Microsoft Azure

A multi-subscription Azure system that takes into account scale, security governance, networking, and identity produces an Azure landing zone. Application modernization, innovation, and migration at enterprise scale in Azure are made possible by an Azure landing zone.

A landing zone provides a consistent and repeatable approach to setting up and managing Azure resources. It typically includes the following key components:

- **Subscription and Governance:**
  Landing zones define the structure and organization of Azure subscriptions, resource groups, and management groups. It establishes policies and governance controls for resource provisioning, access management, compliance, and monitoring.

- **Network Topology:**
  Landing zones define the network architecture and connectivity between resources. It includes the setup of virtual networks, subnets, network security groups, and connectivity to on-premises networks or other cloud environments.

- **Identity and Access Management (IAM):**
  Landing zones establish a framework for managing user identities, access control, and authentication mechanisms. It incorporates Azure Active Directory (Azure AD) for identity management and role-based access control (RBAC) for granting permissions to Azure resources.

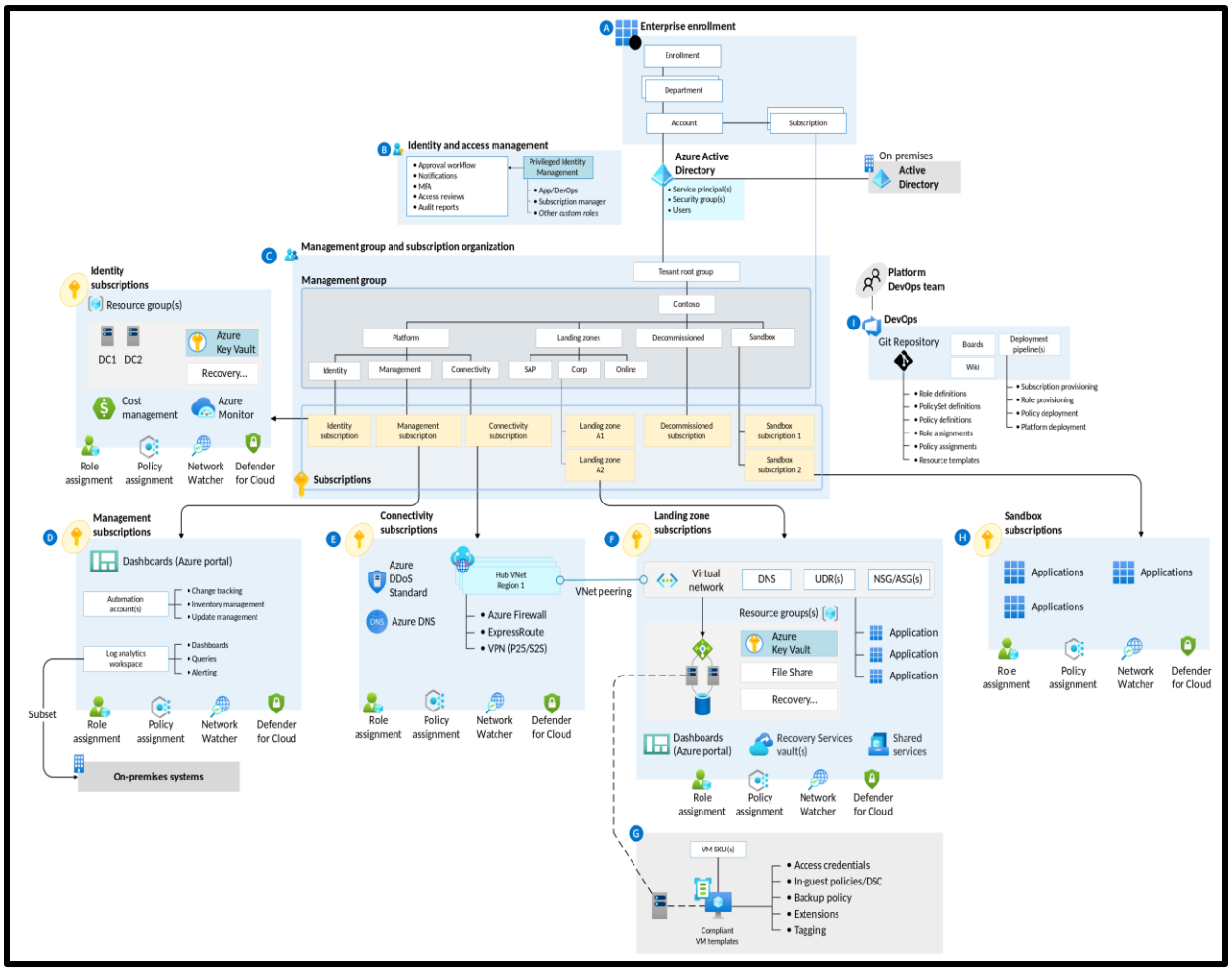
- **Security and Compliance:**
  Landing zones implement security controls and best practices for protecting Azure resources and data. It includes features such as Azure Security Center, Azure Firewall, Azure DDoS Protection, and compliance frameworks like Azure Policy and Azure Blueprints.

