

# Azure security - ultimate security in the cloud era

Tom Janetscheck

Lead Consultant | Microsoft Azure MVP



devoteam | Alegri

Innovative technology consulting for business

# About me

Tom Janetscheck

Lead Consultant – Business Line Enterprise  
Focused on Azure Security, Governance, Infrastructure

Microsoft Azure MVP & P-CSA

Twitter: [@azureandbeyond](https://twitter.com/azureandbeyond)

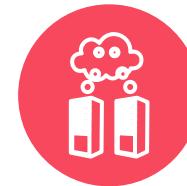
Blog: <https://blog.azureandbeyond.com>



# Cloud momentum continues to accelerate



“The question is no longer:  
‘How do I move to the cloud?’  
Instead, it’s ‘Now that I’m in the  
cloud, how do I make sure I’ve  
**optimized my investment and**  
**risk exposure?’”<sup>1</sup>**

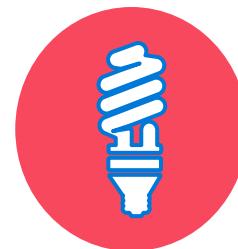
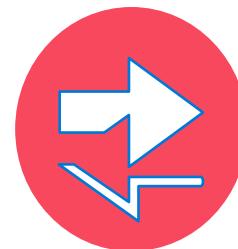
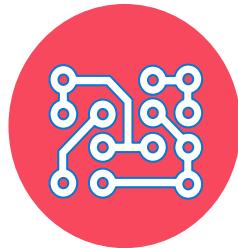


“By 2020 clouds will stop being  
referred to as ‘public’ and  
‘private’. It will simply be **the way**  
**business is done** and IT is  
provisioned.”<sup>2</sup>

<sup>1</sup>KPMG: [2014 Cloud Survey Report, Elevating business in the cloud, December 10, 2014](#)

<sup>2</sup>IDC: [IDC Market Spotlight, Cloud Definitions and Opportunity, April 2015](#)

## But cloud security concerns persist



Management is  
increasingly distributed

Cloud environments  
are more dynamic

Attackers continue to  
innovate

# Cloud Security is a Shared Responsibility

## MICROSOFT COMMITMENT

Securing and managing the cloud foundation



Physical assets



Datacenter operations



Cloud infrastructure

## JOINT RESPONSIBILITY

Securing and managing your cloud resources



Virtual machines



Applications & workloads



Data

# Azure Governance

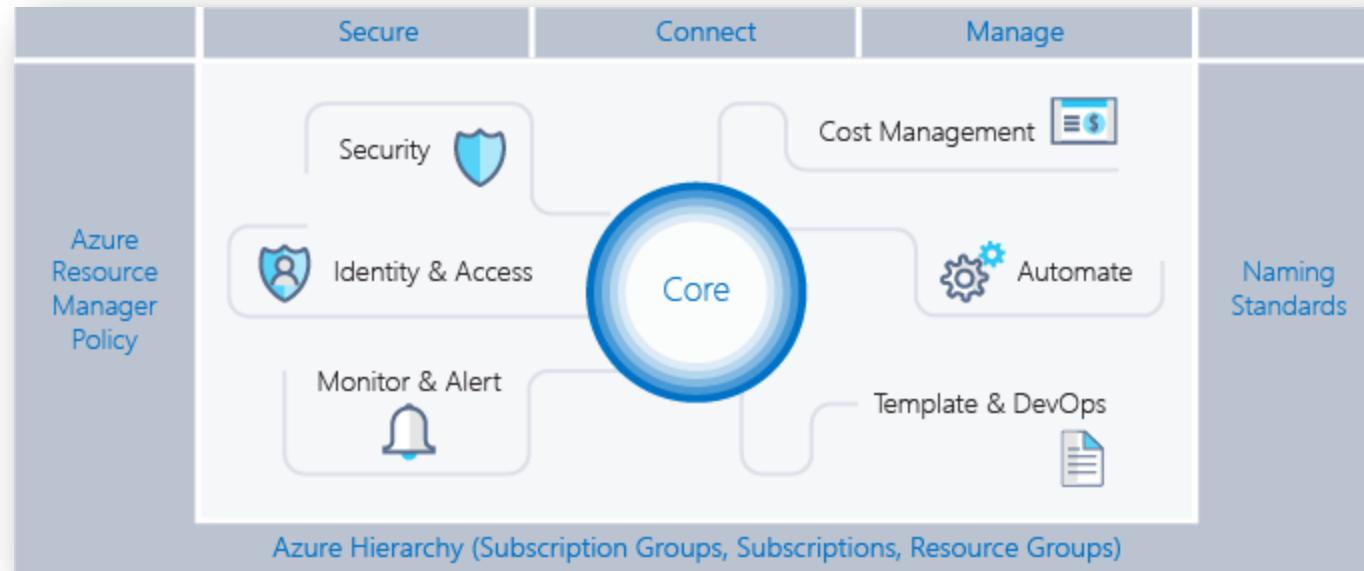


## Governance – a definition

Establishment of **policies**, and continuous **monitoring** of their proper **implementation**, by the members of the governing body of an organization [...]<sup>1</sup>

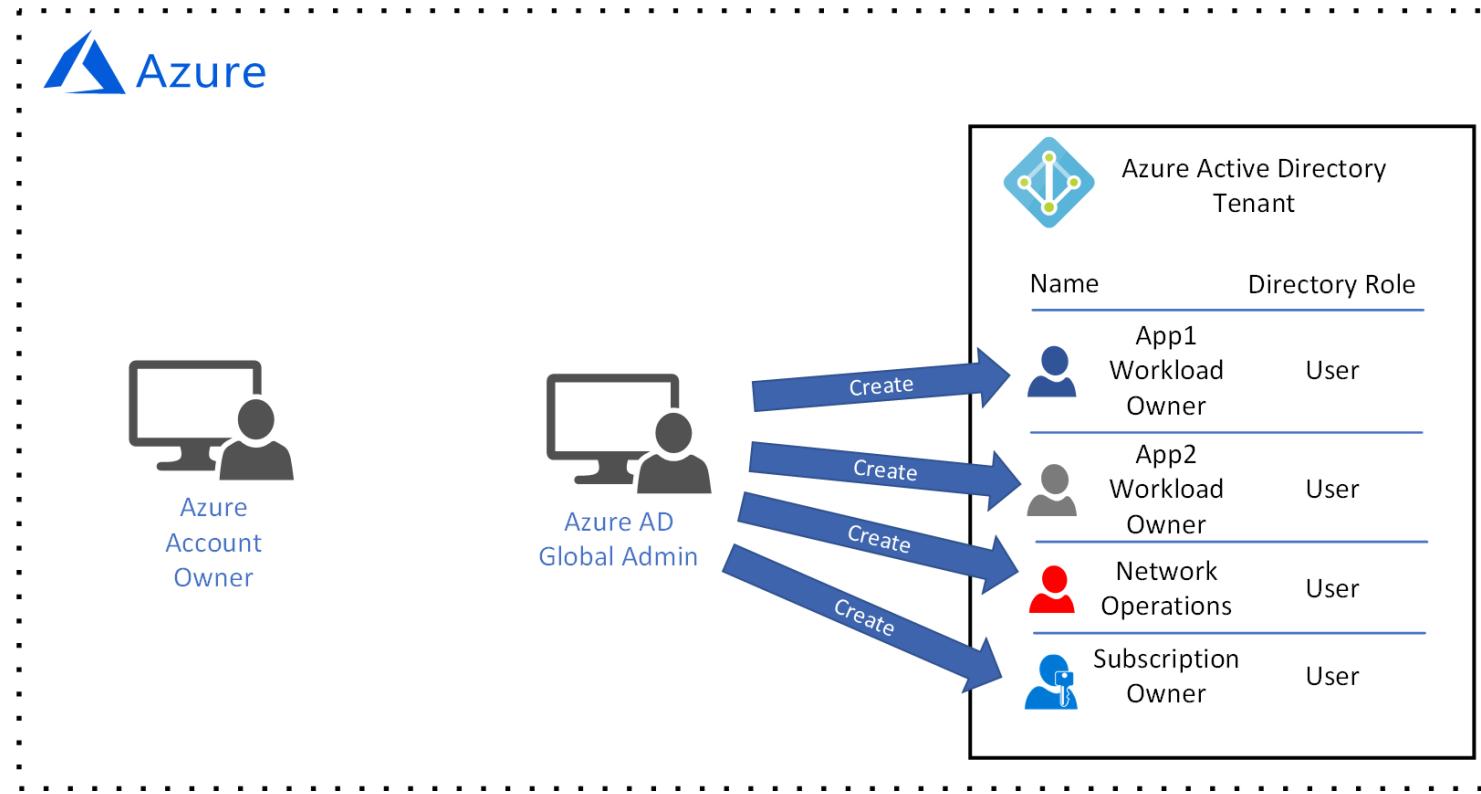
<sup>1</sup>Source: [BusinessDictionary](#)

