

LANET

Azure Landing Zones



Author: Mitesh Chauhan
Date: 2nd January 2024
Contact: hello@lanet.co.uk
Web: lanet.co.uk

Why LA NET ?

LA NET

LA NET is a Microsoft *Azure cloud infrastructure specialist* and Microsoft Cloud Platform Partner. We have been designing and deploying cloud infrastructure solutions on the Azure platform since its release in *2011*. We have completed best practice designs and deployments for many organisations across various sectors *globally*. We provide Azure environment design, deployment, and *managed services*.

Microsoft
Partner



Our Purpose

LA  NET

To give our customers *peace of mind* and the confidence that their cloud platform is in good hands

Microsoft
Partner

What Our Customers Demand



Resilient and *stable* cloud solutions

Minimal or *ZERO* unplanned *outages*

Highly *secure* and best-practice core infrastructure

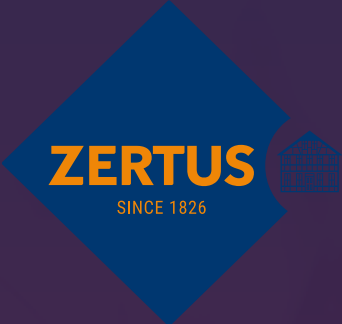
Guidance and *training* for cloud adoption

Reliable and *trusted* service management

Cost management and optimisation

Customers

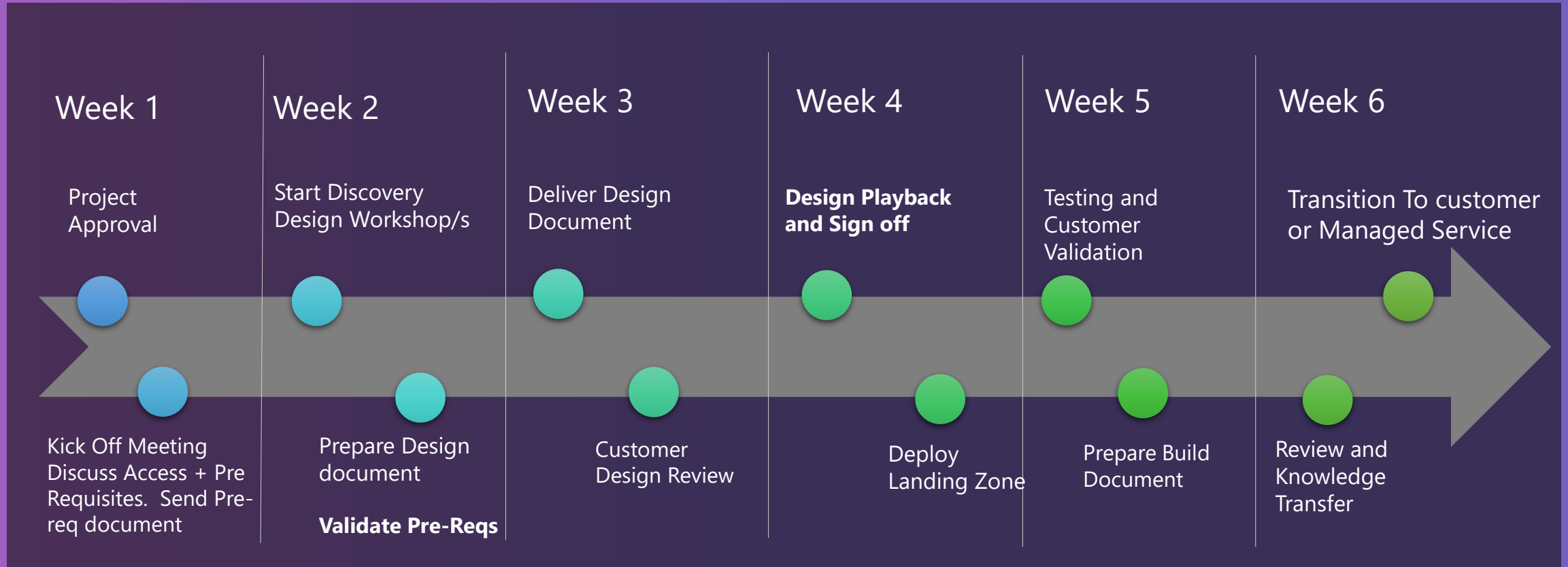
LA NET



- Establish Key Stakeholders
- Access approach for the deployment team
- Pre-Requisites Document
- Project Timelines and Responsibilities

- Fixed Standard Build
- Pre-Requisites must be in place
- Azure DevOps and Bicep
- Single Region
- Microsoft CAF Standard Naming Provided

Azure Landing Zone Process



AZURE LANDING ZONE – AZURE REVIEW MEETING AND PRE REQ'S

Typically: 2-4 Days to review and write up

Customer Stakeholders

- Representatives from Network, Security, and Infrastructure teams
- Project Owner/s

Review Pre-Requisites

- Two named individuals will need read access to Azure Tenant at the root level.
 - Plus, Directory Reader role in Azure Entra ID

Areas Covered

- Resource Organisation
- Identity and Access
- Network Topology
- Governance
- Management and Security

AZURE LANDING ZONE – AZURE DESIGN MEETING **AFTER REVIEW**

Typically: Design phase typically 1-2 weeks

Customer Stakeholders

- Representatives from Network, Security, and Infrastructure teams
- Project Owner/s

Areas Covered

- Resource Organisation
- Identity and Access
- Network Topology
- Governance
- Management and Security

Key Decision Points

- Subscriptions and Management Groups
- Identity and Access Control
 - Groups, Custom Roles, AD
- Network topology and Infrastructure
 - Network Services to deploy including SKUs etc
 - DNS configuration
- Management
 - Monitoring, Logging, alerting, backup
- Governance and Security
 - Azure Policy, Defender for Cloud

Landing Zone – Preparing the Foundations



Getting Started

- Tenant Setup
- Management Groups
- Subscriptions
- Role Based Access
- Deployment
- Inputs to Landing Zone
- Tagging

Governance Baselines

- Azure Policy Baselines
- Defender for Cloud
- Cost Management

Networking

- Hub and Spoke Networking
- VPN / ExpressRoute
- Firewalls
- User Access and Bastion

Management

- User Identity & Access
- Monitoring
- Dashboards
- Alerting setup

Landing Zone – Landing Zone Inputs

Geographies

- Specify Build Regions
- Specify Allowed Regions

Networking

- Private Class C range for Azure
 - e.g. 10.10.0.0/16
- No overlap with existing networks
- Minimum /22 per region
- Split into VNets by Regions and subscriptions
- No DHCP, Addresses managed by Azure
- Select Shared Services

VPN Details

- On Prem VPN Device Internet IP
- On Prem IP Ranges
- Optional
 - VPN Make & Model
 - VPN User Contact

Alert Recipients

- Email Address for Platform Alerts
 - E.g. AzureAlerts@domain.com
- Email Address for Security

Cost Center IDs

- e.g. IT, Data Platform
- If no codes, then above names will be used.

