



Global Azure Bootcamp 2019

Azure Governance & Security Hardening

Agenda

- Management Groups – how to better structure your tenant.
 - DEMO –Management Groups.
- Azure Policy – enforce resource compliance.
 - DEMO – Azure Policy.
- Azure Blueprints – compliance at scale.
- Azure Key Vault – SSL Certificate management.
 - DEMO – Key Vault & SSL certificates.
- Azure Key Vault – Credentials & Encryption keys management.
 - DEMO – VM, SQL and Storage Account BYOK encryption.
 - DEMO – Azure Policy Compliance Monitoring.
- Questions.

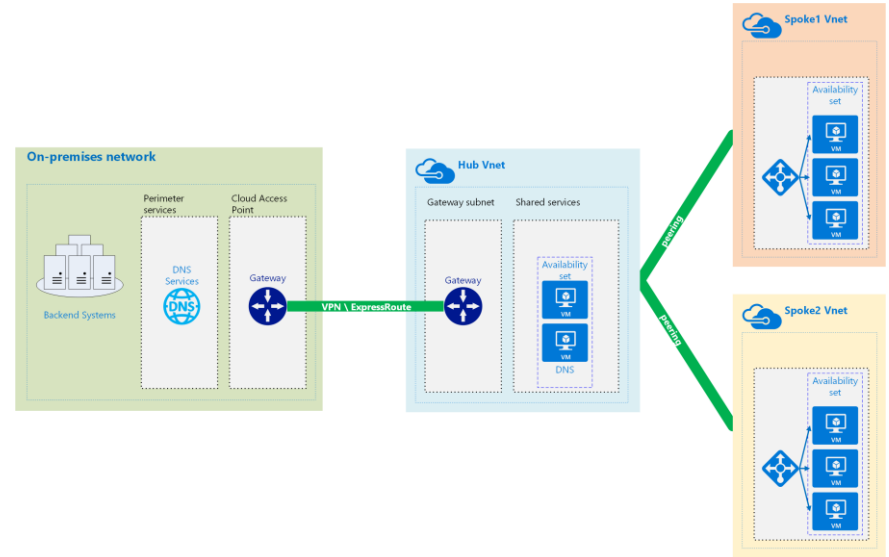
About Me

- Fabien Gilbert – fabien.gilbert@appliedis.com
- 12+ years in IT Consulting in France and in the US.
- Currently Cloud Infrastructure Consultant with AIS.
- Help clients on their journey to the Cloud.



Nice-to-haves

- ✓ Familiarity with Hub & Spoke Topology.
- ✓ Experience with Role Based Access Control.
- ✓ Understanding on Identity & Access Management
- ✓ PowerShell scripting experience.