# Azure Governance Scaffold

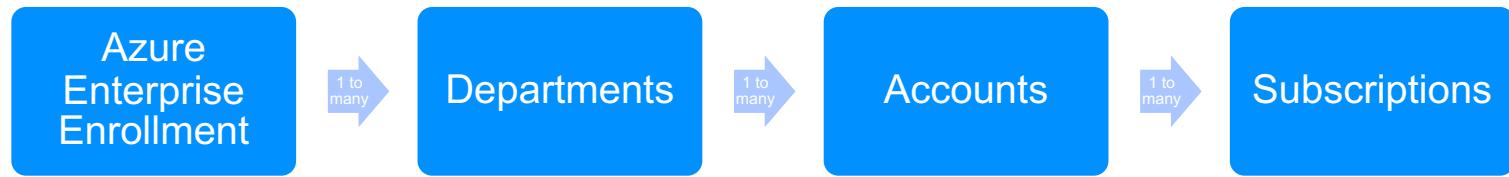


Source: <https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/appendix/azure-scaffold>

# Azure Account Owner vs. Azure AD Global Admin

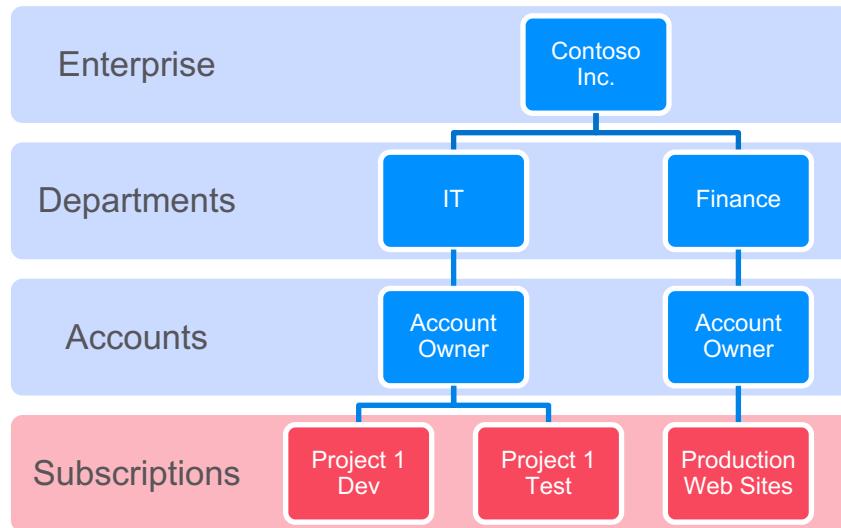


## Define your hierarchy

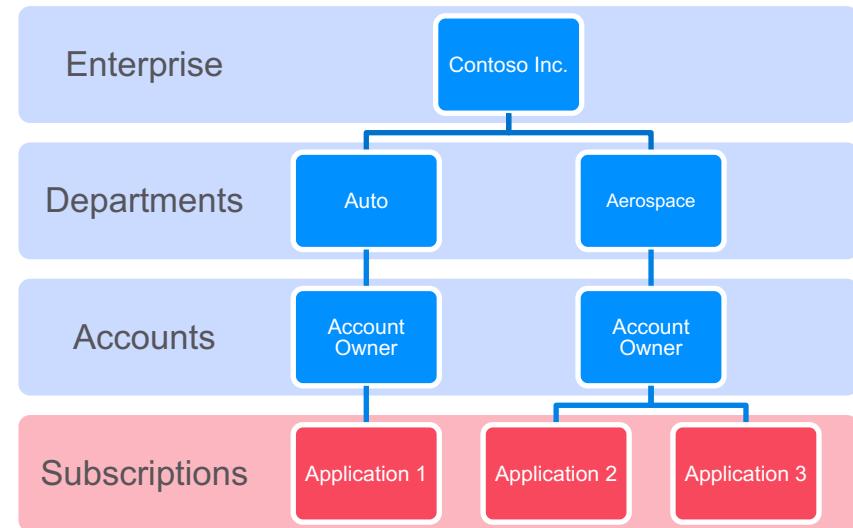


# Plan first, act second!

## Functional Pattern

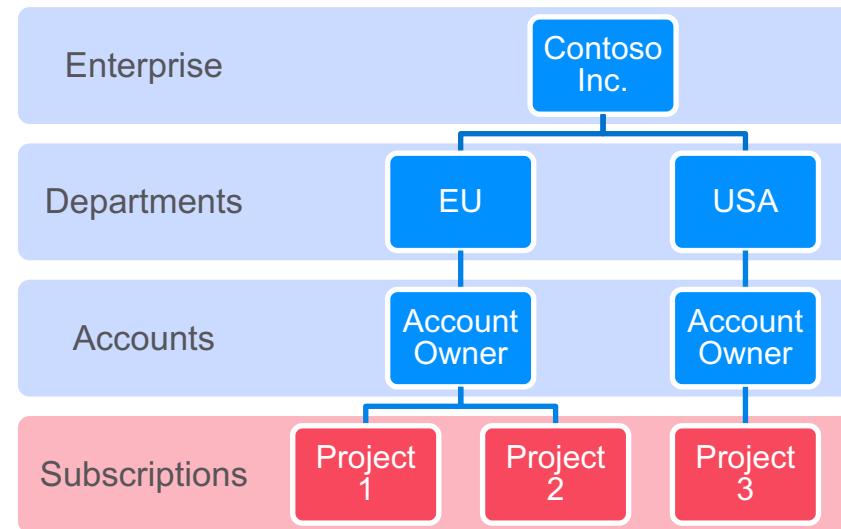


## Business Unit Pattern

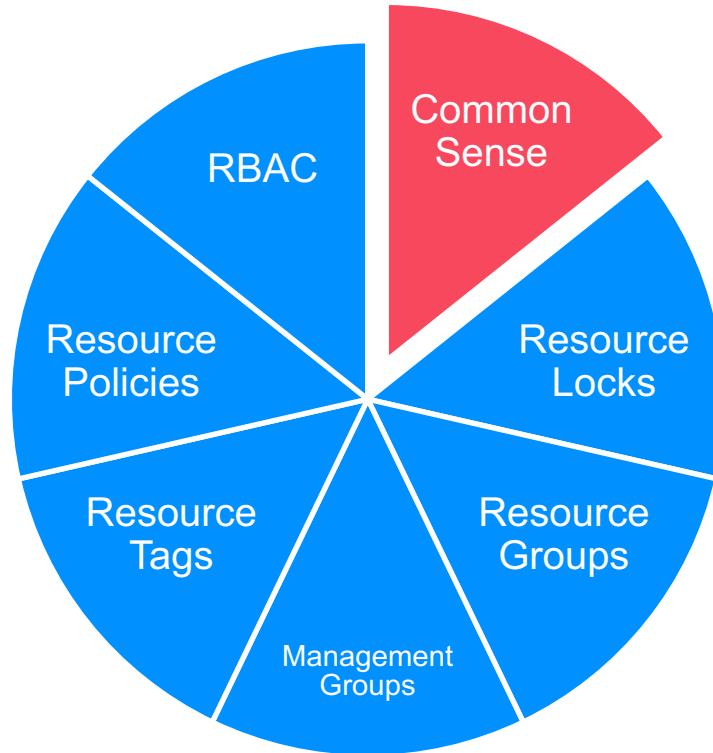


**Plan first, act second!**

## Geographic Pattern



# Azure governance features and capabilities



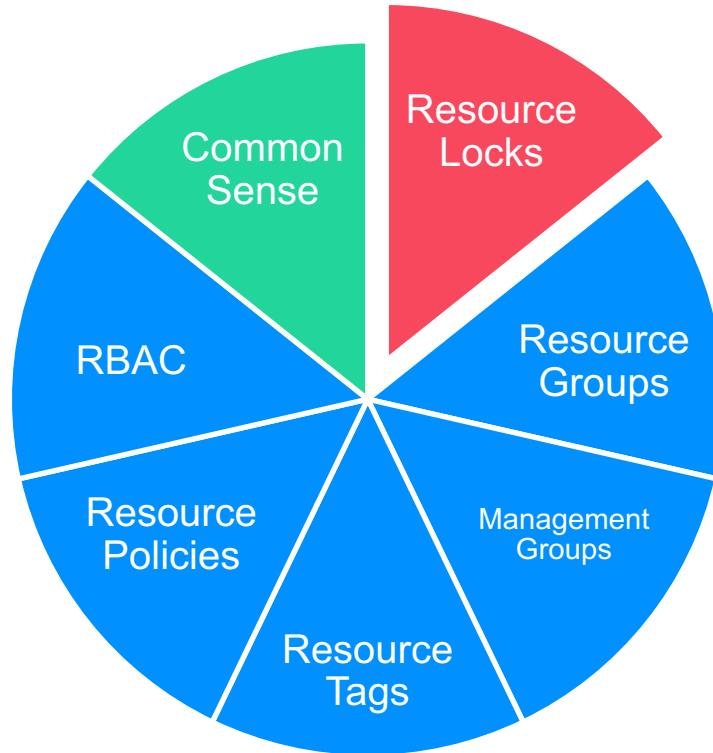
# Common sense...

...is not so common

*Voltaire*



## Resource Locks

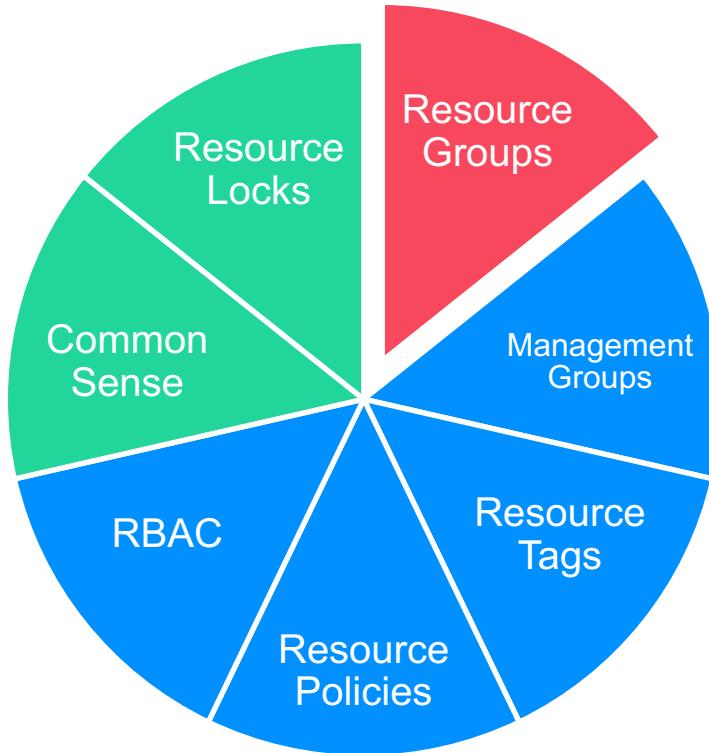


# Resource Locks

- Locks protect resources
  - Delete locks
  - ReadOnly locks
- Define locks in advance
- Use them in combination with common sense (e.g. read only means read only!)