Azure Platform Landing Zone Accelerator

Based on the Microsoft Cloud Adoption Framework for Azure – aka.ms/caf

CAF Design Areas

Entra ID Tenant

Identity and Access

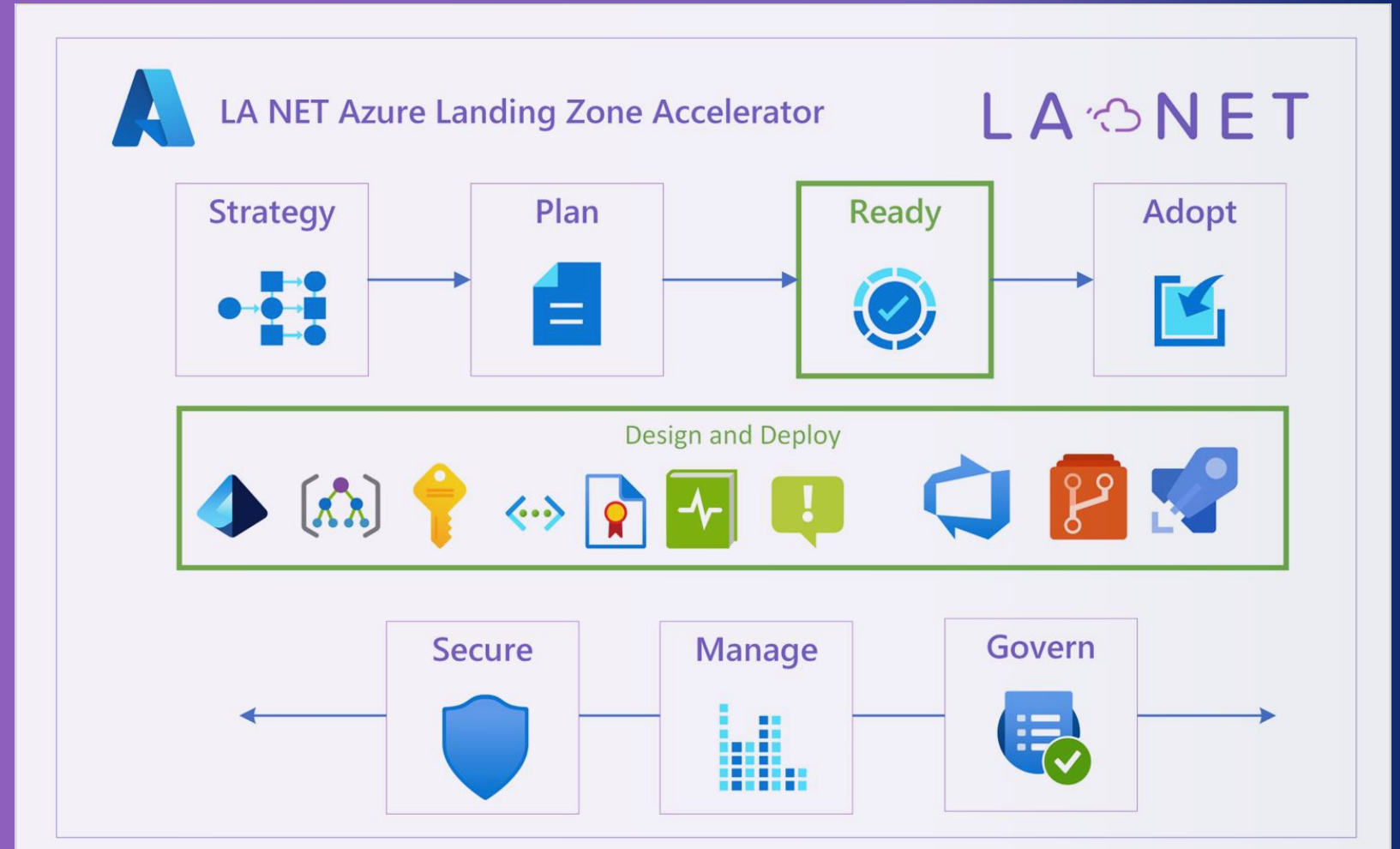
Resource Organisation

Network Topology

Security

Management

Governance



Azure Platform Landing Zone Accelerator

Identity and Access Control

AD / ADDS

Custom Role

Entra ID

(Example Groups)

Best practice Entra ID Groups

Azure AD User / Group Name	Purpose	Scope	Access Level	Typical Members
* Service Principal	Deploy the Landing Zone components from Azure DevOps.	Tenant Root (/)	Owner + User Access Administrator	DevOps
*Azure Platform Admins	Manage All Azure Resources	Root MG	Owner + User Access Administrator **Azure Key Vault Administrator **Azure Blob Storage Contributor ** Management Group contributor	Azure Infra Owners only
Azure Break Glass	Emergency Access	Root MG	Owner User Access Administrator	Emergency Access Only
Azure Database Admins	Manage Database Servers	Root MG	Default Admins of SQL Servers if not specified	Azure SQL Server Owners only
Azure Platform Readers	View Environment Only	Root MG	Reader	Auditors or testers who can view all
Azure Security Admins	Review Security Information	Root MG	Security Admin	SecOps Team
Azure Network Admins	Manage Network configuration	Customer Root MG	Network Contributor	Network Administrators
Azure Cost Reader	View cost data, cost config	Root MG	Cost Management Reader	Finance, Account Manager
Azure Cost Manager	View cost data, manage cost conf	Root MG	Cost Management Contributor	Finance, Account Manager
Azure Help Desk	First Line Support	Landing Zones MG	Custom Support Role	Help Desk Team
*Implementation	Build Environment	Root MG	Contributor + User Access Administrator + App Developer (Azure AD Role)	Build Engineers - Remove after deployment
Data Analytics Deployment	Deploy Data Analytics Solution	Data Analytics Subscriptions	Contributor	Data Analytics Implementors + Admins
CRM Admin	CRM Azure Admins	CRM Subscriptions	Contributor	CRM Implementors + Admins
Power Platform Admins	Power Platform Admins	Power Platform Subscriptions	Contributor	Power Platform Implementors + Admins