Azure tools for IT Governance



Management Groups



Policy

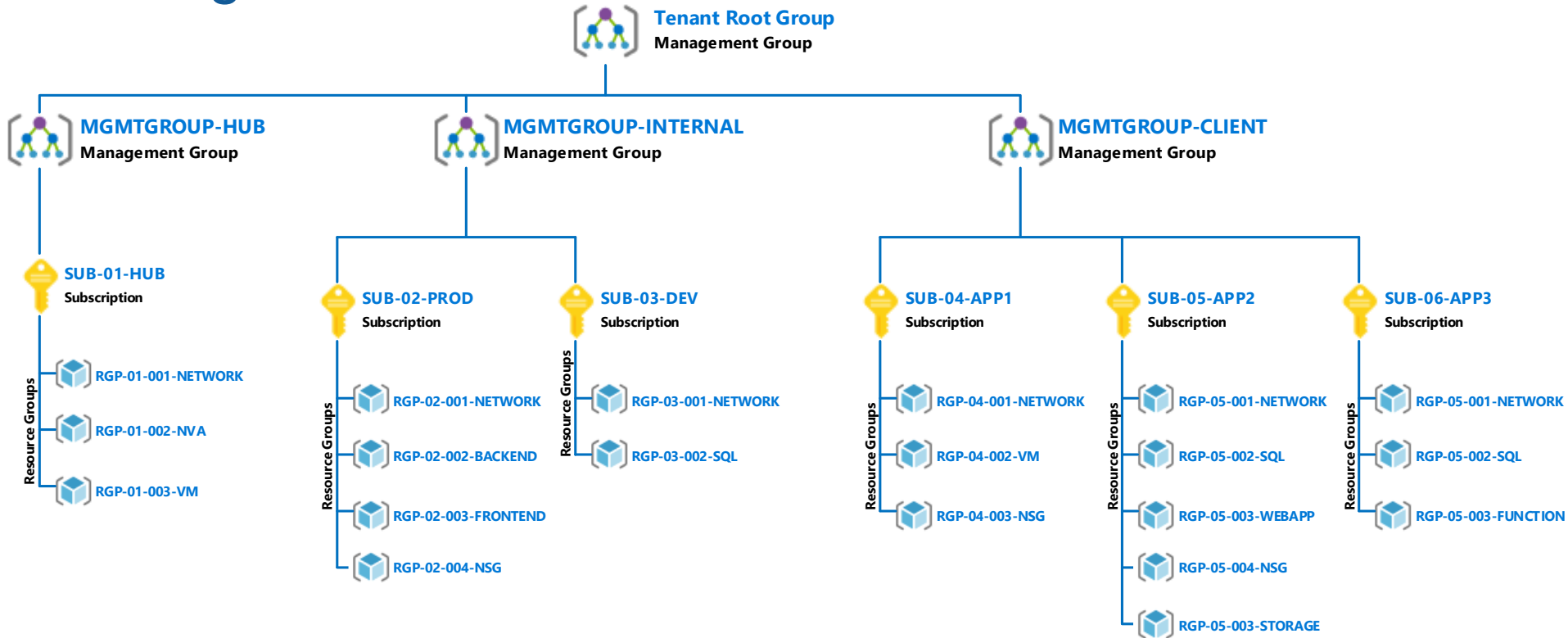


Blueprints

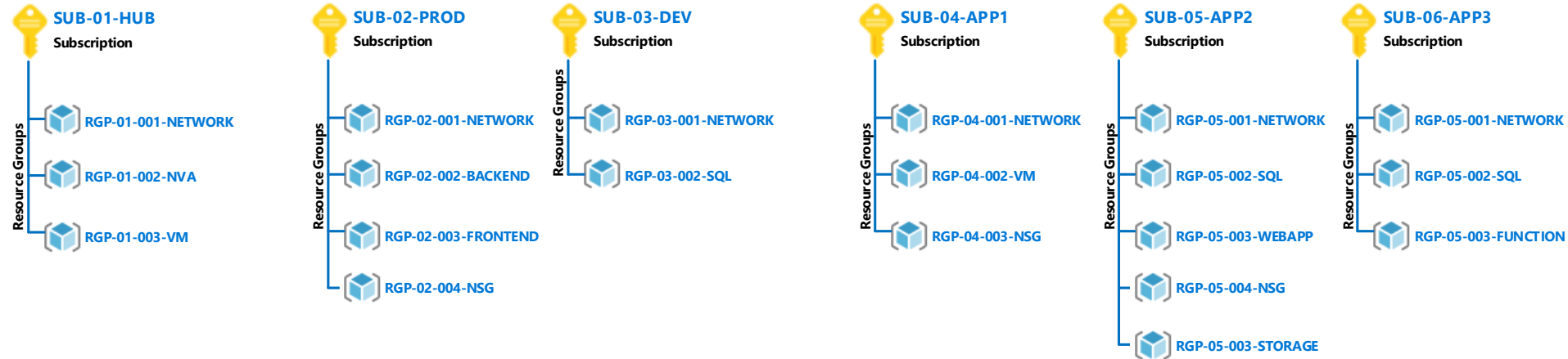


Key Vault

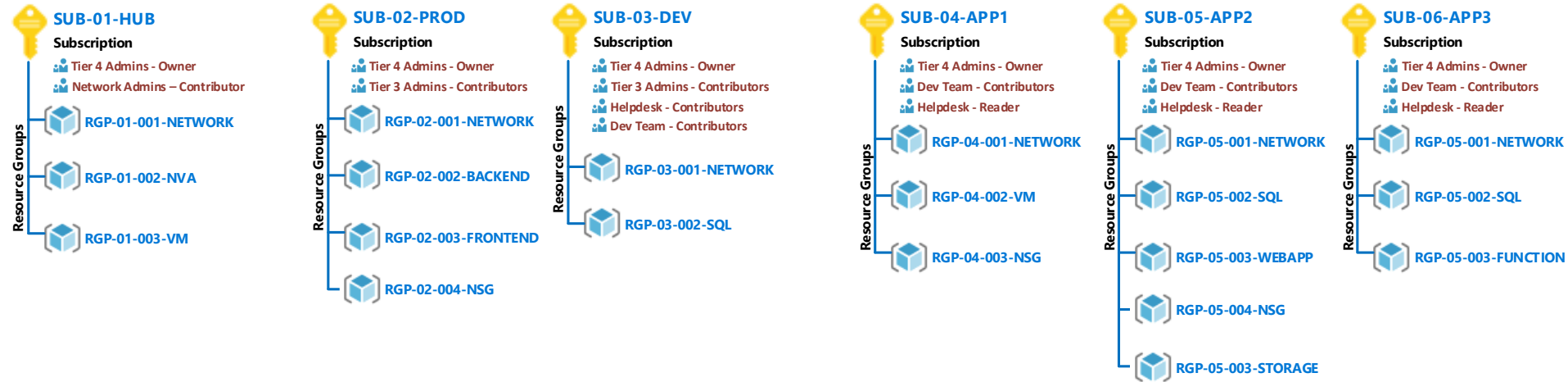
Management Groups



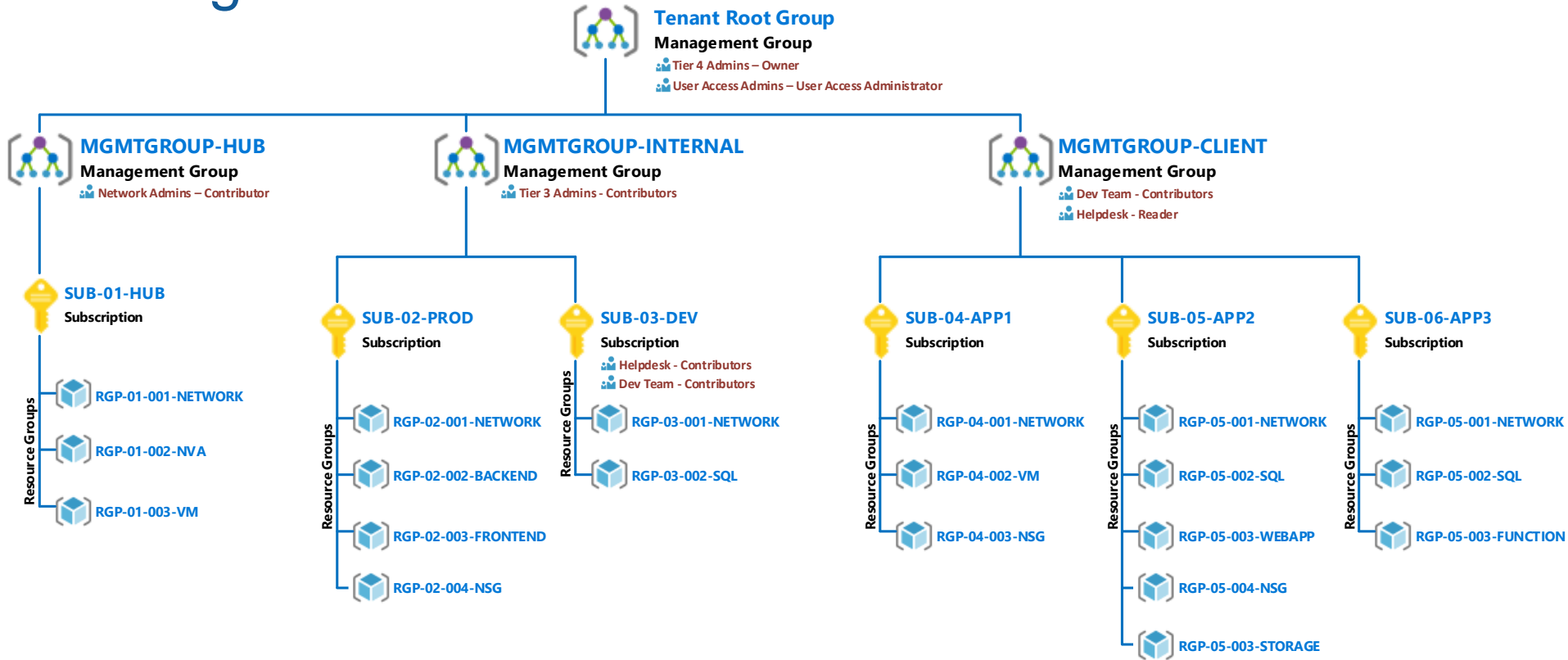
Management Groups



Management Groups



Management Groups





Azure Management Groups

Demo

- Management Groups in the Portal.
- Management Group script creation.
- Management Group child subscription assignment.
- Management Group Role Assignments.

