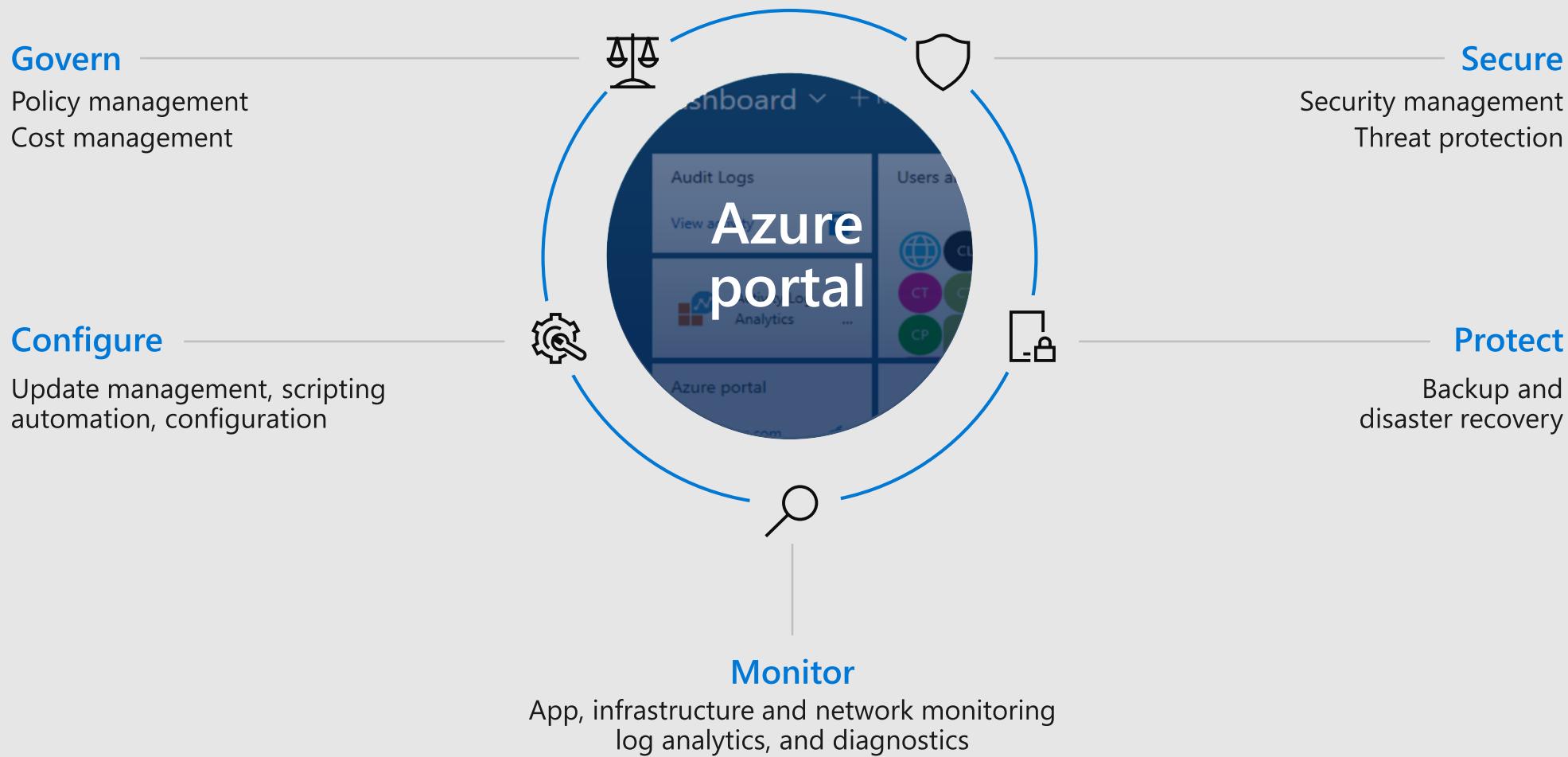
# Azure Compliance

Global										
	ISO 27001	ISO 27018	ISO 27017	ISO 22301	SOC 1 Type 2	SOC 2 Type 2	SOC 3	CSA STAR Self-Assessment	CSA STAR Certification	CSA STAR Attestation
US gov										
	Moderate JAB P-ATO	High JAB P-ATO	DoD DISA SRG Level 2	DoD DISA SRG Level 4	SP 800-171	FIPS 140-2	Section 508 VPAT	ITAR	CJIS	IRS 1075
Industry										
	PCI DSS Level 1	CDSA	MPAA	FACT UK	Shared Assessments	FISC Japan	HIPAA /HITECH Act	HITRUST	GxP 21 CFR Part 11	MARS-E
Regional										
	Argentina PDPA	EU Model Clauses	UK G-Cloud	China DJCP	China GB 18030	China TRUCS	Singapore MTCS	Australia IRAP/CCSL	New Zealand GCIO	Japan My Number Act

# Consistent hybrid environment



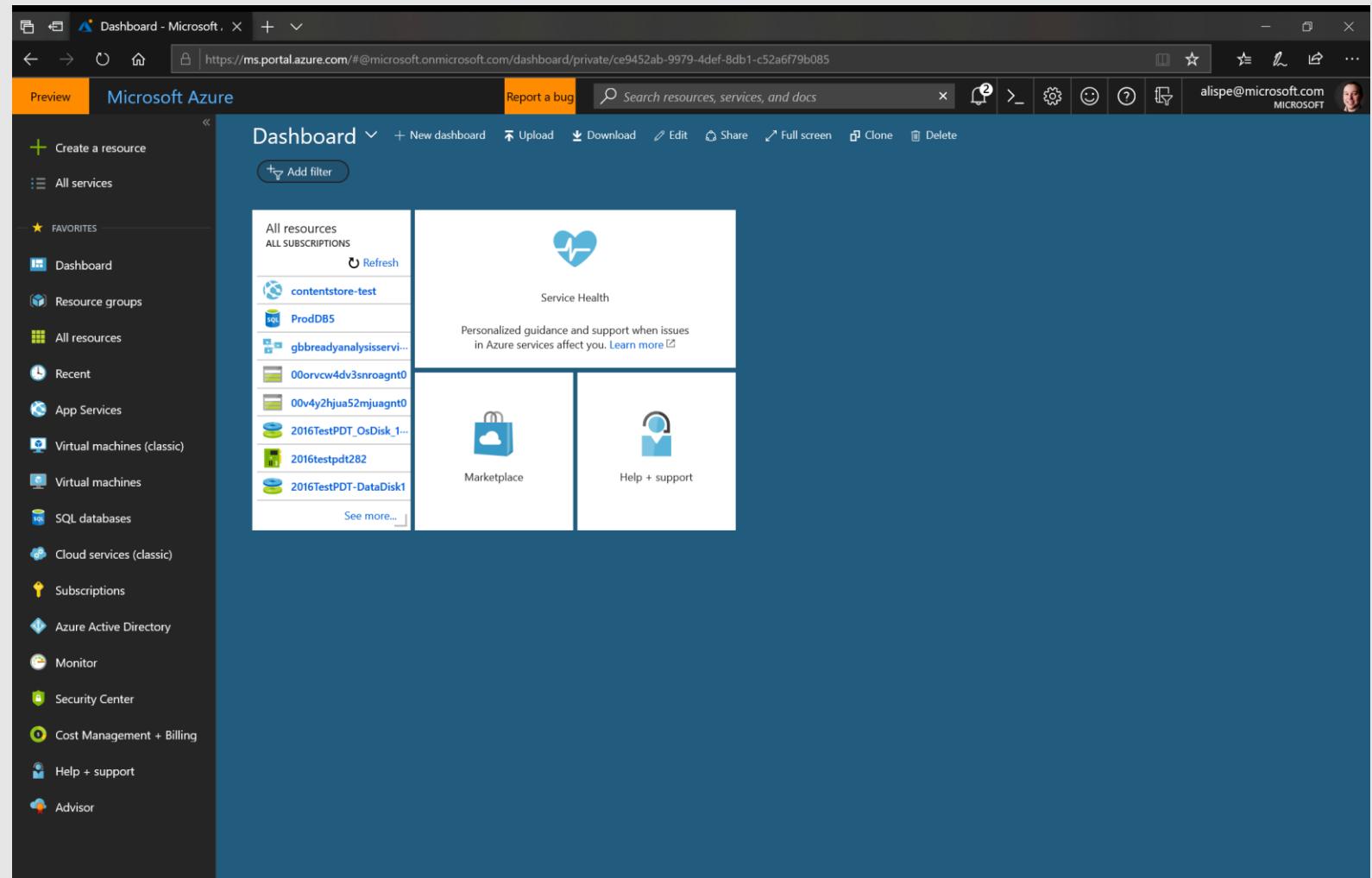
# Azure portal offers enterprise-grade management



# Azure portal is customizable—[portal.azure.com](https://portal.azure.com)

## Recommendation:

Create portal dashboards by key roles,  
(e.g., operations, finance, development),  
key projects, and key service KPIs.