Azure Platform Landing Zone Accelerator

Resource Organisation

Management Group Structure

Subscription Placement

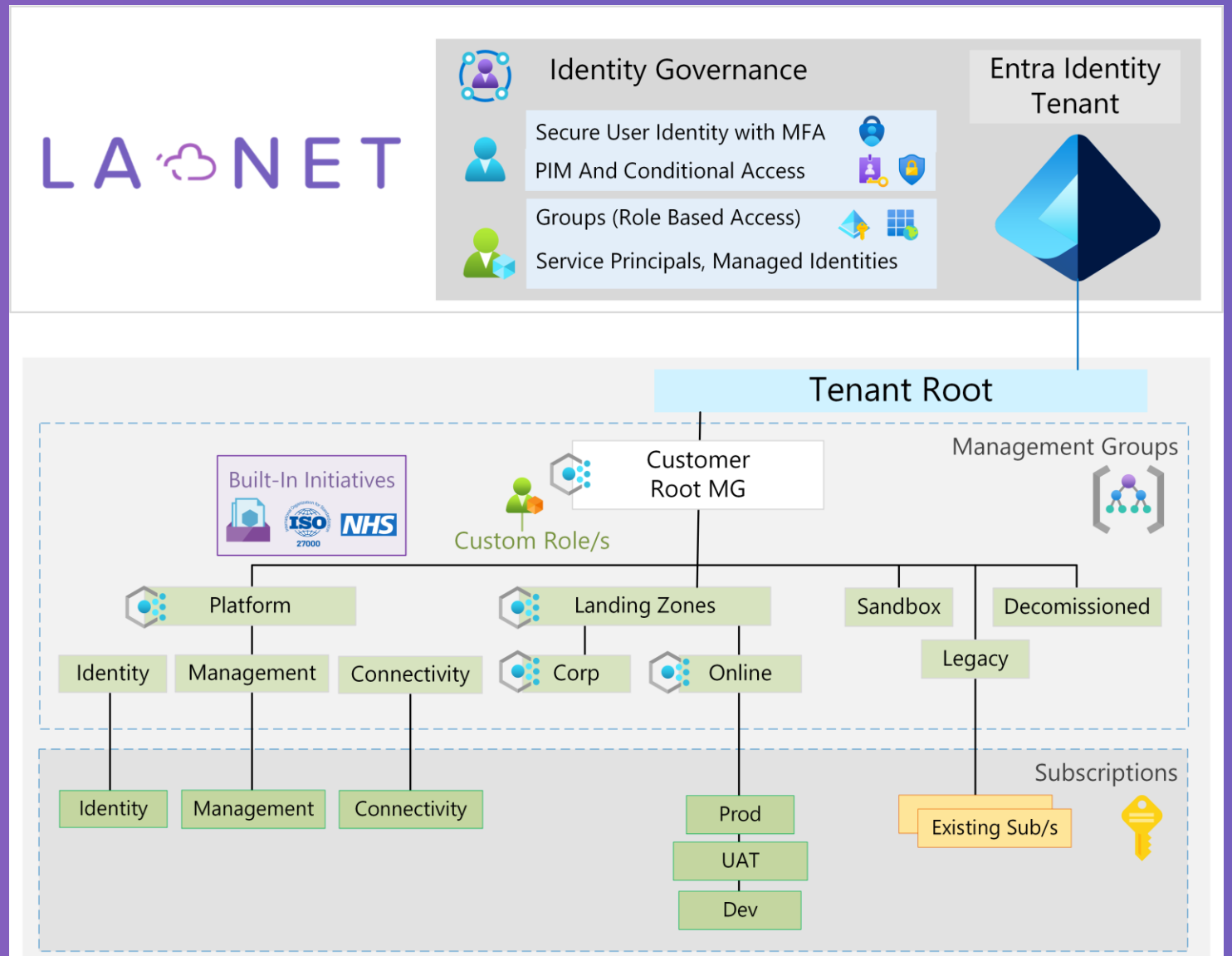
Existing Subscriptions

Pre- Requisites

Tenant Setup

Subscriptions or mechanisms to add

User with Global Admin Rights



Azure Platform Landing Zone Accelerator

Network Topology and Connectivity

Network Structure

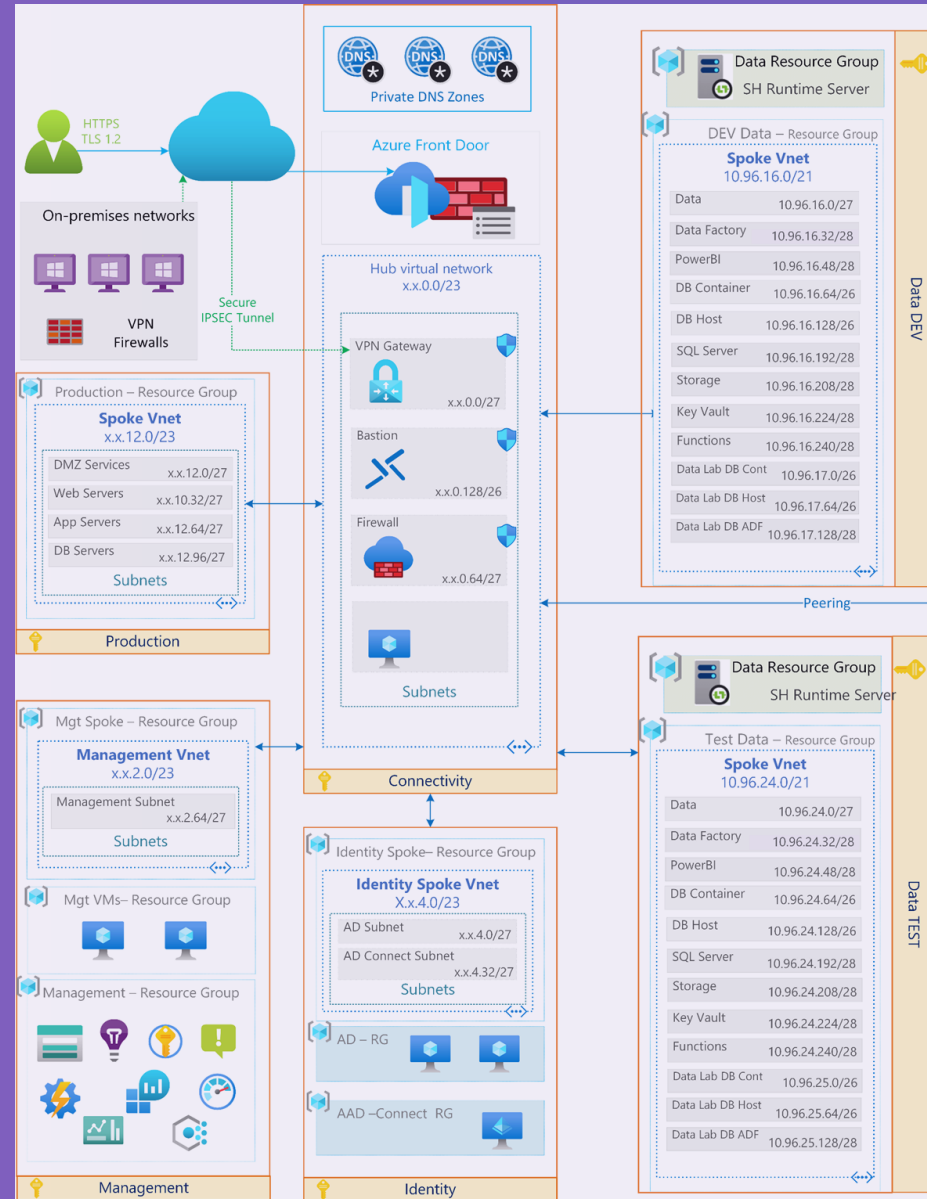
Hub and Spoke

IP Addressing

Connectivity

Network Services

DNS



Azure Platform Landing Zone Accelerator

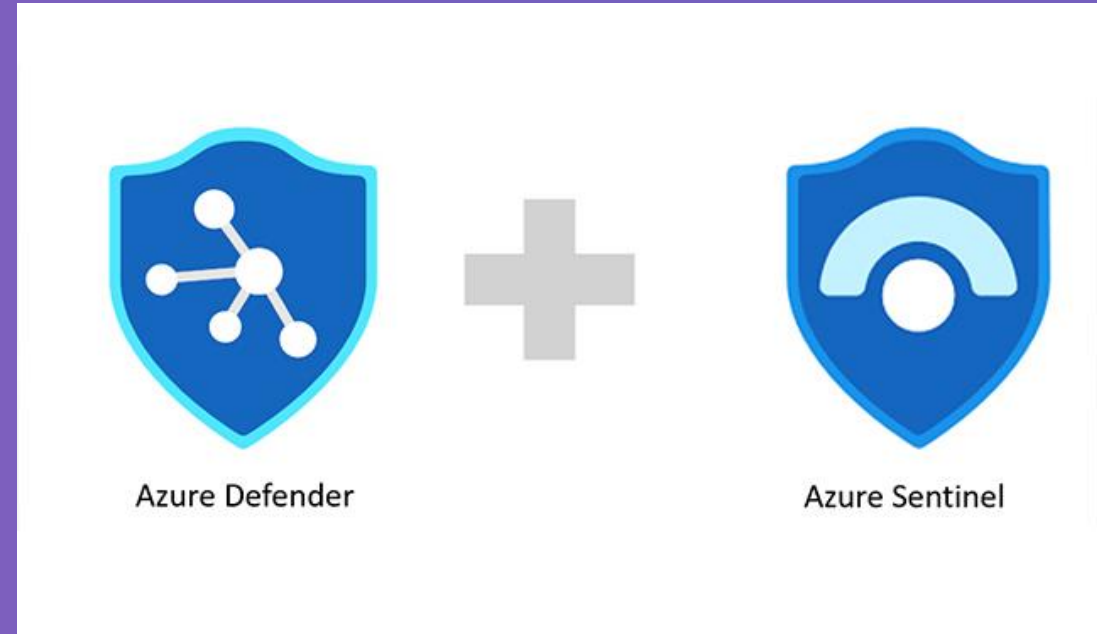
Security

Network Security

Microsoft Defender for Cloud

Azure Policy

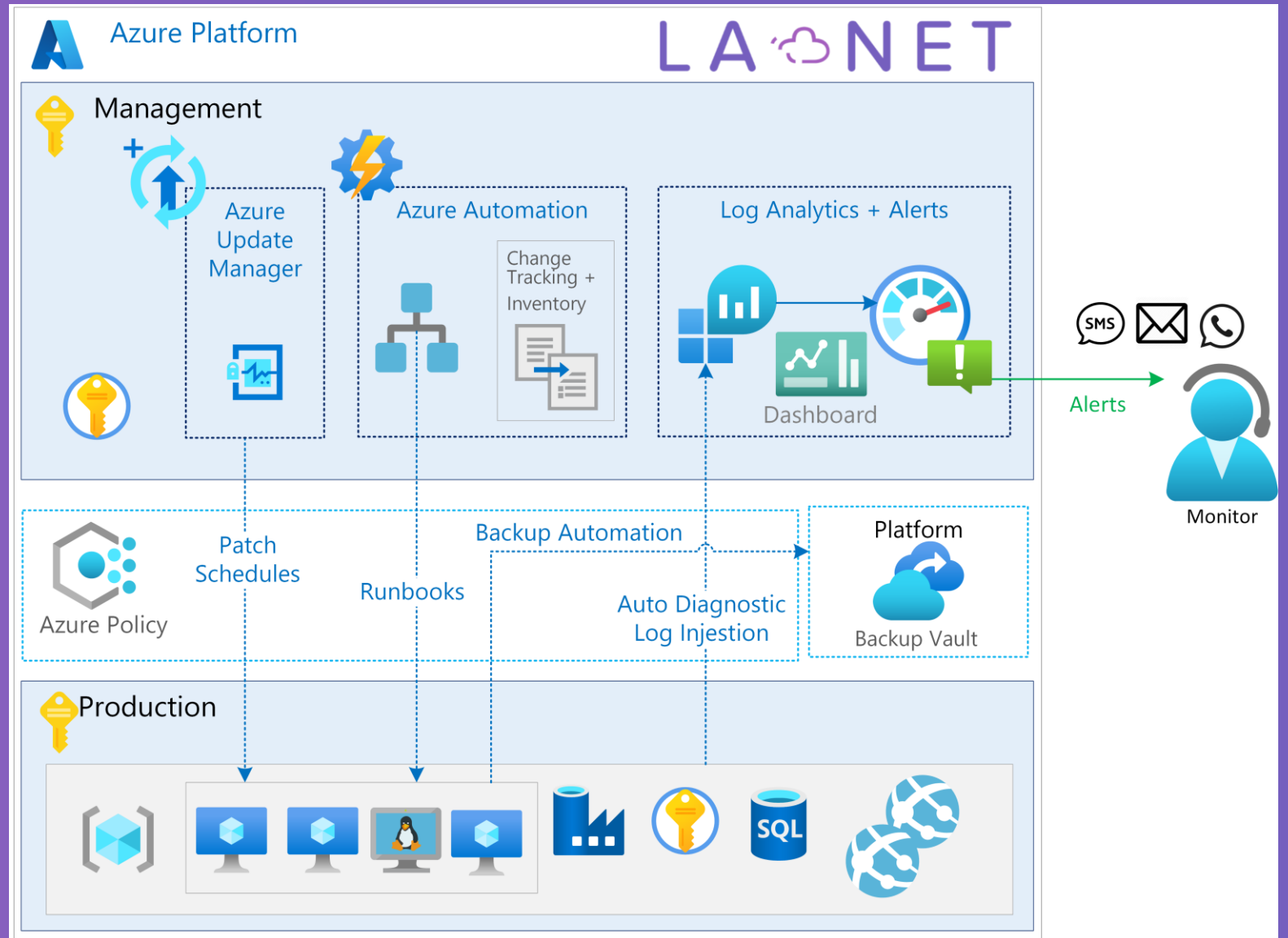
SIEM



Azure Platform Landing Zone Accelerator

Management

- Log Analytics Workspace
- Azure Patch Management
- Automation Account
- Alerts
- Dashboards



Azure Platform Landing Zone Accelerator

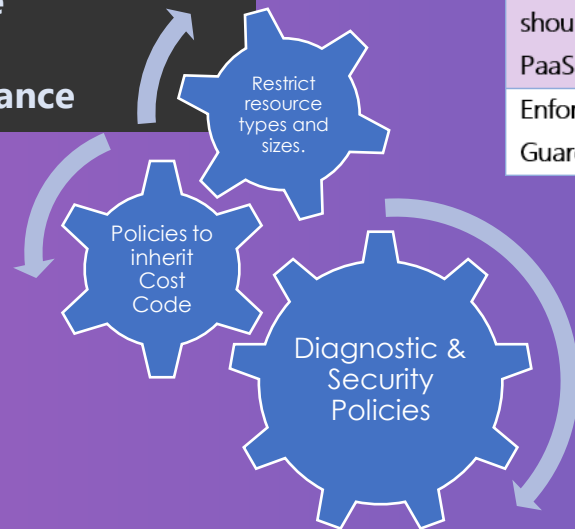
Governance

Microsoft ALZ Baselines Policies

LA NET Custom Policies & Initiatives

Built-In Regulatory Initiatives

- ✓ **Cost Management**
- ✓ **Security Governance**