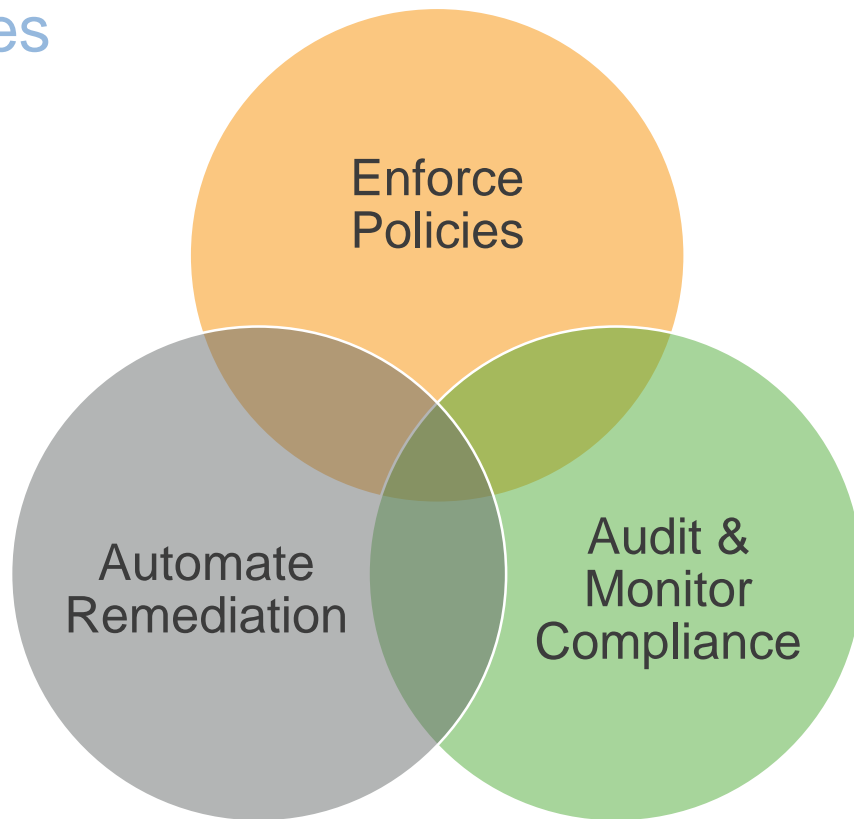


<https://github.com/FabienGilbert/AzureBootcamp>



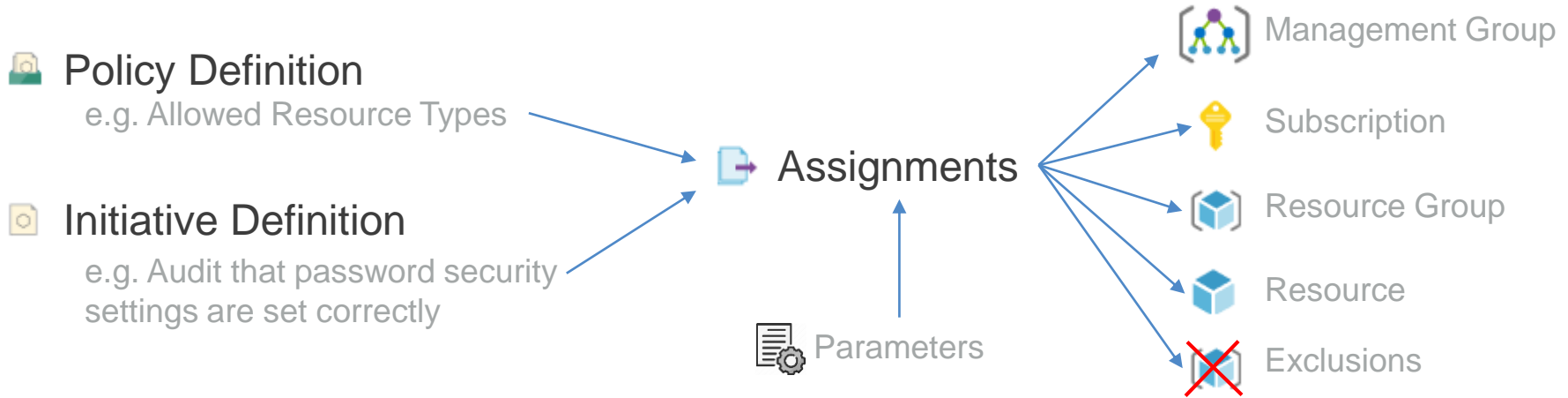
Azure Policy

What it does



Azure Policy

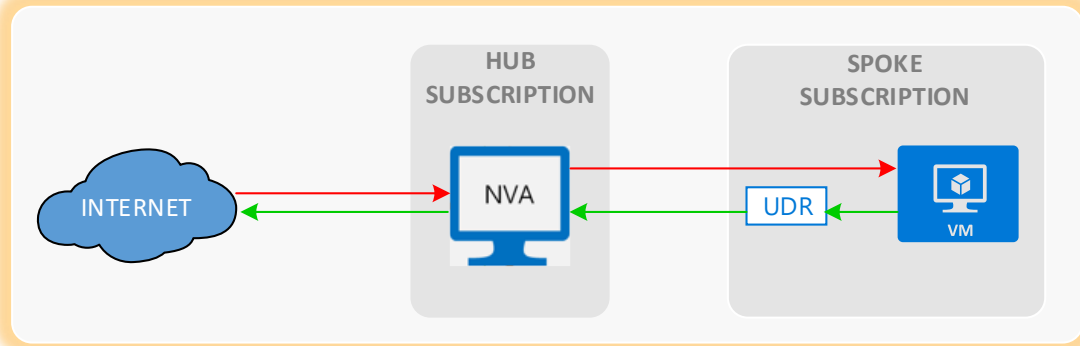
How it works



Enforce geographic boundaries