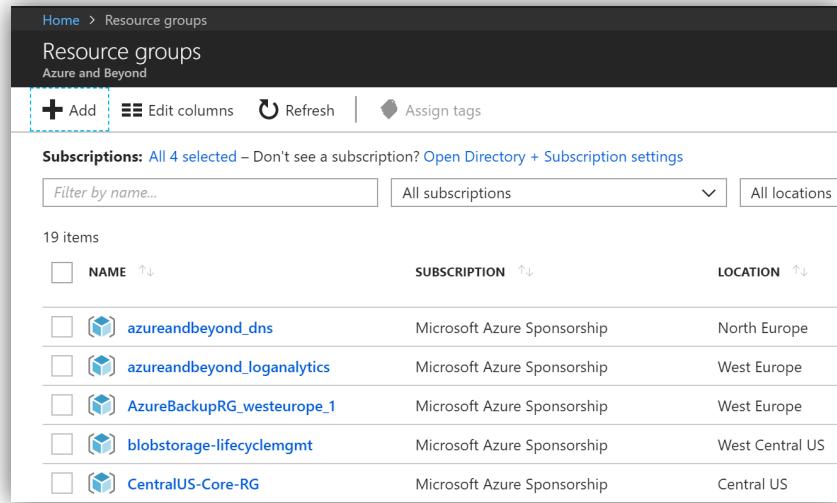
The screenshot shows the Azure portal interface for managing resource locks. The top navigation bar indicates the path: Home > Subscriptions > Microsoft Azure Sponsorship - Resource groups > azureandbeyond\_core > azureandbeyond - Locks. The main area displays a list of configuration items: Configuration, Encryption, Shared access signature, Firewalls and virtual networks, Properties, Locks (which is currently selected and highlighted in blue), and Automation script. On the right, a modal window titled 'Add lock' is open, allowing the creation of a new lock. The 'Lock name' field contains 'StorageAccountLock', and the 'Lock type' dropdown is set to 'Delete'. A note below the fields states 'Prevent deleting azureandbeyond storage account in RG azureandbeyond\_core'. At the bottom of the modal are 'OK' and 'Cancel' buttons.

