Azure Virtual Data Centre Architecture

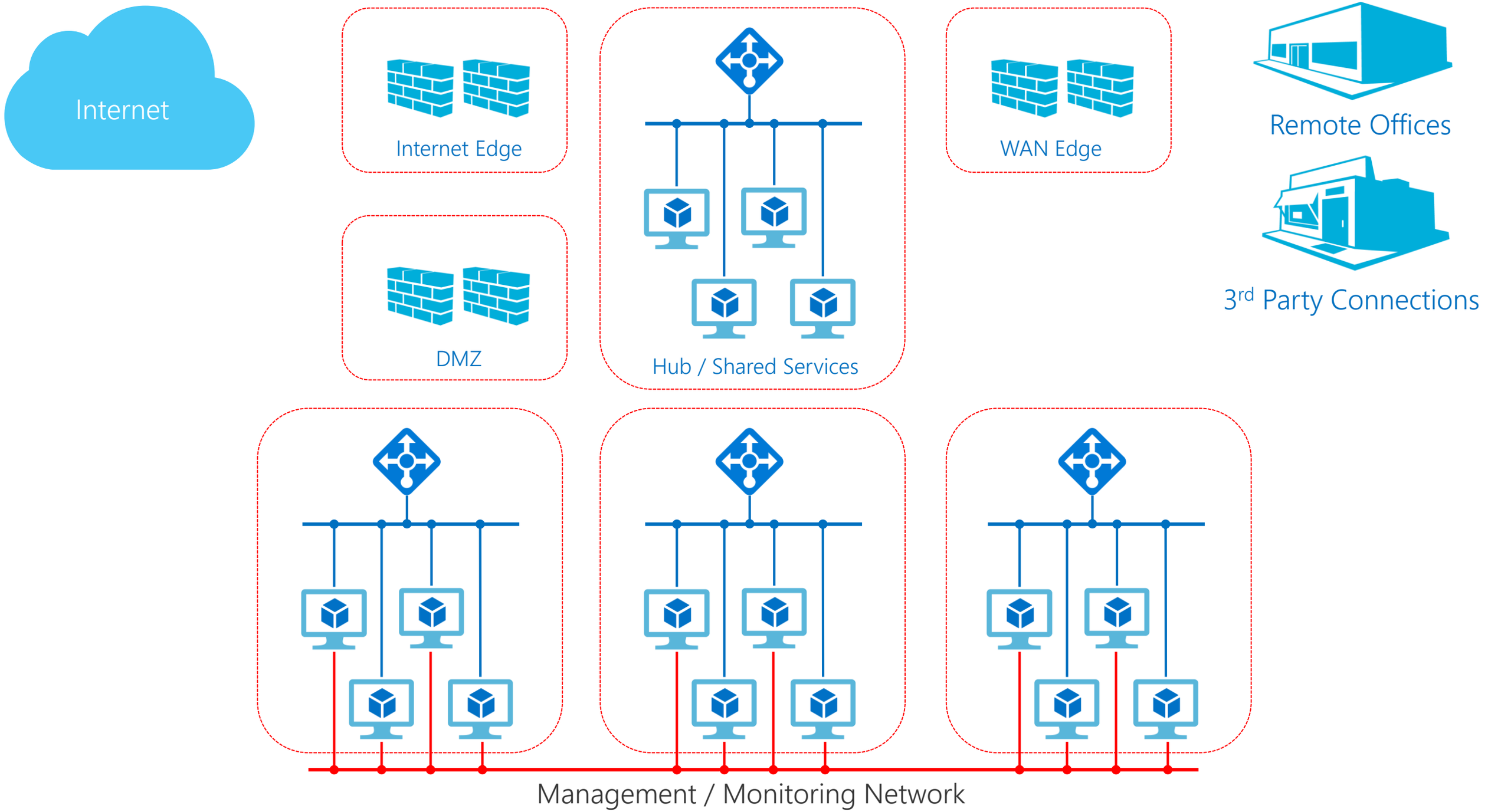
Richard Cheney
Cloud Solution Architect

Microsoft

Before we start, kick off the lab build process!

