Security Control Trends Across Public Cloud Providers

TELASA | SECURITY

Survey

- How many organizations use the following Cloud Providers?
  - Azure
  - Google Cloud
  - Amazon Web Services

- How many organizations use two Providers?

- How many organizations use all three Providers?

About Me

Brian Greidanus

bgreidan@telasasecurity.com

- 25 years of security and compliance experience delivering consulting and managed services to enterprises, governments, and education.

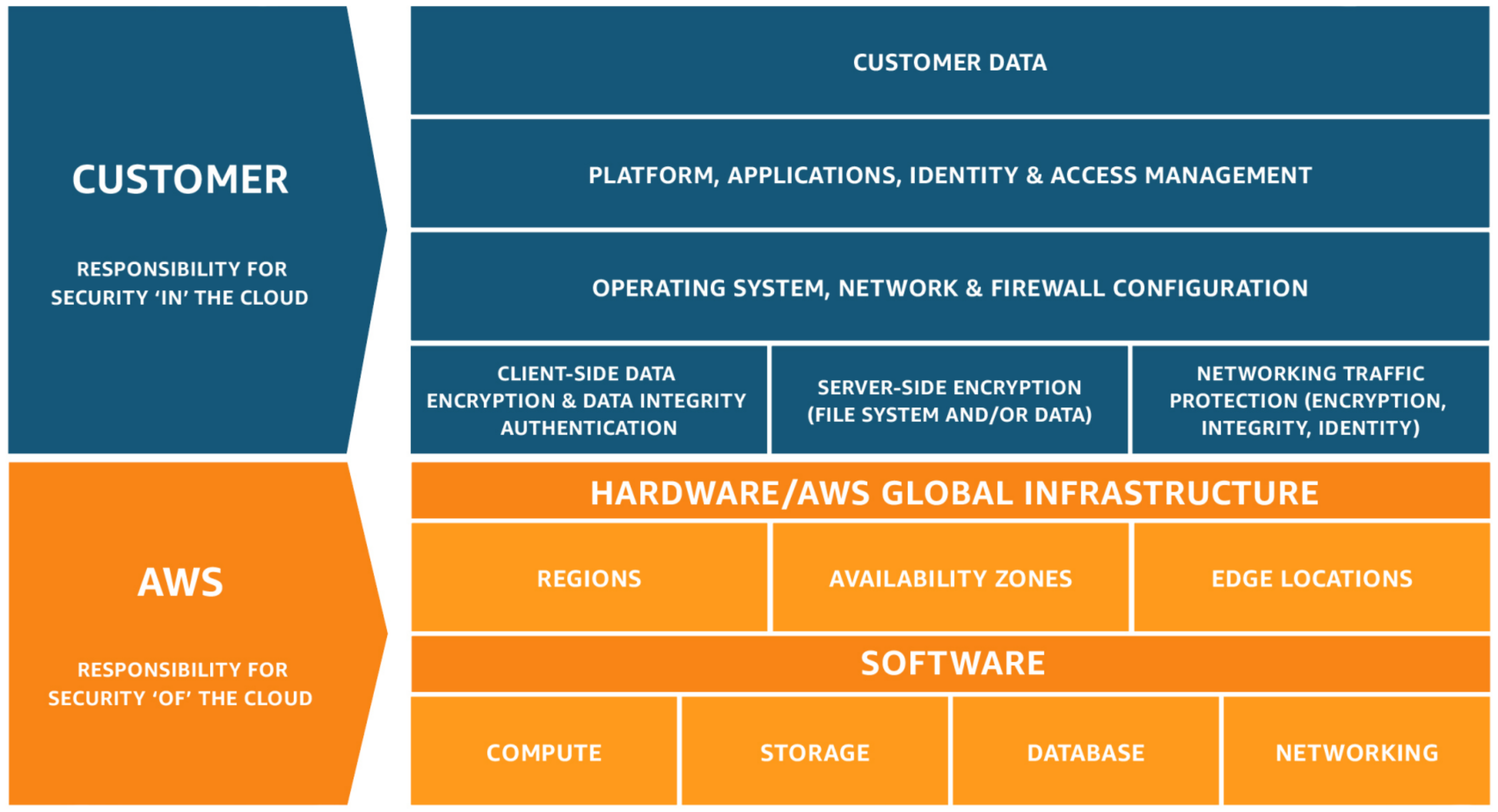
- Current focus:
  - Strategic and technical consulting
  - Cloud security architecture and assessment

Scope of this Presentation

- If you attended presentation earlier this week focus was on key security controls in Microsoft 365, which is Microsoft's SaaS platform

- Focus of this presentation is on security control trends at three major IaaS/SaaS cloud providers
  - Amazon Web Services
  - Microsoft Azure
  - Google Cloud Platform

AWS IaaS Shared Responsibility Model



CUSTOMER

RESPONSIBILITY FOR
SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR
SECURITY 'OF' THE CLOUD

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

SOFTWARE

COMPUTE

STORAGE

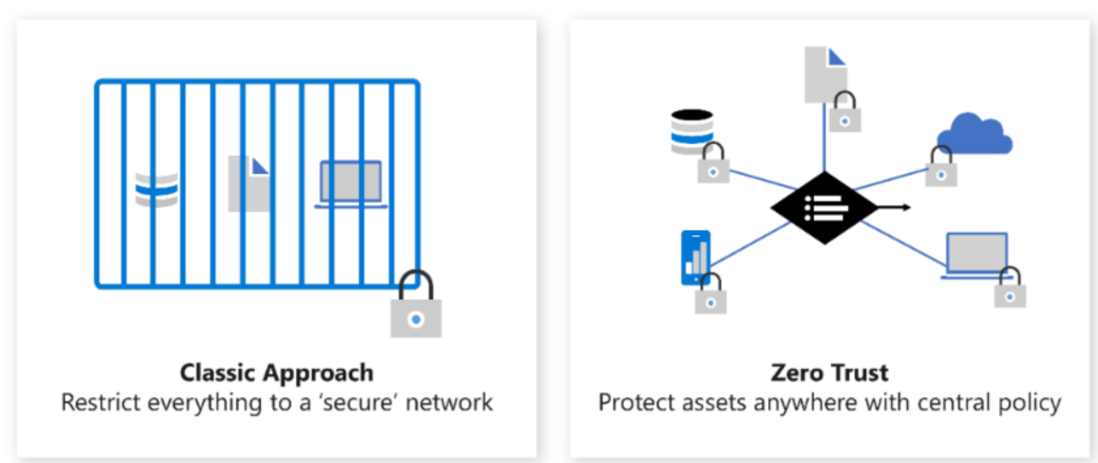
DATABASE

NETWORKING

AWS Link

Popular Topics not Directly Discussed in this Presentation

- Some popular topics that are not direct focus of this presentation
  - “Zero Trust” Architecture - Implicit in almost all topics that we will discuss
    - “Assume Breach” – assume even internal communication may be malicious
    - Want to have controls at every interaction and boundary



Classic Approach
Restrict everything to a ‘secure’ network

Zero Trust
Protect assets anywhere with central policy

Popular Topics not Directly Discussed in this Presentation

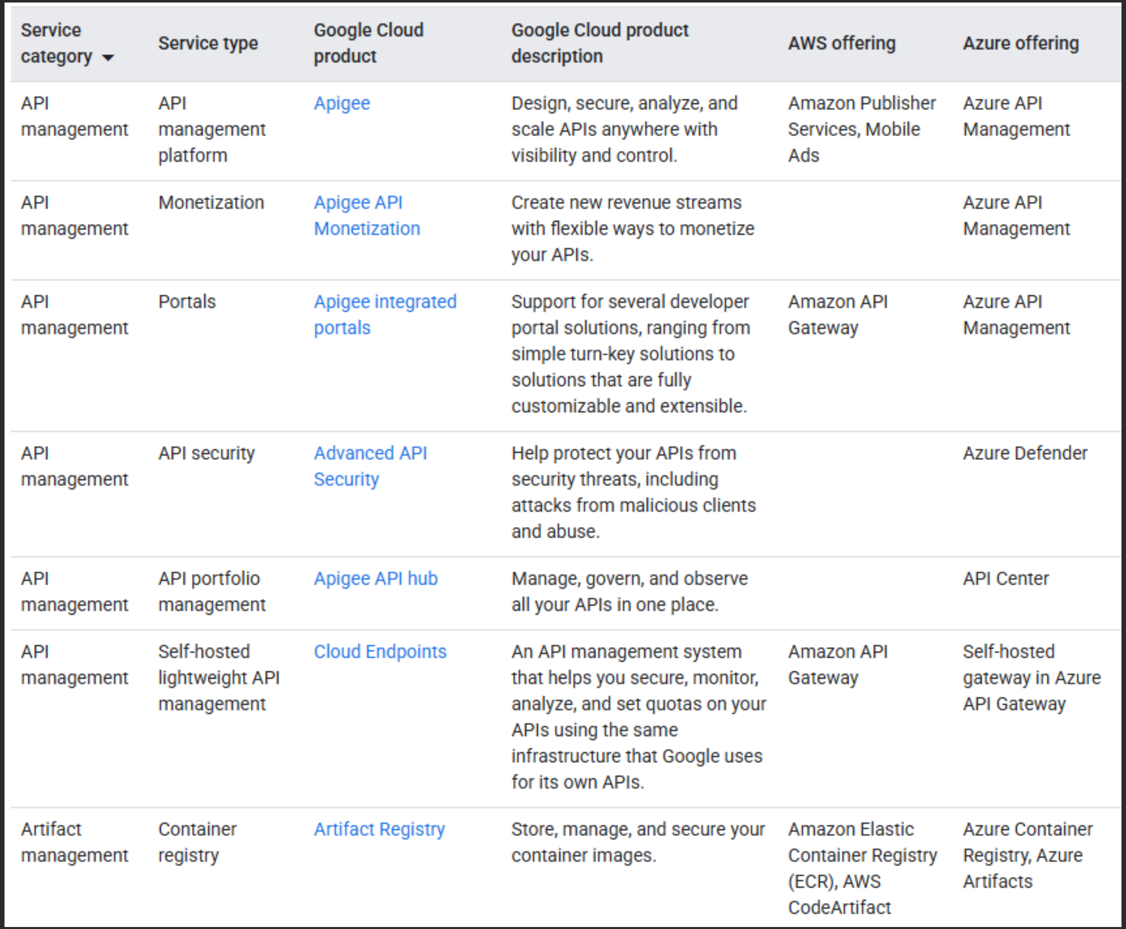
- Two popular topics that are not direct focus of this presentation
  - Artificial Intelligence – will continue to see AI ingrained in all aspects of security and audit
    - Not a direct security control, so not a focus of this presentation

General Cloud Security Control Trends

- Introduction
- Private Connectivity and Limiting External Exposure
- Security Monitoring Infrastructure
- Privileged Identity Management
- Security Guardrails
- Infrastructure As Code

Comparing Offerings Across Cloud Providers

- https://cloud.google.com/docs/get-started/aws-azure-gcp-service-comparison

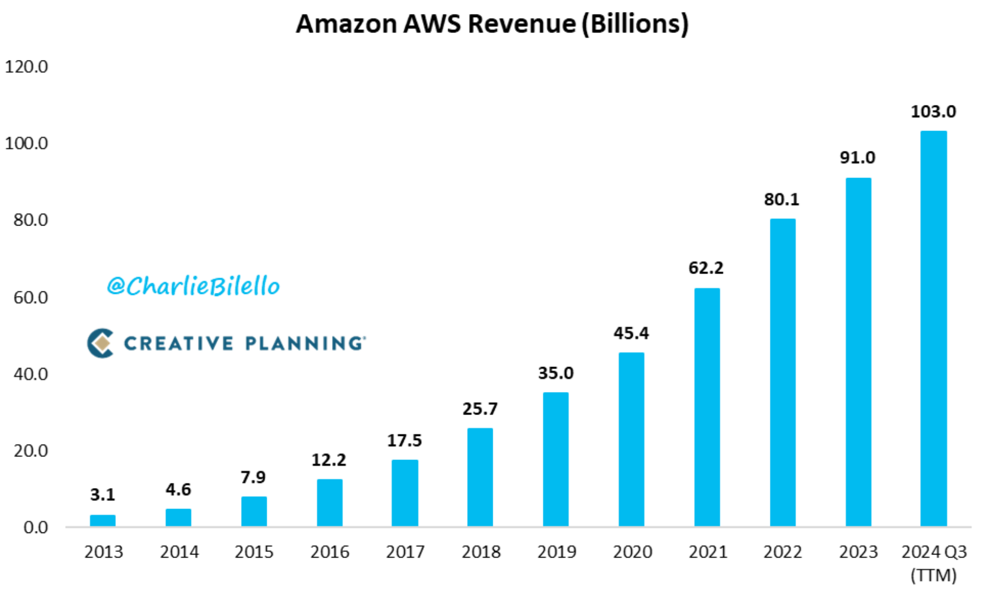


Service category ▾	Service type	Google Cloud product	Google Cloud product description	AWS offering	Azure offering
API management	API management platform	Apigee	Design, secure, analyze, and scale APIs anywhere with visibility and control.	Amazon Publisher Services, Mobile Ads	Azure API Management
API management	Monetization	Apigee API Monetization	Create new revenue streams with flexible ways to monetize your APIs.		Azure API Management
API management	Portals	Apigee integrated portals	Support for several developer portal solutions, ranging from simple turn-key solutions to solutions that are fully customizable and extensible.	Amazon API Gateway	Azure API Management
API management	API security	Advanced API Security	Help protect your APIs from security threats, including attacks from malicious clients and abuse.		Azure Defender
API management	API portfolio management	Apigee API hub	Manage, govern, and observe all your APIs in one place.		API Center
API management	Self-hosted lightweight API management	Cloud Endpoints	An API management system that helps you secure, monitor, analyze, and set quotas on your APIs using the same infrastructure that Google uses for its own APIs.	Amazon API Gateway	Self-hosted gateway in Azure API Gateway
Artifact management	Container registry	Artifact Registry	Store, manage, and secure your container images.	Amazon Elastic Container Registry (ECR), AWS CodeArtifact	Azure Container Registry, Azure Artifacts

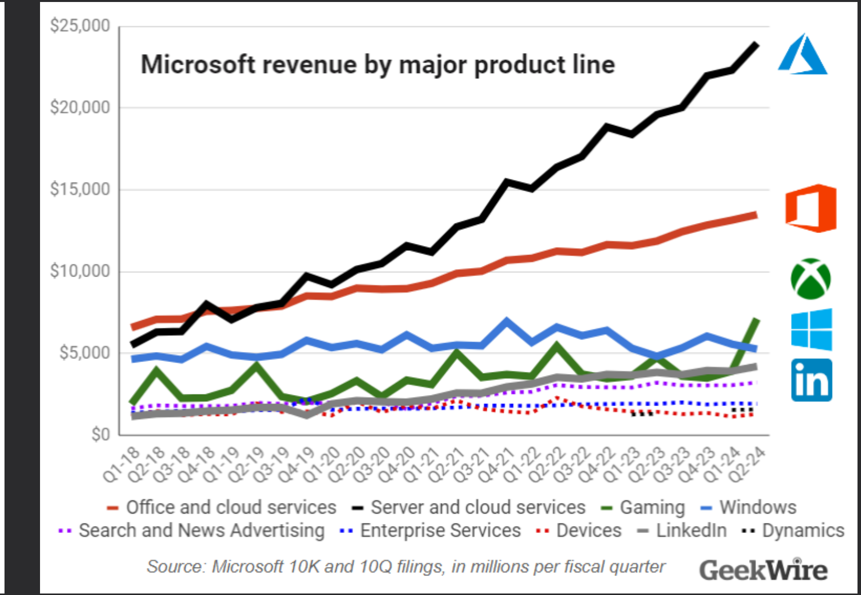
Introduction

Introduction

- Continued massive growth in major cloud providers



Amazon AWS Revenue (Billions)



Microsoft revenue by major product line

Source: Microsoft 10K and 10Q filings, in millions per fiscal quarter

Introduction

- What is driving security control trends?
    - Maturation – need to have equivalent functionality in cloud as on prem
    - Treating cloud environments as extensions of physical networks
    - How do we protect ourselves if a cloud provider is compromised?