## Resource Groups



# Resource Groups

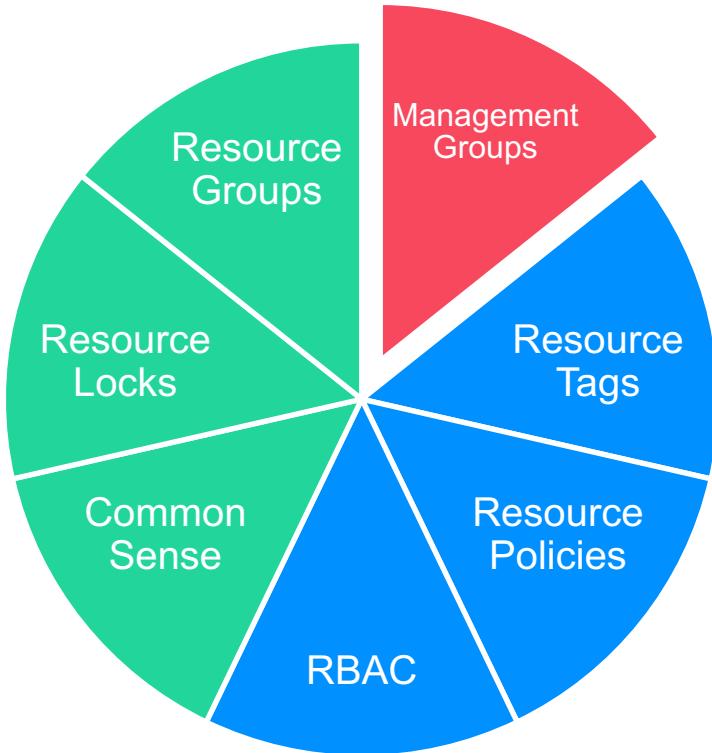
- Management containers for Azure resources
- RGs contain resources with the same deployment lifecycle
- RGs stick to one region but can contain resources that reside in different regions
- Every resource can only exist in one RG
- Resources can be moved between RGs



The screenshot shows the Azure portal's "Resource groups" blade. At the top, there are buttons for "+ Add", "Edit columns", "Refresh", and "Assign tags". Below that, a section titled "Subscriptions" shows "All 4 selected" with a link to "Open Directory + Subscription settings". There are filters for "Filter by name...", "All subscriptions", and "All locations". The main area displays 19 items in a table with columns: NAME, SUBSCRIPTION, and LOCATION. The data is as follows:

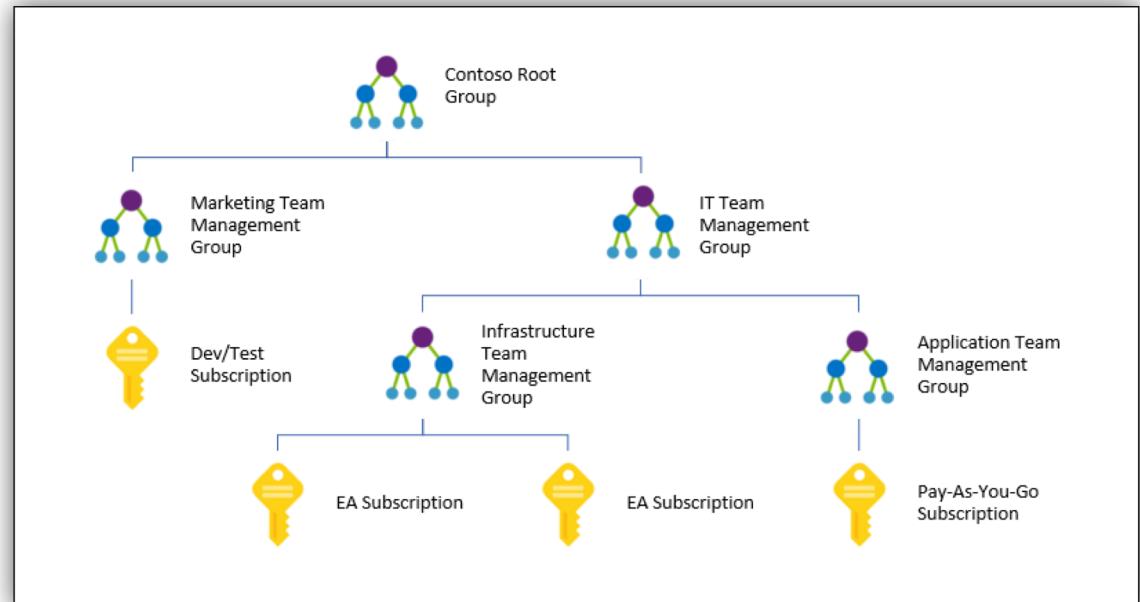
NAME	SUBSCRIPTION	LOCATION
azureandbeyond_dns	Microsoft Azure Sponsorship	North Europe
azureandbeyond_loganalytics	Microsoft Azure Sponsorship	West Europe
AzureBackupRG_westeurope_1	Microsoft Azure Sponsorship	West Europe
blobstorage-lifecyclemgmt	Microsoft Azure Sponsorship	West Central US
CentralUS-Core-RG	Microsoft Azure Sponsorship	Central US

## Management Groups



# Management Groups

- efficiently manage access, policies, and compliance
- level of scope above subscriptions

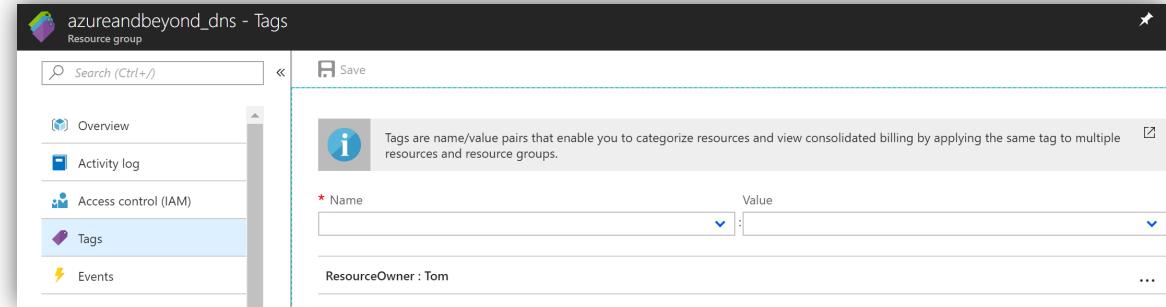


## Resource Tags



# Resource Tags

- Name:Value, e.g. CostCenter:ProdIT, ResourceOwner:Tom
- Help to define responsibility and view consolidated billing
- Always tag RGs
  - Owner
  - Dept
  - CostCenter
  - [...]
- Tag resources as needed
- Define tags in advance