- ✓ **Environment Compliance**

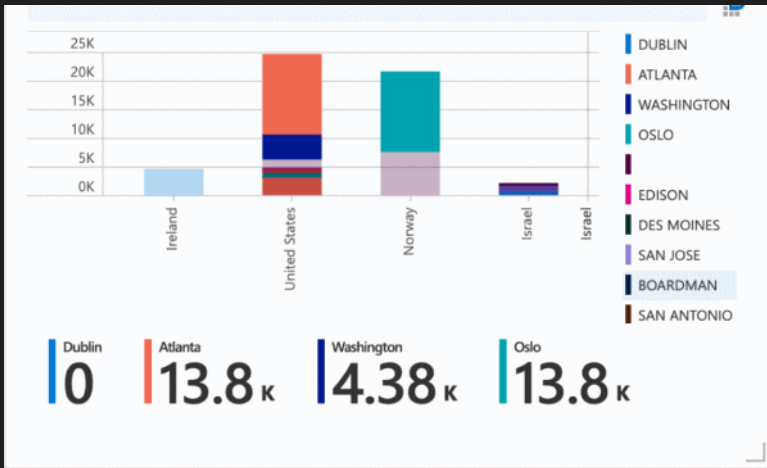


Policy	MG Scope	Description
Deploy Diagnostic Settings to Azure Services	Customer Root	This policy set, deploys the configurations of application Azure resources to forward diagnostic logs and metrics to an Azure Log Analytics workspace.
Deploy Microsoft Defender for Cloud configuration	Customer Root	Configures all the MDFC settings, such as Microsoft Defender for Cloud per individual service, security contacts, and export from MDFC to Log Analytics workspace
Subnets should have a Network Security Group	Platform/Identity	This policy denies the creation of a subnet without a Network Security Group. NSG help to protect traffic across subnet-level.
Public network access should be disabled for PaaS services	Landing Zones/Corp	This policy initiative is a group of policies that prevents creation of Azure PaaS services with exposed public endpoints
Enforce ALZ Sandbox Guardrails	Sandbox	This initiative will help enforce and govern subscriptions that are placed within the Sandbox Management Group.