Private Connectivity and Limiting External Exposure

Private Connectivity and Limiting External Exposure

- Private Connectivity to Cloud Endpoints
- Private Connectivity Between On-Premise and Cloud Environments
- Private Connectivity Between Cloud Resources

Private Connectivity to Cloud Endpoints

Security Problem Statement

- Administrators and users require ability to access cloud-based virtual machines.

- Historically, this access has required organizations to expose remote access services (most commonly SSH and Remote Desktop/Terminal Services) to the Internet.

- This makes the devices vulnerable to brute force attacks

- Additionally, since these devices can be created and spun up by developers, they may not have passwords that comply with organizational standards

- Cloud Service Providers have developed services to enable Virtual Machines over the Internet without assigning public IP addresses to the Virtual Machines. Azure Bastion provides Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to Virtual Machines using TLS within a web browser.

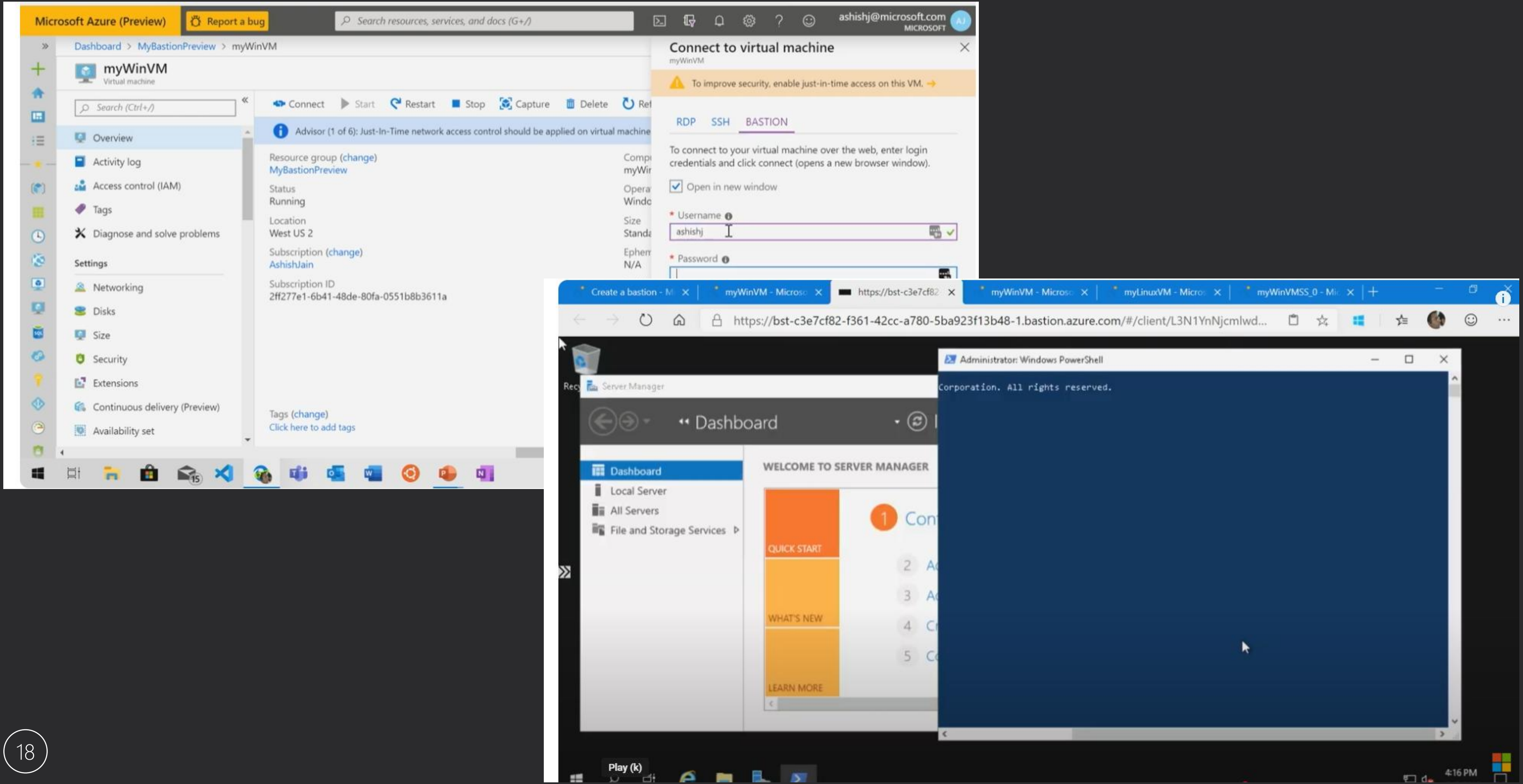
CSP Solutions

- Cloud providers have services that permit remote access to cloud devices without exposure of services to the Internet
  - Protects devices from brute force / password spray attacks
  - Ensures that service provider level authentication is required prior to accessing devices

- From an auditing perspective, organizations should ensure that these services are used wherever possible.

- Solutions provide in-browser access to SSH / RDP services on virtual instances in cloud environments.

Screen Shots of Azure Bastion



Microsoft Azure (Preview) | Report a bug | Search resources, services, and docs (G+/) | ashishj@microsoft.com MICROSOFT

Dashboard > MyBastionPreview > myWinVM

myWinVM
Virtual machine

Connect | Start | Restart | Stop | Capture | Delete | Ref

Advisor (1 of 6): Just-In-Time network access control should be applied on virtual machine

Resource group (change)
MyBastionPreview

Status
Running

Location
West US 2

Subscription (change)
AshishJain

Subscription ID
2ff277e1-6b41-48de-80fa-0551b8b3611a

Tags (change)
Click here to add tags

Connect to virtual machine
myWinVM

To improve security, enable just-in-time access on this VM. →

RDP | SSH | BASTION

To connect to your virtual machine over the web, enter login credentials and click connect (opens a new browser window).

☑ Open in new window

* Username: ashishj

* Password:

https://bst-c3e7cf82-f361-42cc-a780-5ba923f13b48-1.bastion.azure.com/#/client/L3N1YnNjcmlwd...

Administrator: Windows PowerShell

```
Corporation. All rights reserved.
```

Service References

Cloud Provider	Service Name	URL to Service Documentation
Amazon Web Services	AWS Systems Manager Session Manager	AWS Systems Manager Session Manager
Microsoft Azure	Azure Bastion	Azure Bastion
Google Cloud Platform	SSH-in-browser Identity-Aware Proxy	SSH-in-browser Identity Aware Proxy

Private Connectivity
Between On-Premise and Cloud Environments

Security Problem Statement

- Organizations need to connect from on-premises network to Cloud Service Providers

- Connections have historically occurred via
  - API access
  - Exposing services to the Internet
  - VPN (All major cloud providers provide VPN services)

Security Problem Statement

- As organizations move more services and infrastructure to cloud environments, cloud environments need to be treated as extension of corporate environment.
    - High performance
    - Dedicated, private connectivity

- Major cloud service providers all have services that address this issue.

- Data travels over a private connection rather than the public internet, reducing exposure to potential security threats, ensuring a private and secure pathway for your data to the cloud.

CSP Solutions

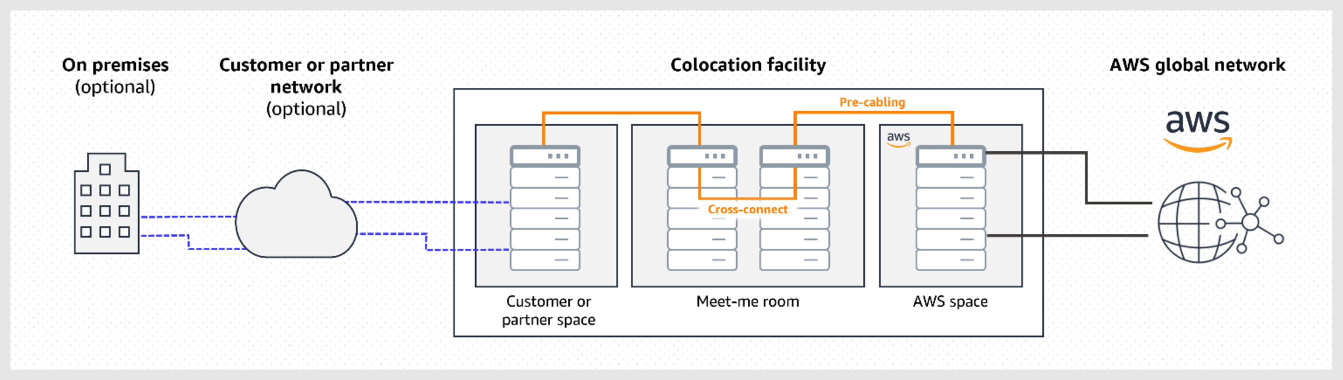
- Cloud Service Providers have developed a mix of private connectivity solutions:

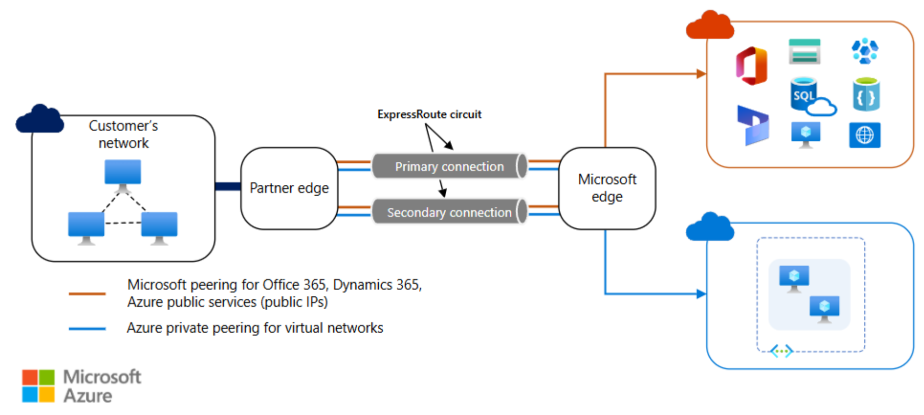
- Google
  - Dedicated Interconnect – Direct connection to Google via colocation facilities
  - Partner Interconnect – Private, high-speed connection to Google via Service Provider

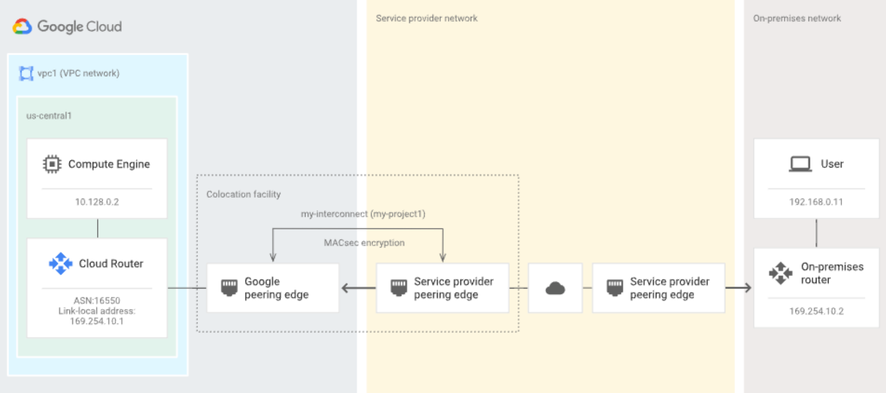
- AWS DirectConnect
  - Dedicated Connect (up to 400 GBPS)
  - Hosted Connect

- Azure ExpressRoute

Similar Offerings Across Providers




Customer's
network
ExpressRoute circuit
Partner edge
Primary connection
Secondary connection
Microsoft
edge
SQL
Microsoft peering for Office 365, Dynamics 365,
Azure public services (public IPs)
Azure private peering for virtual networks
Microsoft
Azure



Service References

Cloud Provider	Service Name	URL to Service Documentation
Amazon Web Services	AWS Direct Connect	AWS DirectConnect
Microsoft Azure	Azure ExpressRoute	Azure ExpressRoute
Google Cloud Platform	Cloud Interconnect	Google Cloud Interconnect

Private Connectivity Between Cloud Resources

Security Problem Statement

- Standard mechanisms for interconnection between cloud services have been complex.

- Let’s say we wanted to add a database to an Azure environment to begin storing customer data. We would need to:

    1. Enable service endpoint on subnet(s)
    2. Configure multiple SQL firewall rules
    3. Update NSG rules for outbound traffic
    4. Manage DNS resolution and potential region issues
    5. Repeat for each VNet requiring access

Security Problem Statement

- In many instances, connections between services requires access to public APIs, use of public IP addresses

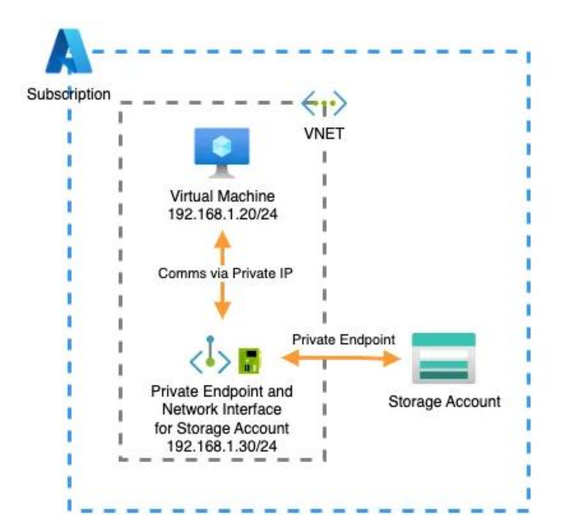
- Management of resources can become complex

- Service complexity can lead to security misconfigurations, inadvertent resource exposures

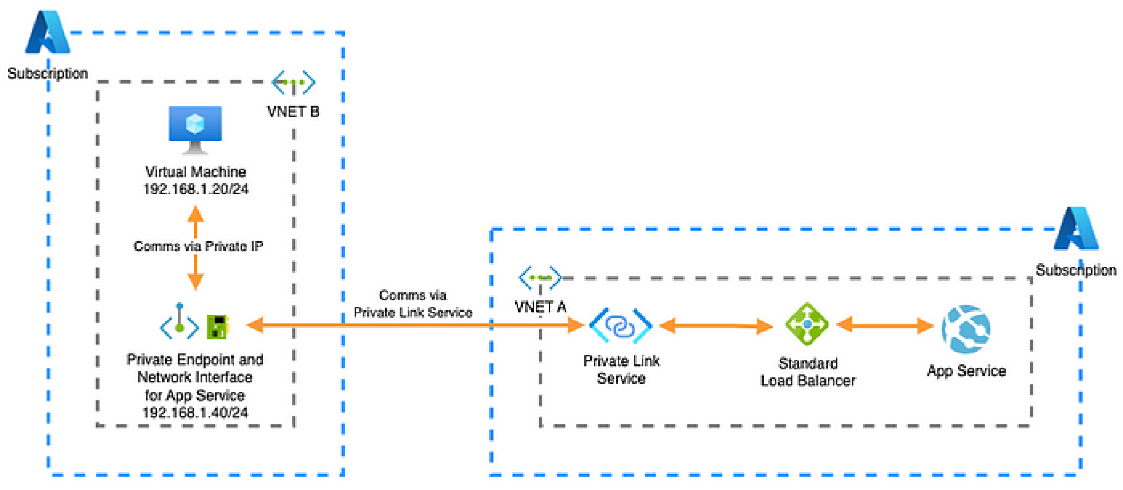
Azure Solution – Private Links / Private Endpoints

1. Create private endpoint for SQL Database
    - Automatically registers DNS entries
    - Creates network interface in VNet with private IP
    - Networking managed by Microsoft

- The most significant simplification is eliminating the need to manage service endpoints, firewall rules, and complex networking configurations while gaining true private connectivity. Your SQL server now appears as if it's directly deployed in your VNet with a private IP address.