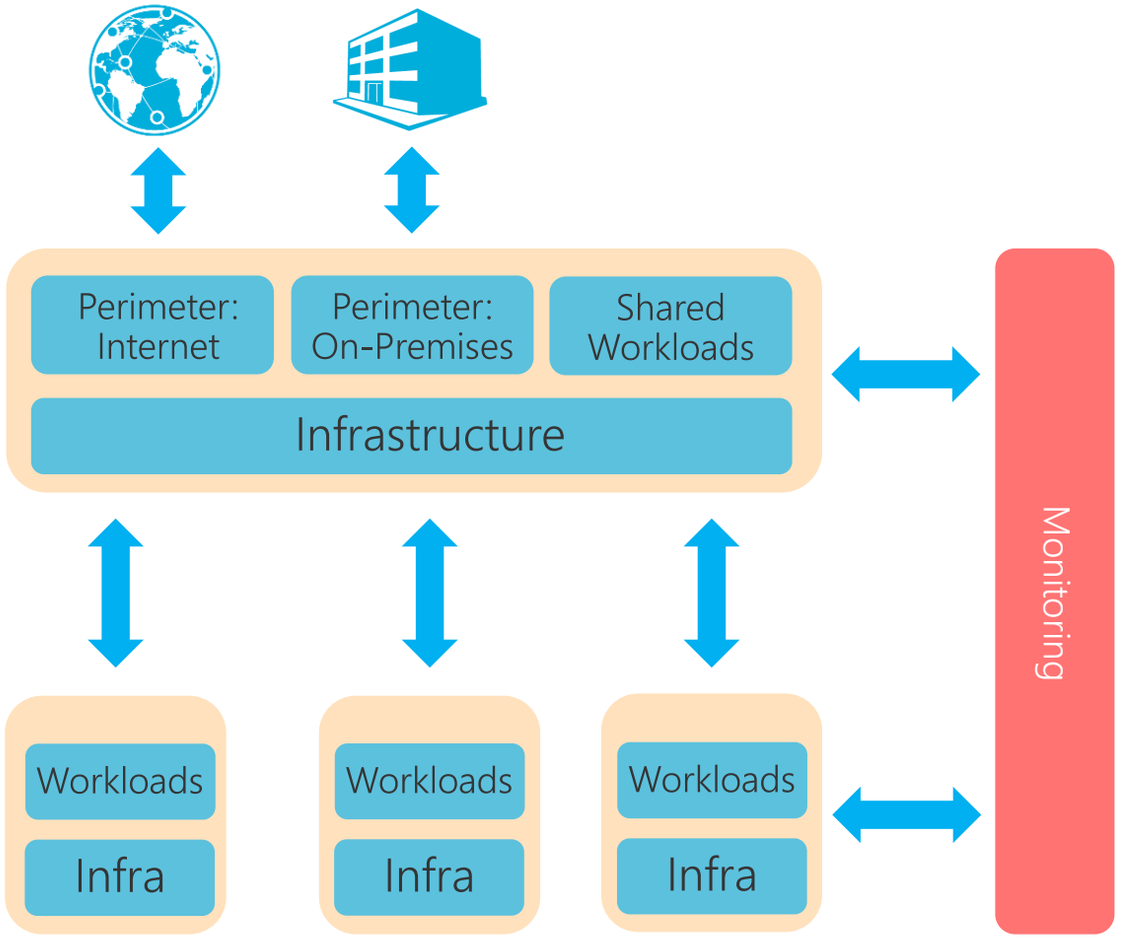
Aka.ms/citadel/vdc

What is a VDC and why do we need it?

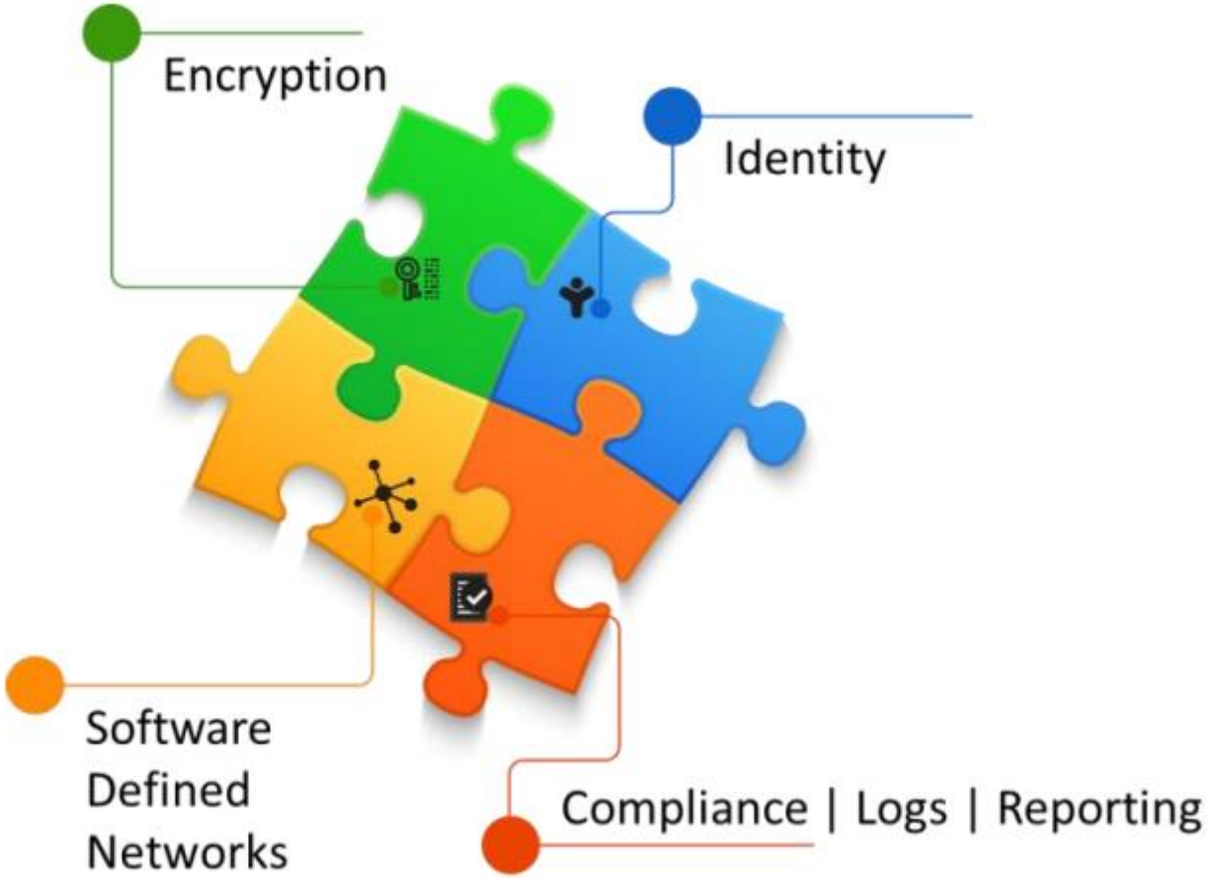

Internet
Internet Edge
DMZ
Hub / Shared Services
WAN Edge
Remote Offices
3rd Party Connections
Management / Monitoring Network




Customers want the same levels of isolation, security policy, monitoring and identity that they have in their DCs today.