AZURE LANDING ZONE – BASELINE MONITORING AND ALERTS

Management Systems

- Add Monitoring



Dashboards

Infrastructure

- Platform Activity
- Create / Delete Objects
- Resource Changes
- Azure AD Logs

Networking Activity

- Firewall Rule Changes
- Firewall Service
- Front Door / App GW
- VPN Gateway

Resource Usage

- Database DTU / CPU
- VM CPU / Memory
- Web App



Hourly Alert checks

Virtual Machines

- CPU > 90%
- Memory > 90%
- Disk Space < 15%

SQL Database

- Free Space < 15%
- Failed Connections >2
- DTU Usage > 90%

Web Applications

- Response Times
- Availability

Management and Automation

- Automation Runbook Errors
- Firewall & NSG Changes

Service Health

- Resource Types by Region

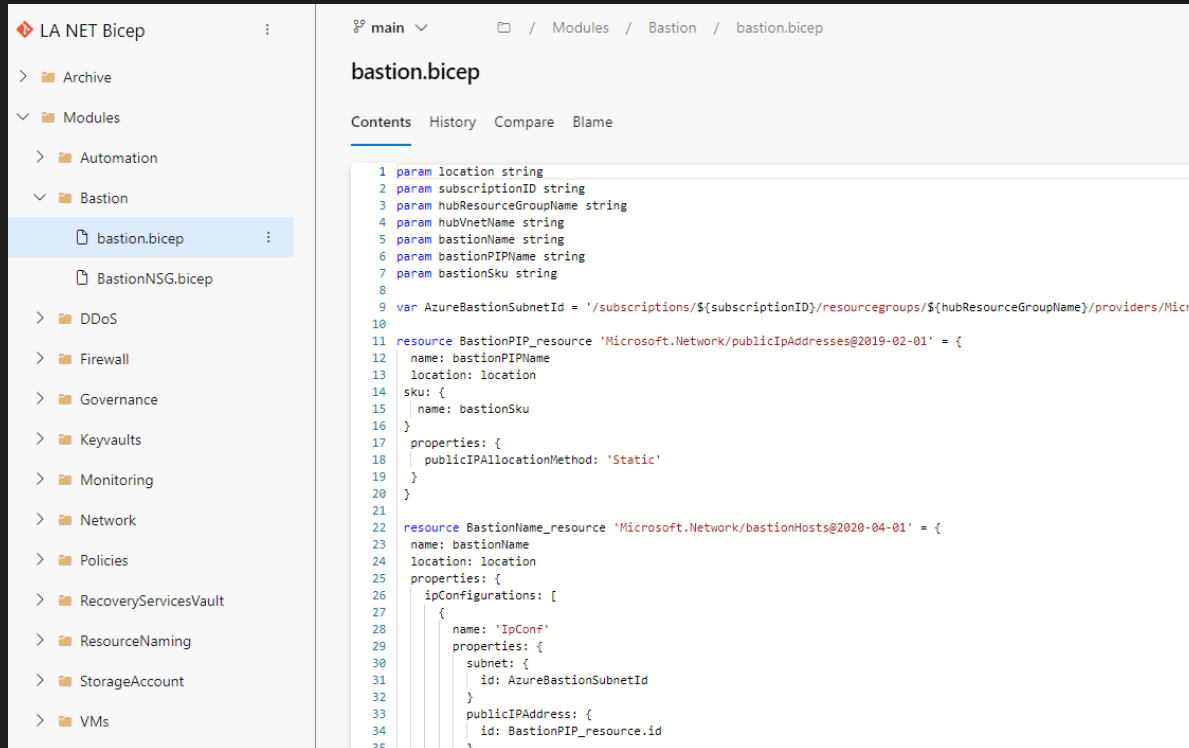
TEST PLAN EXAMPLE

Example of Test Plan for the Landing Zone Deployment

Test ID	Category	Sub Category	Sub Sub Category	Test	Expected result	Pass / Fail
<div style="background-color: #4F81BD; color: white; padding: 5px;"> Customer Environment Tester Name Tester Email Address Test Date </div>						
001	Resource Organisation	Management Groups		Landing Zone MG under root MG	MG exists under Customer Root MG	
002	Resource Organisation	Management Groups		Platform MG under root MG	MG exists under Customer Root MG	
003	Resource Organisation	Management Groups		Connectivity under Platform MG	MG exists under Platform MG	
004	Resource Organisation	Management Groups		Identity under Platform MG	MG exists under Platform Root MG	
005	Resource Organisation	Management Groups		Management under Platform MG	MG exists under Platform Root MG	
006	Resource Organisation	Management Groups		Sandbox MG under root MG	MG exists under Customer Root MG	
007	Resource Organisation	Subscriptions		Connectivity Subscription under Connectivity MG	Subscription exists under Connectivity MG	
008	Resource Organisation	Subscriptions		Identity Subscription under Identity MG	Subscription exists under Identity MG	
009	Resource Organisation	Subscriptions		Management Subscription under Management MG	Subscription exists under Management MG	
010	Network Topology and connectivity	Topology		Hub Vnet in Connectivity Subscription	Hub Vnet is deployed in Connectivity Sub	
011	Network Topology and connectivity	Topology		Identity spoke Vnet in Identity subscription	Identity spoke Vnet is deployed in Identity Sub	
012	Network Topology and connectivity	Topology		Management spoke Vnet in Mgmt subscription	Management spoke Vnet is deployed in Mgmt Sub	
013	Network Topology and connectivity	Topology		Identity spoke peering	Identity spoke is peered to Hub Vnet	
014	Network Topology and connectivity	Topology		Management spoke peering	Management spoke is peered to Hub Vnet	
015	Network Topology and connectivity	Topology				
016	Network Topology and connectivity	Topology				
017	Network Topology and connectivity			Private DNS Zones	Private DNS Zones are deployed and have vnet links to required Vnets.	
018	Network Topology and connectivity	Connectivity		VPN deployment	VPN Gateway and Local gateway are both deployed and have appropriate associations	
019	Management	Inventory and Visibility	Security and Logging	Have all subscriptions for Email for high severity Security incidents		
020	Management	Inventory and Visibility	Security and Logging	Subscriptions are sending Activity Logs to Log Analytics	Enabled through policy	
021	Management	Inventory and Visibility	Security and Logging	NSG Flow Logs enabled and sending logs to LA	Log analytics can query NSG flows and logs are showing in the infra storage account	
022	Management	Inventory and Visibility	Security and Logging	Azure diagnostic services, logs, and metrics, Azure Key Vault audit events, network security group (NSG) flow logs, and event logs	Logs for each resource can be seen in the relevant storage accounts and log analytics workspace	