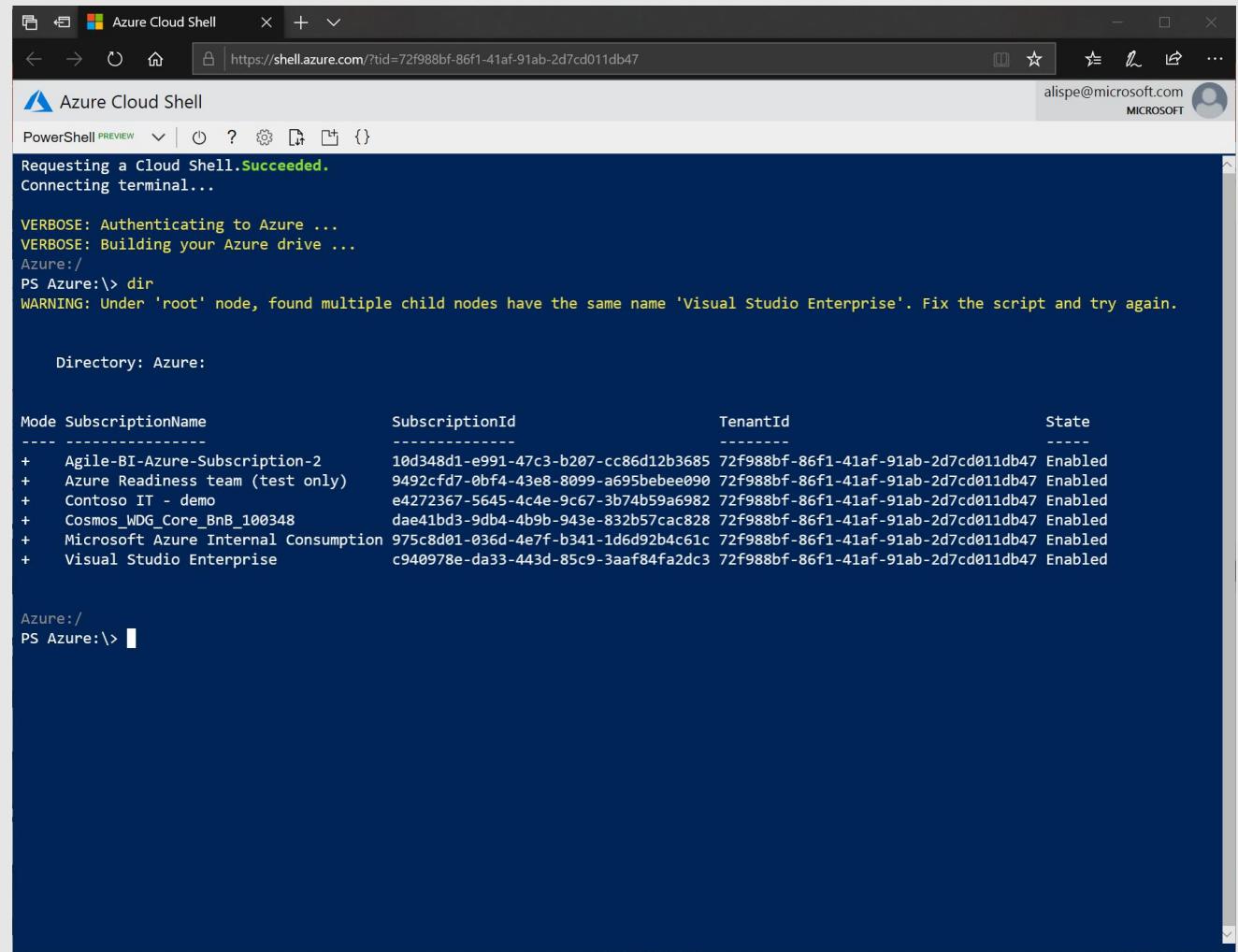


# Azure supports automation

## Recommendations:

Define ARM templates for commonly used resource configurations

Use Azure Policy to define which resources you allow teams to provision



The screenshot shows the Azure Cloud Shell interface in a browser window. The title bar says "Azure Cloud Shell". The address bar shows the URL "https://shell.azure.com/?tid=72f988bf-86f1-41af-91ab-2d7cd011db47". The user name "alispe@microsoft.com" is visible in the top right corner.

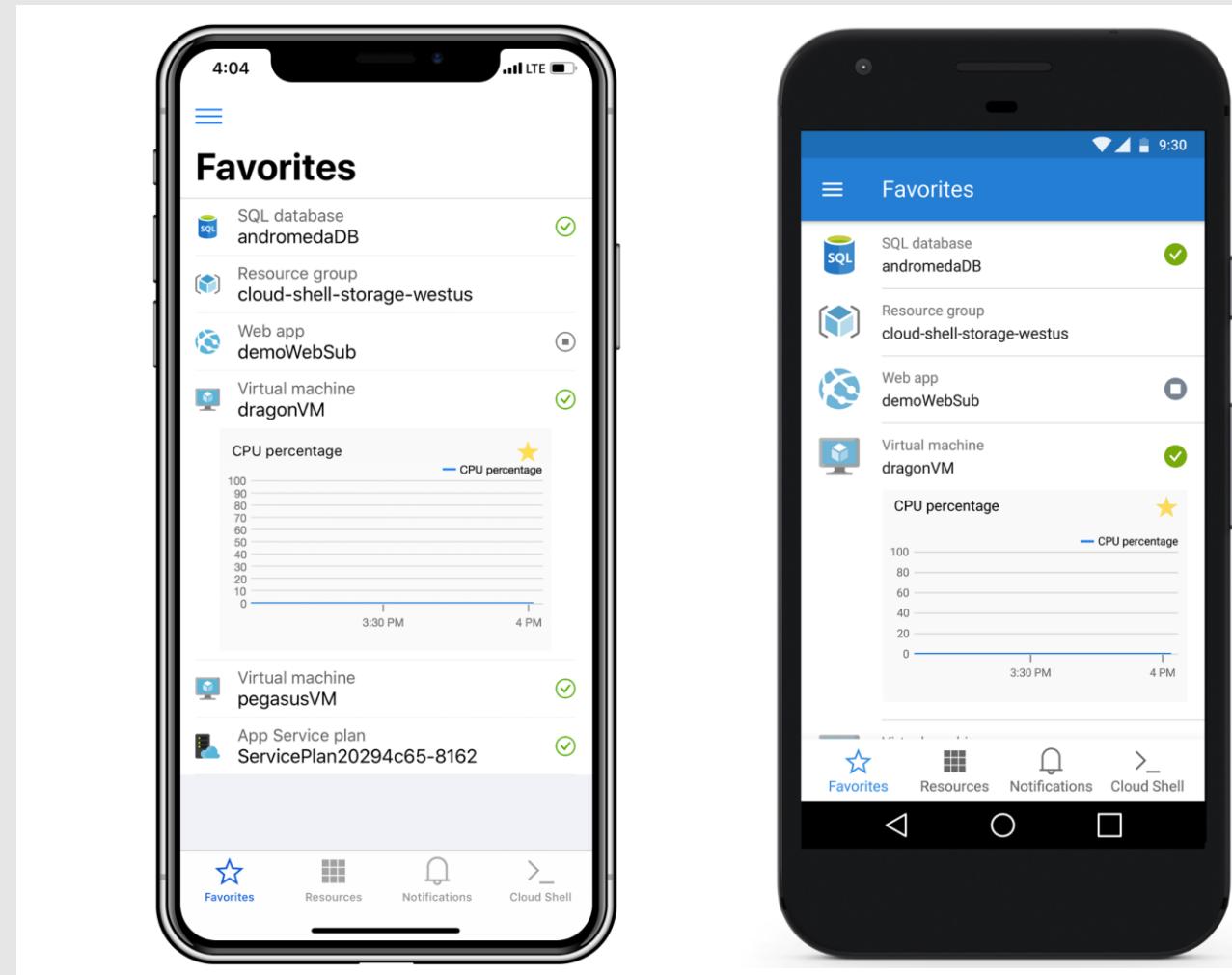
The PowerShell session is running in PREVIEW mode. The output shows:

```
Requesting a Cloud Shell. Succeeded.  
Connecting terminal...  
  
VERBOSE: Authenticating to Azure ...  
VERBOSE: Building your Azure drive ...  
Azure:/  
PS Azure:\> dir  
WARNING: Under 'root' node, found multiple child nodes have the same name 'Visual Studio Enterprise'. Fix the script and try again.  
  
Directory: Azure:  
  
Mode SubscriptionName SubscriptionId TenantId State  
---- -- -- -- --  
+ Agile-BI-Azure-Subscription-2 10d348d1-e991-47c3-b207-cc86d12b3685 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled  
+ Azure Readiness team (test only) 9492cf7-0bf4-43e8-8099-a695bebee090 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled  
+ Contoso IT - demo e4272367-5645-4c4e-9c67-3b74b59a6982 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled  
+ Cosmos_WDG_Core_BnB_100348 dae41bd3-9db4-4b9b-943e-832b57cac828 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled  
+ Microsoft Azure Internal Consumption 975c8d01-036d-4e7f-b341-1d6d92b4c61c 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled  
+ Visual Studio Enterprise c940978e-da33-443d-85c9-3aaaf84fa2dc3 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled  
  
Azure:/  
PS Azure:\>
```