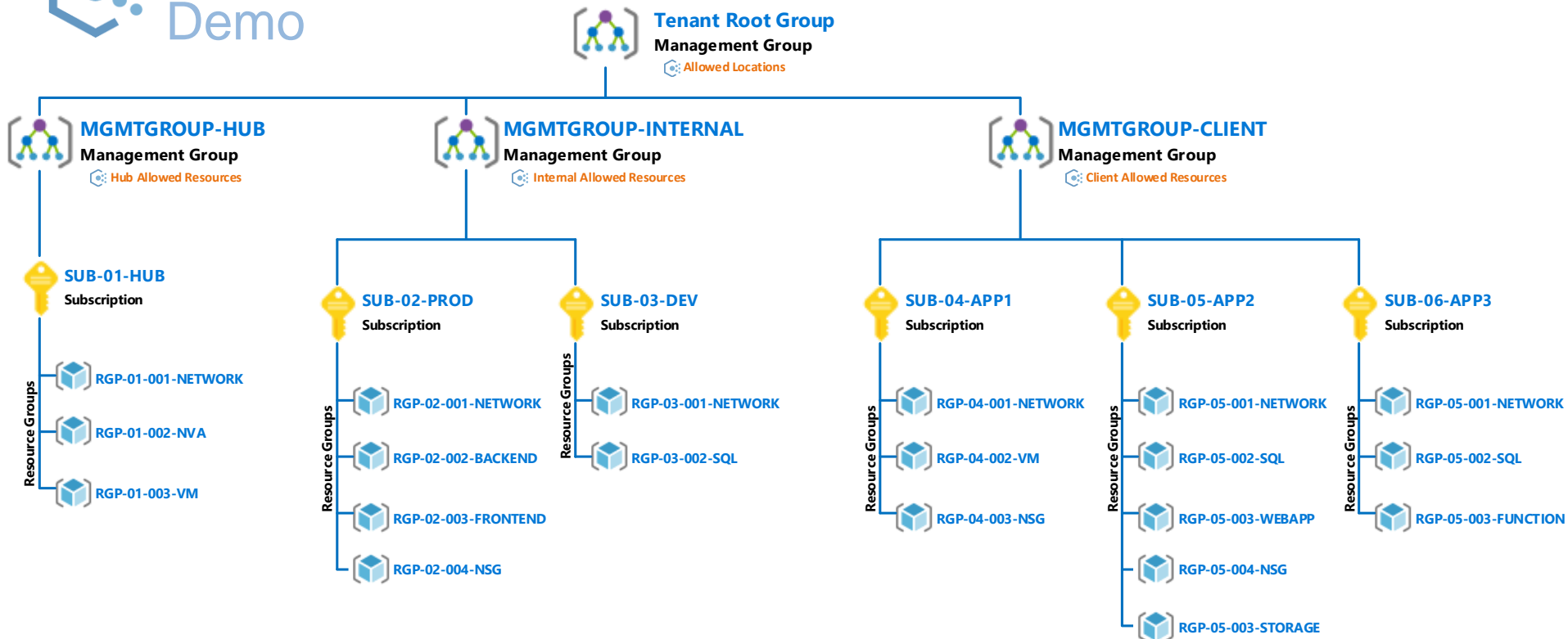
Enforce network boundaries



Prevent cost overruns



Azure Policy Demo





Azure Policy

Demo

- Policy management in the portal.
- Policy assignment script.
- Policy-restricted resource creation.