- **Resource Hierarchy and Resource Management:**
  Landing zones define the structure and organization of Azure resources using resource groups, tags, and naming conventions. It establishes guidelines for resource deployment, management and lifecycle management.

Levels of Azure Landing Zone:

- **Level 100**
- **Level 200**
- **Level 300**
- **Level 400**

Azure Landing Zone Design Areas and Conceptual Architecture



Level 100:

Azure Landing Zone Level 100 refers to an introductory or beginner-level understanding of Azure landing zones. At this level, you can expect to learn the fundamental concepts and components of Azure landing zones, providing a starting point for further exploration and understanding.

Level 200:

Azure Landing Zone Level 200 builds upon the foundational knowledge gained at Level 100 and delves deeper into the intermediate concepts and practices related to Azure landing zones. At this level, you can expect to explore more advanced topics and gain a more comprehensive understanding of designing, deploying, and managing landing zones in Azure.

Here are some key aspects typically covered at Azure Landing Zone Level 200:

- **Landing Zone Design Patterns:**
  Learn about different design patterns and architectural considerations for implementing landing zones based on specific organizational requirements, such as multi-subscription, multi-region, or hybrid cloud scenarios.

- **Landing Zone Automation:**
  Explore the automation capabilities available in Azure for provisioning and managing landing zones. Understand how to leverage tools like Azure Resource Manager Templates, Azure CLI, Azure PowerShell, and Azure DevOps to automate the deployment and configuration of landing zones.

- **Advanced Networking:**
  Dive deeper into networking concepts within a landing zone, such as virtual network peering, network security groups (NSGs), Azure ExpressRoute, and Azure Virtual WAN. Gain an understanding of advanced connectivity options and network segmentation strategies.

- **Advanced Identity and Access Management:**
  Extend your knowledge of Azure Active Directory (Azure AD) and advanced identity and access management scenarios within a landing zone. Learn about Azure AD Connect for hybrid identity, conditional access policies, and implementing Azure AD Privileged Identity Management (PIM).

- **Security and Compliance Best Practices:**
  Explore advanced security practices and strategies for securing resources within a landing zone. Cover topics like Azure Security Center advanced threat protection, Azure Monitor for logging and monitoring, Azure Key Vault for

secrets management, and implementing security baselines and compliance frameworks.

- **Governance and Cost Management:**
  Gain insights into advanced governance practices for managing and controlling resources in a landing zone. Understand how to implement Azure Policy for policy enforcement, Azure Cost Management and Billing for cost optimization, and resource tagging strategies for better resource management.

At Level 200, the focus is on building upon the foundational knowledge and expanding into more advanced topics related to Azure landing zones. It aims to equip individuals with the expertise needed to design and implement scalable, secure, and well-governed landing zones in Azure.

Level 300:

Azure Landing Zone Level 300 represents an advanced level of understanding and expertise in designing, deploying, and managing Azure landing zones. At this level, you can expect to explore complex scenarios, advanced configurations, and optimization techniques to build highly scalable and resilient landing zones in Azure.

Here are some key aspects typically covered at Azure Landing Zone Level 300:

- **Landing Zone Architecture:**
  Dive deeper into landing zone architecture design principles, including considerations for scalability, high availability, disaster recovery, and fault tolerance. Explore advanced concepts such as hub-and-spoke architecture, global peering, and load balancing.