# Azure mobile app

Stay connected to your Azure resources – anytime, anywhere

- Monitor the health and status of your Azure resources on the go
- Get quick access to your favorite resources
- Get notifications and alerts about important health issues
- Quickly diagnose and fix issues from your mobile device
- Run Azure Cloud Shell scripts (PowerShell or Bash) from the app
- Control access to resources using Role Based Access Control
- Now available on iOS and Android



[Learn more.](#)

# Azure communicates incidents, upcoming maintenance and health advisories via Azure Service Health

## Recommendation:

Set up Azure Service Health alerts, for example:

- An alert to email your dev team when a resource in a test/dev subscription is impacted
- An alert to update ServiceNow via webhook when a resource in production is impacted
- An alert to send an SMS to a specific number when resources in a given region are impacted

The screenshot displays the Azure Service Health interface with two main sections: "Service Health - Service issues" and "Service Health - Health history".

**Service Health - Service issues (Top Section):**

- ACTIVE EVENTS:** Shows three categories: "Service issues" (selected), "Planned maintenance", and "Health advisories".
- HISTORY:** Shows a "Health history" section.
- Filtering and Alerts:** Includes filters for "Subscription" (Contoso IT - demo), "Region" (28 selected), and "Service". A tooltip suggests pinning a personalized Service Health world map to the dashboard.

**Service Health - Health history (Bottom Section):**

- ACTIVE EVENTS:** Shows three categories: "Service issues" (selected), "Planned maintenance", and "Health advisories".
- ISSUE LIST:** Displays a table of issues with columns: ISSUE NAME, TRACKING ID, EVENT TYPE, SERVICE(S), REGION(S), START TIME, and UPDATED. Two entries are shown:
  - Log Analytics - West Europe, SFJA-PK0, Service issue, Log Analytics, West Europe, 17:42 UTC, 02/07/2018, 5 d ago
  - Action Required Regarding Your Azure Backup ser..., G8\_S\_-K0, Health advisory, Backup, Australia East..., 16:02 UTC, 02/07/2018, 5 d ago
- Summary:** Provides details for the first issue: Tracking ID SFJA-PK0, Get a link, Share this link with your team or use it for reference in your problem management system. It also lists Impacted services (Log Analytics) and Impacted regions (West Europe). A note states: "Last update (5 d ago)" followed by a detailed summary of the impact, cause, and mitigation.
- Actions:** Includes links to download the issue summary as a PDF, track it on mobile, and connect with experts via Twitter.

# Stay informed of changes in Azure

## [Azure.com/updates](#)

**Azure updates** is the single source of truth for product updates and roadmap changes

Subscribe to customized RSS Feed to stay informed on updates you care about

Includes packaging, licensing and region availability changes

The screenshot shows the Azure updates page with a dark header. The top navigation bar includes links for Overview, Solutions, Products, Documentation, Pricing, Training, Marketplace, Partners, Support, Blog, More, and a Free account button. The main title is "Azure updates" with a sub-instruction: "Learn about important Azure product updates, roadmap, and announcements. Subscribe to notifications to stay informed." Below this is a banner for "Get the latest Azure announcements from Microsoft Ignite 2018". The page features a search bar and filters for "Products" (Browse, Search for a product, Filter icon) and "Update type" (All, RSS feed). A horizontal navigation bar at the top of the update list allows filtering by "All", "Now available", "In preview", and "In development". The update list is organized by month. Each update entry includes a date, a title, a brief description, and category tags. The "Explore" sidebar on the right provides links to the Azure blog, feedback options, and regional availability information.

Date	Title	Description	Category Tags
Oct 4	PHP minor version update for November 2018	In November 2018, Azure App Service will update the PHP stacks to the latest available versions.	Features, SDK and Tools
Oct 4	Azure SQL Database Managed Instance name change and GUID migration	Region names and resource GUIDs for Managed Instance General Purpose SQL License were changed on September 27, 2018.	Azure SQL Database, Services
Oct 4	Public preview: Azure Database for MariaDB	Azure Database for MariaDB is in public preview.	Azure Database for MariaDB, Microsoft Ignite, Services
Oct 4	Deprecation of preview API versions for Azure Database for MySQL	For Azure Database for MySQL, all customers who use the preview APIs must switch to the new API version.	

# Azure AD for Azure



# Azure AD – How To Start

## Single Tenant, Multiple Domains

1. Create a single tenant which is shared between Azure and Office365
2. Register public resolvable custom DNS domain names for admin and non-admin roles
3. Create AAD groups for end users, governance owners, subscription owners, contributors, and readers
4. Assign subscription owners the AAD Application developer role, so that they can register applications and service principals
5. Elevate access to manage all Azure subscriptions and management groups and configure the Root Management Group: [How To](#)

mikepet.onmicrosoft.com	✓ Available
petersen.cloud	✓ Verified

NAME	GROUP TYPE	MEMBERSHIP TYPE
AD AAD DC Administrators	Security	Assigned
AU All Users	Security	Dynamic
SC Subscription Contributors	Security	Assigned
SO Subscription Owners	Security	Assigned
SR Subscription Readers	Security	Assigned

Application developer	Can create application registrations independent of the 'Users can register applications' setting.
-----------------------	--

### Access management for Azure resources

Michael Petersen (michael@petersen.cloud) can manage access to all Azure subscriptions and management groups in this directory. [Learn more](#)

[Yes](#)   [No](#)

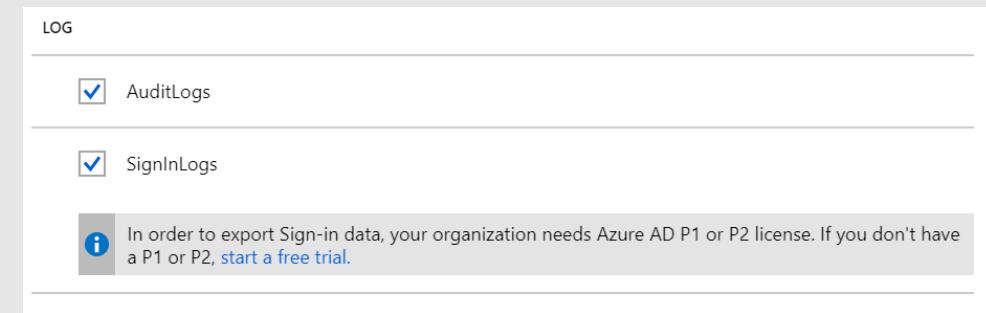
# Azure AD – How To Start

## Auditing and Identities

6. Configure central Storage Account and Log Analytics workspace to collect Audit/SignIn logs for auditing purposes

7. Understand roles in
  - Azure AD
  - and in Azure RBAC
  - ... and assign identities to them
  - [ARM Provider Operations](#)

8. Applications and Service Principals
  - Application is a global definition in its home AAD tenant
  - Service Principal is local to an AAD tenant where the application accesses protected resources
  - [Background Information](#) and [Why](#)
  - Create Subscription Creator App/SP



Exchange administrator	Can manage all aspects of the Exchange product.
Global administrator	Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.
Guest inviter	Can invite guest users independent of the 'members can invite guests' setting.