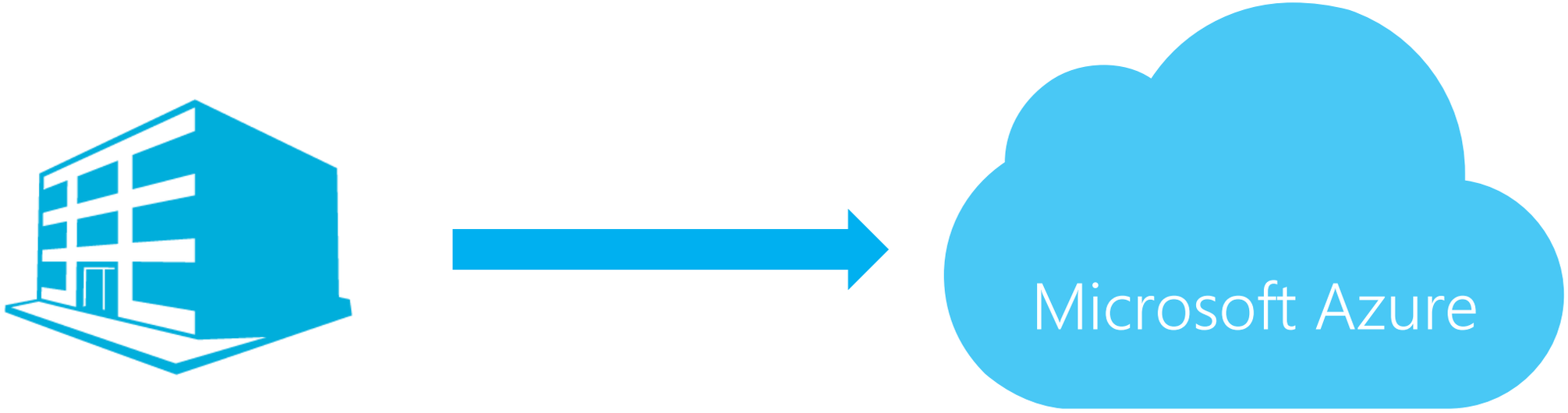


Azure VDCs bring together networking, security, management and identity to meet these requirements.


Encryption
Identity
Software
Defined
Networks
Compliance | Logs | Reporting

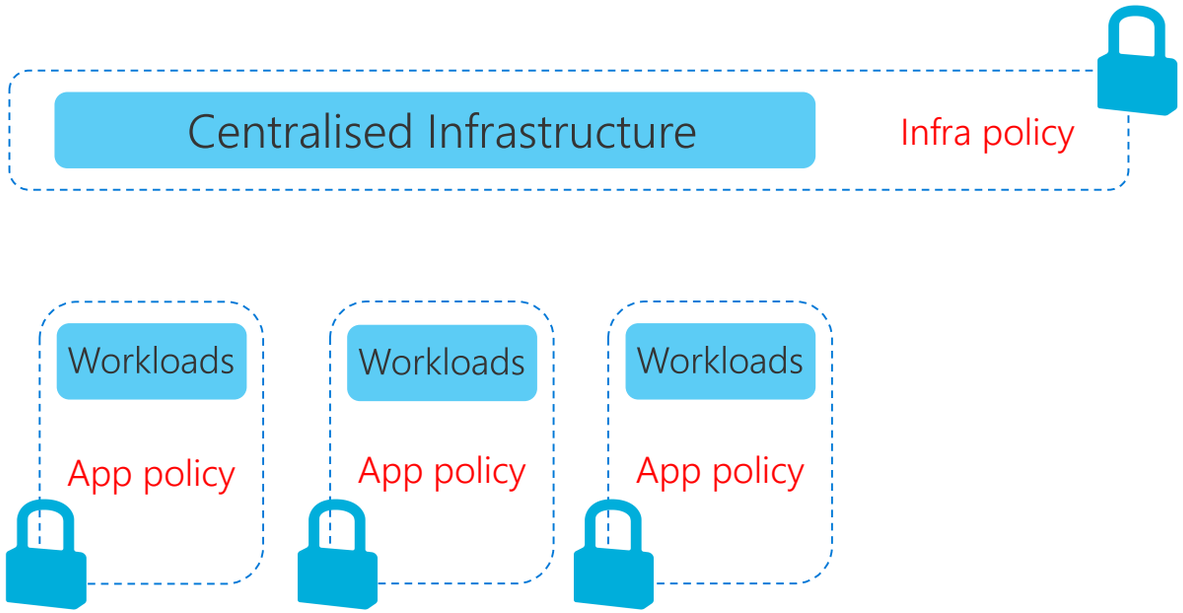
How can VDCs help?

Migrating on-premises workloads into Azure



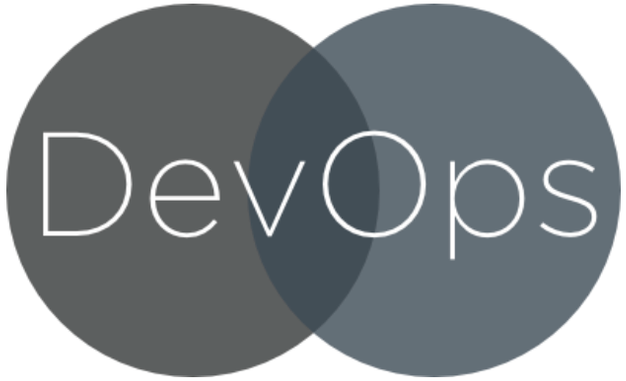
How can VDCs help?