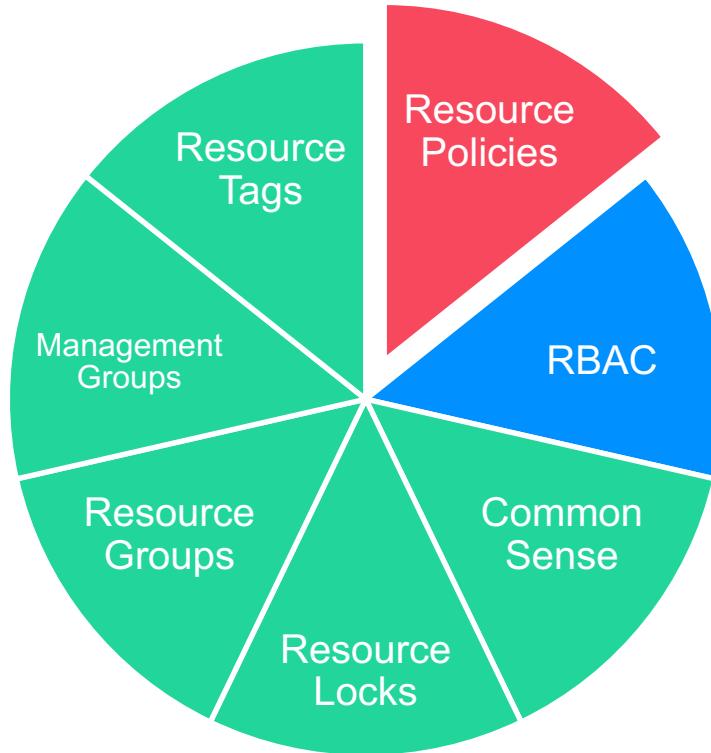
```
PS C:\> Get-AzureRmResource -TagName ResourceOwner -TagValue Tom | ft
```

Name	ResourceGroupName	ResourceType	Location
azureandbeyond.eu	azureandbeyond_dns	Microsoft.Network/dnszones	global
lifecycletest	blobstorage-lifecyclemgmt	Microsoft.Storage/storageAccounts	westcentralus

## Resource Tags

- **Billing;** Grouping resources and associating them with billing or charge back codes.
- **Service Context Identification;** Identify groups of resources across Resource Groups for common operations and grouping
- **Access Control and Security Context;** Administrative role identification based on portfolio, system, service, app, instance, etc.

## Resource Policies



# Resource Policies

- Rule enforcements on MG, subscription or RG level
- Initiative definitions vs. Policy definitions
- Effect types:
  - Append
  - Deny
  - Audit

MicrosoftIgnite2018  
Initiative Definition

Assign Edit initiative

Name MicrosoftIgnite2018  
Description Initiative definition with two policies to demonstrated at Microsoft Ignite 2018  
Category General

Filter by policy name or definition id... All effects

POLICY	EFFECT TYPE
Apply tag and its default value	Append
Allowed locations	Deny
Audit usage of custom RBAC rules	Audit

# Resource Policies

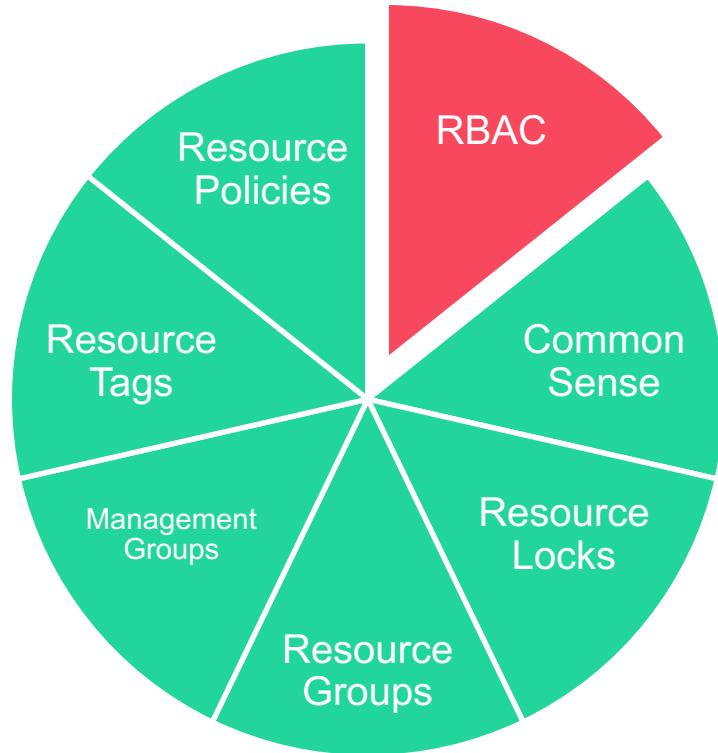
```
1  {
2      "$schema": "http://schema.management.azure.com/schemas/2015-10-01-preview/policyDefinition.json",
3      "if": {
4          "not": {
5              "field": "location",
6              "in" : ["northeurope" , "westeurope"]
7          }
8      },
9      "then": {
10         "effect": "deny"
11     }
12 }
```

# Resource Policies

- Create initiatives on MG level
- Assign initiatives on MG or subscription level
  - Resource ownership
  - Geo-compliance
  - Cost management
- Assign RG initiatives if needed

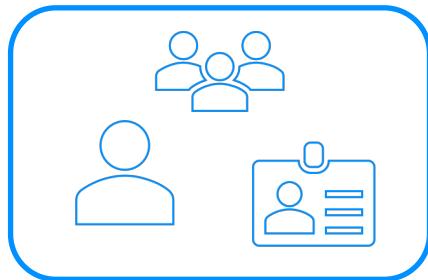
NAME	DEFINITION LOCATION	POLICIES	TYPE	DEFINIT...	CATEGORY
[Preview]: Enable Monitoring in A...		38	Built-in	Initiative	Security Center
Microsoft Ignite 2018	Tenant Root Group	3	Custom	Initiative	General
MicrosoftIgnite2018	Microsoft Azure Sponsorship	3	Custom	Initiative	General
Audit enabling of diagnostic logs i...			Built-in	Policy	Data Lake
Audit VMs that do not use manag...			Built-in	Policy	Compute