NAME	TYPE	USERS	GROUPS
Owner	BuiltInRole	1	1
Contributor	BuiltInRole	1	1
Reader	BuiltInRole	0	1
User Access Administrator	BuiltInRole	1	0

To access resources that are secured by an Azure AD tenant, the entity that requires access must be represented by a security principal. This is true for both users (user principal) and applications (service principal).

The Managed Identities for Azure feature provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

[Managed Identities for Azure](#)

# Azure AD – How To Start

## External Collaboration

9. Configure organizational relationships

10. Define who can invite external guests

11. Azure AD creates “proxy” accounts for guests that point to external accounts but can be used to authorize access to Azure resources protected by Azure AD

- Identity provider for Google Accounts available
- External Azure AD und Microsoft Accounts supported
- Any other account type mapped to newly created Microsoft Account with a separate password and identical username

Guest users permissions are limited [i](#)

Yes

No

Admins and users in the guest inviter role can invite [i](#)

Yes

No

Members can invite [i](#)

Yes

No

Guests can invite [i](#)

Yes

No

Enable Email One-Time Passcode for guests (Preview) [i](#)

[Learn more](#)

Yes

No

## Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)  
 Deny invitations to the specified domains  
 Allow invitations only to the specified domains (most restrictive)



[i](#) Invited users who own an Azure Active Directory account or a Microsoft Account can automatically sign in without further configuration.

## Social identity providers

NAME

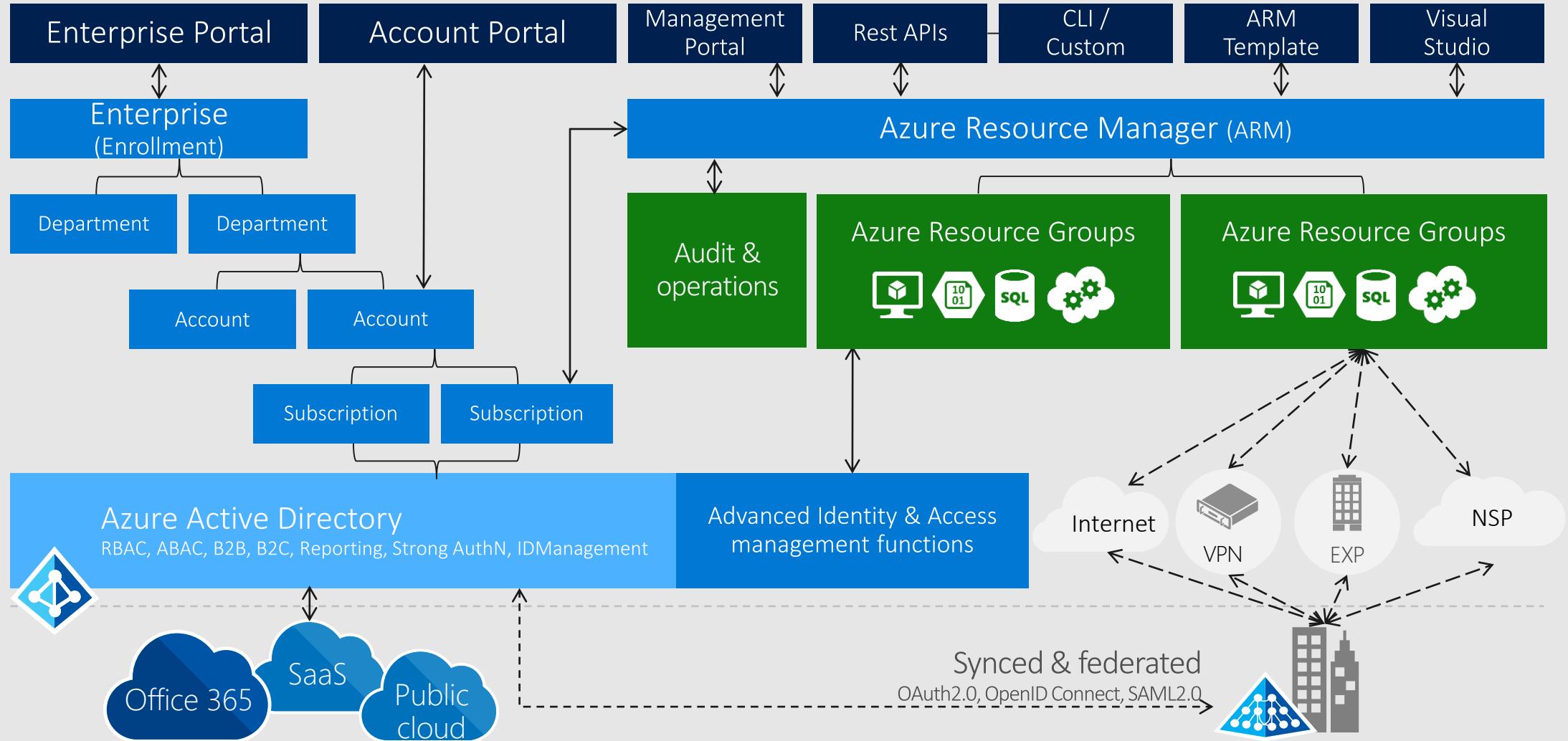
Google

USER TYPE	SOURCE
Guest	<a href="#">Microsoft Account</a>
Guest	<a href="#">External Azure Active Directory</a>
Guest	<a href="#">Google</a>

# Cloud Security and Governance



# Azure Enrollment Overview



# Azure – How To Start

## Enterprise Portal

1. Formula: 1 Azure enrollment -> 1 AAD tenant  
-> 1-N enrollment accounts -> 50-200 subscriptions
2. Recommendation: please ignore departments and enrollment accounts and use enrollment accounts only as technical container for Azure subscriptions: account-1, account-2, ...

The screenshot shows the Azure Enterprise Portal interface. On the left is a dark sidebar with navigation links: Manage, Reports, Notification, Help, and See related accounts. The main area has tabs at the top: Enrollment (selected), Department, Account, and Subscription. The Enrollment Detail section displays information for enrollment number 100, including Company Name (Test Enrollment (Direct)), Country (United States), Auth Level (Mixed Account), Start/End Date (7/1/2013 - 6/30/2018), Billing Cycle (Quarterly), Status (Active), Support Level (Standard), Support Coverage (8/6/2015 - 6/30/2016), Azure Marketplace (Enabled), DA view charges (Enabled), and AO view charges (Enabled). The Enrollment Accounts section lists several administrators and notification contacts, each with email, auth type, notification frequency, lifecycle notification suppression, and a read-only flag. The administrators listed are bilitest339823@live.com, bilitest397830@live.com, bilitest698326@live.com, chewan@microsoft.com, and cts-gcrdsd@live.com. The notification contacts listed are 123456@naver.com, bharat.gangavarapu@hotmail.com, v-il@microsoft.com, and v-il@microsoft.com.