Implementing centralised security and access policies for workloads



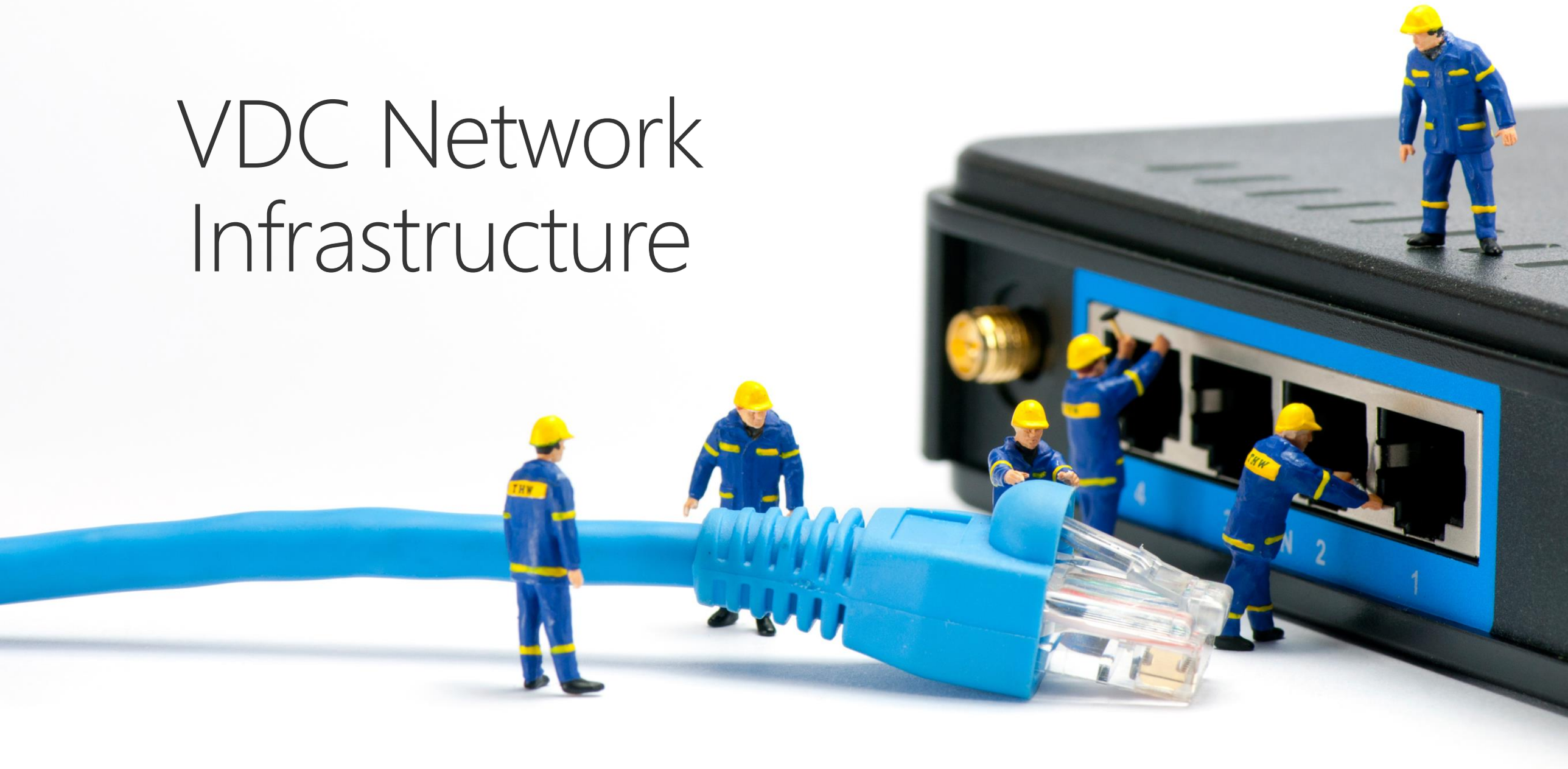
How can VDCs help?