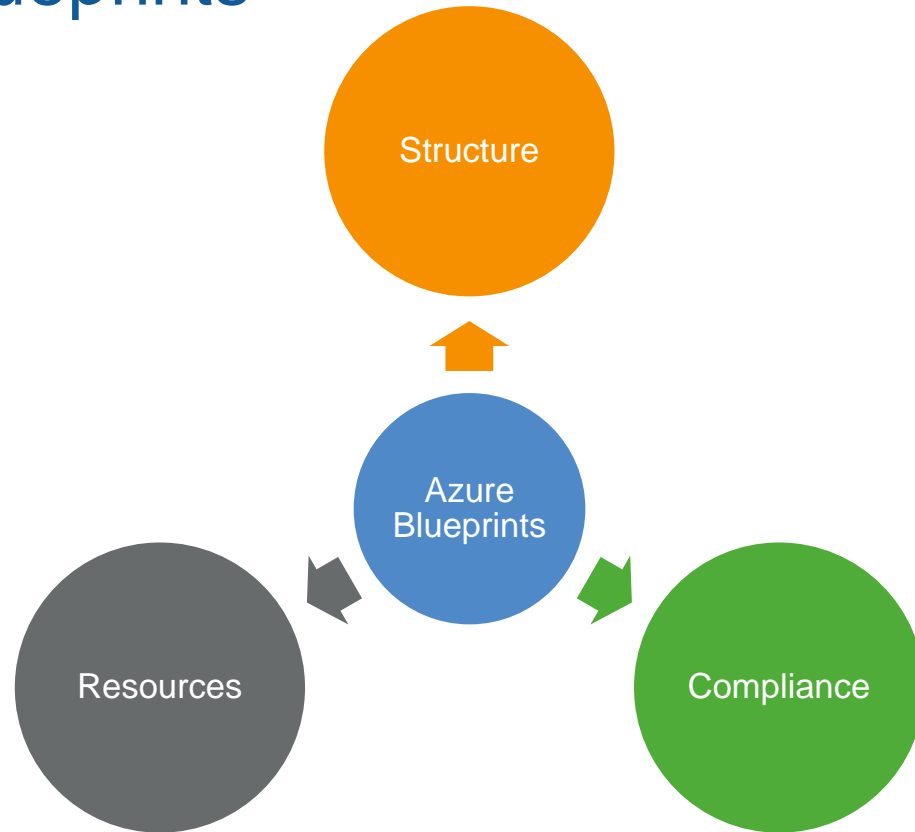


<https://github.com/FabienGilbert/AzureBootcamp>



Azure Blueprints

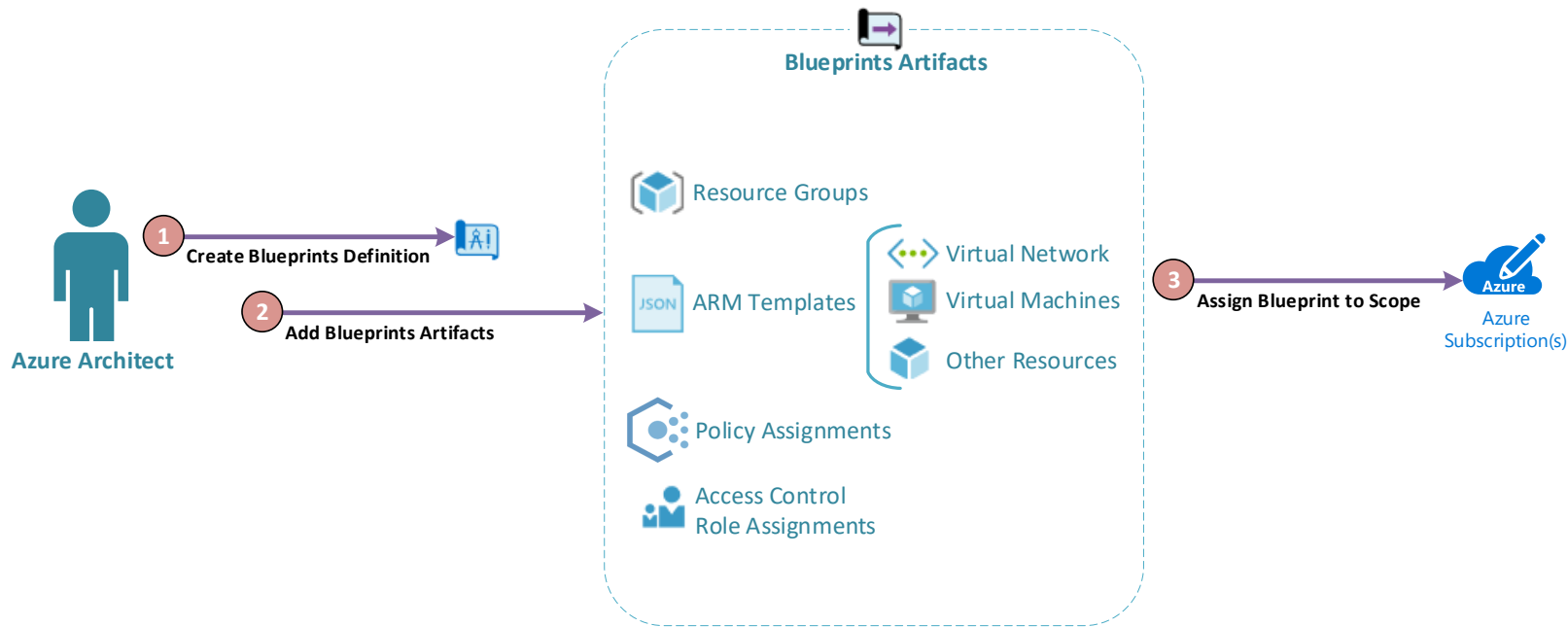
Basics

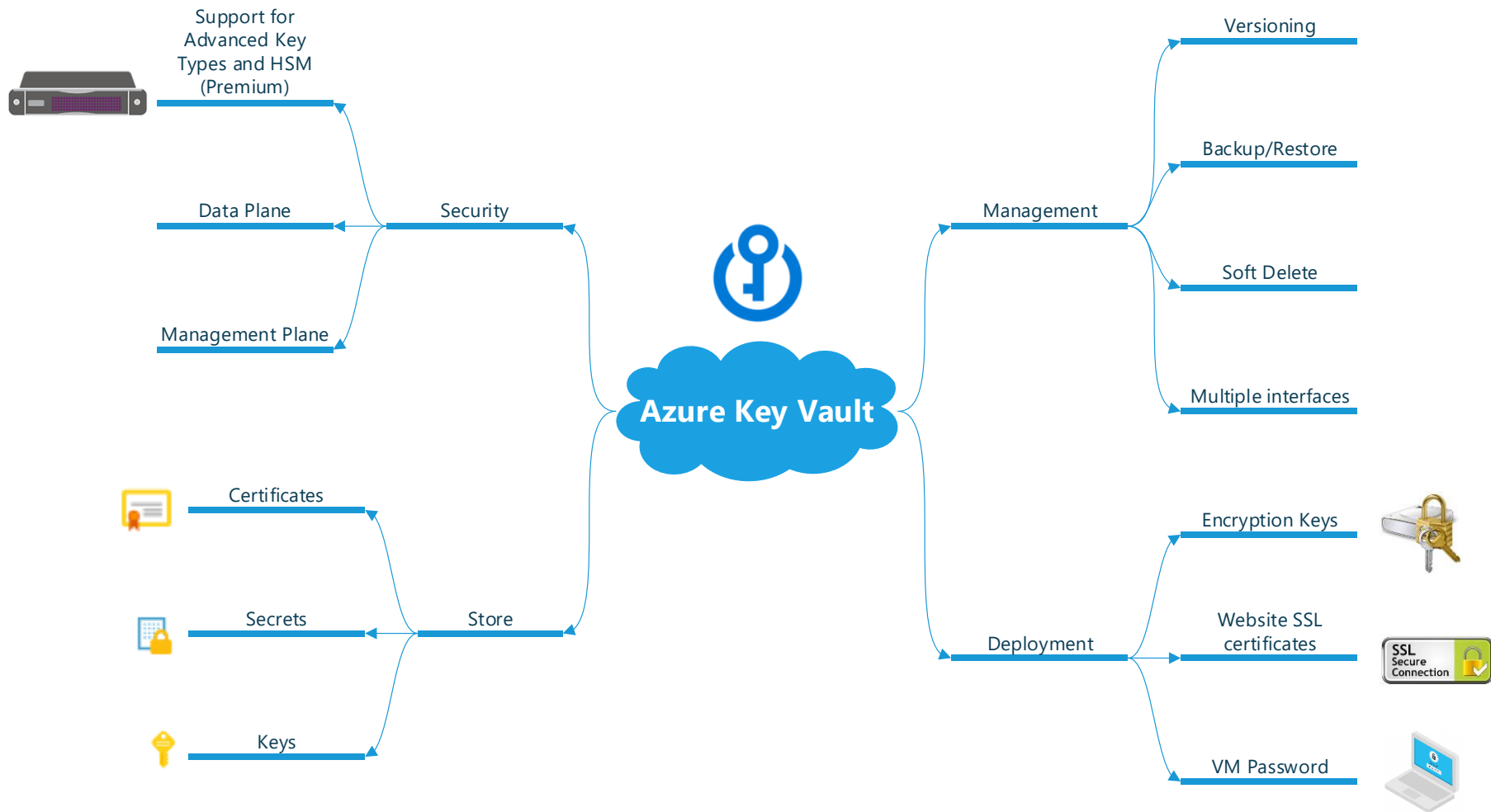




Azure Blueprints

How it works







Azure Key Vault

Management Plane & Data Plane

LABKV1 - Access control (IAM)

Key vault

Search (Ctrl+/)

+ Add Edit columns Refresh Remove

Check access **Role assignments** Deny assignments Classic administrators Roles

Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments. [Learn more](#)

Name Type Role

Scope Group by

6 items (6 Groups)

| NAME | TYPE | ROLE | SCOPE |
|-------------------------------|-------|------------------------|------------------------------|
| BILLING READER | | | |
| RB Root Billing Read Only | Group | Billing Reader | Management group (Inherited) |
| CONTRIBUTOR | | | |
| LC Lab Contributors | Group | Contributor | Management group (Inherited) |
| COST MANAGEMENT READER | | | |
| RB Root Billing Read Only | Group | Cost Management Reader | Management group (Inherited) |
| OWNER | | | |

LABKV1 - Access policies

Key vault

Search (Ctrl+/)

Save Discard Refresh

Click to show advanced access policies

+ Add new

- ff281ffe-705c-4f53-9f37-a40e6f2c68f3
- AGT-S-APP-01-004 (Directory ID: 9ee7103a-35c1-4595-91...)
- Fabien Gilbert USER (Directory ID: 9ee7103a-35c1-45...)