## Role-based access control



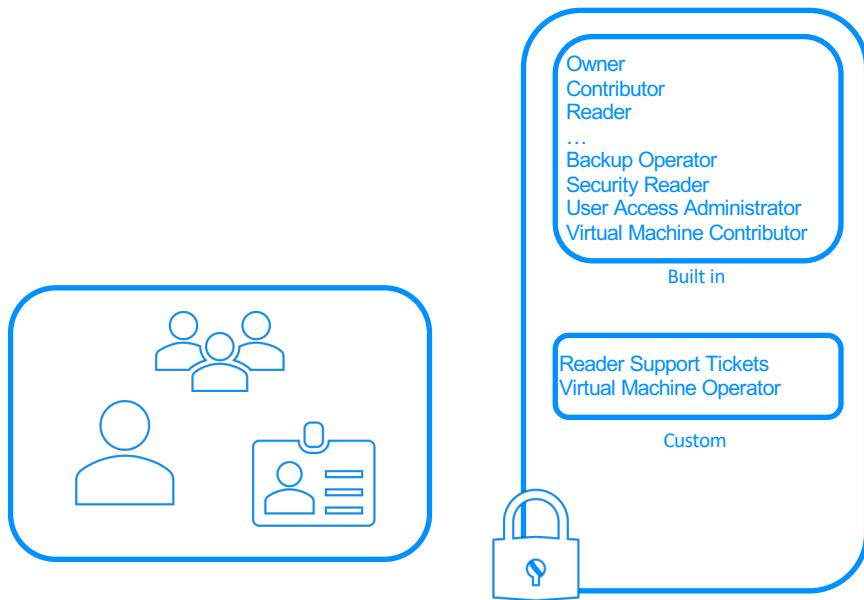
# Role-based access control

1. Security principal = user, group, service principal



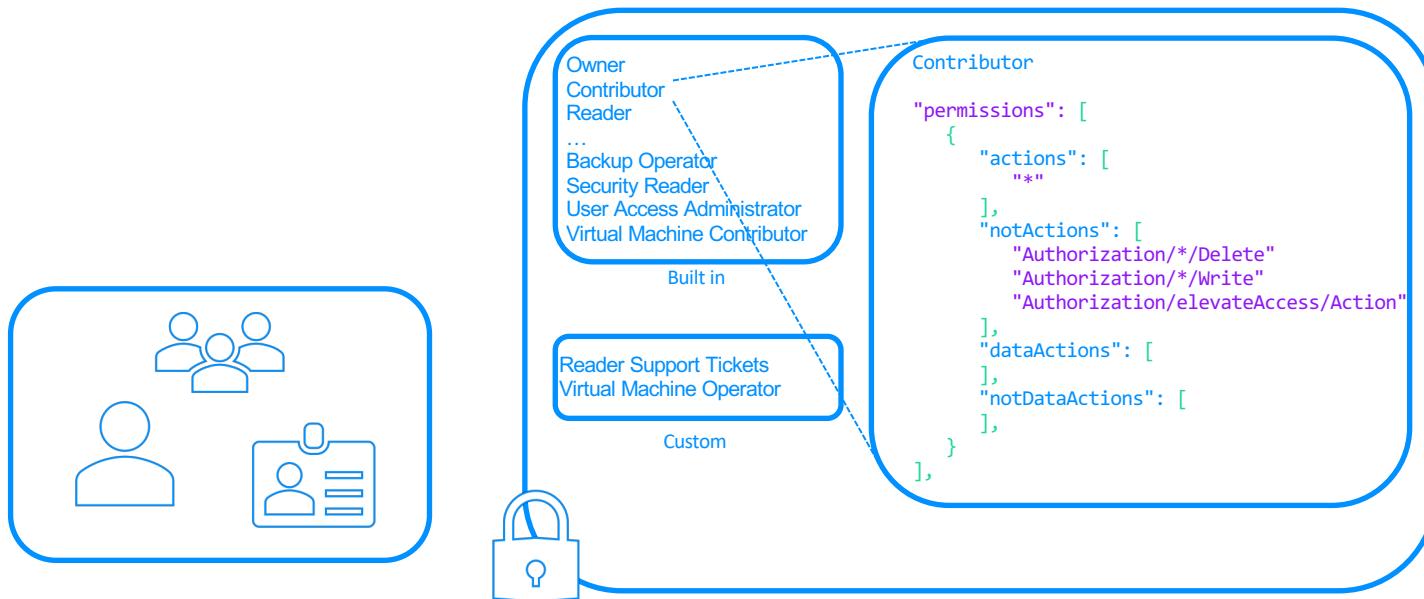
# Role-based access control

1. Security principal = user, group, service principal
2. Role definition = set of management rights



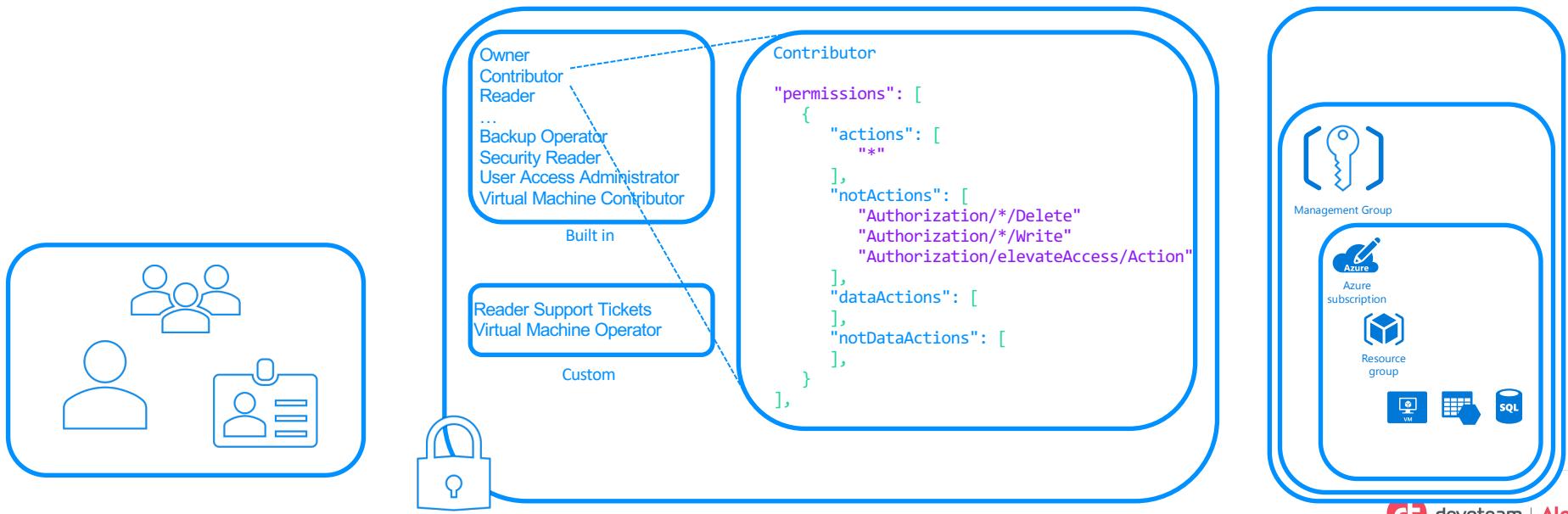
# Role-based access control

1. Security principal = user, group, service principal
2. Role definition = set of management rights

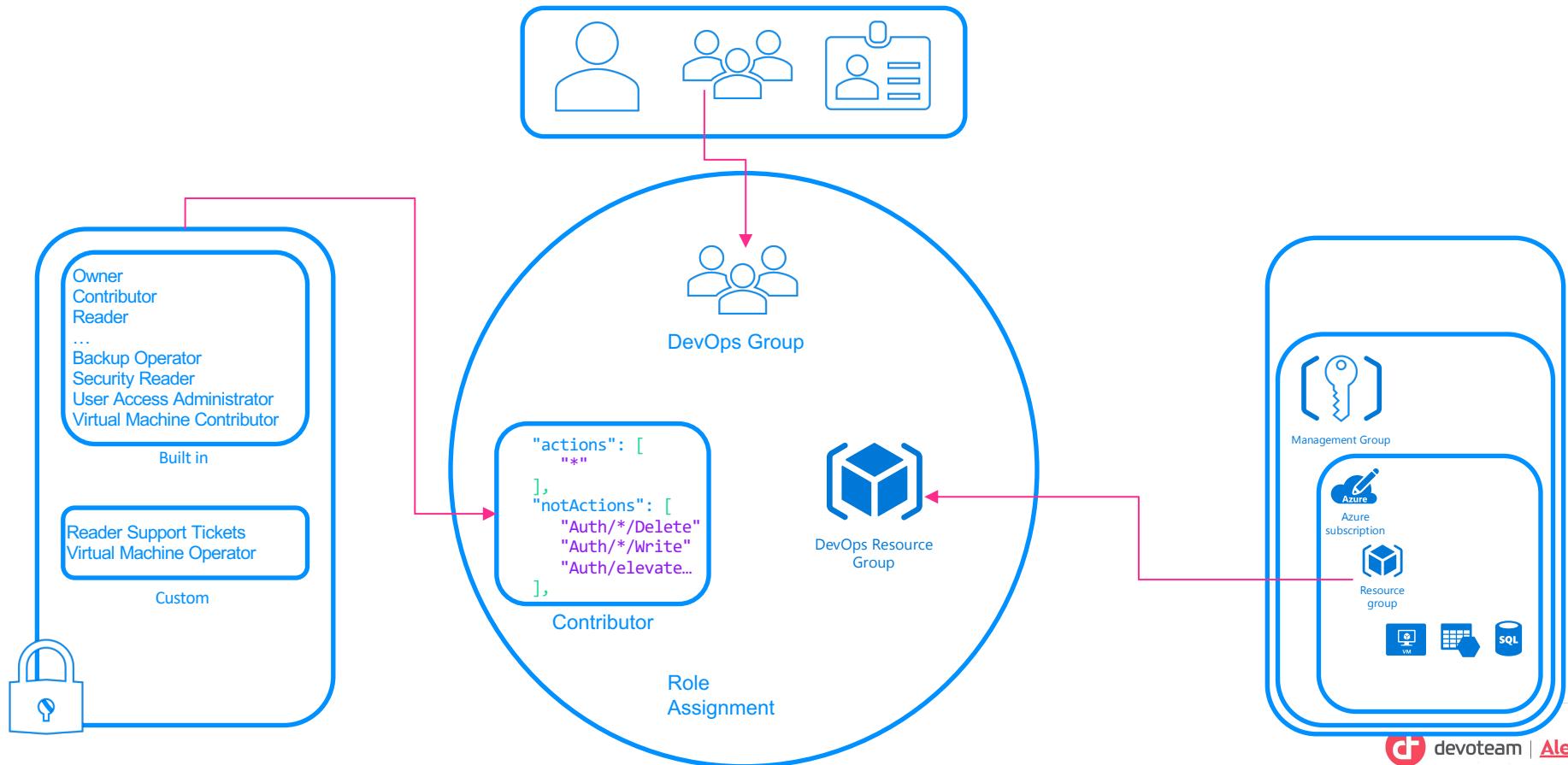


# Role-based access control

1. Security principal = user, group, service principal
2. Role definition = set of management rights
3. Scope = MG, subscription, RG, resource



# Role-based access control – Role assignment



# Announced at MS Ignite 2018: Azure Blueprints & Quickstart Center public previews



devoteam | Alegri

Innovative technology consulting for business

# Azure Blueprints

## Deployment orchestration of

- ARM templates
- Role assignments
- Policy assignments
- Resource groups
- Resource Locks

MSIgnite2018-DemoBlueprint

Blueprints

Edit Blueprint Assign Blueprint Delete Blueprint

Name	State
MSIgnite2018-DemoBlueprint	Published

Management Group  
Tenant Root Group  
Latest published version  
msignite2018V02

Description --

Latest Artifacts Published versions

ARTIFACT NAME	RESOURCE TYPE
Assigned Subscription	Subscription
Ben BJ. Janetscheck (ben@azureandbeyond.com) : Virtual Machine Administrator Login	Role Assignment
Enforce tag and its value	Policy Assignment
MSIgnite2018-core	Resource Group
Apply tag and its default value to resource groups	Policy Assignment

# Azure Portal Quickstart Center

Home > Quickstart Center

 Quickstart Center  
Microsoft Azure ✖️

## How do you want to start?

 **Create an Azure service**  
Tell us what you'd like to do and we'll recommend the best Azure services to meet your needs.

[Select >](#)

 **Set up your Azure environment**  
Learn how to setup your Azure environment effectively for your organization with step-by-step guidance.

[Select >](#)

# Azure Security



devoteam | Alegri

Innovative technology consulting for business

# Automation

```
1 #!/bin/bash
2
3 # Change these variables according to your needs
4 RESOURCE_GROUP_NAME=terraformstate
5 STORAGE_ACCOUNT_NAME=tfstate$RANDOM
6 CONTAINER_NAME=tfstate
7 VAULT_NAME=yourKeyVault$RANDOM
8 SECRET_NAME=yourSecret
9
10 # Create Resource Group, Storage Account and Container for Terraform backend
11
12 # Create resource group
13 az group create --name $RESOURCE_GROUP_NAME --location westeurope
14
15 # Create storage account
16 az storage account create --resource-group $RESOURCE_GROUP_NAME --name $ST
17
18 # Get storage account key