Mix DevOps and centralised IT

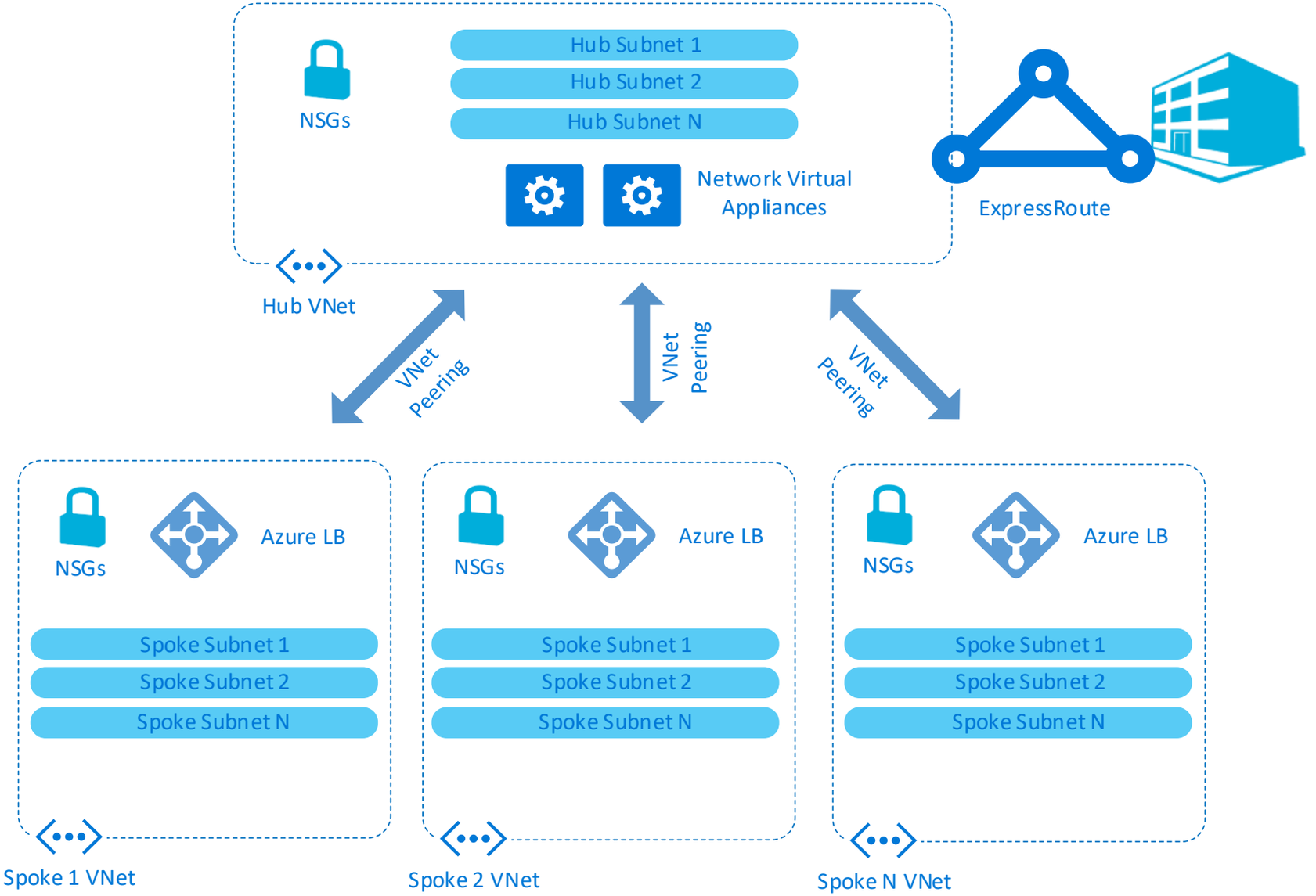


+

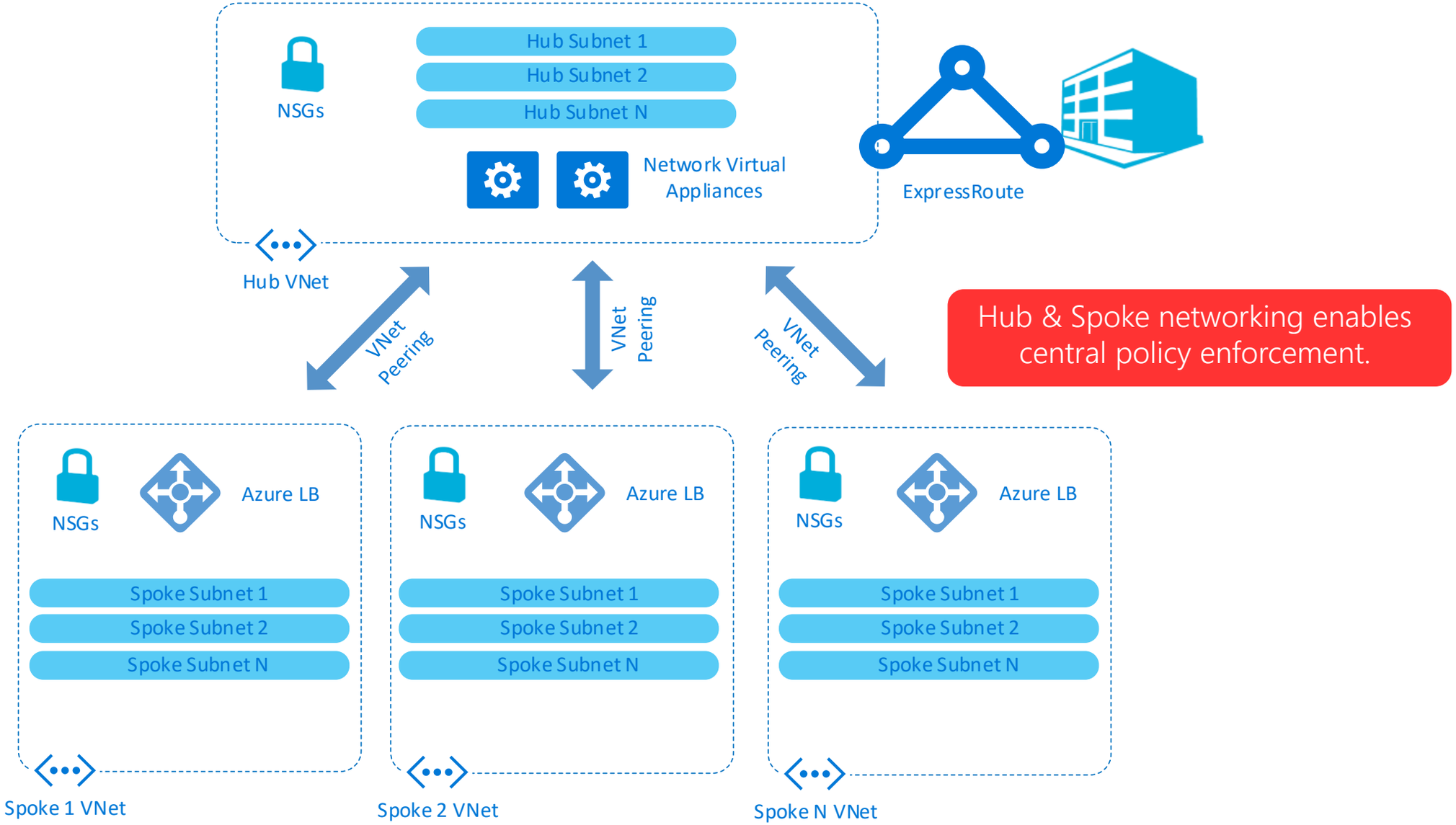
VDC Network Infrastructure