Azure Key Vault

Demo

- Key Vault ARM template creation.
- Key Vault SSL Certificate generation.
- BYOK Encrypted Storage Account.
- Key Vault Secrets for admin logins.
- VM deployment with Disk Encryption.
- Key Vault SSL Certificate deployment to VM.
- Azure Policy Compliance.

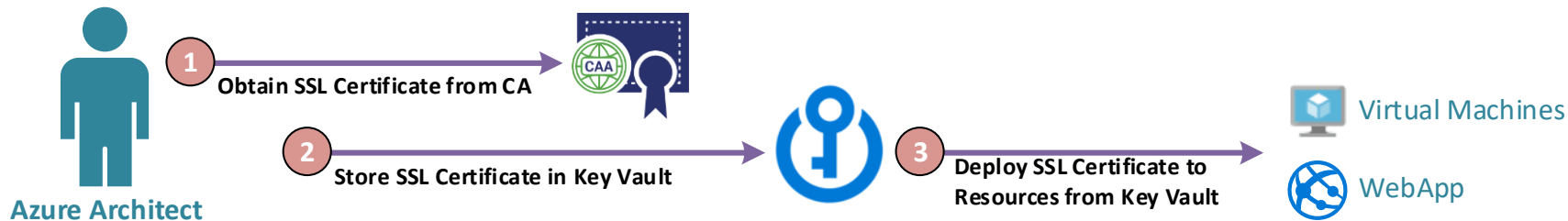


<https://github.com/FabienGilbert/AzureBootcamp>



Azure Key Vault

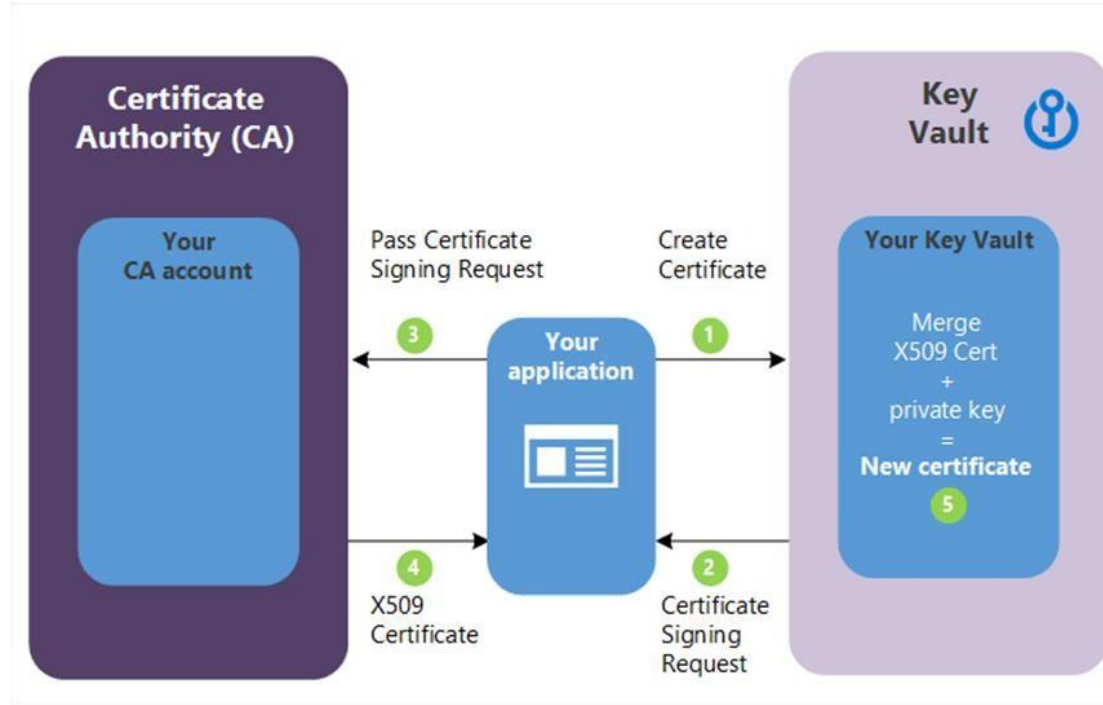
Key Vault SSL Certificate Management





Azure Key Vault

SSL Certificate Generation





Thank You