3. Assign account owners to enrollment accounts

- RBAC assignment of an AAD user to the enrollment account
- AAD User Object ID
- Role = 'Owner'
- Scope = '/providers/Microsoft.Billing/enrollmentAccounts/{guid}'
- [Grant Access](#) and [Create Subscription](#)

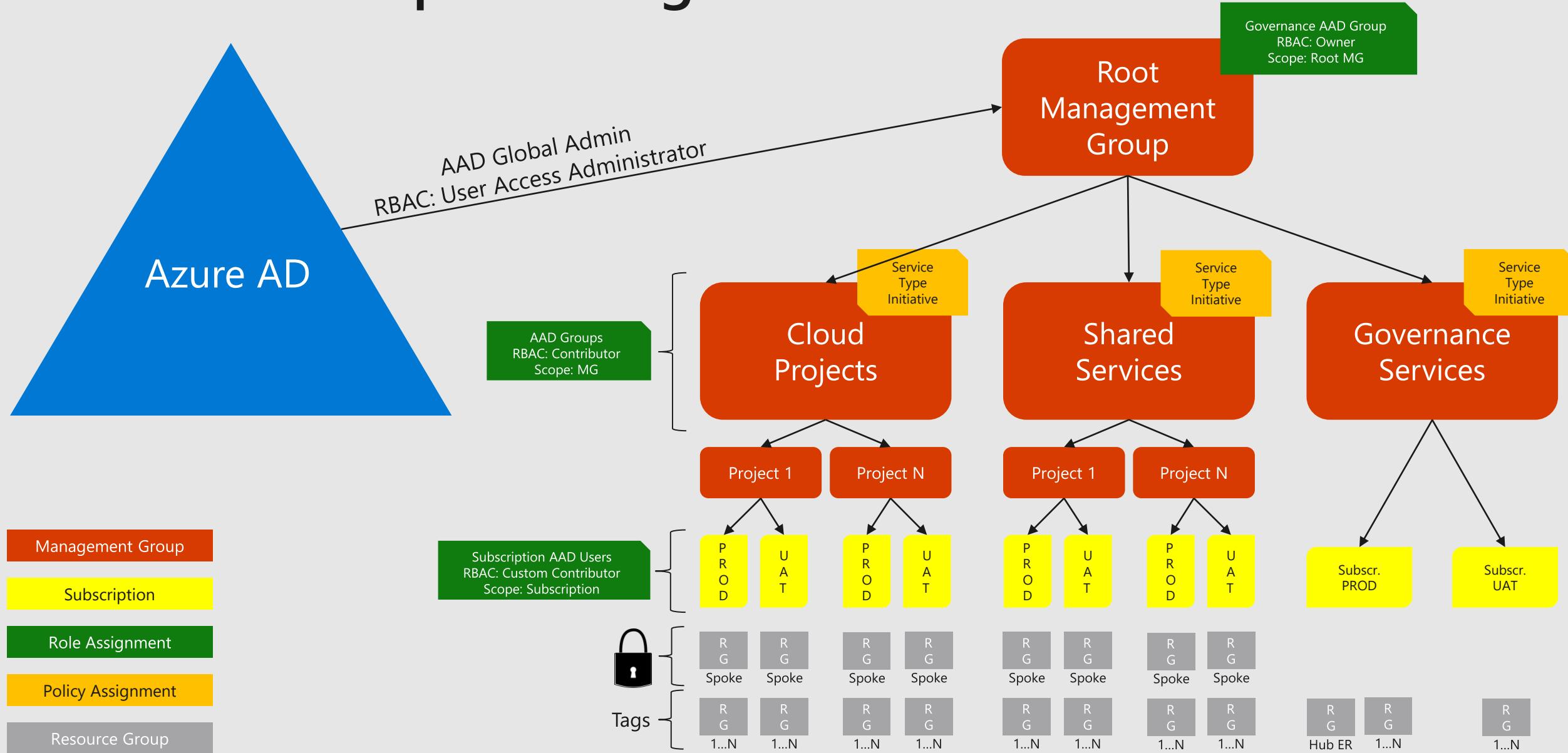
Get-AzEnrollmentAccount

```
New-AzRoleAssignment -RoleDefinitionName Owner  
-ObjectId <userObjectId>  
-Scope /providers/Microsoft.Billing/enrollmentAccounts/<GUID>
```

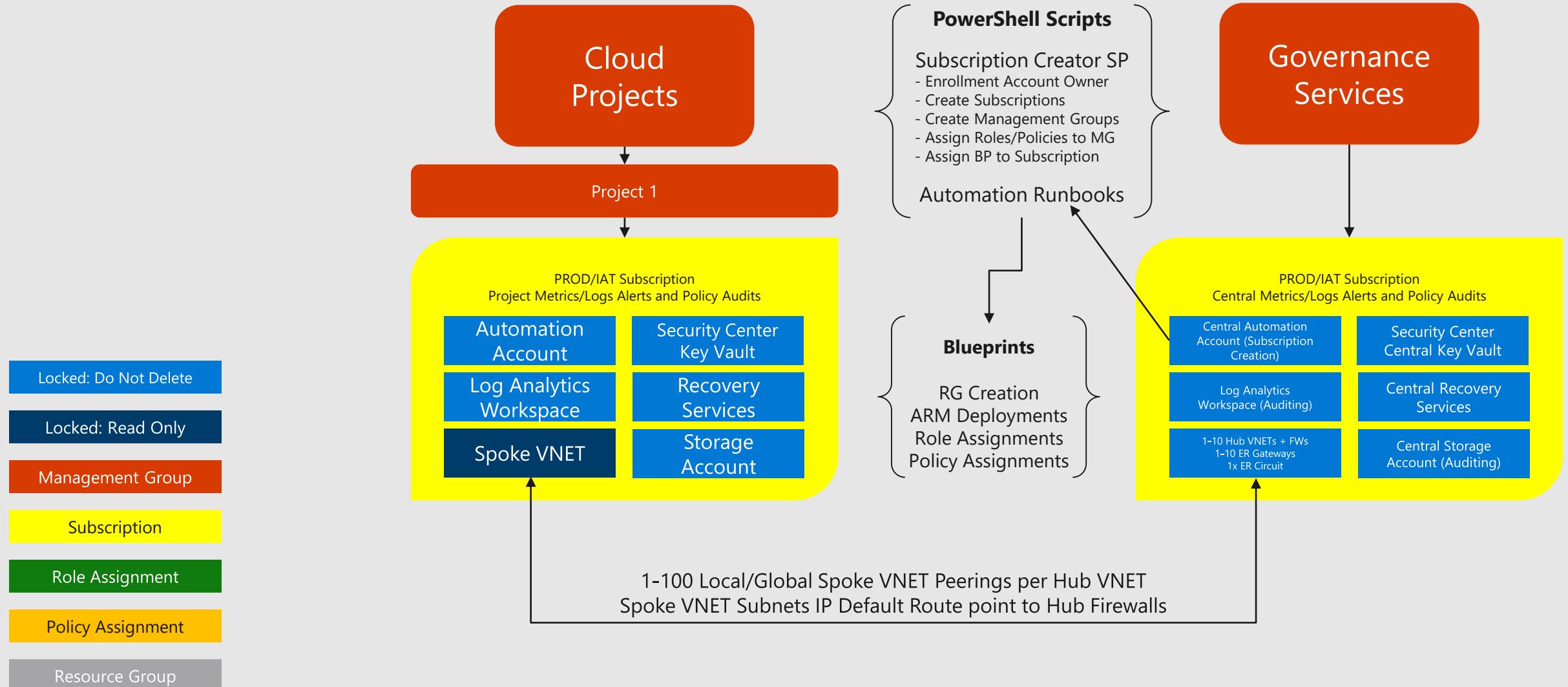
```
New-AzSubscription -OfferType MS-AZR-0017P  
-Name "Subscription Name" -EnrollmentAccountObjectId <GUID>  
-OwnerObjectId <userObjectId>, <servicePrincipalObjectId>
```

# Azure Subscriptions Organization

Billing and Permission hierarchy is identical in this concept (no EA portal usage)



# Azure Subscriptions Blueprint



# Governance – What To Learn

## Understand Inheritance

1. Management Groups, Subscriptions, Resource Groups, and Resources build an inheritance hierarchy with respect to permissions and policies
2. Azure Policy is an explicit deny system (everything is allowed by default). If you denied something, you cannot allow it again later.
3. Azure RBAC is an explicit allow system (everything is denied by default). If you allow something, you cannot deny it again later on.
  - This will change in the future: [Deny Assignments](#)

## Define core set of Azure Policies

4. Enforce NSG rules, image publishers, locations, managed disks, encryption, resource types, ...
5. Look at built-in policies and samples on GitHub: <https://github.com/Azure/azure-policy>

# Subscriptions Organization – Deep Dive

## Walkthroughs

### 1. PowerShell

- Management Groups
- Policies, Custom Roles

```
9 # Create first level of Management Groups
l0 New-AzManagementGroup -GroupName 'cloud-projects' -DisplayName 'Cloud Projects' -ParentId $parentId
l1 New-AzManagementGroup -GroupName 'shared-services' -DisplayName 'Shared Services' -ParentId $parentId
l2 New-AzManagementGroup -GroupName 'governance-services' -DisplayName 'Governance Services' -ParentId $parentId
```

### 2. Blueprints

- Create and analyze results
- What is happening in the background
- What is a Deny Assignment

The screenshot shows the Azure Blueprints blade. On the left, there's a sidebar with 'Getting started', 'Blueprint definitions' (which is selected and highlighted in blue), and 'Assigned blueprints'. On the right, there's a table with the following data:

NAME	LATEST VERSION
locked-storageaccount	1.0
two-rgs-with-role-assignments	1.01

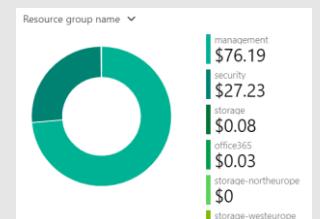
### 3. Security Center

- Enable Security Center (coverage)
- Understand security policies and settings
- Recommendations
- Adaptive Application Controls
- JIT VM Access

The screenshot shows the Azure Security Center blade. It has three main sections: 'Recommendations' (2 total, 1 High Severity, 0 Medium Severity, 1 Low Severity), 'Resource health monitoring' (Compute & apps: 0, Networking: 2, IoT hubs & resources: 0), and 'Unhealthy resources' (3).