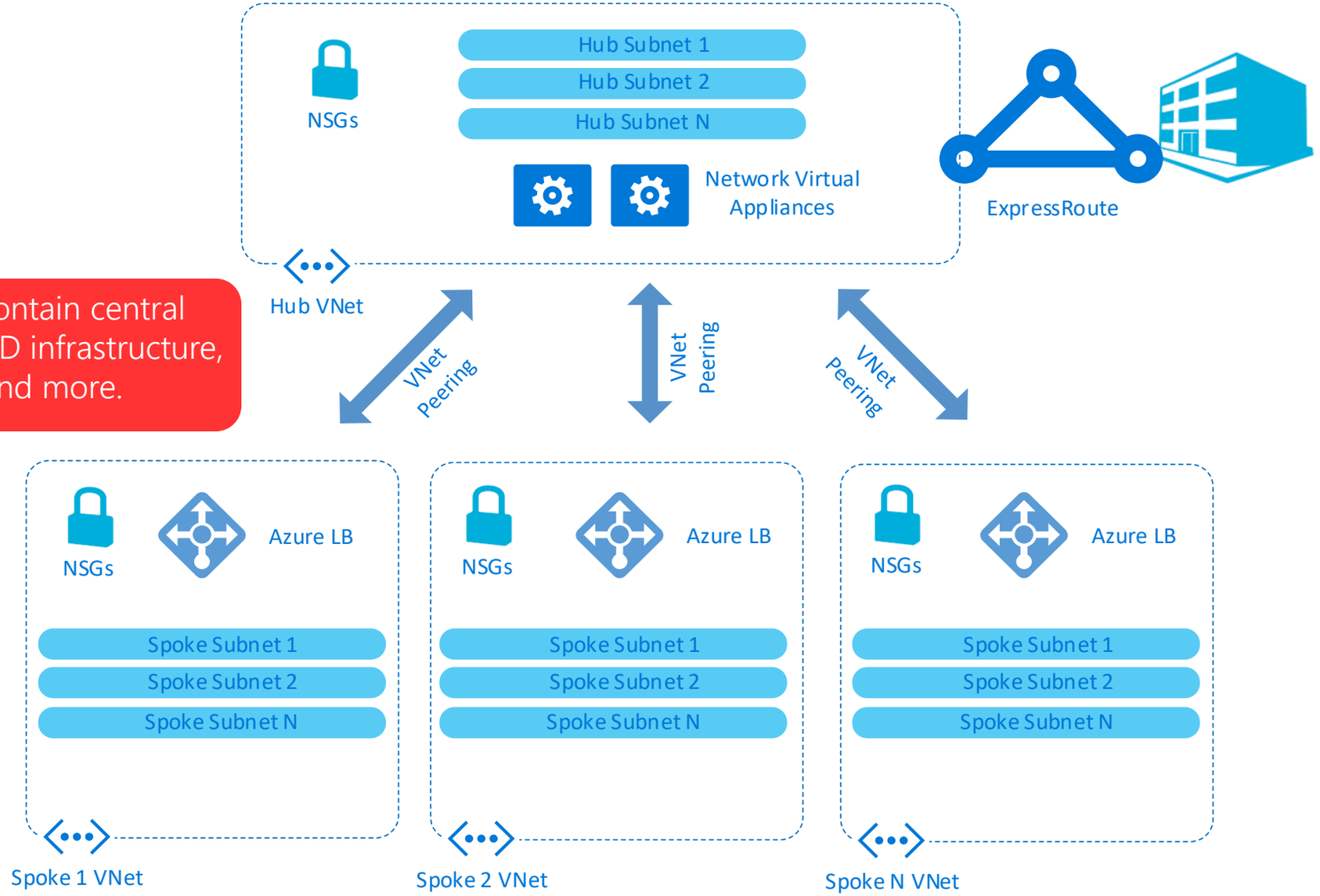
Network Infrastructure



Network Infrastructure

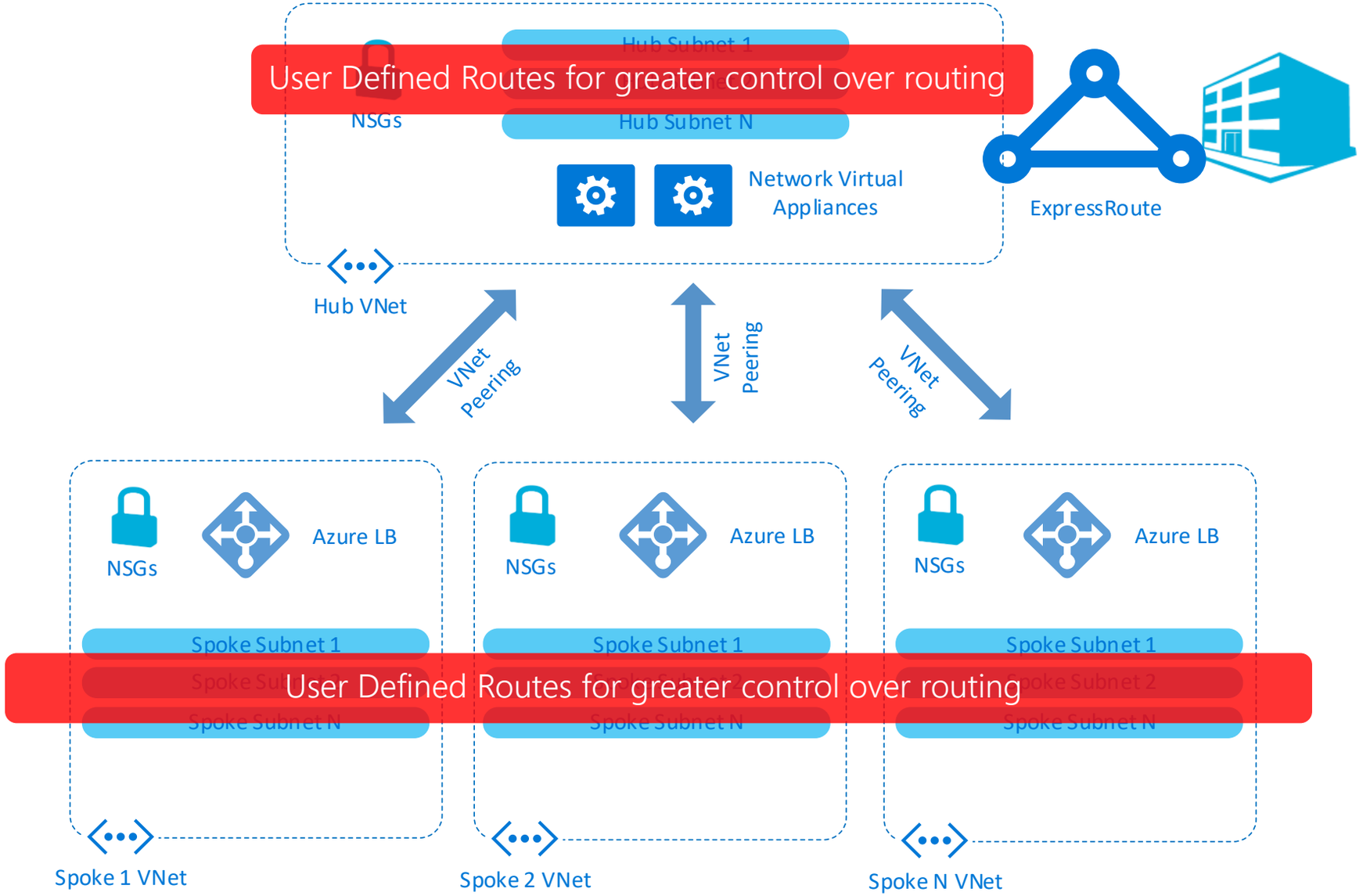