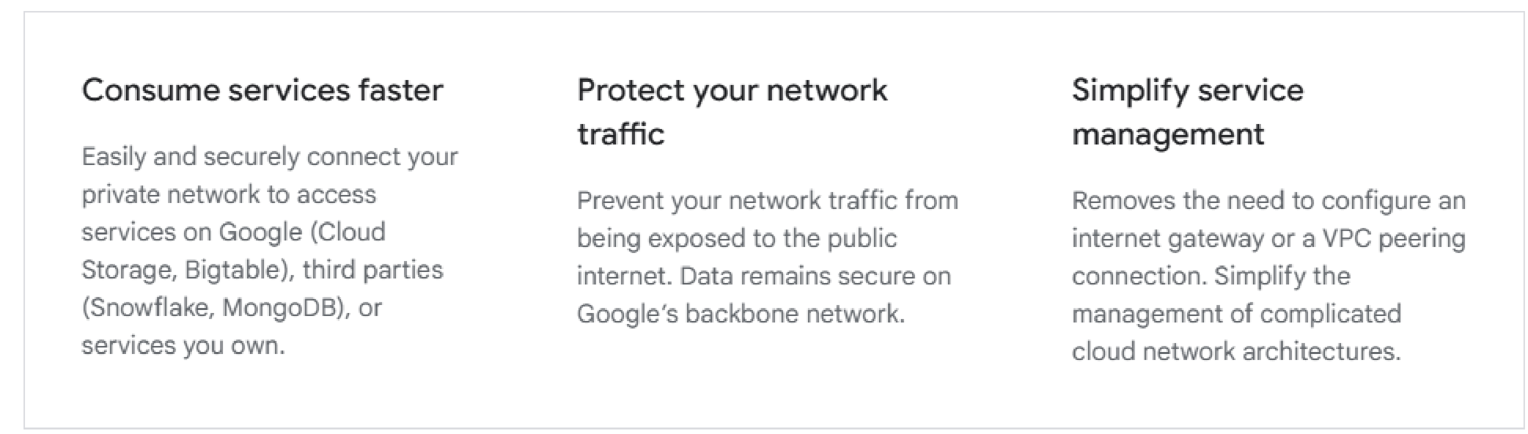
Private Endpoint



Private Link Service

Service Names in Different Cloud Environments

Cloud Provider	Service Name	URL to Service Documentation
Amazon Web Services	AWS PrivateLink	
Microsoft Azure	Azure Private Link	Private Links vs Private Endpoints
Google Cloud Platform	Private Service Connect	Google Private Service Connect



Consume services faster

Easily and securely connect your private network to access services on Google (Cloud Storage, Bigtable), third parties (Snowflake, MongoDB), or services you own.

Protect your network traffic

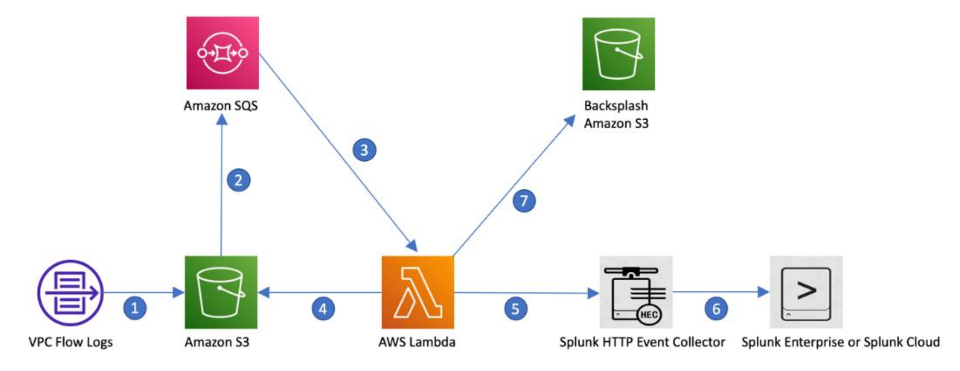
Prevent your network traffic from being exposed to the public internet. Data remains secure on Google's backbone network.

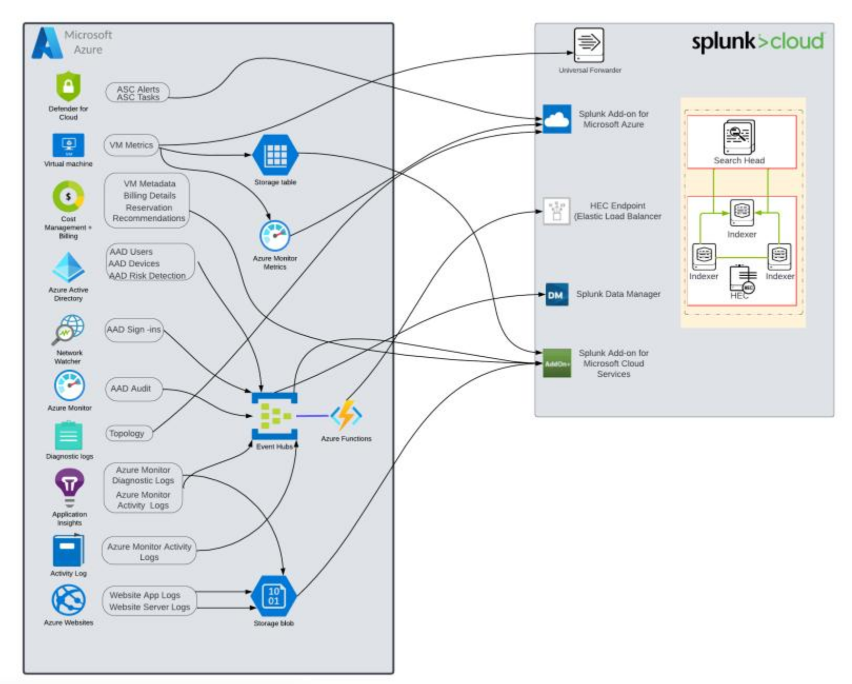
Simplify service management

Removes the need to configure an internet gateway or a VPC peering connection. Simplify the management of complicated cloud network architectures.

Security Monitoring Infrastructure

Azure and AWS Logging to send to Splunk





Security Problem Statement

- Complexity involved to get logs out of cloud environments
- Enterprise policies require using industry standard Infrastructure as Code tools and processes for production cloud deployments
- Ensuring that when new resources are created that they implement desired control set (familiar – we are solving a similar problem as GuardRails)
- There are multiple ways to deploy infrastructure as code in cloud providers – every provider has custom solution, and Terraform is widely adopted as industry standard

Service Names in Different Cloud Environments

Cloud Provider	Service Name	URL to Service Documentation
Amazon Web Services		
Microsoft Azure		
Google Cloud Platform		

Security Guardrails

Security Problem Statement

- Enforcement of consistent configuration

- Reducing likelihood of user error

- Ensuring that when new resources are created that they implement desired control set

Types of Guardrail Controls

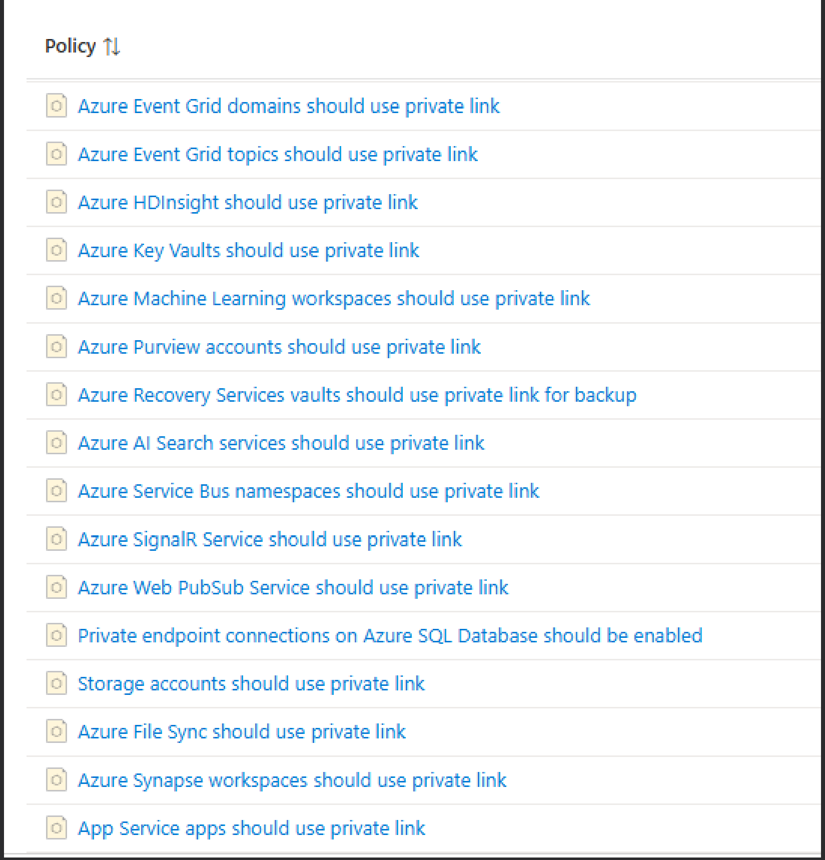
- **Preventive** – Do not permit this setting to be put in place
- **Detective** – Notify when this setting is in place
- **Corrective** – Implement correct setting when incorrect setting is detected.

Different Guardrails across Providers

- Azure
  - Azure Policy
- AWS
  - AWS Config
  - AWS Control Tower
  - AWS Organizations Service Control Policies
- GCP
  - Organization Policy Service

Azure Policy – Audit Private Link Implementation

- **Detective Controls** - Built In Azure Policies audit if Azure Private Link is in use.

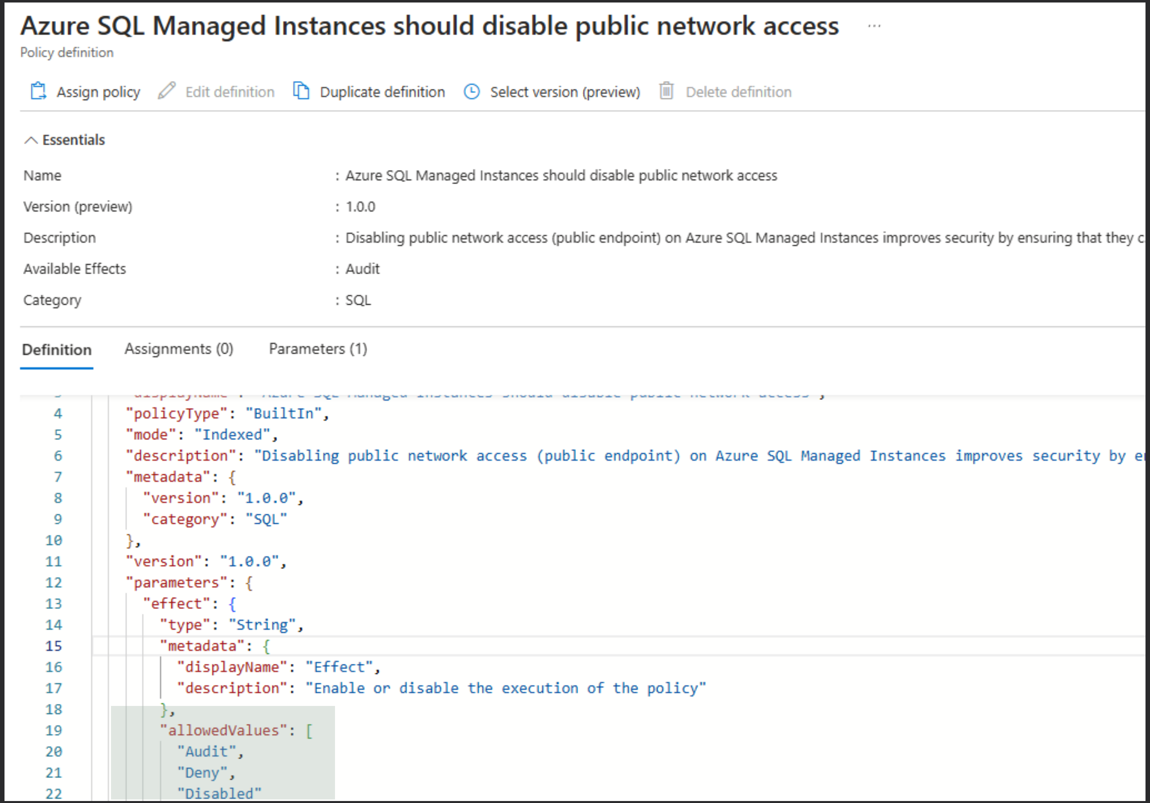


Policy ⇅

- Azure Event Grid domains should use private link
- Azure Event Grid topics should use private link
- Azure HDInsight should use private link
- Azure Key Vaults should use private link
- Azure Machine Learning workspaces should use private link
- Azure Purview accounts should use private link
- Azure Recovery Services vaults should use private link for backup
- Azure AI Search services should use private link
- Azure Service Bus namespaces should use private link
- Azure SignalR Service should use private link
- Azure Web PubSub Service should use private link
- Private endpoint connections on Azure SQL Database should be enabled
- Storage accounts should use private link
- Azure File Sync should use private link
- Azure Synapse workspaces should use private link
- App Service apps should use private link

Azure Policy Initiative – Public Access to SQL Servers Should be Disabled

- **Preventive Controls** – Deny creation of resources that are not in compliance



Azure SQL Managed Instances should disable public network access

Policy definition

Name : Azure SQL Managed Instances should disable public network access

Version (preview) : 1.0.0

Description : Disabling public network access (public endpoint) on Azure SQL Managed Instances improves security by ensuring that they c

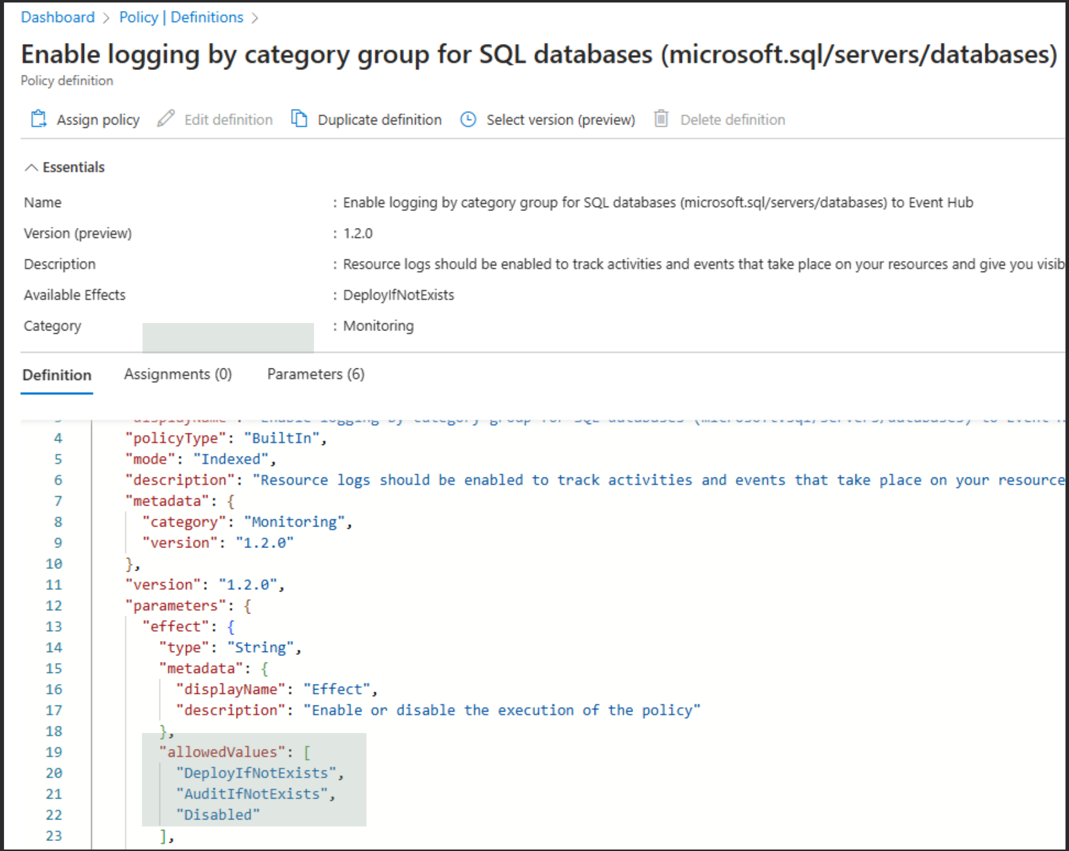
Available Effects : Audit

Category : SQL

```
  "displayName": "Azure SQL Managed Instances should disable public network access",
  "policyType": "BuiltIn",
  "mode": "Indexed",
  "description": "Disabling public network access (public endpoint) on Azure SQL Managed Instances improves security by e
  "metadata": {
    "version": "1.0.0",
    "category": "SQL"
  },
  "version": "1.0.0",
  "parameters": {
    "effect": {
      "type": "String",
      "metadata": {
        "displayName": "Effect",
        "description": "Enable or disable the execution of the policy"
      },
      "allowedValues": [
        "Audit",
        "Deny",
        "Disabled"
```

Azure Policy Initiative – Enable Logging for SQL Databases

- **Corrective Control** – if the correct setting is not enabled, it is turned on – ‘DeployIfNotExists’.