19 ACCOUNT_KEY=$(az storage account keys list --resource-group $RESOURCE_GROU
20

$outputs = (new-azurermresou
    -Name AzSecLab-Core
    -ResourceGroupName $r
    -TemplateUri https://
    -VaultName $vaultName
    -SecretName $secret.N
    -VaultResourceGroup $V
).Outputs
```

## Data sources

With data sources in Terraform we can reference external objects that are needed during deployments. The passage

```
# Azure Key Vault data source to access local admin password
data "azurerm_key_vault_secret" "mySecret" {
    name      = "labuser"
    vault_uri = "https://yourKeyVault.vault.azure.net/"
}

# get my external IP address to enter into NSG rule
data "http" "myExtIp" {
    url = "http://ident.me/"
}

"resources": [
```

creates references to an Azure KeyVault external IP address from the website

```
"resources": [
  {
    "apiVersion": "2017-05-10",
    "name": "linkedTemplate",
    "type": "Microsoft.Resources/deployments",
    "properties": {
      "mode": "Incremental",
      <nested-template-or-external-template>
    }
  }
]
```

<https://github.com/azureandbeyond/AzureSecurity/Terraform>

# Azure Security Services and Capabilities

## Network Security

- Virtual Network Service Endpoints
- DDoS Protection
- Network Security Groups
- NSG Service Tags
- NSG Application Security Groups
- NSG Augmented Rules
- Global Virtual Network Peering
- Azure DNS Private Zones
- Site-to-Site VPN
- Point-to-Site VPN
- ExpressRoute
- Azure Virtual Networks
- Virtual Network Appliances
- Azure Load Balancer
- Azure Load Balancer HA Ports
- Azure Application Gateway
- Azure Firewall
- Azure Web Application Firewall
- Service Endpoints

## Monitoring and Logging

- Azure Log Analytics
- Azure Monitor
- Network Watcher
- VS AppCenter Mobile Analytics

## Compliance Program

- Microsoft Trust Center
- Service Trust Platform
- Compliance Manager
- Azure IP Advantage (legal)

## Identity and Access Management

- Azure Active Directory
- Azure Active Directory B2C
- Azure Active Directory Domain Services
- Azure Active Directory MFA
- Conditional Access
- Azure Active Directory Identity Protection
- Azure Active Directory Privileged Identity Management
- Azure Active Directory App Proxy
- Azure Active Directory Connect
- Azure RBAC
- Azure Active Directory Access Reviews
- Azure Active Directory Managed Service Identity

## Security Docs Site

- Azure Security Information Site on [Azure.com](https://Azure.com)

## DDoS Mitigation

- Azure DDoS Protection
- Azure Traffic Manager
- Autoscaling
- Azure CDN
- Azure Load Balancers
- Fabric level edge protection

## Infrastructure Security

- Comes with Azure Data Centers
- Azure Advanced Threat Protection
- Confidential Computing