- **Infrastructure as Code (IaC):**
  Deepen your understanding of Infrastructure as Code practices for provisioning and managing landing zones. Learn advanced techniques using Azure Resource Manager templates, Azure Bicep, Terraform, or other IaC tools to enable repeatable and automated deployments.

- **Advanced Networking and Connectivity:**
  Explore advanced networking capabilities and scenarios within a landing zone. This may include implementing Azure Virtual WAN for global connectivity, integrating with Azure Firewall, leveraging Azure Front Door for content delivery, or setting up advanced VPN or Express Route configurations.

- **Identity and Access Management (IAM) Federation:**

  Extend your knowledge of IAM by exploring federation scenarios, including integrating Azure AD with on-premises Active Directory or other identity providers. Learn advanced identity federation techniques such as Azure AD Connect, Azure AD Application Proxy, or Azure AD B2B/B2C.

- **Security and Compliance Governance:**

  Deep dive into advanced security and compliance governance practices within a landing zone. This may include implementing advanced threat protection features, configuring Azure Security Center policies, setting up advanced monitoring and alerting, implementing data encryption, or applying industry-specific compliance standards.

- **Advanced Resource Management and Automation:**

  Explore advanced techniques for managing resources within a landing zone. This may include custom role definitions and RBAC assignments, implementing Azure Policy initiatives, advanced resource tagging strategies, or leveraging Azure Automation for continuous deployment and management.

At Level 300, the focus is on mastering advanced concepts and techniques related to Azure landing zones. It aims to equip individuals with the skills necessary to design, deploy, and manage highly scalable, secure, and resilient landing zones in complex enterprise scenarios.

Level 400:

Azure Landing Zone Level 400 represents an expert level of understanding and proficiency in designing, deploying, and managing Azure landing zones. At this advanced level, you can expect to explore highly specialized and intricate topics, focusing on optimizing performance, achieving advanced governance, and implementing advanced cloud-native architectures.

Here are some key aspects typically covered at Azure Landing Zone Level 400:

- **Advanced Landing Zone Architectures:**

  Explore advanced architectural patterns and strategies for landing zones, such as serverless architectures, microservices, event-driven architectures, and containerized deployments using Azure Kubernetes Service (AKS). Learn how to optimize for performance, scalability, and cost efficiency.

- **Advanced Networking and Hybrid Connectivity:**

Deepen your knowledge of advanced networking and hybrid connectivity scenarios within a landing zone. This may include implementing Azure Virtual Network peering across regions, connecting multiple Azure AD tenants, integrating with Azure Private Link, or setting up advanced hybrid networking configurations with Azure ExpressRoute or Azure Arc.

- **Advanced Security and Compliance:**
  Dive into advanced security and compliance practices within a landing zone. Explore topics such as Azure Sentinel for advanced threat detection and response, Azure Information Protection for data classification and protection, Azure Security Center's advanced features and integration with third-party tools, and achieving industry-specific compliance certifications.

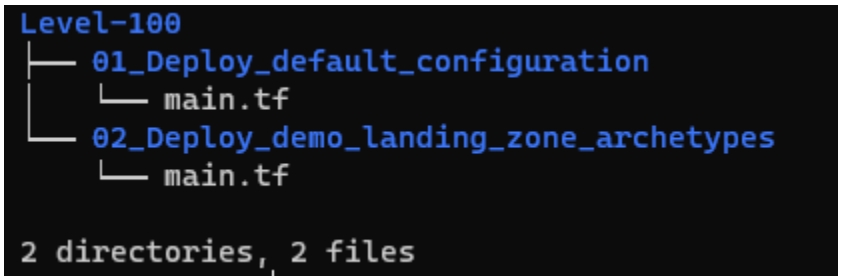
- **Governance at Scale:**
  Learn advanced governance techniques for managing and governing resources at scale within a landing zone. This may involve implementing Azure Management Groups and Azure Policy initiatives for large-scale deployments, designing and implementing custom RBAC roles, and establishing complex resource hierarchy and subscription structures.

- **DevOps and CI/CD Integration:**
  Explore advanced DevOps practices and continuous integration/continuous deployment (CI/CD) workflows within a landing zone. Learn how to implement advanced release management strategies, use Azure DevOps or other CI/CD tools for automated deployments, and integrate infrastructure deployments with application deployments.