Enable logging by category group for SQL databases (microsoft.sql/servers/databases)

Policy definition

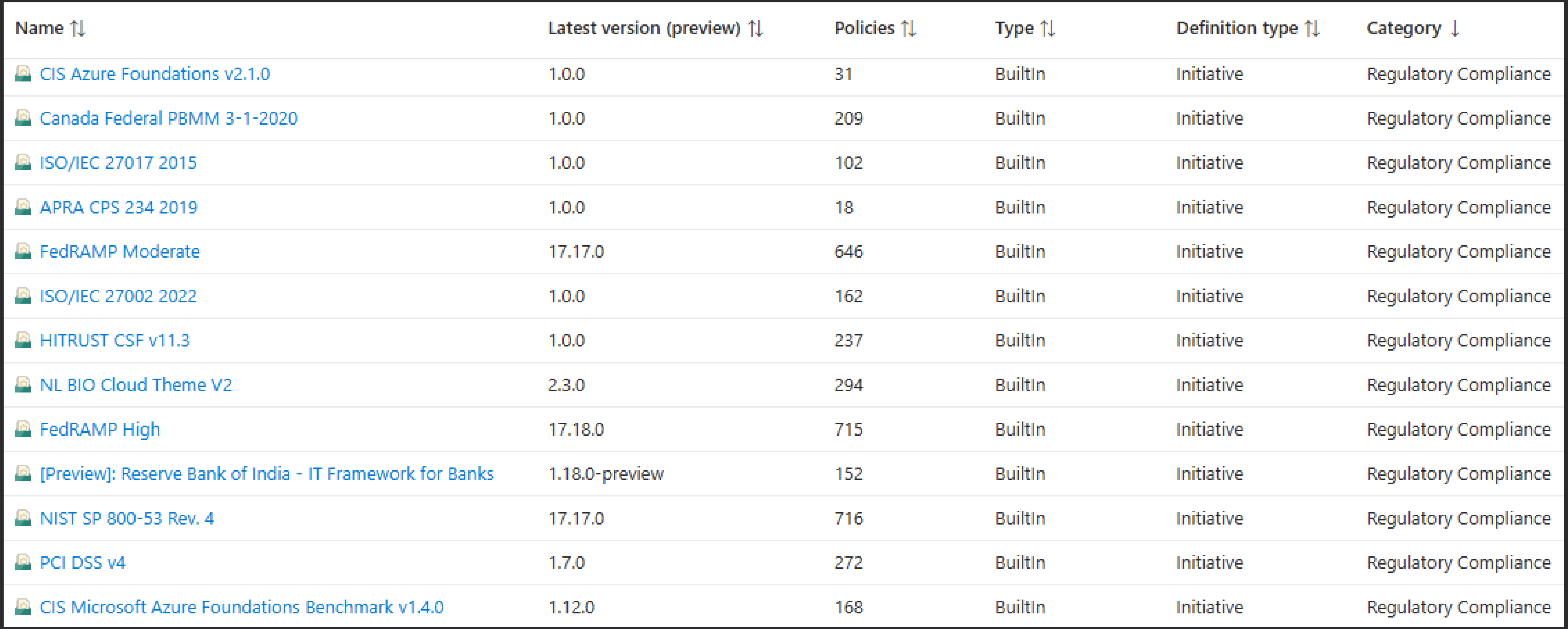
Essentials

Name	: Enable logging by category group for SQL databases (microsoft.sql/servers/databases) to Event Hub
Version (preview)	: 1.2.0
Description	: Resource logs should be enabled to track activities and events that take place on your resources and give you visib
Available Effects	: DeployIfNotExists
Category	: Monitoring

```
  "displayName": "Enable logging by category group for SQL databases (microsoft.sql/servers/databases) to Event H
  "policyType": "BuiltIn",
  "mode": "Indexed",
  "description": "Resource logs should be enabled to track activities and events that take place on your resource
  "metadata": {
    "category": "Monitoring",
    "version": "1.2.0"
  },
  "version": "1.2.0",
  "parameters": {
    "effect": {
      "type": "String",
      "metadata": {
        "displayName": "Effect",
        "description": "Enable or disable the execution of the policy"
      },
      "allowedValues": [
        "DeployIfNotExists",
        "AuditIfNotExists",
        "Disabled"
      ],
```

Managing Large Numbers of Policies

Azure Policy Initiatives – policy groupings aligned to regulatory/guidance frameworks or security concepts. Example Policy Initiatives presented below:



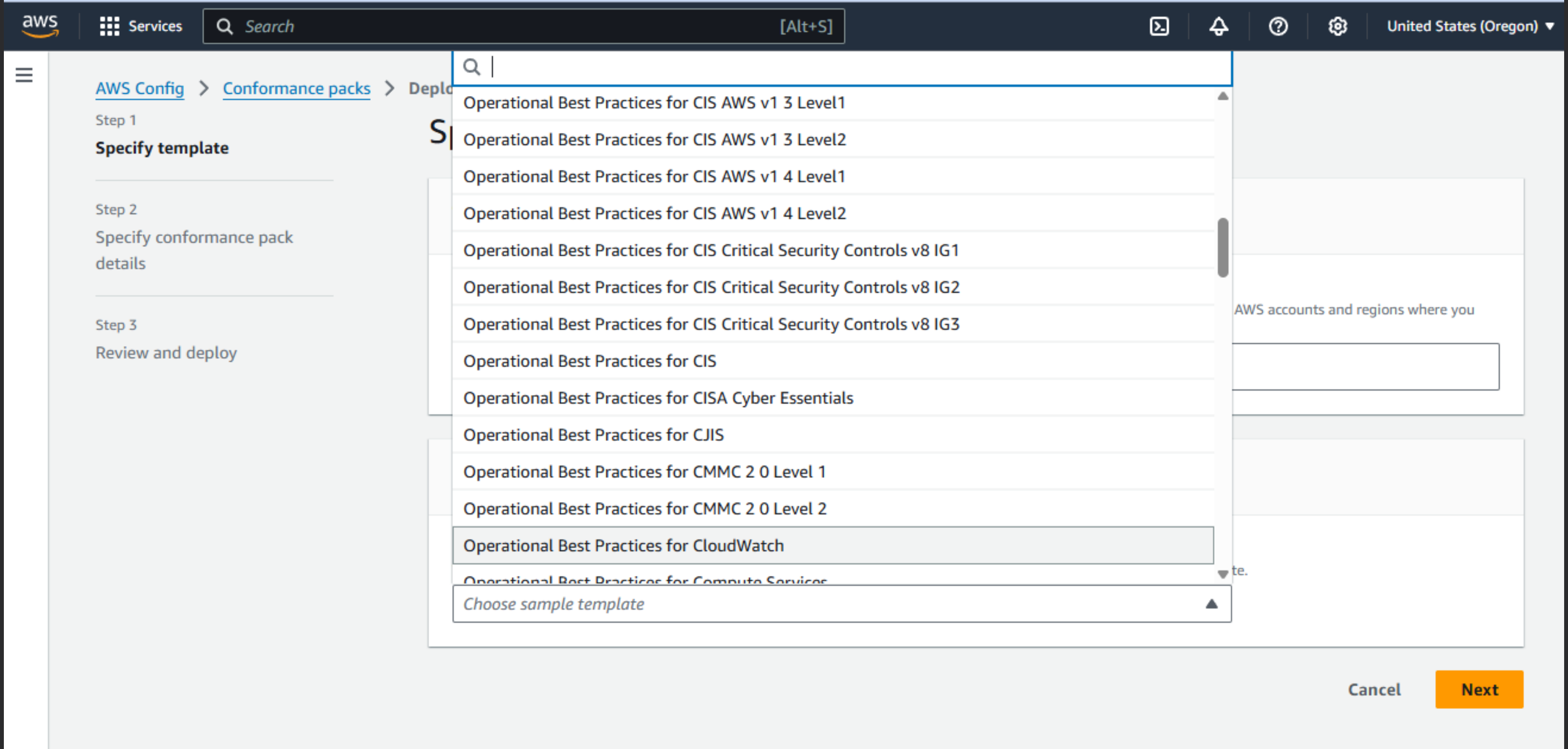
Name ↑↓	Latest version (preview) ↑↓	Policies ↑↓	Type ↑↓	Definition type ↑↓	Category ↓
CIS Azure Foundations v2.1.0	1.0.0	31	BuiltIn	Initiative	Regulatory Compliance
Canada Federal PBMM 3-1-2020	1.0.0	209	BuiltIn	Initiative	Regulatory Compliance
ISO/IEC 27017 2015	1.0.0	102	BuiltIn	Initiative	Regulatory Compliance
APRA CPS 234 2019	1.0.0	18	BuiltIn	Initiative	Regulatory Compliance
FedRAMP Moderate	17.17.0	646	BuiltIn	Initiative	Regulatory Compliance
ISO/IEC 27002 2022	1.0.0	162	BuiltIn	Initiative	Regulatory Compliance
HITRUST CSF v11.3	1.0.0	237	BuiltIn	Initiative	Regulatory Compliance
NL BIO Cloud Theme V2	2.3.0	294	BuiltIn	Initiative	Regulatory Compliance
FedRAMP High	17.18.0	715	BuiltIn	Initiative	Regulatory Compliance
[Preview]: Reserve Bank of India - IT Framework for Banks	1.18.0-preview	152	BuiltIn	Initiative	Regulatory Compliance
NIST SP 800-53 Rev. 4	17.17.0	716	BuiltIn	Initiative	Regulatory Compliance
PCI DSS v4	1.7.0	272	BuiltIn	Initiative	Regulatory Compliance
CIS Microsoft Azure Foundations Benchmark v1.4.0	1.12.0	168	BuiltIn	Initiative	Regulatory Compliance

AWS Config + AWS Service Control Policies – Similar Capabilities to Azure Policy

- AWS Config are detective controls
  - AWS Config is a service that enables assessment, auditing, and evaluation of AWS resource configuration.
  - AWS Config continuously monitors and records AWS resource configurations and automatically evaluates recorded configurations against desired configurations.
- AWS Service Control Policies are preventive controls.
  - SCPs act as guardrails by defining the maximum permissions available to accounts in AWS organization.
  - SCPs work by explicitly denying access to services and actions that fall outside governance boundaries, preventing users from performing unauthorized actions before they happen.

AWS Config Has Similar Approach – Called Conformance Packs

Examples of Conformance Packs for AWS presented:

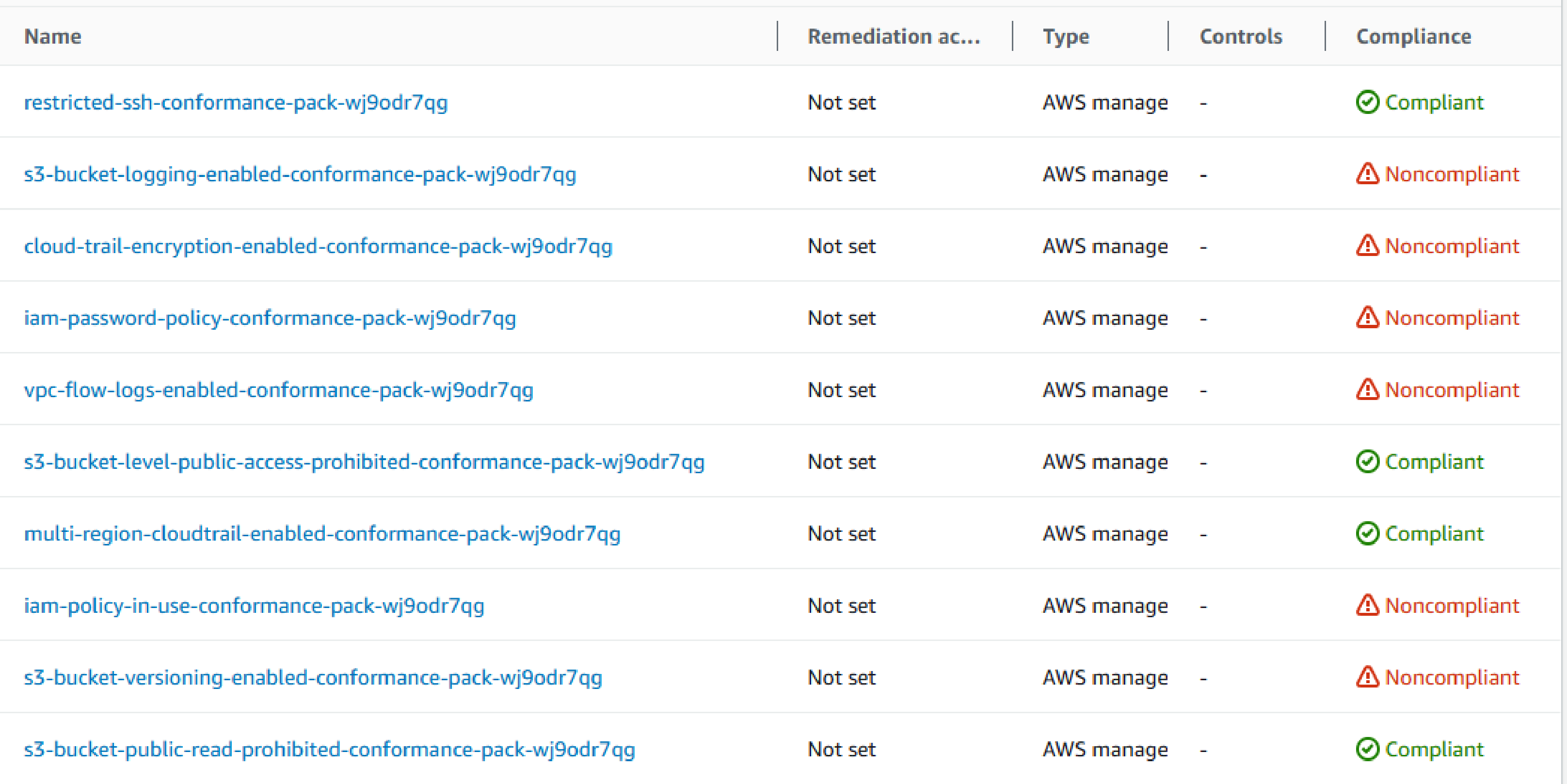


- Operational Best Practices for CIS AWS v1 3 Level1
- Operational Best Practices for CIS AWS v1 3 Level2
- Operational Best Practices for CIS AWS v1 4 Level1
- Operational Best Practices for CIS AWS v1 4 Level2
- Operational Best Practices for CIS Critical Security Controls v8 IG1
- Operational Best Practices for CIS Critical Security Controls v8 IG2
- Operational Best Practices for CIS Critical Security Controls v8 IG3
- Operational Best Practices for CIS
- Operational Best Practices for CISA Cyber Essentials
- Operational Best Practices for CJIS
- Operational Best Practices for CMMC 2 0 Level 1
- Operational Best Practices for CMMC 2 0 Level 2
- Operational Best Practices for CloudWatch
- Operational Best Practices for Compute Services