Network Infrastructure

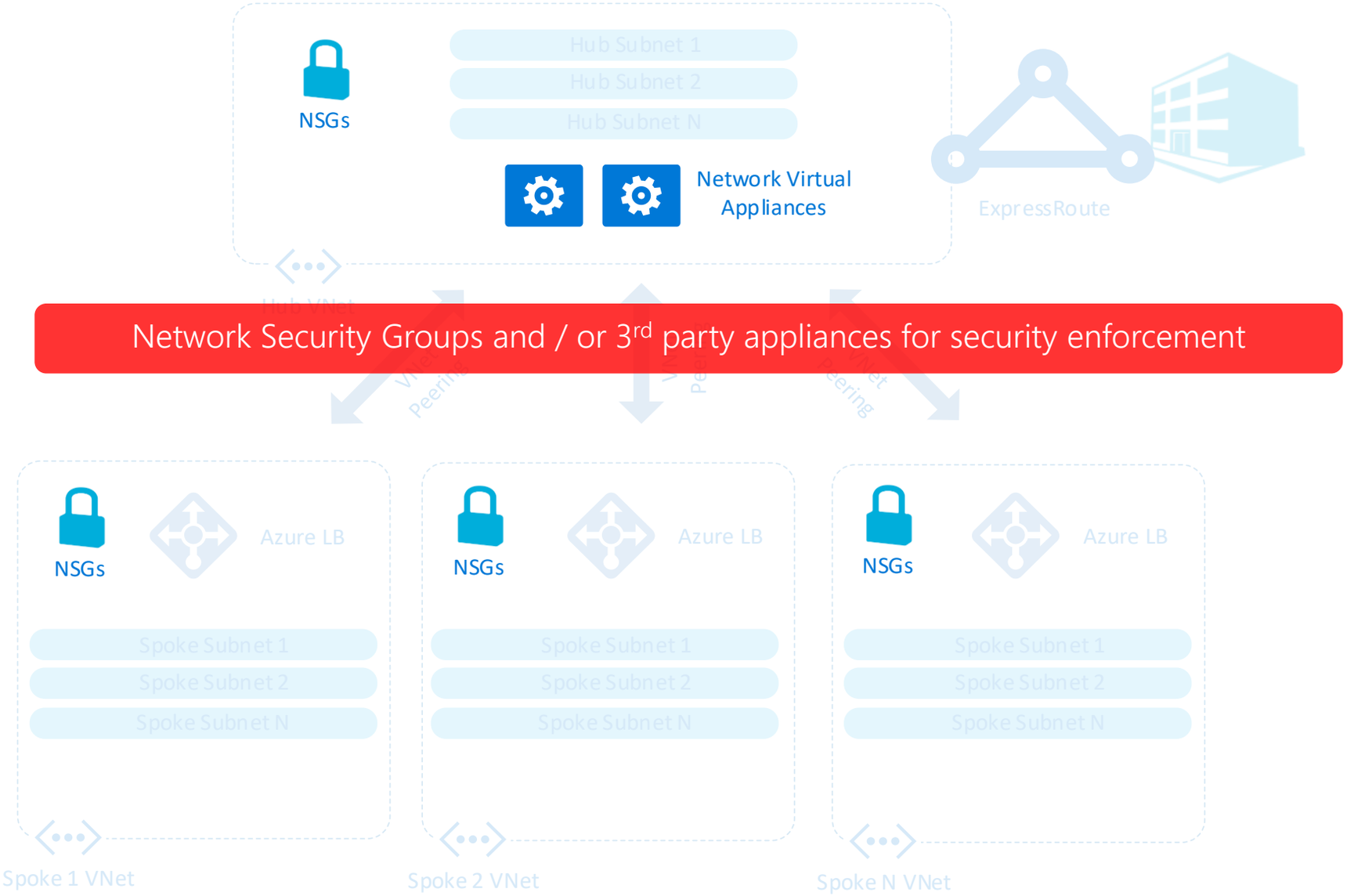


The hub may contain central services such as AD infrastructure, DNS, PKI and more.