## Pen Testing

- Per AUP
- Per TOS
- No contact required

## Data Loss Prevention

- Cloud App Discovery
- Azure Information Protection

## Encryption

- Azure Key Vault
- Azure client-side encryption library
- Azure Storage Service Encryption
- Azure Disk Encryption
- SQL Transparent Data Encryption
- SQL Always Encrypted
- SQL Cell/Column Level Encryption
- Azure CosmosDB encrypt by default
- Azure Data Lake encrypt by default
- VPN protocol encryption (ssl/ipsec)
- SMB 3.0 wire encryption

## Configuration and Management

- Azure Security Center
- Azure Resource Manager
- Azure Resource Graph
- ARM Management Groups
- Azure Policy
- Azure Blueprints
- Azure Automation
- Azure Advisor
- Azure API Gateway

# Azure Security Services and Capabilities

## Network Security

- Virtual Network Service Endpoints
- DDoS Protection
- [Network Security Groups](#)
- NSG Service Tags
- NSG Application Security Groups
- NSG Augmented Rules
- Global Virtual Network Peering
- Azure DNS Private Zones
- Site-to-Site VPN
- Point-to-Site VPN
- ExpressRoute
- Azure Virtual Networks
- Virtual Network Appliances
- Azure Load Balancer
- Azure Load Balancer HA Ports
- Azure Application Gateway
- Azure Firewall
- Azure Web Application Firewall
- Service Endpoints

## Monitoring and Logging

- [Azure Log Analytics](#)
- [Azure Monitor](#)
- Network Watcher
- VS AppCenter Mobile Analytics

## Compliance Program

- Microsoft Trust Center
- Service Trust Platform
- Compliance Manager
- Azure IP Advantage (legal)

## Identity and Access Management

- Azure Active Directory
- Azure Active Directory B2C
- Azure Active Directory Domain Services
- [Azure Active Directory MFA](#)
- Conditional Access
- Azure Active Directory Identity Protection
- [Azure Active Directory Privileged Identity Management](#)
- Azure Active Directory App Proxy
- Azure Active Directory Connect
- [Azure RBAC](#)
- Azure Active Directory Access Reviews
- Azure Active Directory Managed Service Identity

## Security Docs Site

- Azure Security Information Site on Azure.com

## DDoS Mitigation

- Azure DDoS Protection
- Azure Traffic Manager
- Autoscaling
- Azure CDN
- Azure Load Balancers
- Fabric level edge protection

## Infrastructure Security

- Comes with Azure Data Centers
- Azure Advanced Threat Protection
- Confidential Computing

## Pen Testing

- Per AUP
- Per TOS
- No contact required

## Data Loss Prevention

- Cloud App Discovery
- Azure Information Protection

## Encryption

- [Azure Key Vault](#)
- Azure client-side encryption library
- Azure Storage Service Encryption
- Azure Disk Encryption
- SQL Transparent Data Encryption
- SQL Always Encrypted
- SQL Cell/Column Level Encryption
- Azure CosmosDB encrypt by default
- Azure Data Lake encrypt by default
- VPN protocol encryption (ssl/ipsec)
- SMB 3.0 wire encryption

## Configuration and Management

- [Azure Security Center](#)
- Azure Resource Manager
- [Azure Resource Graph](#)
- ARM Management Groups
- Azure Policy
- Azure Blueprints
- Azure Automation
- Azure Advisor
- Azure API Gateway

# Microsoft Azure Security Center

Unify security management and enable advanced threat protection for hybrid cloud workloads



## Unified visibility and control

Dynamically discover and manage the security of your hybrid cloud workloads in a single cloud-based console



## Adaptive threat prevention

Enable actionable, adaptive protections that identify and mitigate risk to reduce exposure to attacks



## Intelligent detection and response

Use advanced analytics and Microsoft Intelligent Security Graph to rapidly detect and respond to evolving cyber threats

# Azure Security Center Pipeline

Data sources:



Computers



Azure Services



Security Data  
& Alerts



REST APIs

## DETECT



Built-in Analytics &  
Machine Learning



Custom Alert Rules



Enrichment



Threat Intelligence



Prioritization



Fusion

## RESPOND



Search



Alert Exploration

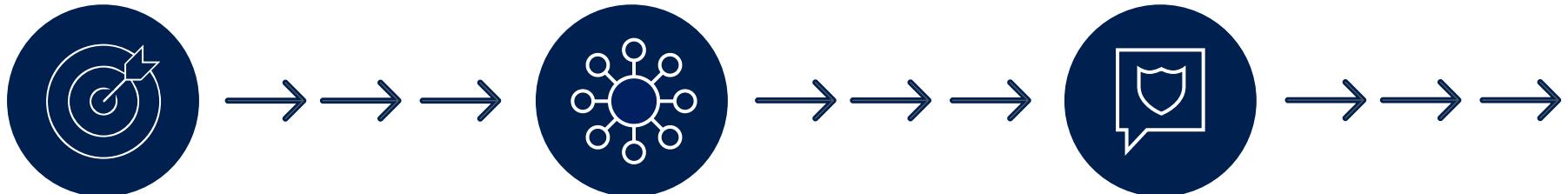


Investigation



Automation &  
Orchestration

## Detect threats across the kill chain



### TARGET AND ATTACK

Inbound brute force RDP, SSH, SQL attacks and more

Application and DDoS attacks (WAF partners)

Intrusion detection (NG Firewall partners)

### INSTALL AND EXPLOIT

In-memory malware and exploit attempts

Suspicious process execution

Lateral movement

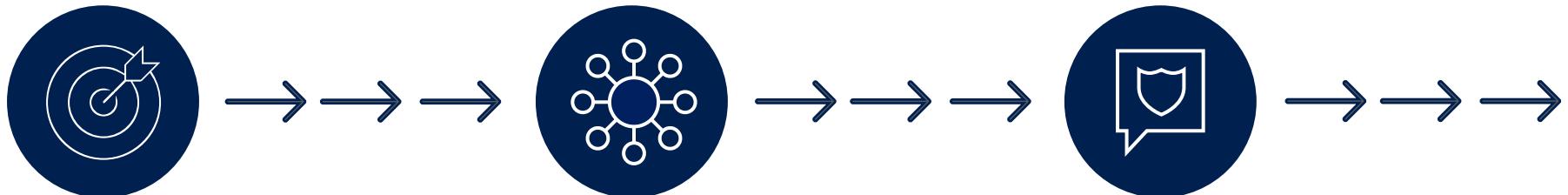
Internal reconnaissance

### POST BREACH

Communication to a known malicious IP (data exfiltration or command and control)

Using compromised resources to mount additional attacks (outbound port scanning, brute force RDP/SSH attacks, DDoS, and spam)

# Detect threats across the kill chain



## TARGET AND ATTACK

Inbound brute force RDP, SSH, SQL attacks and more

Application and DDoS attacks (WAF partners)

Intrusion detection (NG Firewall partners)

## INSTALL AND EXPLOIT

In-memory malware and exploit attempts

Suspicious process execution

Lateral movement

Internal reconnaissance

## POST BREACH

Communication to a known malicious IP (data exfiltration or command and control)

Using compromised resources to mount additional attacks (outbound port scanning, brute force RDP/SSH attacks, DDoS, and spam)

# Demo



devoteam | Alegri

Innovative technology consulting for business

# Thank you!

@azureandbeyond

<https://blog.azureandbeyond.com>



devoteam | Alegri

Innovative technology consulting for business