Choose sample template ▲

AWS Config Has Similar Approach – Called Conformance Packs

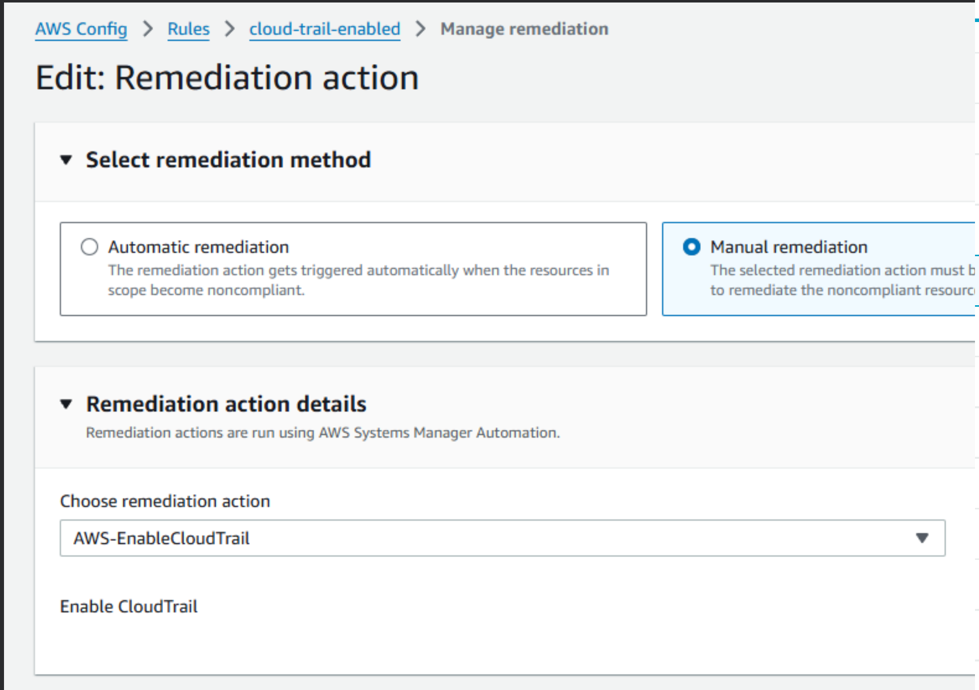
Conformance Pack Outputs:



Name	Remediation ac...	Type	Controls	Compliance
restricted-ssh-conformance-pack-wj9odr7qg	Not set	AWS manage	-	✓ Compliant
s3-bucket-logging-enabled-conformance-pack-wj9odr7qg	Not set	AWS manage	-	⚠ Noncompliant
cloud-trail-encryption-enabled-conformance-pack-wj9odr7qg	Not set	AWS manage	-	⚠ Noncompliant
iam-password-policy-conformance-pack-wj9odr7qg	Not set	AWS manage	-	⚠ Noncompliant
vpc-flow-logs-enabled-conformance-pack-wj9odr7qg	Not set	AWS manage	-	⚠ Noncompliant
s3-bucket-level-public-access-prohibited-conformance-pack-wj9odr7qg	Not set	AWS manage	-	✓ Compliant
multi-region-cloudtrail-enabled-conformance-pack-wj9odr7qg	Not set	AWS manage	-	✓ Compliant
iam-policy-in-use-conformance-pack-wj9odr7qg	Not set	AWS manage	-	⚠ Noncompliant
s3-bucket-versioning-enabled-conformance-pack-wj9odr7qg	Not set	AWS manage	-	⚠ Noncompliant
s3-bucket-public-read-prohibited-conformance-pack-wj9odr7qg	Not set	AWS manage	-	✓ Compliant

AWS Config Has Similar Approach – Called Conformance Packs

AWS has more flexibility in remediation actions for violations – ability to build custom automated or manual responses



AWS Config > Rules > cloud-trail-enabled > Manage remediation

Edit: Remediation action

▼ **Select remediation method**

○ Automatic remediation
The remediation action gets triggered automatically when the resources in scope become noncompliant.

● Manual remediation
The selected remediation action must b
to remediate the noncompliant resourc

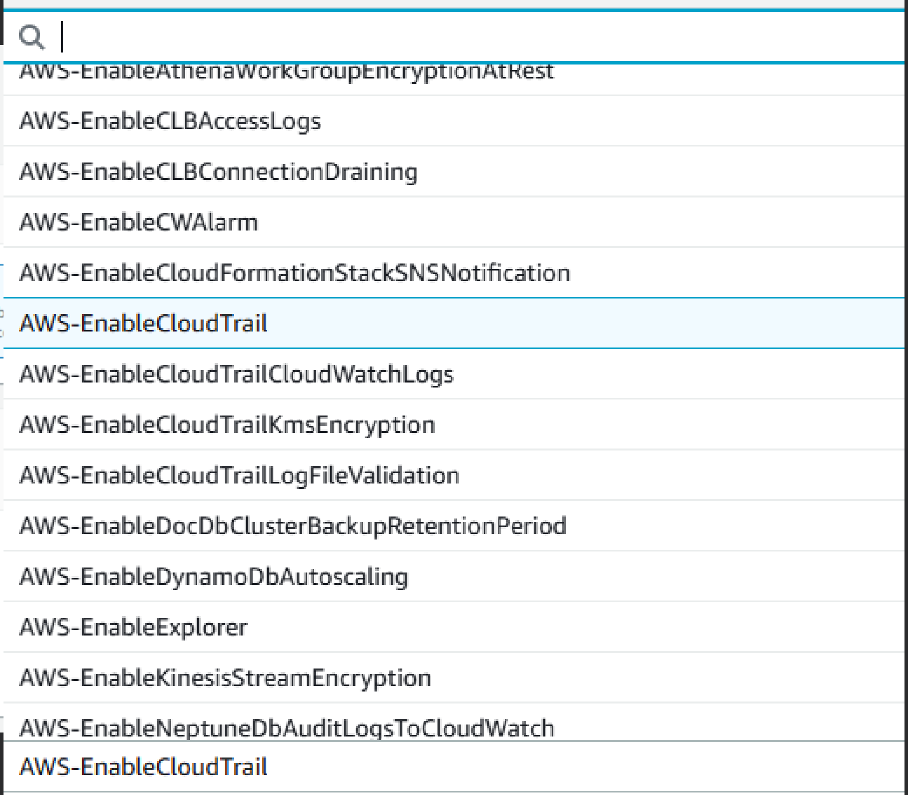
▼ **Remediation action details**

Remediation actions are run using AWS Systems Manager Automation.

Choose remediation action

AWS-EnableCloudTrail ▼

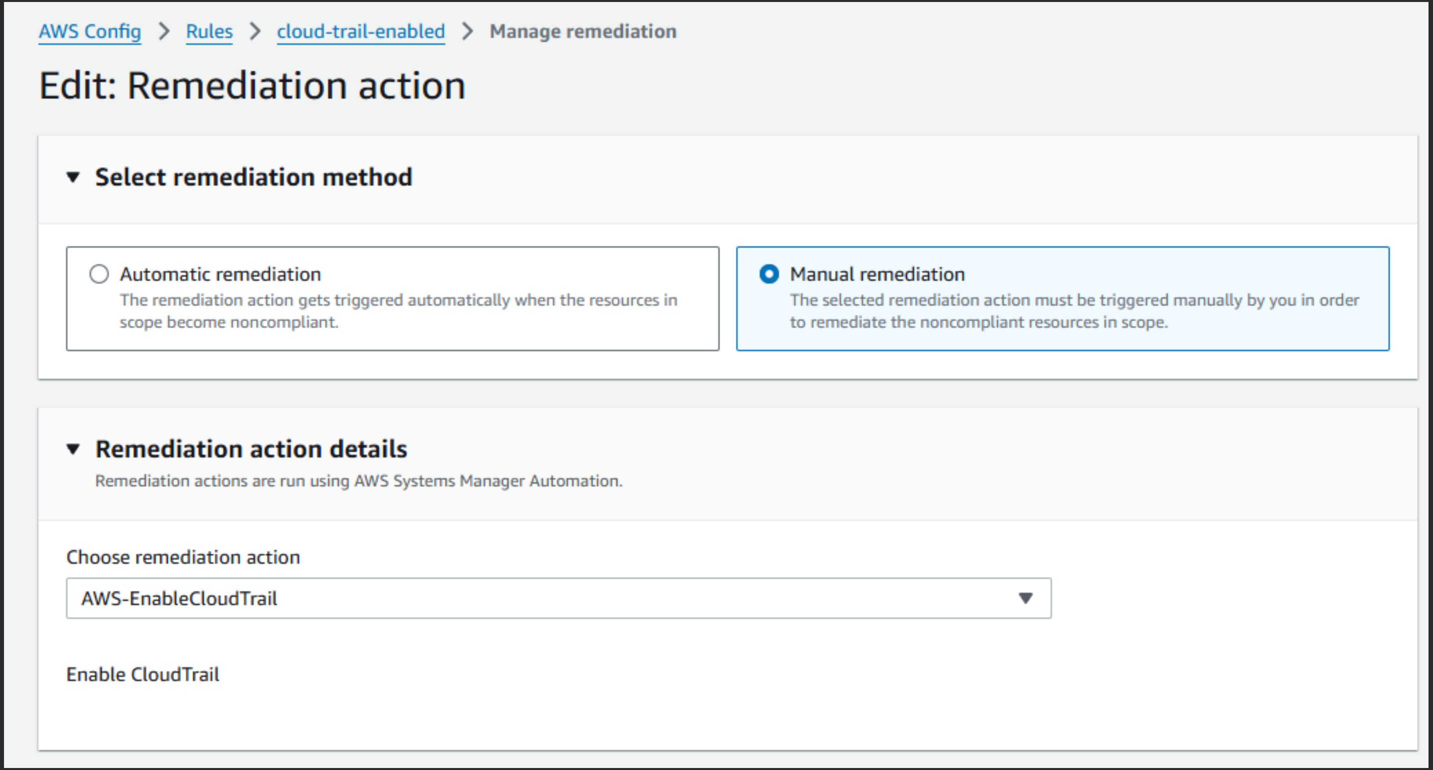
Enable CloudTrail



AWS-EnableAthenaWorkGroupEncryptionAtRest
AWS-EnableCLBAccessLogs
AWS-EnableCLBConnectionDraining
AWS-EnableCWAlarm
AWS-EnableCloudFormationStackSNSNotification
AWS-EnableCloudTrail
AWS-EnableCloudTrailCloudWatchLogs
AWS-EnableCloudTrailKmsEncryption
AWS-EnableCloudTrailLogFileValidation
AWS-EnableDocDbClusterBackupRetentionPeriod
AWS-EnableDynamoDbAutoscaling
AWS-EnableExplorer
AWS-EnableKinesisStreamEncryption
AWS-EnableNeptuneDbAuditLogsToCloudWatch
AWS-EnableCloudTrail

AWS Config Has Similar Approach – Called Conformance Packs

AWS has more flexibility in remediation actions for violations – ability to build custom responses



AWS Config > Rules > cloud-trail-enabled > Manage remediation

Edit: Remediation action

▼ Select remediation method

○ Automatic remediation
The remediation action gets triggered automatically when the resources in scope become noncompliant.

● Manual remediation
The selected remediation action must be triggered manually by you in order to remediate the noncompliant resources in scope.

▼ Remediation action details

Remediation actions are run using AWS Systems Manager Automation.

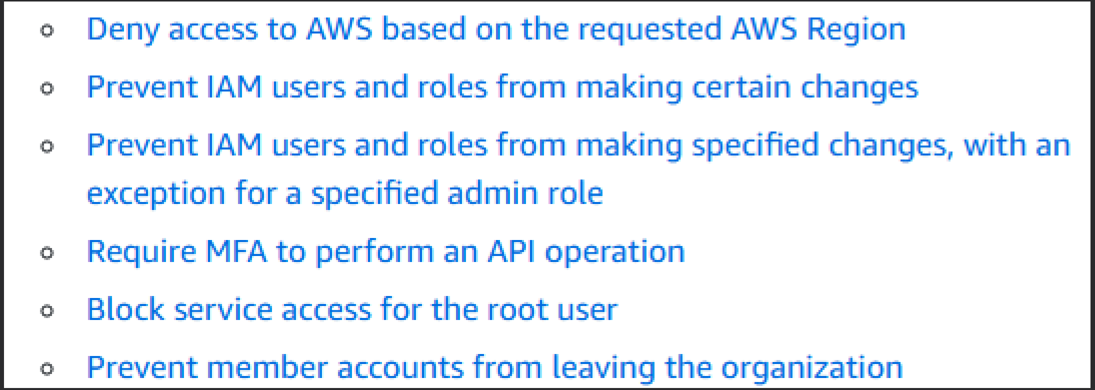
Choose remediation action

AWS-EnableCloudTrail ▼

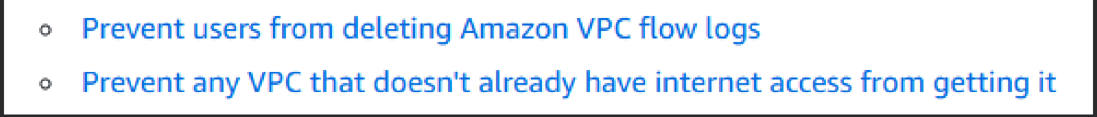
Enable CloudTrail

Service Control Policy – Preventive Examples

Service Control Policies are preventive controls – some examples



- Deny access to AWS based on the requested AWS Region
- Prevent IAM users and roles from making certain changes
- Prevent IAM users and roles from making specified changes, with an exception for a specified admin role
- Require MFA to perform an API operation
- Block service access for the root user
- Prevent member accounts from leaving the organization



- Prevent users from deleting Amazon VPC flow logs
- Prevent any VPC that doesn't already have internet access from getting it

Service Names in Different Cloud Environments

Cloud Provider	Service Name	URL to Service Documentation
Amazon Web Services	AWS Config Service Control Policies	
Microsoft Azure	Azure Policy	
Google Cloud Platform	Organizational Policy Service	