### 4. Cost Center

- Create budgets with alerts and exports

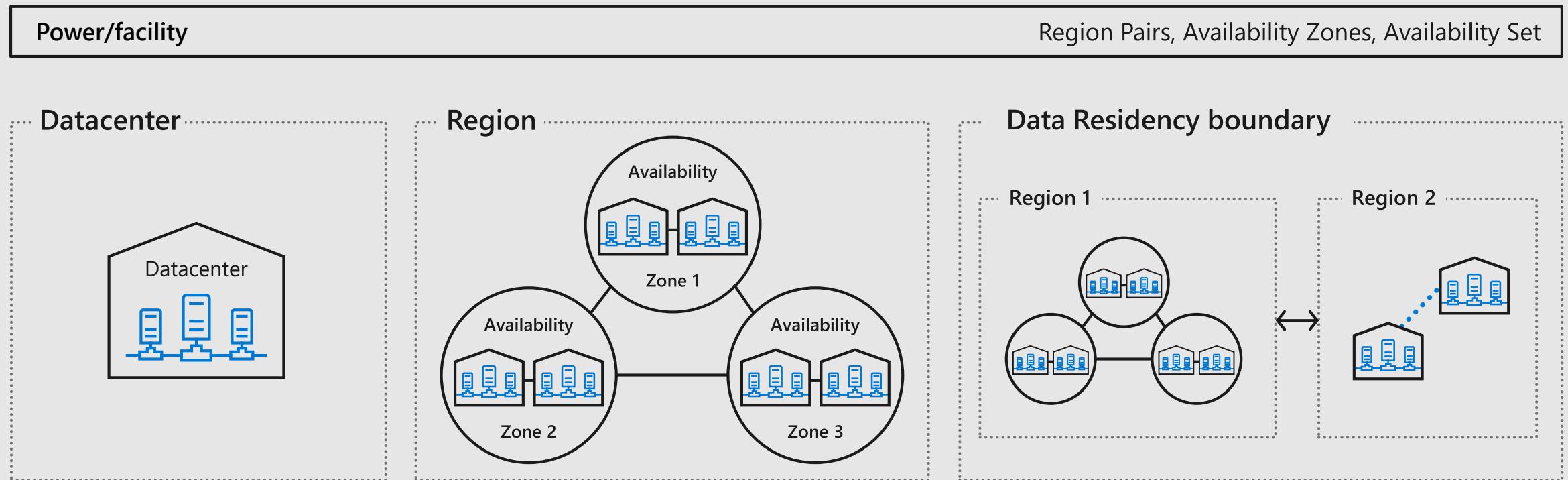


# Operations for the Cloud



# Azure Resiliency as a Platform

Resilient from hardware, datacenter, and regional outages



## Availability Sets

High availability protection from hardware failures in a datacenter

## Availability Zones

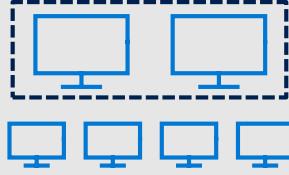
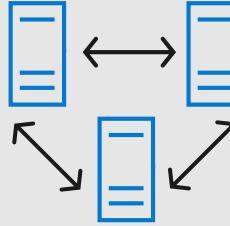
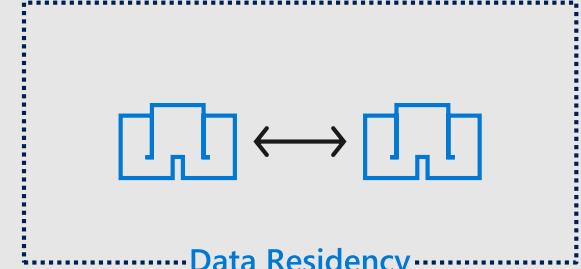
High availability protection against loss of datacenters. Multiple datacenters per physically separated zone. Each zone features independent network, cooling, and power

## Region Pairs

Protection for your data and applications from the loss of an entire region with Geo-redundant storage (GRS) and Azure Site Recovery

# Azure Resiliency as a Platform

## Industry-leading high availability SLA

Power/facility	Region Pairs, Availability Zones, Availability Set		
Industry-only	• Industry-leading high availability SLA	• Industry-leading broadest choice of Data Residency	•
VM SLA 99.9%	VM SLA 99.95%	VM SLA 99.99%	Regions 54
			 Data Residency
Single VM Protection with Premium Storage	Availability Sets Protection against failures within datacenters	Availability Zones Protection from entire datacenter failures	Region Pairs Protection from disaster with Data Residency compliance

# Azure Storage Resiliency Solutions

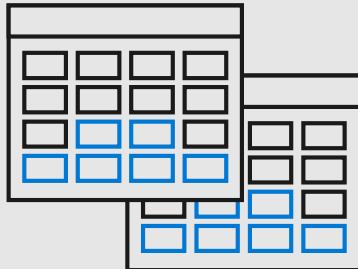
Azure storage provides replication options based on availability needs