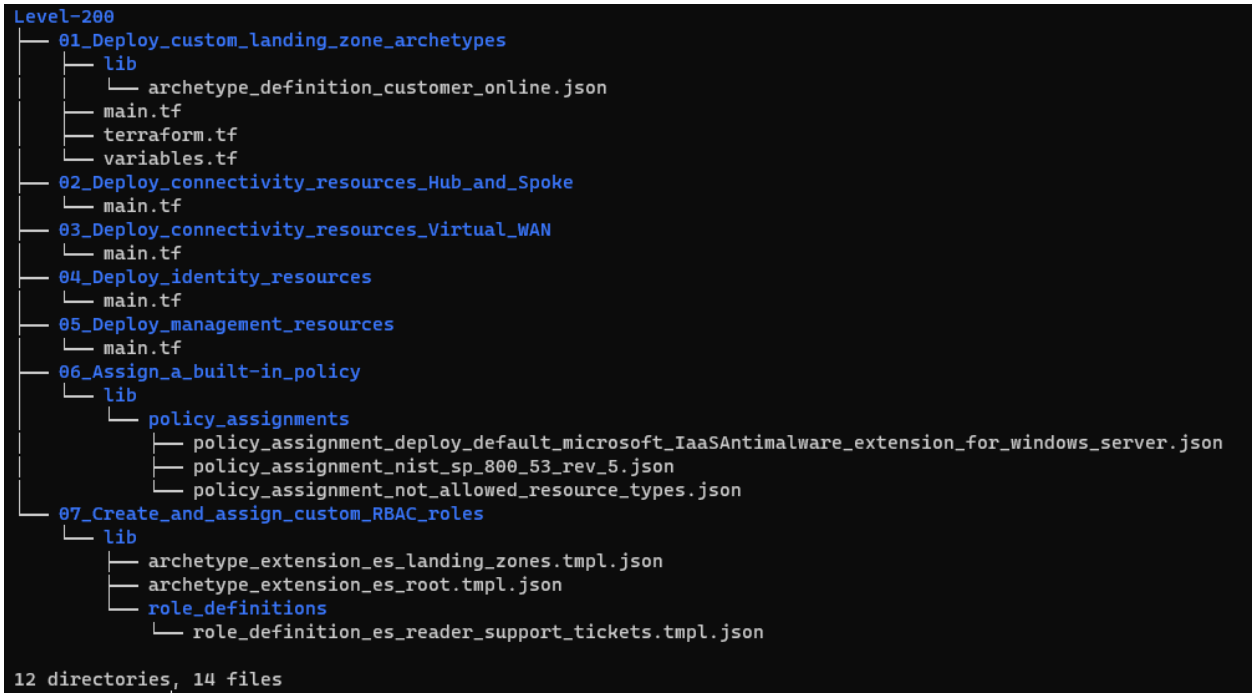
- **Advanced Monitoring and Analytics:**
  Deep dive into advanced monitoring and analytics capabilities within a landing zone. This may include leveraging Azure Monitor, Log Analytics, and Azure Application Insights for advanced monitoring, implementing advanced alerting and autoscaling based on custom metrics, and utilizing Azure Data Explorer for real-time analytics.

At Level 400, the focus is on acquiring expert-level knowledge and skills in designing, deploying, and managing highly advanced and complex Azure landing zones. It prepares individuals to tackle intricate challenges and optimize landing zones for performance, scalability, security, and cost efficiency in enterprise-scale environments.

Tree Structure of Level 100:



Tree Structure of Level 200:



Tree Structure of Level 300:

```
Level-300
├── 01-Deploy connectivity resources with custom settings (Hub and Spoke)
├── 01_Deploy_connectivity_resources_with_custom_settings_(Hub_and_Spoke)
│   ├── Deploy Connectivity Resources With Custom Settings.pdf
│   ├── main.tf
│   ├── settings.connectivity.tf
│   ├── terraform.tf
│   └── variables.tf
├── 02_Deploy_connectivity_resources_with_custom_settings_(Virtual_WAN)
│   ├── VWAN.pdf
│   ├── main.tf
│   ├── settings.connectivity.tf
│   ├── terraform.tf
│   └── variables.tf
├── 03_Deploy_identity_resources_with_custom_settings
│   ├── Identity-Resources.pdf
│   ├── main.tf
│   ├── settings.identity.tf
│   ├── terraform.tf
│   └── variables.tf
├── 04_Deploy_management_resources_with_custom_settings
│   ├── Deploy Management Resources With Custom Settings.pdf
│   ├── main.tf
│   ├── settings.management.tf
│   ├── terraform.tf
│   └── variables.tf
├── 05_Expand_built_in_archetype_definitions
│   ├── extended-archetypes.pdf
│   ├── lib
│   │   ├── archetype_exclusion_es_landing_zones.tmpl.json
│   │   └── archetype_extension_es_landing_zones.tmpl.json
│   └── main.tf
├── 06_Create_custom_policies_,_policy_sets_and_assignments
│   ├── Custom-Policies-Policy-Sets-and-Assignments.pdf
│   └── lib
│       ├── policy_assignments
│       │   ├── policy_assignment_es_deny_nic_nsg.json
│       │   ├── policy_assignment_es_enforce_mandatory_tagging.json
│       │   ├── policy_assignment_es_enforce_resource_tags.json
│       │   └── policy_assignment_es_enforce_rg_tags.json
│       ├── policy_definitions
│       │   ├── policy_definition_es_deny_nic_nsg.json
│       │   ├── policy_definition_es_enforce_resource_tags.json
│       │   └── policy_definition_es_enforce_rg_tags.json
│       └── policy_set_definitions
│           └── policy_set_definition_enforce_mandatory_tagging.json
├── 07_Override_module_role_assignments
│   ├── Override Module Role Assignments.pdf
│   ├── lib
│   │   ├── archetype_definitions
│   │   │   └── archetype_definition_customer_online.json
│   │   └── policy_assignments
│   │       ├── policy_assignment_dhh_policy_set_definition.json
│   │       └── policy_assignment_dsa_policy_set_definition.json
│   ├── main.tf
│   ├── terraform.tf
│   └── variables.tf
├── 08_Deploy_policies_without_enforcing_them
│   ├── Deploy policies without enforcing them.pdf
│   ├── archetype_config_overrides.tf
│   ├── main.tf
│   ├── terraform.tf
│   └── variables.tf
└── 09_Combined_Deployment_of_Management_and_Connectivity_Resources_individual_subscriptions
    ├── Combine Deployment Of Connectivity And Management Resources In Individual Subscription.pdf
    ├── main.tf
    ├── settings.connectivity.tf
    ├── settings.management.tf
    ├── terraform.tf
    └── variables.tf

18 directories, 51 files
```

Tree Structure of Level 400:

```
Level-400
├── 01_Deploy_using_module_nesting
│   ├── Deploy Using Module Nesting.pdf
│   ├── lib
│   │   └── archetype_definition_customer_online.json
│   ├── main.tf
│   ├── terraform.tf
│   └── variables.tf
├── 02_Deploy_using_multiple_module_declarations_with_orchestration
│   ├── Deploy using multiple module declarations with orchestration.pdf
│   └── root_module
│       ├── main.tf
│       ├── modules
│       │   ├── connectivity
│       │   │   ├── main.tf
│       │   │   ├── output.tf
│       │   │   ├── settings.connectivity.tf
│       │   │   └── variables.tf
│       │   ├── core
│       │   │   ├── lib
│       │   │   │   └── archetype_definition_customer_online.json
│       │   │   ├── main.tf
│       │   │   ├── settings.core.tf
│       │   │   ├── settings.identity.tf
│       │   │   └── variables.tf
│       │   └── management
│       │       ├── main.tf
│       │       ├── output.tf
│       │       ├── settings.management.tf
│       │       └── variables.tf
│       └── variables.tf
└── 03_Deploy_using_multiple_module_declarations_with_remote_state
    ├── Deploy using multiple module declarations with remote state.pdf
    ├── connectivity
    │   ├── main.tf
    │   ├── output.tf
    │   ├── settings.connectivity.tf
    │   └── variables.tf
    ├── core
    │   ├── lib
    │   │   └── archetype_definition_customer_online.json
    │   ├── main.tf
    │   ├── remote.tf
    │   ├── settings.core.tf
    │   ├── settings.identity.tf
    │   └── variables.tf
    └── management
        ├── main.tf
        ├── output.tf
        ├── settings.management.tf
        └── variables.tf

14 directories, 36 files
```

--END--