Infrastructure as Code

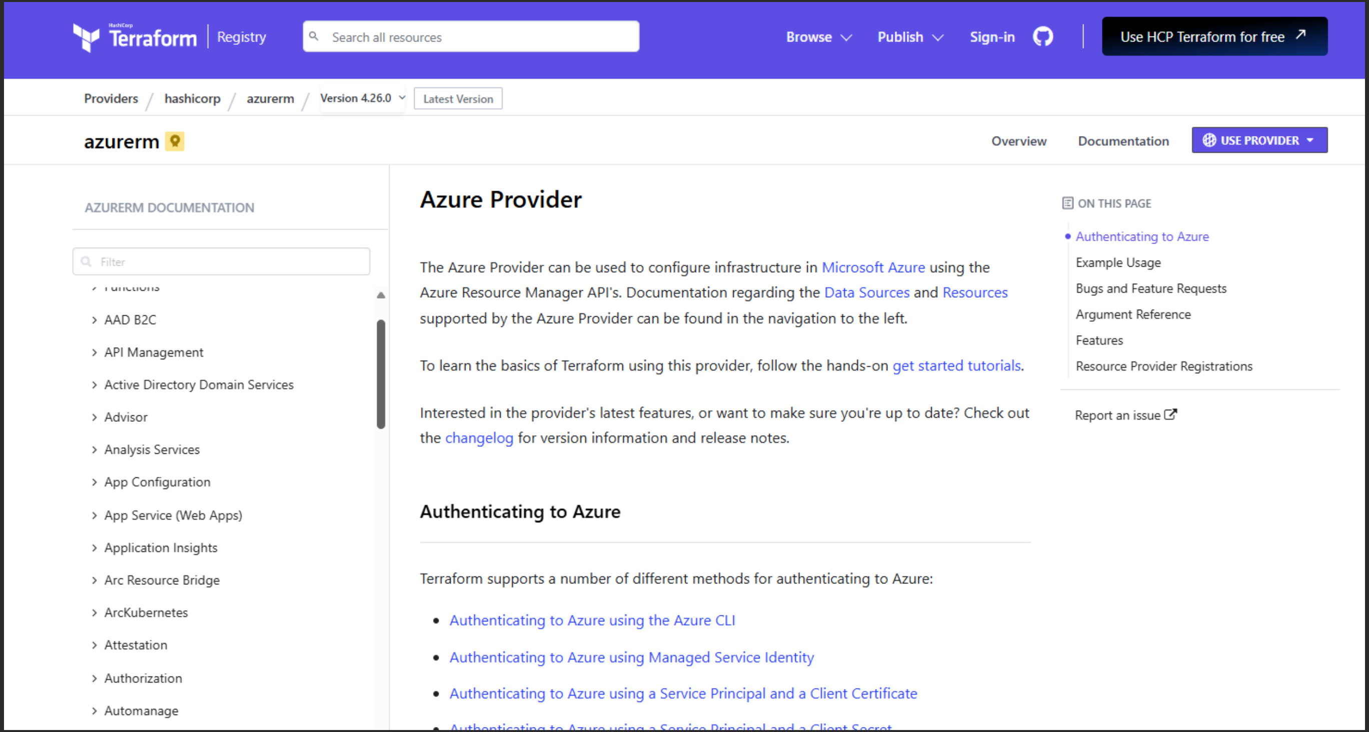
Security Problem Statement

- ClickOps does not scale
- Enterprise policies require using industry standard Infrastructure as Code tools and processes for production cloud deployments
- Ensuring that when new resources are created that they implement desired control set (familiar – we are solving a similar problem as GuardRails)
- There are multiple ways to deploy infrastructure as code in cloud providers – every provider has custom solution, and Terraform is widely adopted as industry standard

Infrastructure as Code in Azure – Terraform Example

Terraform Provider for Azure

https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs



Azure Provider

The Azure Provider can be used to configure infrastructure in Microsoft Azure using the Azure Resource Manager API's. Documentation regarding the Data Sources and Resources supported by the Azure Provider can be found in the navigation to the left.

To learn the basics of Terraform using this provider, follow the hands-on get started tutorials.

Interested in the provider's latest features, or want to make sure you're up to date? Check out the changelog for version information and release notes.

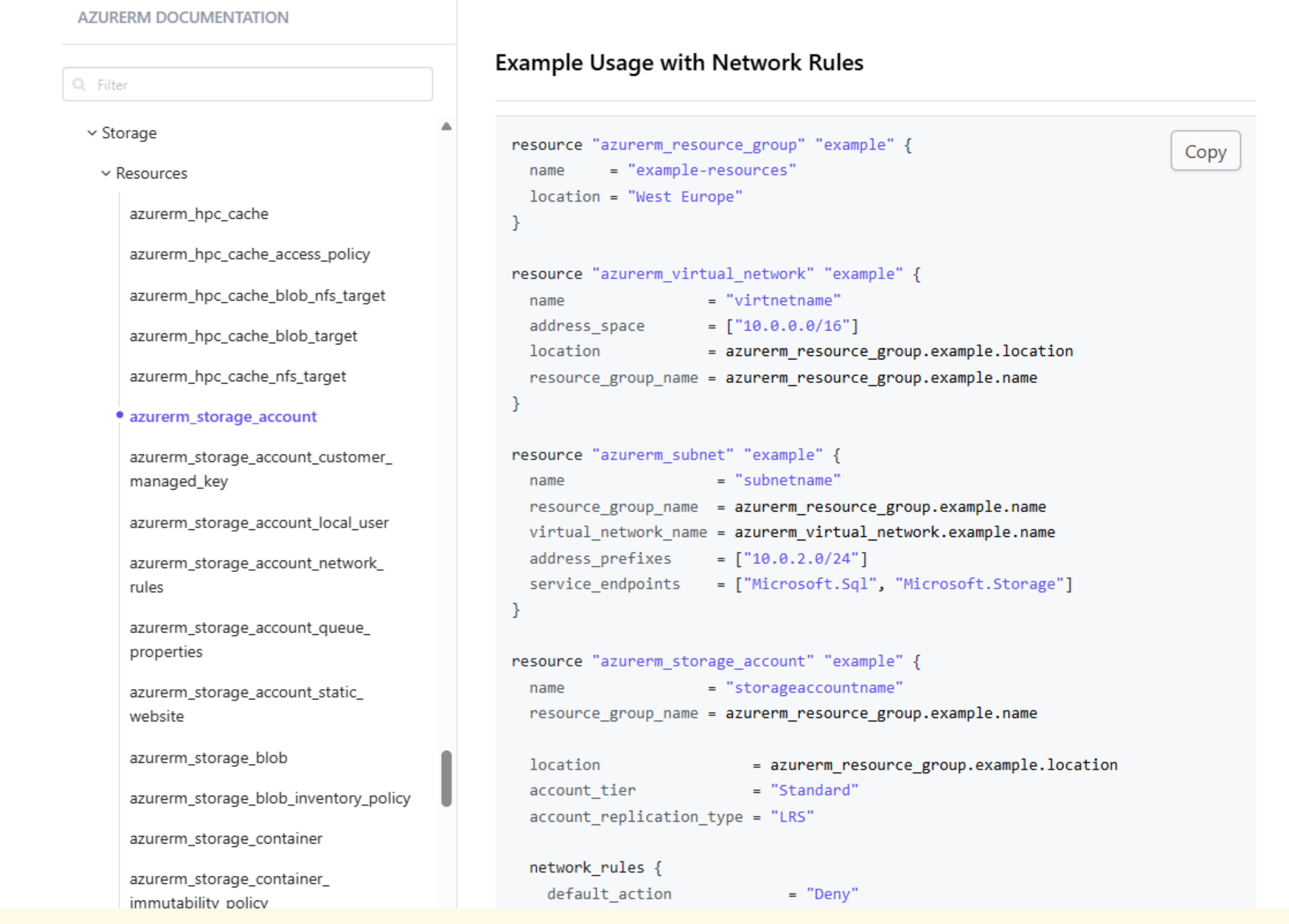
Authenticating to Azure

Terraform supports a number of different methods for authenticating to Azure:

- Authenticating to Azure using the Azure CLI
- Authenticating to Azure using Managed Service Identity
- Authenticating to Azure using a Service Principal and a Client Certificate
- Authenticating to Azure using a Service Principal and a Client Secret

Infrastructure as Code in Azure – Terraform Example

Example Terraform Module for creation of Azure Storage Account

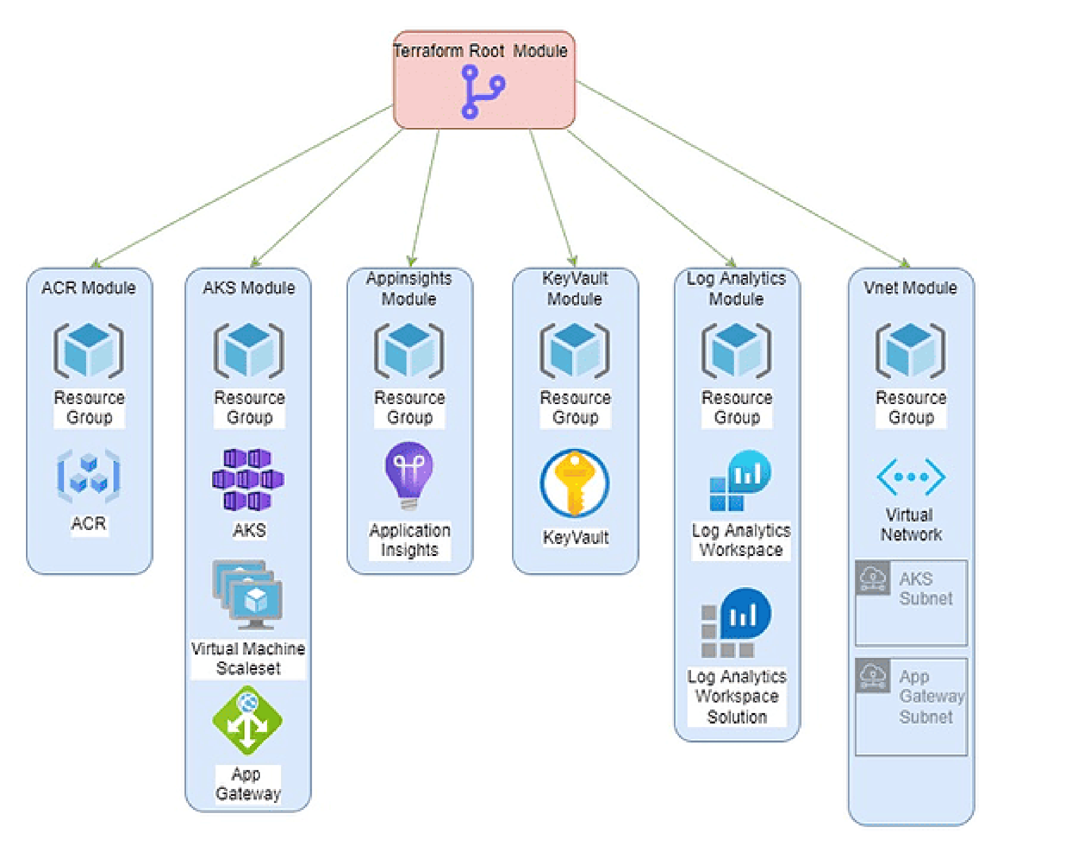

AZURERM DOCUMENTATION
Filter
Storage
Resources
azurerm_hpc_cache
azurerm_hpc_cache_access_policy
azurerm_hpc_cache_blob_nfs_target
azurerm_hpc_cache_blob_target
azurerm_hpc_cache_nfs_target
azurerm_storage_account
azurerm_storage_account_customer_managed_key
azurerm_storage_account_local_user
azurerm_storage_account_network_rules
azurerm_storage_account_queue_properties
azurerm_storage_account_static_website
azurerm_storage_blob
azurerm_storage_blob_inventory_policy
azurerm_storage_container
azurerm_storage_container_immutability_policy
Copy

Example Usage with Network Rules

```
resource "azurerm_resource_group" "example" {
  name     = "example-resources"
  location = "West Europe"
}

resource "azurerm_virtual_network" "example" {
  name                = "virtnetname"
  address_space       = ["10.0.0.0/16"]
  location            = azurerm_resource_group.example.location
  resource_group_name = azurerm_resource_group.example.name
}

resource "azurerm_subnet" "example" {
  name                 = "subnetname"
  resource_group_name  = azurerm_resource_group.example.name
  virtual_network_name = azurerm_virtual_network.example.name
  address_prefixes     = ["10.0.2.0/24"]
  service_endpoints    = ["Microsoft.Sql", "Microsoft.Storage"]
}

resource "azurerm_storage_account" "example" {
  name                = "storageaccountname"
  resource_group_name = azurerm_resource_group.example.name

  location                 = azurerm_resource_group.example.location
  account_tier             = "Standard"
  account_replication_type = "LRS"

  network_rules {
    default_action             = "Deny"
```

Build Module Sets in Terraform

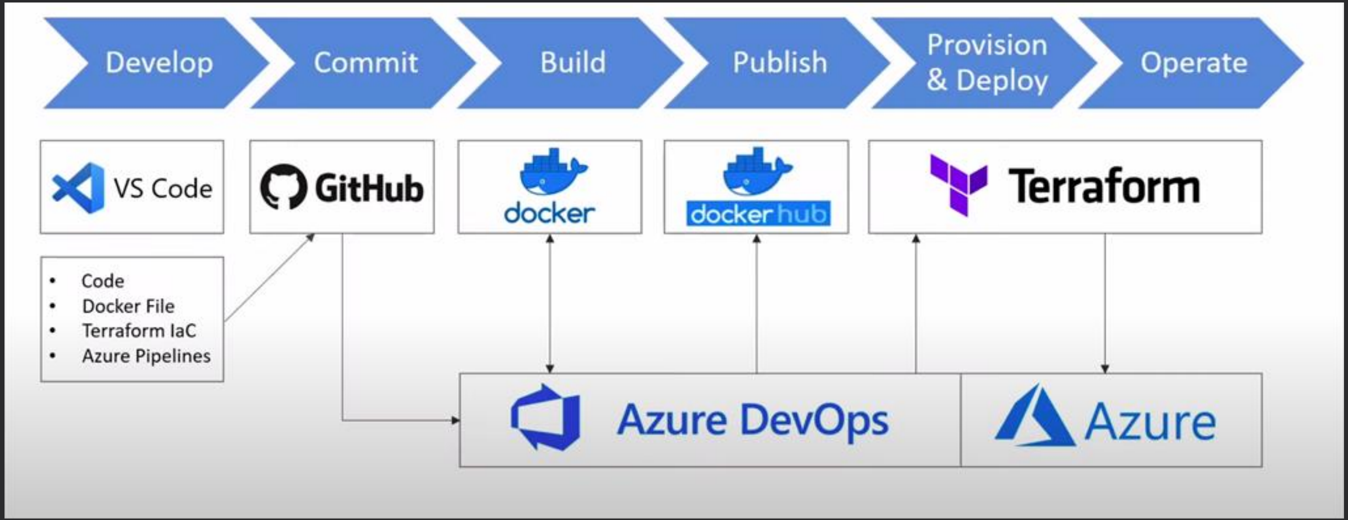
Sets of Terraform Modules for large environments



How does Terraform code get deployed?