Deployment and Code

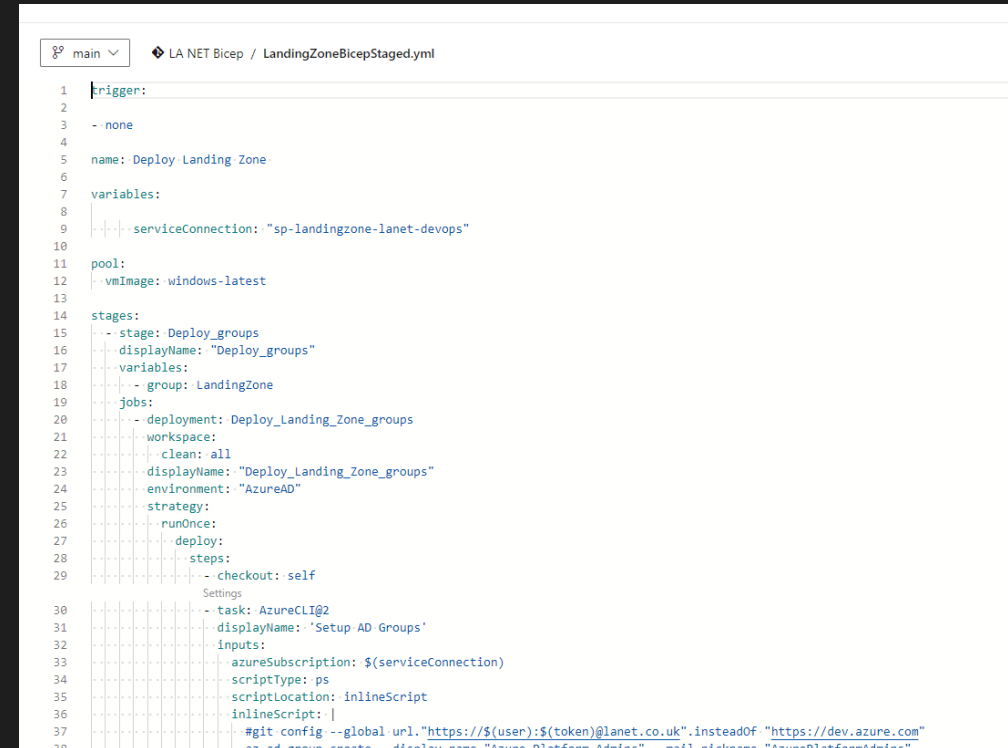
Azure DevOps Repo



The screenshot shows the Azure DevOps web interface for a repository named 'LA NET Bicep'. The left sidebar displays a file tree with folders for 'Archive', 'Modules', 'Automation', 'Bastion', 'DDoS', 'Firewall', 'Governance', 'Keyvaults', 'Monitoring', 'Network', 'Policies', 'RecoveryServicesVault', 'ResourceNaming', 'StorageAccount', and 'VMs'. The 'Bastion' folder is expanded, showing 'bastion.bicep' and 'BastionNSG.bicep'. The main area displays the content of 'bastion.bicep' with the following code:

```
1 param location string
2 param subscriptionID string
3 param hubResourceGroupName string
4 param hubVnetName string
5 param bastionName string
6 param bastionPIPName string
7 param bastionSku string
8
9 var AzureBastionSubnetId = '/subscriptions/${subscriptionID}/resourcegroups/${hubResourceGroupName}/providers/Micro
10
11 resource BastionPIP_resource 'Microsoft.Network/publicIpAddresses@2019-02-01' = {
12   name: bastionPIPName
13   location: location
14   sku: {
15     name: bastionSku
16   }
17   properties: {
18     publicIPAllocationMethod: 'Static'
19   }
20 }
21
22 resource BastionName_resource 'Microsoft.Network/bastionHosts@2020-04-01' = {
23   name: bastionName
24   location: location
25   properties: {
26     ipConfigurations: [
27       {
28         name: 'IpConf'
29         properties: {
30           subnet: {
31             id: AzureBastionSubnetId
32           }
33           publicIPAddress: {
34             id: BastionPIP_resource.id
35           }
36         }
37       }
38     ]
39   }
40 }
```

Azure DevOps Yaml Pipeline



The screenshot shows the Azure DevOps web interface for a pipeline named 'LA NET Bicep / LandingZoneBicepStaged.yml'. The main area displays the content of the pipeline definition with the following code:

```
1 trigger:
2
3   - none
4
5 name: Deploy Landing Zone
6
7 variables:
8
9   - serviceConnection: "sp-landingzone-lanet-devops"
10
11 pool:
12   - vmImage: windows-latest
13
14 stages:
15   - stage: Deploy_groups
16     displayName: "Deploy_groups"
17     variables:
18       - group: LandingZone
19     jobs:
20       - deployment: Deploy_Landing_Zone_groups
21         workspace:
22           clean: all
23         displayName: "Deploy_Landing_Zone_groups"
24         environment: "AzureAD"
25         strategy:
26           runOnce:
27             deploy:
28               steps:
29                 - checkout: self
30                   Settings
31                 - task: AzureCLI@2
32                   displayName: "Setup AD Groups"
33                   inputs:
34                     azureSubscription: $(serviceConnection)
35                     scriptType: ps
36                     scriptLocation: inlineScript
37                     inlineScript: |
38                       #git config --global url."https://$(user):$(token)@lanet.co.uk".insteadOf "https://dev.azure.com"
39                       az ad group create --display-name "Azure Platform Admins" --mail-nickname "AzurePlatformAdmins"
```