## Storage

\* Designed to provide durability of objects over a given year

### LRS

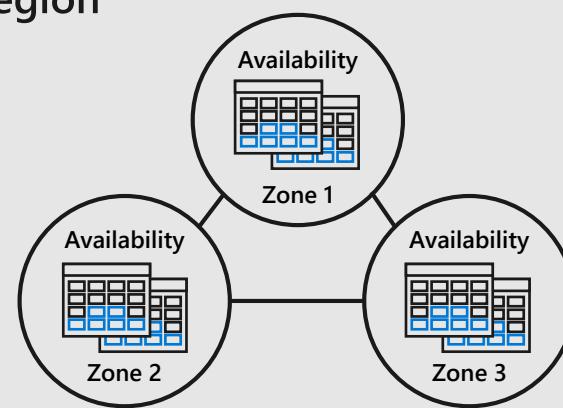
99.99999999% (11 9s) \*



### ZRS

99.999999999% (12 9s) \*

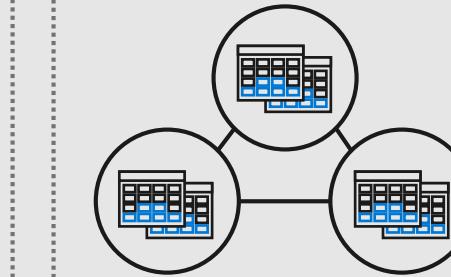
### Region



### GRS

99.9999999999999% (16 9s) \*

### Region 1



### Region 2



## Locally redundant storage

The simplest, low-cost replication strategy that Azure Storage offers

## Zone-redundant storage

A simple option for high availability and durability

## Geo-redundant storage

Cross-regional replication to protect against region-wide unavailability

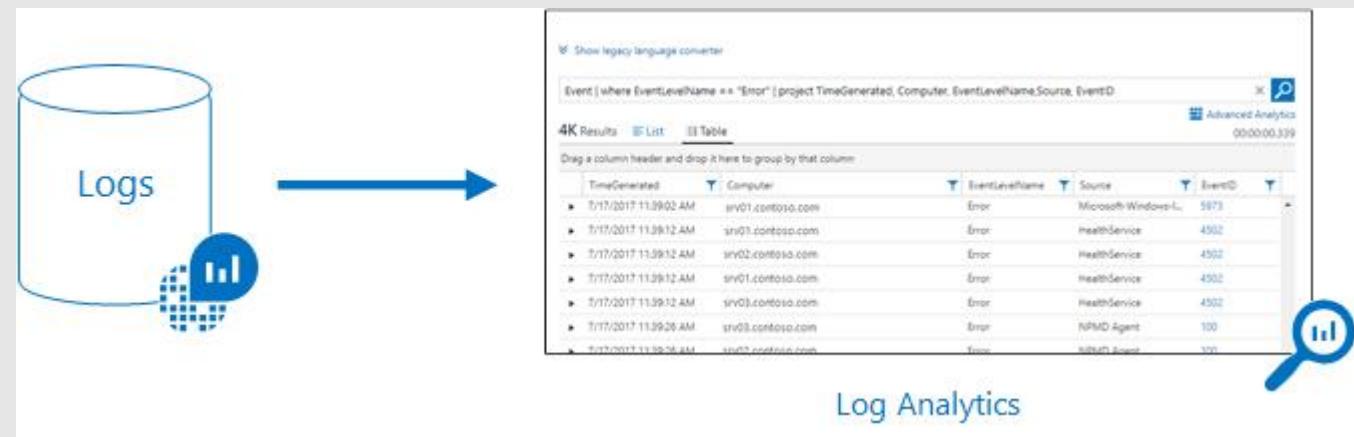
# Azure Monitor

## Metrics and Logs

- All data collected by Azure Monitor fits into one of two fundamental types, metrics and logs.
- Metrics are numerical values that describe some aspect of a system at a particular point in time.



- Logs contain different kinds of data organized into records with different sets of properties for each type. Telemetry such as events and traces are stored as logs.





# Azure Monitor

Application

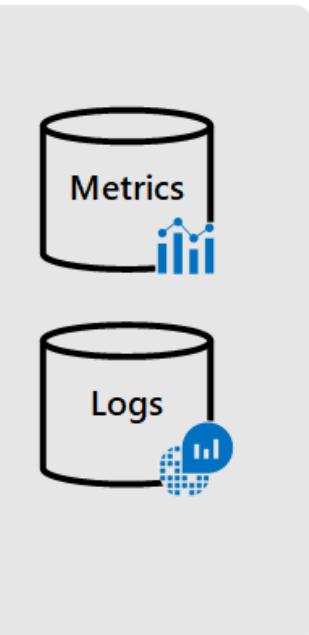
Operating System

Azure Resources

Azure Subscription

Azure Tenant

Custom Sources



## Insights



Application



Container



VM



Monitoring Solutions

## Visualize



Dashboards



Views



Power BI



Workbooks

## Analyze



Metric Analytics



Log Analytics

## Respond



Alerts



Autoscale

## Integrate



Event Hubs



Logic Apps



Ingest & Export APIs

# Monitor – Deep Dive

## Walkthroughs

### 1. Activity Logs

- PUT, POST, DELETE on any subscription resource
- Stored for 90 days, read only
- Log Profiles for central auditing
- [Activity Logs Overview](#)
- [Export Activity Log with Log Profiles](#)

### 2. Alerts, Alert Rules, Action Groups

- Create CPU alert for VM

### 3. Metrics

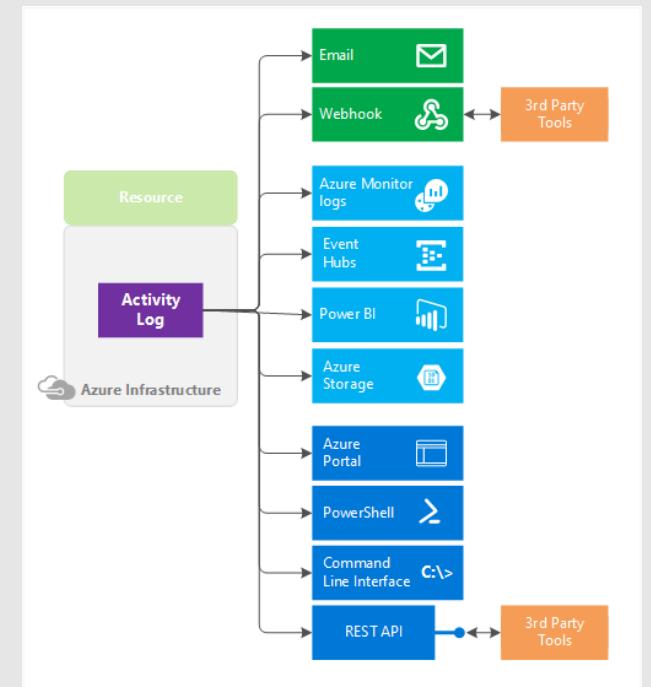
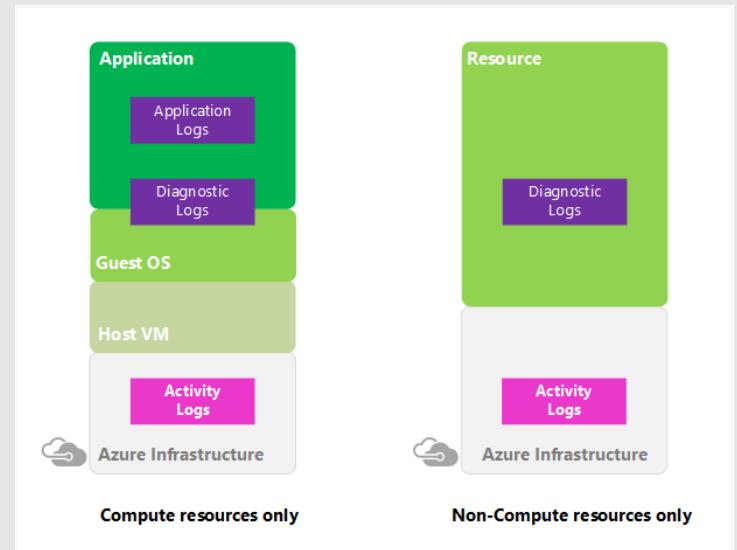
- Create CPU and IOPS/s chart for VM

### 4. Service Health

- Service Issues, Planned Maintenance, Health Advisories, Health History, Resource Health, Health Alerts

### 5. Diagnostics Settings

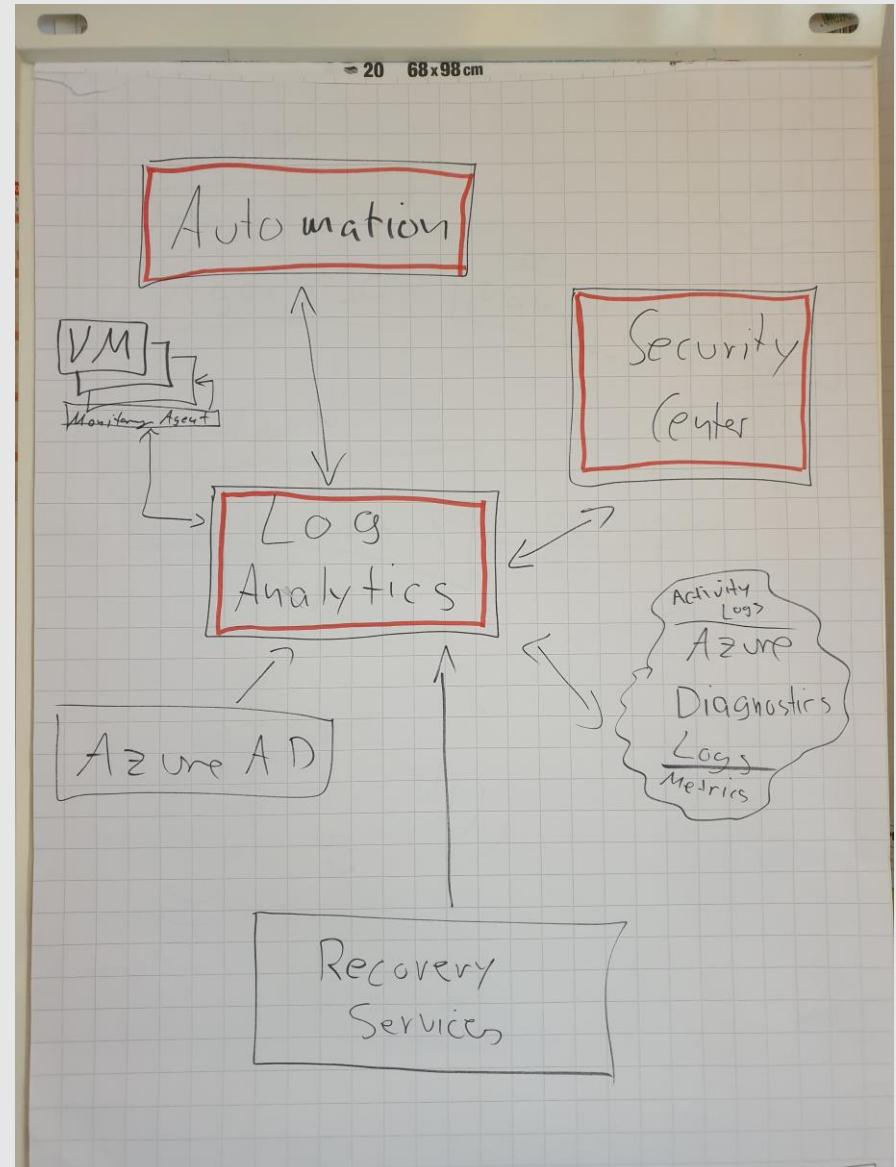
- Collect diagnostics logs from any resource