Think about software development pipelines, as in this example

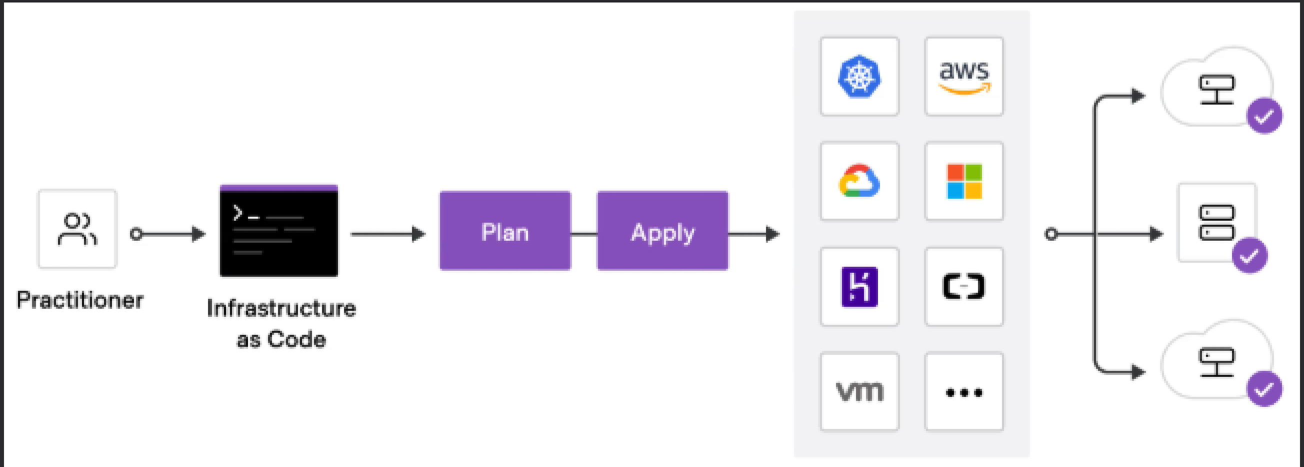
[Software Deployment Pipeline Example]



Deployment of Infrastructure as Code

Infrastructure as Code deployed in a similar manner

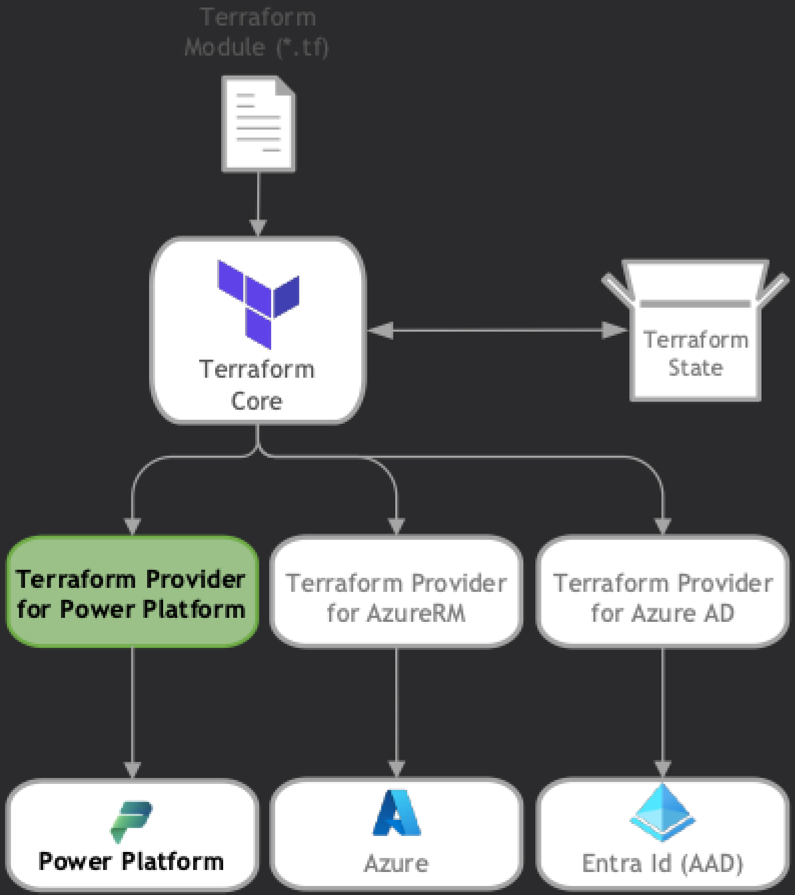
https://developer.hashicorp.com/terraform/tutorials/aws-get-started/infrastructure-as-code



IAC/Terraform not just for Infrastructure

Terraform can be used to deploy Entra ID as well as Microsoft Power Platform

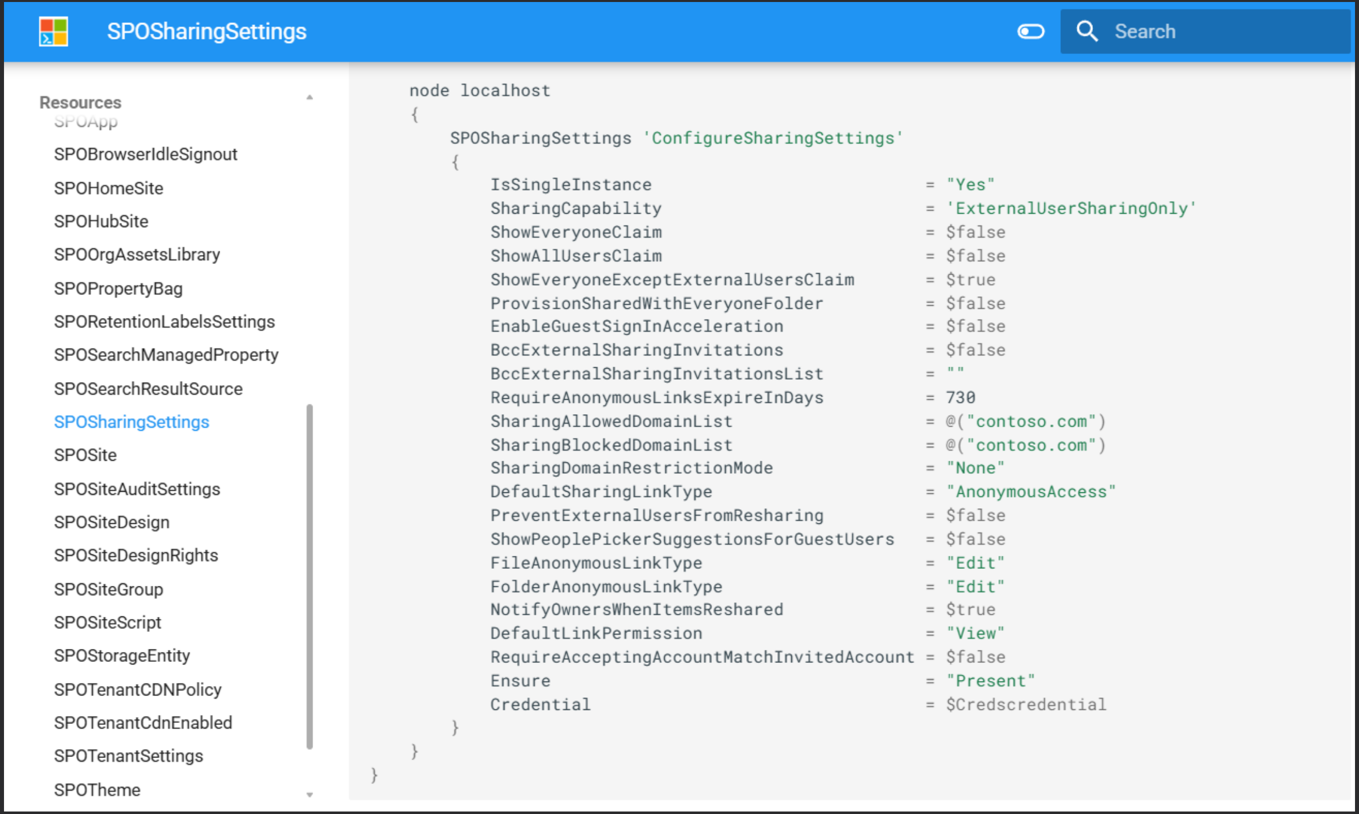
https://learn.microsoft.com/en-us/business-applications/playbook/enterprise-solutions/power-platform-terraform-provider/


Terraform Module (*.tf)
Terraform Core
Terraform State
Terraform Provider for Power Platform
Terraform Provider for AzureRM
Terraform Provider for Azure AD
Power Platform
Azure
Entra Id (AAD)

Configuration as Code in M365 – Microsoft365 DSC Example

Example configuration settings for SharePoint Online sharing

https://microsoft365dsc.com/resources/sharepoint/SPOSharingSettings/



```
    node localhost
    {
        SPOSharingSettings 'ConfigureSharingSettings'
        {
            IsSingleInstance                           = "Yes"
            SharingCapability                          = 'ExternalUserSharingOnly'
            ShowEveryoneClaim                          = $false
            ShowAllUsersClaim                          = $false
            ShowEveryoneExceptExternalUsersClaim       = $true
            ProvisionSharedWithEveryoneFolder          = $false
            EnableGuestSignInAcceleration              = $false
            BccExternalSharingInvitations              = $false
            BccExternalSharingInvitationsList          = ""
            RequireAnonymousLinksExpireInDays          = 730
            SharingAllowedDomainList                   = @("contoso.com")
            SharingBlockedDomainList                   = @("contoso.com")
            SharingDomainRestrictionMode               = "None"
            DefaultSharingLinkType                     = "AnonymousAccess"
            PreventExternalUsersFromResharing          = $false
            ShowPeoplePickerSuggestionsForGuestUsers   = $false
            FileAnonymousLinkType                      = "Edit"
            FolderAnonymousLinkType                    = "Edit"
            NotifyOwnersWhenItemsReshared              = $true
            DefaultLinkPermission                      = "View"
            RequireAcceptingAccountMatchInvitedAccount = $false
            Ensure                                     = "Present"
            Credential                                 = $Credscredential
        }
    }
}
```

Service References

Cloud Provider	Service Name	URL to Service Documentation
Amazon Web Services	AWS Cloud Formation Terraform	
Microsoft Azure	Azure Resource Manager Bicep Terraform	
Google Cloud Platform	Infrastructure Manager (replacement for Cloud Deployment Manager) Terraform	Infrastructure Manager

Privileged Identity Management

Privileged Identity Management

- Privileged Identity Management (PIM) provides Just-in-time (JIT) privileged access to privileged roles. PIM helps to mitigate the risk of excessive, unnecessary, or misused access rights.

- Wherever possible users should authenticate to Entra ID without any role assignments. PIM should then be used to elevate privileges for necessary activities. Service accounts should be excluded from PIM requirements.

Use minimum permissions for role-based activity

- Users should be granted minimum roles necessary to accomplish tasks in PIM and only use privileges when required.

- For instance, a user who reviews security information day to day, but may occasionally perform more sensitive tasks, such as managing named locations should be eligible for two roles – Security Reader and Security Administrator. For their day-to-day role, the Security Reader role should be utilized, and the Security Administrator role should be utilized only when necessary.

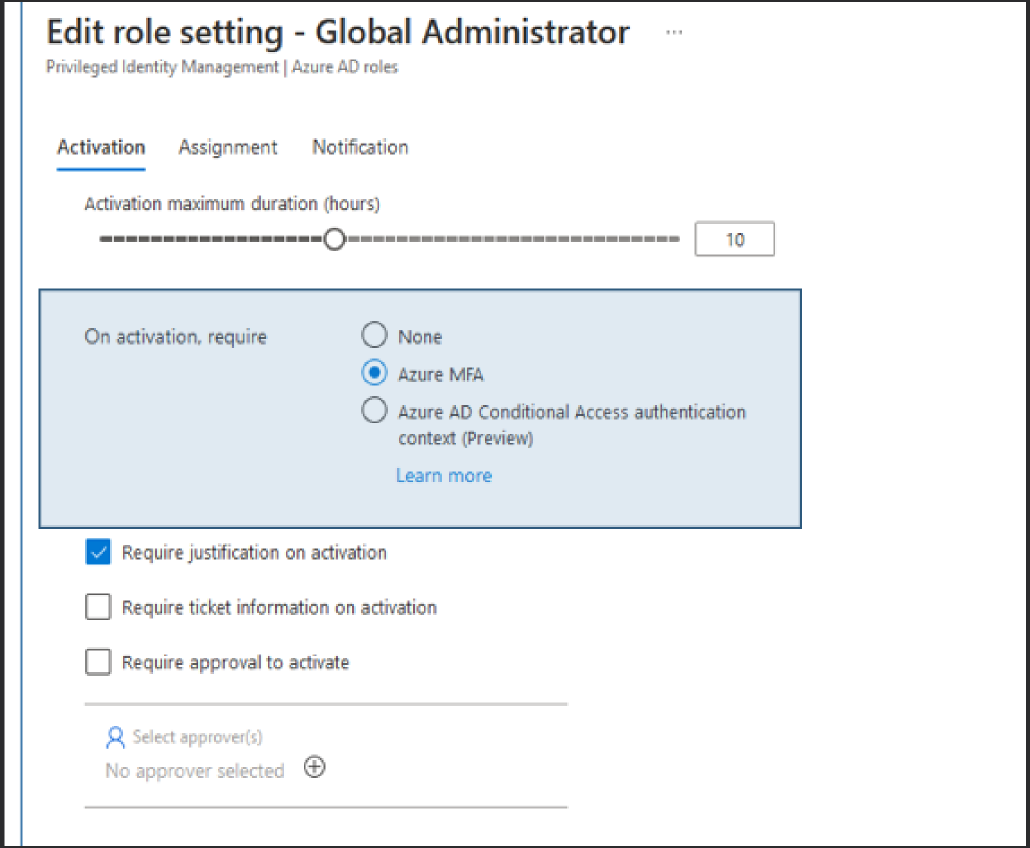
Privileged Identity Management

- Using Conditional Access authentication context, users who are eligible for a role in PIM can be required to satisfy Conditional Access Policy requirements prior to elevation. For example, certain roles could only be assumed from a specific IP address, or must use specific authentication methods, or require an Intune compliant device.

- AUDIT CHECK: All users granted eligible roles in PIM should be reviewed regularly to confirm that role eligibility remains appropriate.

PIM Authentication Contexts

Require specific MFA authentication for specific elevations in PIM (e.g., Global admin needs to have FIDO key, can only elevate from specific location):



Edit role setting - Global Administrator ...