Deployment and Code

Azure DevOps Repo

LA NET Bicep

> Archive

Modules

> Automation

Bastion

bastion.bicep

BastionNSG.bicep

> DDoS

> Firewall

> Governance

> Keyvaults

> Monitoring

> Network

> Policies

> RecoveryServicesVault

> ResourceNaming

> StorageAccount

main

Modules / Bastion / bastion.bicep

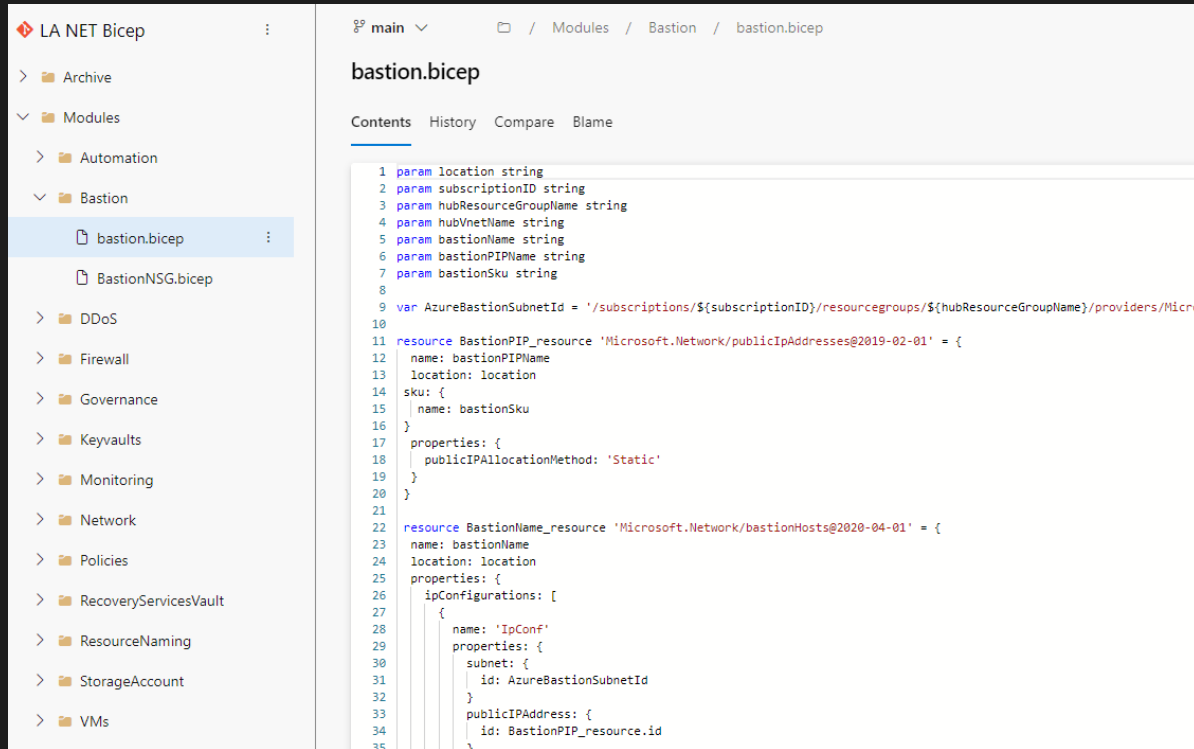
bastion.bicep

Contents History Compare Blame

```
1 param location string
2 param subscriptionID string
3 param hubResourceGroupName string
4 param hubVnetName string
5 param bastionName string
6 param bastionPIPName string
7 param bastionSku string
8
9 var AzureBastionSubnetId = '/subscriptions/${subscriptionID}/resourcegroups/${hubResourceGroupName}/providers/Microso
10
11 resource BastionPIP_resource 'Microsoft.Network/publicIpAddresses@2019-02-01' = {
12   name: bastionPIPName
13   location: location
14   sku: {
15     name: bastionSku
16   }
17   properties: {
18     publicIPAllocationMethod: 'Static'
19   }
20 }
21
22 resource BastionName_resource 'Microsoft.Network/bastionHosts@2020-04-01' = {
23   name: bastionName
24   location: location
25   properties: {
26     ipConfigurations: [
27       {
28         name: 'IpConf'
29         properties: {
30           subnet: {
31             id: AzureBastionSubnetId
32           }
33         }
34       }
35     ]
36   }
37 }
```

Deployment and Code

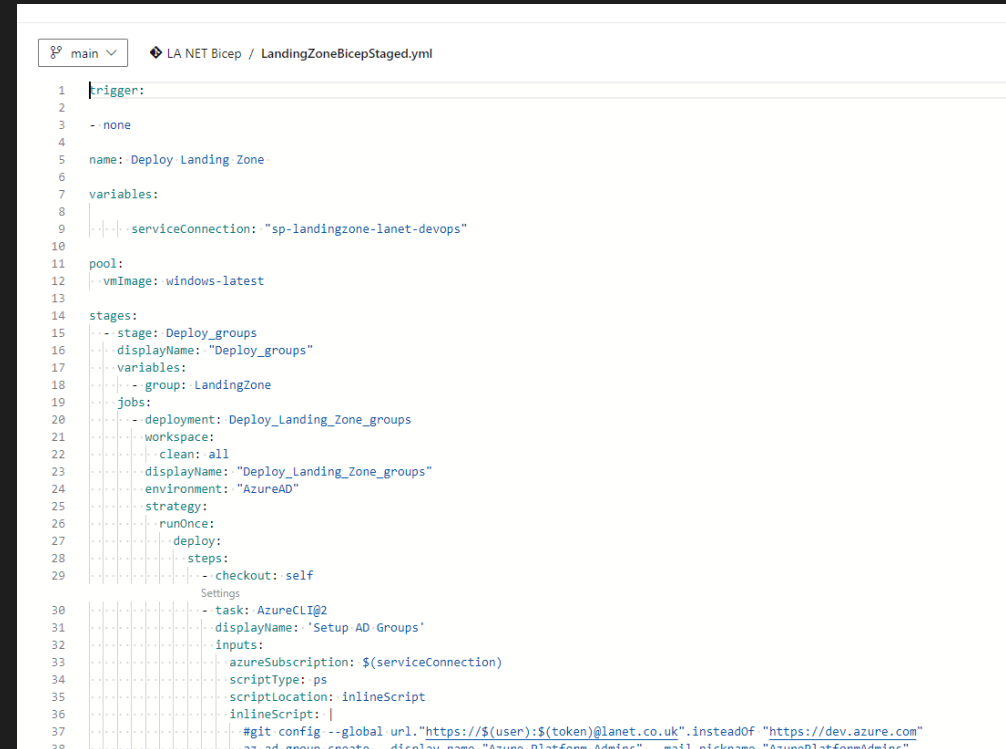
Azure DevOps Repo



The screenshot shows the Azure DevOps web interface for a repository named 'LA NET Bicep'. The left sidebar displays a file tree with folders for 'Archive', 'Modules', 'Automation', 'Bastion', 'DDoS', 'Firewall', 'Governance', 'Keyvaults', 'Monitoring', 'Network', 'Policies', 'RecoveryServicesVault', 'ResourceNaming', 'StorageAccount', and 'VMs'. The 'Bastion' folder is expanded, showing 'bastion.bicep' and 'BastionNSG.bicep'. The main area displays the content of 'bastion.bicep' with the following code:

```
1 param location string
2 param subscriptionID string
3 param hubResourceGroupName string
4 param hubVnetName string
5 param bastionVnetName string
6 param bastionPIPName string
7 param bastionSku string
8
9 var AzureBastionSubnetId = '/subscriptions/${subscriptionID}/resourcegroups/${hubResourceGroupName}/providers/Micro
10
11 resource BastionPIP_resource 'Microsoft.Network/publicIpAddresses@2019-02-01' = {
12   name: bastionPIPName
13   location: location
14   sku: {
15     name: bastionSku
16   }
17   properties: {
18     publicIPAllocationMethod: 'Static'
19   }
20 }
21
22 resource BastionName_resource 'Microsoft.Network/bastionHosts@2020-04-01' = {
23   name: bastionName
24   location: location
25   properties: {
26     ipConfigurations: [
27       {
28         name: 'IpConf'
29         properties: {
30           subnet: {
31             id: AzureBastionSubnetId
32           }
33           publicIPAddress: {
34             id: BastionPIP_resource.id
35           }
36         }
37       }
38     ]
39   }
40 }
```

Azure DevOps Yaml Pipeline



The screenshot shows the Azure DevOps web interface for a pipeline named 'LA NET Bicep / LandingZoneBicepStaged.yml'. The main area displays the content of the pipeline file with the following code:

```
1 trigger:
2
3   - none
4
5 name: Deploy Landing Zone
6
7 variables:
8
9   - serviceConnection: "sp-landingzone-lanet-devops"
10
11 pool:
12   vmImage: windows-latest
13
14 stages:
15   - stage: Deploy_groups
16     displayName: "Deploy_groups"
17     variables:
18       - group: LandingZone
19     jobs:
20       - deployment: Deploy_Landing_Zone_groups
21         workspace:
22           clean: all
23         displayName: "Deploy_Landing_Zone_groups"
24         environment: "AzureAD"
25         strategy:
26           runOnce:
27             deploy:
28               steps:
29                 - checkout: self
30                   Settings
31                 - task: AzureCLI@2
32                   displayName: "Setup AD Groups"
33                   inputs:
34                     azureSubscription: $(serviceConnection)
35                     scriptType: ps
36                     scriptLocation: inlineScript
37                     inlineScript: |
38                       #git config --global url."https://$(user):$(token)@lanet.co.uk".insteadOf "https://dev.azure.com"
39                       az ad group create --display-name "Azure Platform Admins" --mail-nickname "AzurePlatformAdmins"
```