# Automate Operations – Deep Dive

## Walkthroughs

1. Log Analytics
  - Workspace Data Sources
  - Advanced Settings
  - Automation Account
2. Enable VM Insights based on Log Analytics on Virtual Machine Blade (Monitoring/Insights)
  - [VM Insights At Scale with Policies](#)
3. Automation
  - Configuration Management
  - Update Management
  - Hybrid Worker Groups
  - Process Automation (Runbooks/Jobs)
4. Recovery Services Vault
  - Azure Backup & Restore

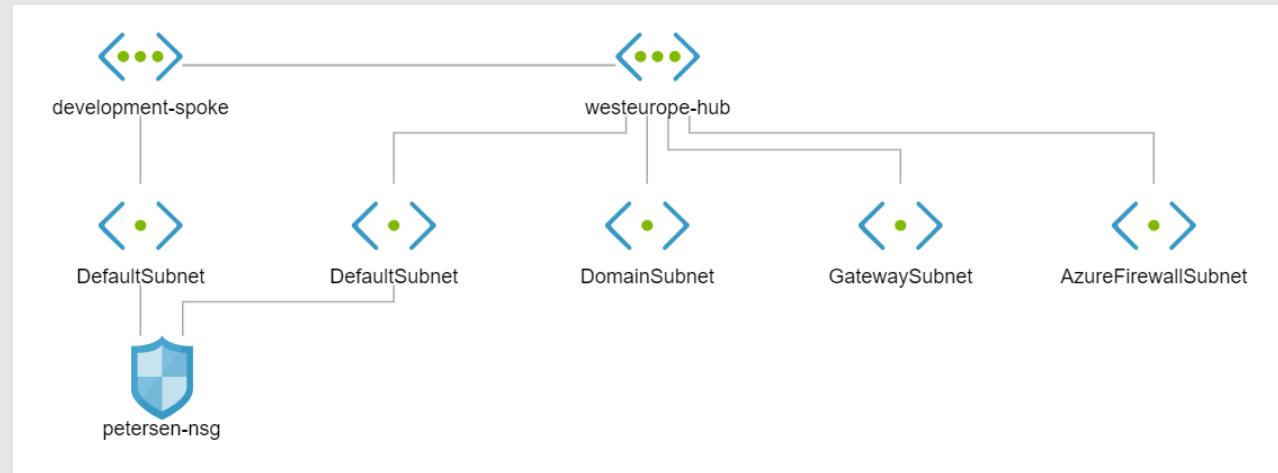


# Network Watcher – Deep Dive

## Walkthroughs

### 1. Network Watcher

- Topology
- Connection Monitor (e.g. Web -> SQL)
- IP Flow Verify
- Next Hop
- Effective Security Rules
- Packet Capture



SOURCE	SOURCE PORTS	DESTINATION	DESTINATION PORTS	PROTOCOL	ACCESS
[REDACTED]/16	0-65535	Virtual network (2 prefixes)	22-22,3389-3389,5985-5...	TCP	Allow
Virtual network (2 prefixes)	0-65535	Virtual network (2 prefixes)	0-65535	All	Allow
Azure load balancer (1 prefixes)	0-65535	0.0.0.0/0	0-65535	All	Allow
0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	All	Deny

SOURCE	SOURCE PORTS	DESTINATION	DESTINATION PORTS	PROTOCOL	ACCESS
Virtual network (2 prefixes)	0-65535	Virtual network (2 prefixes)	0-65535	All	Allow
0.0.0.0/0	0-65535	Internet (122 prefixes)	0-65535	All	Allow
0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	All	Deny

# Terraform Support in Azure

## Strong support for Terraform in the Azure Cloud

1. The Azure Provider can be used to configure infrastructure in Microsoft Azure using the Azure Resource Manager API's: <https://www.terraform.io/docs/providers/azurerm/index.html>
2. Azure Documentation Hub for Terraform: <https://docs.microsoft.com/en-us/azure/terraform/>
3. Large amount of examples for the Terraform Azure Provider: <https://github.com/terraform-providers/terraform-provider-azurerm/tree/master/examples>

## Tools for Terraform related to Azure

4. Azure Cloud Shell preconfigured for Terraform: <https://docs.microsoft.com/en-us/azure/terraform/terraform-cloud-shell>
5. Azure Storage as Terraform State Backend: <https://docs.microsoft.com/en-us/azure/terraform/terraform-backend>
6. Azure Marketplace provides preconfigured Linux VM with Managed Identity: <https://docs.microsoft.com/en-us/azure/terraform/terraform-vm-msi>
7. Azure Terraform VS Code Extensions: <https://docs.microsoft.com/en-us/azure/terraform/terraform-vscode-extension>
8. Terraform Build and Release Tasks for Azure DevOps: <https://marketplace.visualstudio.com/items?itemName=charleszipp.azure-pipelines-tasks-terraform>

# Automate Builds and Deployments – Deep Dive

## Visual Studio Community Edition – ARM Automation

1. Create empty project and understand ARM fundamentals
2. Quickstart Templates for Azure and Blueprint ARM Templates
3. Create Virtual Machine with Key Vault Integration and Custom Script Extension

## Visual Studio Code – Terraform Automation

4. Understand Terraform extensions for Azure
5. Deploy Getting Started and optionally Kubernetes Cluster or Virtual Machine

## Azure DevOps – Automate Everything with Pipelines

4. Understand Pipelines to automate CI (build) and CD (deploy)
5. Deploy Azure resources with ARM Templates
6. Infrastructure deployments in the Azure Cloud with Terraform, see also  
<https://azureddevopslabs.com/labs/vstsextend/terraform/>
7. Custom Build Servers and Deployment Groups
8. How to integrate Git Lab with Azure DevOps Pipelines, see also  
<https://marketplace.visualstudio.com/items?itemName=onlyutkarsh.gitlab-integration>

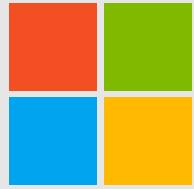
# Cryptographic Security – What To Learn

## Data At Rest, Data In Transit

1. For any application and storage system it is mandatory to understand the encryption technologies in use while data is stored (at rest) and transferred (in transit)
2. Two examples: Azure Storage, Azure SQL Database
  - Storage: Storage Service Encryption (at rest) and HTTPS (in transit), [Storage Security Guide](#)
  - SQL: Transparent Data Encryption (at rest) and TDS+TLS (in transit), [SQL Security](#)

## Key Management, Secret Management, Certificate Management

4. Azure Key Vault: a FIPS 140-2 Level 2 validated HSM (in premium edition), [Key Vault Overview](#)
5. To manage:
  - application secrets, store secrets and access them via Managed Identities (e.g. a Web App instance)
  - encryption keys, generate/import them; cannot be exported but used to encrypt data/keys or sign hashes; access them via Key Vault access policies (VMs, ARM, Disk Encryption) or Managed Identities
  - certificates, create/import them and let you notify at a given percentage lifetime; connect GlobalSign or DigiCert; stored as secrets and accessed via Managed Identities or access policies (VMs)
6. ARM Templates can reference Key Vault secrets and certificates
7. Azure DevOps Pipelines, Azure Storage, Azure SQL Database, ... are integrated with Azure Key Vault



# Microsoft Azure

---

Productive + Hybrid + Intelligent + Trusted