Privileged Identity Management | Azure AD roles

Activation maximum duration (hours): 10

On activation, require
○ None
● Azure MFA
○ Azure AD Conditional Access authentication context (Preview)

☑ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

Select approver(s)

No approver selected

Service Names in Different Cloud Environments

Cloud Provider	Service Name	URL to Service Documentation
Amazon Web Services		
Microsoft Azure	Privileged Identity Management	
Google Cloud Platform		

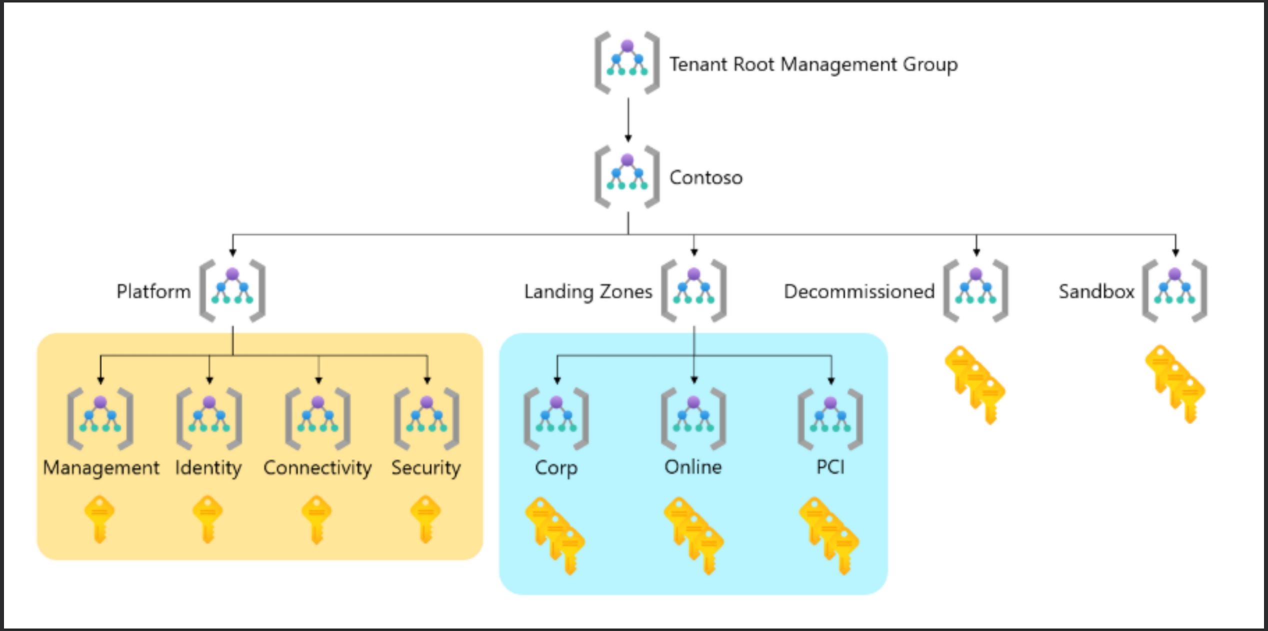
Preconfigured Landing Zones

Preconfigured Landing Zones

- Landing Zones – preconfigured, compliant environments for organizations to develop resources:
  - Azure Landing Zones
  - AWS Control Tower
  - GCP Organizational Policy Service

Azure Landing Zone Example

- Policy enforcement at each level of the Landing Zone



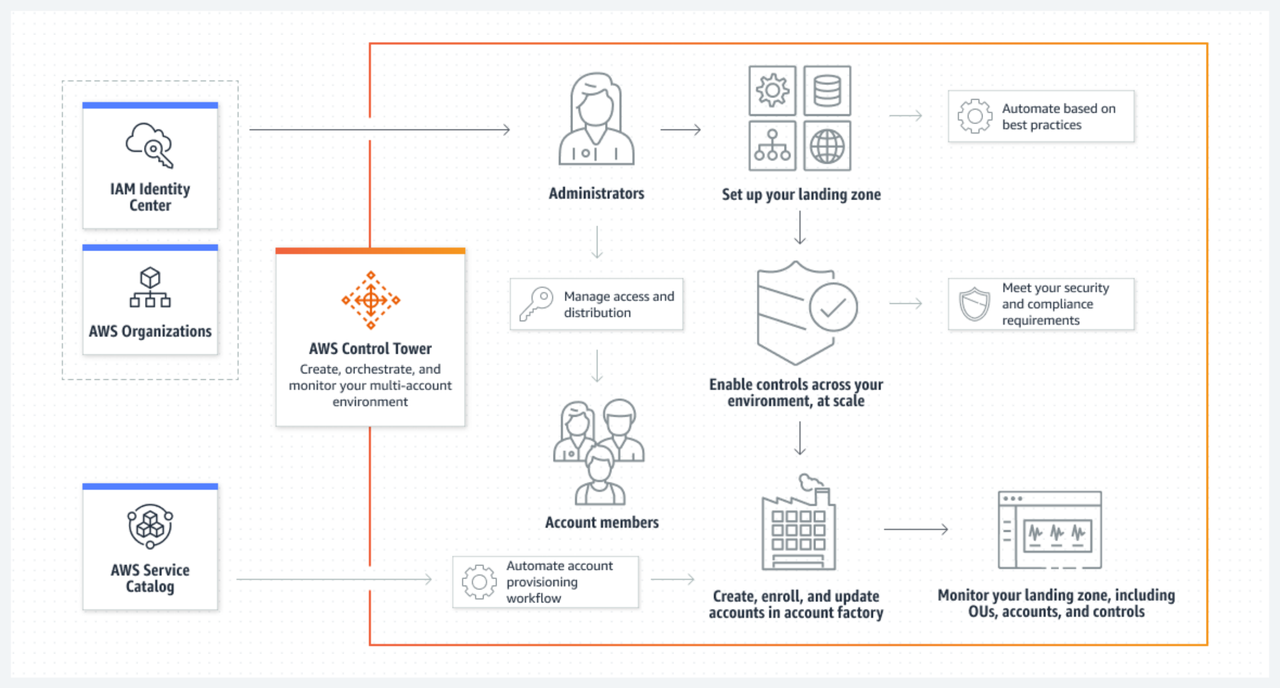
Azure Landing Zone Example

Scenario where a new landing zone subscription is provisioned and placed in the "corp" management group. DINE and Modify policies then take the following actions for the landing zone subscription:

- Enable Microsoft Defender for Cloud. Configure Defender for Cloud exports to the central Log Analytics workspace in the management subscription.
- Enable Defender for Cloud for the different supported offerings based on the policy parameters configured on the policy assignment.
- Configure the Azure Activity logs to be sent to the central Log Analytics workspace in the management subscription.
- Configure the diagnostic settings for all resources to be sent to the central Log Analytics workspace in the management subscription.
- Deploy the required Azure Monitor agents for virtual machines and Azure Virtual Machine Scale Sets, including Azure Arc connected servers. Connect them to the central Log Analytics workspace in the management subscription.

AWS Control Tower Example

- Policy enforcement at each level of the Landing Zone


IAM Identity Center
AWS Organizations
AWS Service Catalog
AWS Control Tower
Create, orchestrate, and monitor your multi-account environment
Administrators
Set up your landing zone
Automate based on best practices
Manage access and distribution
Enable controls across your environment, at scale
Meet your security and compliance requirements
Account members
Automate account provisioning workflow
Create, enroll, and update accounts in account factory
Monitor your landing zone, including OUs, accounts, and controls

Service Names in Different Cloud Environments

Cloud Provider	Service Name	URL to Service Documentation
Amazon Web Services	AWS Control Tower	
Microsoft Azure	Azure Landing Zones	
Google Cloud Platform		

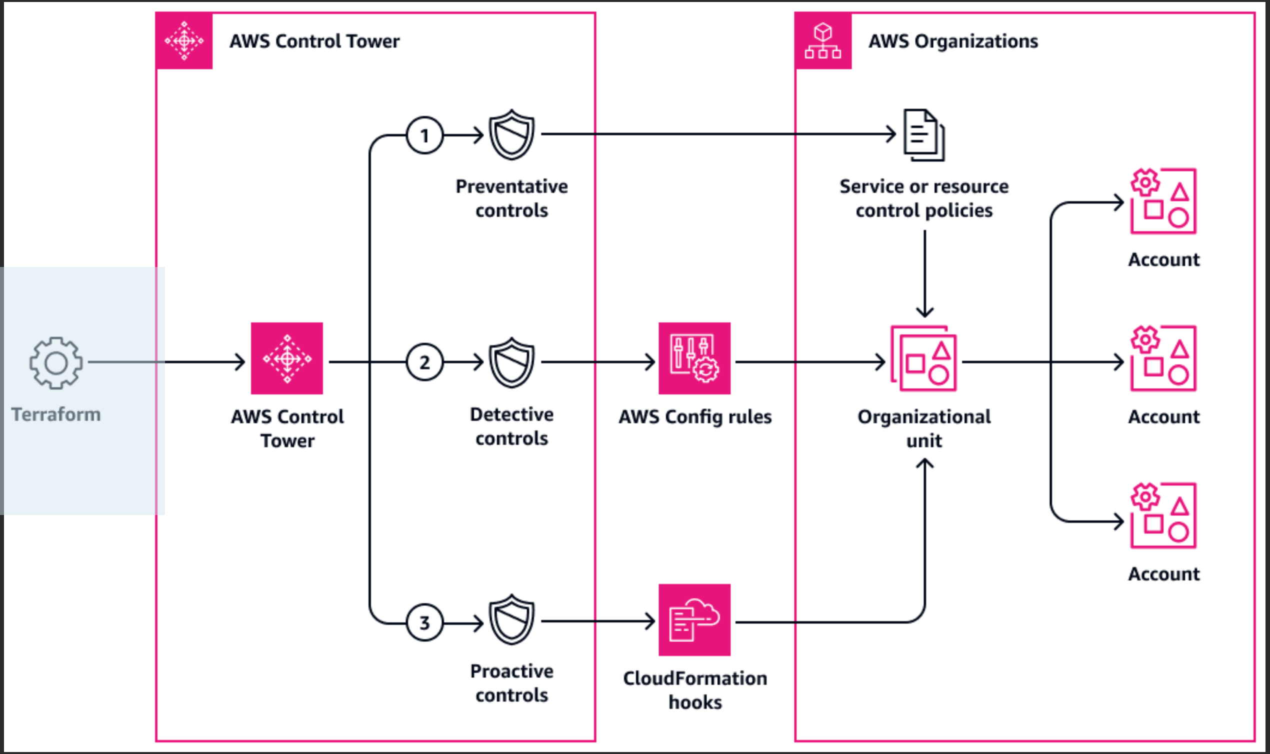
Putting the Components Together

Reference Environments

- We will review an environment that puts together most of the pieces that we discussed today.

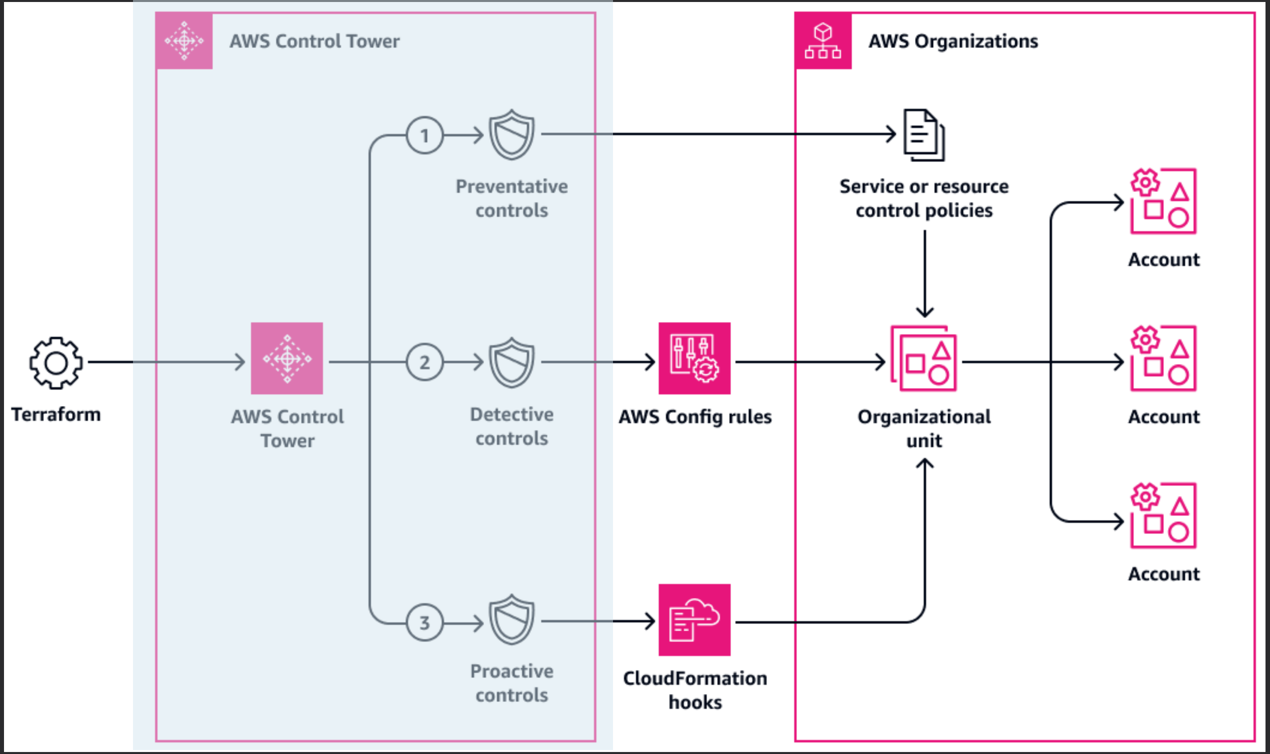
Reference AWS Environment

(1) Infrastructure as Code



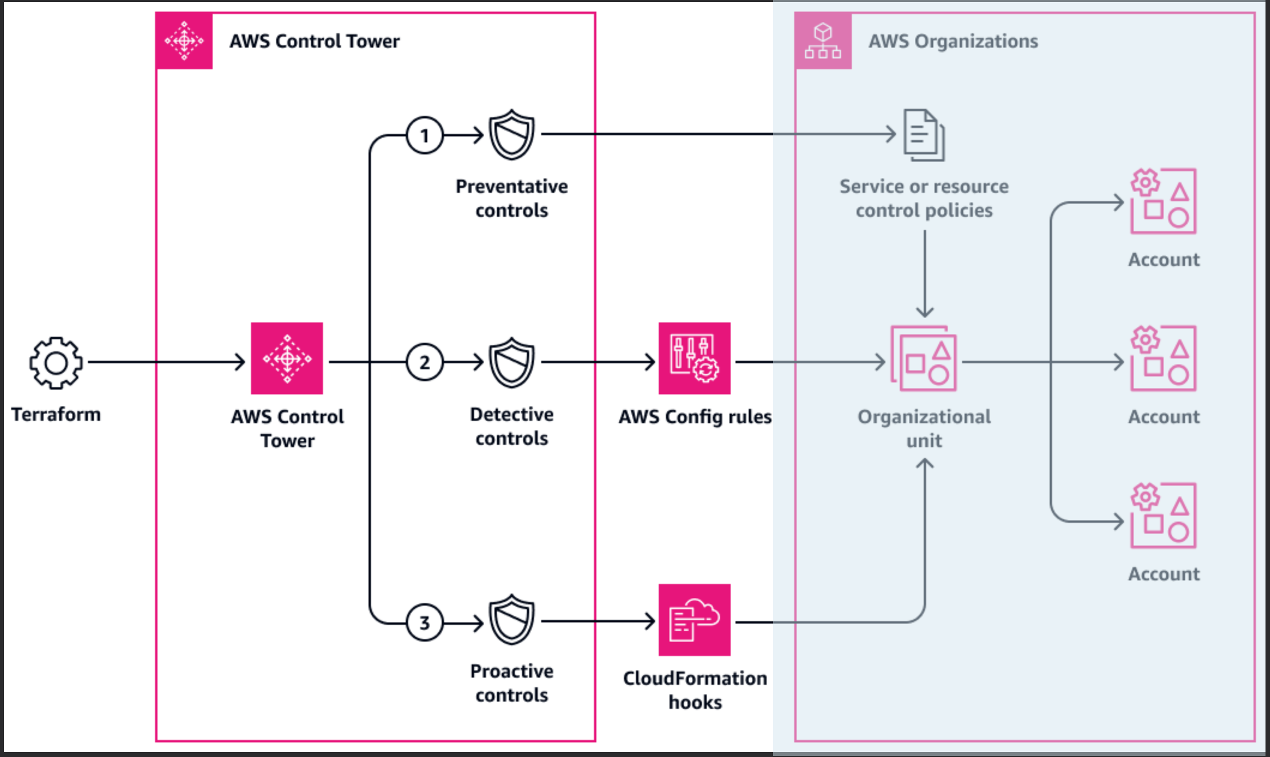
Reference AWS Environment

(2) Creates
Landing Zones



Reference AWS Environment

(3) Deploys Guardrails


AWS Control Tower
AWS Organizations
Terraform
AWS Control Tower
1
Preventative controls
2
Detective controls
3
Proactive controls
AWS Config rules
CloudFormation hooks
Service or resource control policies
Organizational unit
Account
Account
Account