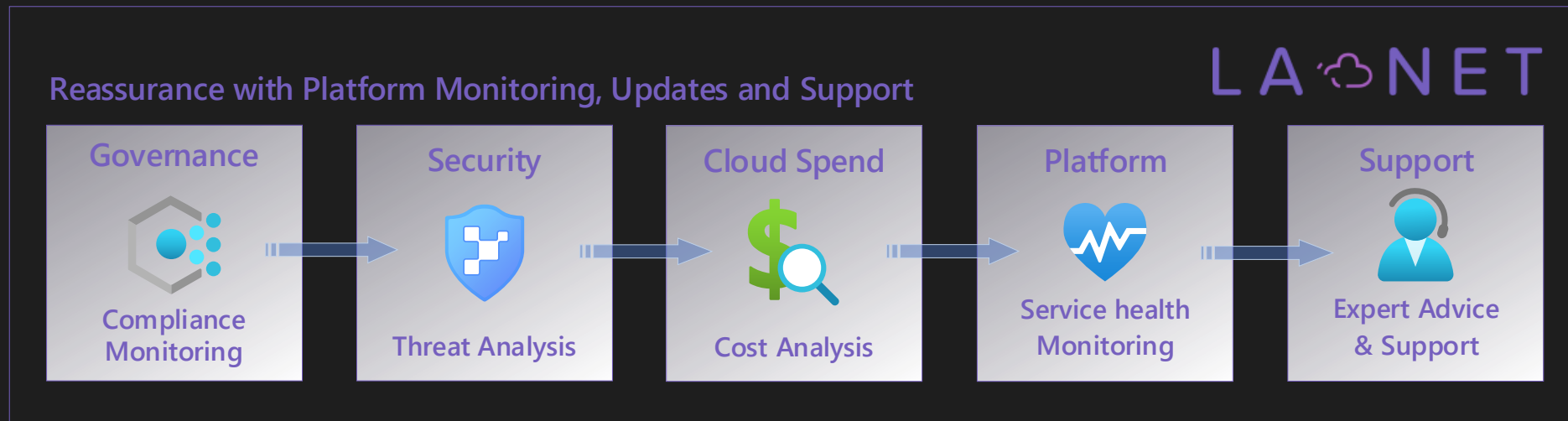

Deployment and Code

Azure DevOps YamI Pipeline

```
main ▾ LA NET Bicep / LandingZoneBicepStaged.yml
1 trigger:
2
3   - none
4
5   name: Deploy Landing Zone
6
7   variables:
8
9     - serviceConnection: "sp-landingzone-lanet-devops"
10
11   pool:
12     vmImage: windows-latest
13
14   stages:
15     - stage: Deploy_groups
16       displayName: "Deploy_groups"
17       variables:
18         - group: LandingZone
19       jobs:
20         - deployment: Deploy_Landing_Zone_groups
21           workspace:
22             clean: all
23             displayName: "Deploy_Landing_Zone_groups"
24             environment: "AzureAD"
25             strategy:
26               runOnce:
27                 deploy:
28                   steps:
29                     - checkout: self
30                       Settings
31                     - task: AzureCLI@2
32                       displayName: 'Setup AD Groups'
33                       inputs:
34                         azureSubscription: $(serviceConnection)
```

Managed Services

- Keep Code and Documentation up to date
- Update with new policies and platform changes
- Maintenance and updates of resources and Automation
- Advise on cost, security & architecture
- Review compliance and security
- Proactive monitoring



AZURE LANDING ADMINISTRATION – TRAINING LINKS

Badges	Role + Exam Code	Comments and job role	Cert Level	Learning Plans and Links
	Azure Fundamentals AZ-900	Fundamentals can be useful for someone with no experience. Role = 1st line Azure Support	Azure Fundamentals	https://docs.microsoft.com/en-us/learn/certifications/azure-fundamentals/
	Azure Administrator Associate AZ-104	Base Starting Point should be Azure Administrator. Role = Azure Administrator	Azure Administrator Associate	https://docs.microsoft.com/en-us/learn/certifications/roles/administrator
	Azure Solutions Architect Expert AZ-305	Advisable for those managing and architecting Azure solutions. Certification with experience is a <i>must</i> to do this role properly. Role = Azure Architect	Azure Administrator Associate	https://docs.microsoft.com/en-us/learn/roles/solutions-architect
	Azure Security Engineer AZ-500	For organisations that require a good understanding and ability to manage security aspects. Role = Azure Security Engineer	Azure Security Engineer Associate	https://docs.microsoft.com/en-us/learn/roles/security-engineer
	Azure Network Engineer AZ-700	For organisations that make heavy use of Azure networking services such as VPN, ExpressRoute, Peering, Azure Firewall, App Gateway, Traffic Manager etc.	Azure Network Engineer Associate	https://learn.microsoft.com/en-us/certifications/azure-network-engineer-associate/

AZURE LANDING ZONE – KNOWLEDGE TRANSFER

Typically: 2 x two-hour training workshops

Customer Stakeholders

- Representatives from Network, Security, and Infrastructure teams
- Project Owner/s

Part 1 - Management

- Azure Policy
- Monitoring with Azure Log Analytics
- Azure Automation
- VM Builds

Part 2 - Networking

- Azure Networking
- Bastion > Management Servers
- NSGs, Azure Firewall Policies
- VPN and Connectivity

Design Decisions

Regional Requirements and Management

- Allowed Regions – Scope of Rule
- Log Analytics Workspace
- Management Servers
- Microsoft Defender for Cloud

Security and Compliance

- Azure Bastion
- Application Gateway
- Azure Front Door
- Azure Firewall
 - SKU – Standard vs Premium
- DDoS protection Standard Plans Vs IP Protection
- Policy Initiatives
- Microsoft Defender for Cloud

Design Decisions

Azure Billing and Entra ID Tenant

- Tenant ID and Entra ID Domain Name
- Subscriptions

Access and Identity Management

- Customer Tenant User IDs for Deployment teams or invite to Entra ID?
- Any Active Directory Considerations or Requirements?
 - ADDS, Domain Controllers etc

Networking topology and Connectivity

- VNet IP addressing - /16 Per Region
 - **Must not overlap with any existing networks**
- On-Premises access from Azure and Vice Versa
- On Prem <> Azure Name Resolution
- VPN Vs ExpressRoute

Design Decisions

VM Configuration

- Management Servers
- VM Configuration and Management
 - “Encryption At Host” with Trusted Launch and vTPM Enabled.
 - All VMs to be Gen 2 only
 - Patching – Azure Update Management Solution
- AV – Azure Anti-Malware Extension + Microsoft ATP
- VM Internet Access
 - Native, Yes / No, Azure Firewall, NAT Gateway
- Disk Configuration
 - Standard SSD, OS Drives 128GB read/write caching enabled
 - DC’s Data Drive with caching set to “None”



Summary

At LA NET, we believe in doing what is right for the customer and not for the cloud vendor or ourselves. We specialise in Azure infrastructure which allows us to keep up to date on the latest updates and features. This ensures our customers are always up to date and have the best possible Azure cloud infrastructure environment.

LA  NET