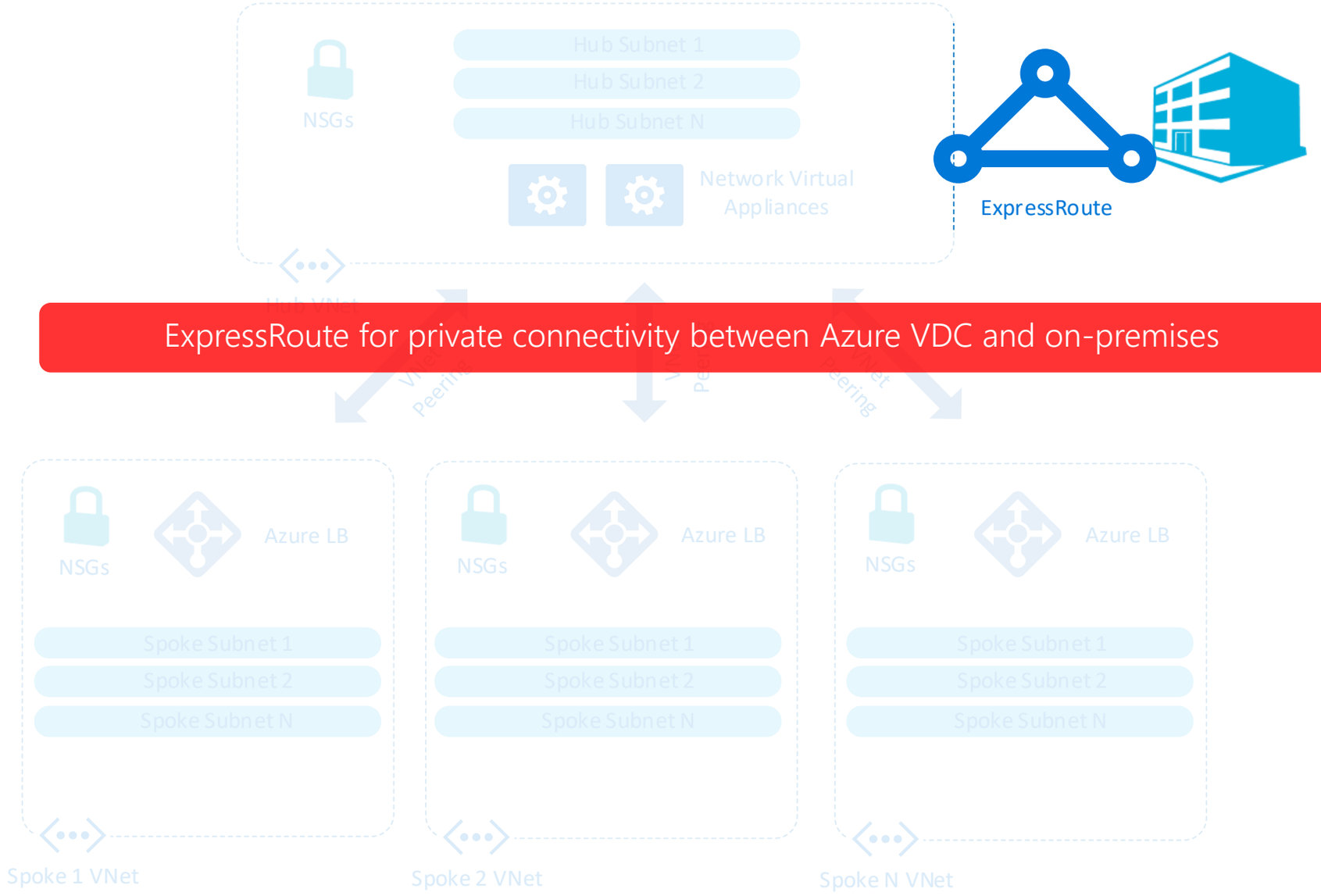
Network Infrastructure



Network Infrastructure



Network Infrastructure

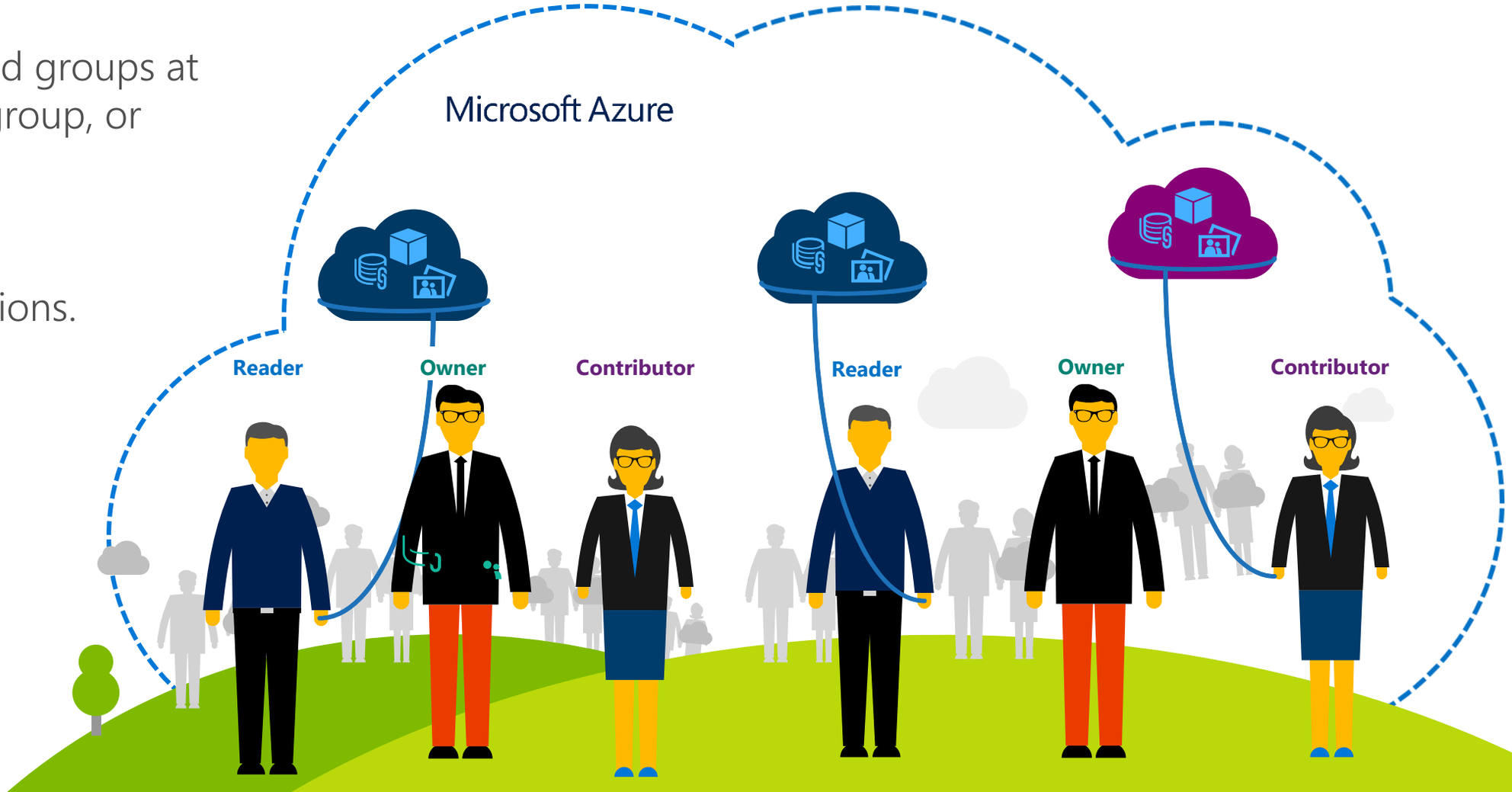


Identity and Security in the VDC Environment

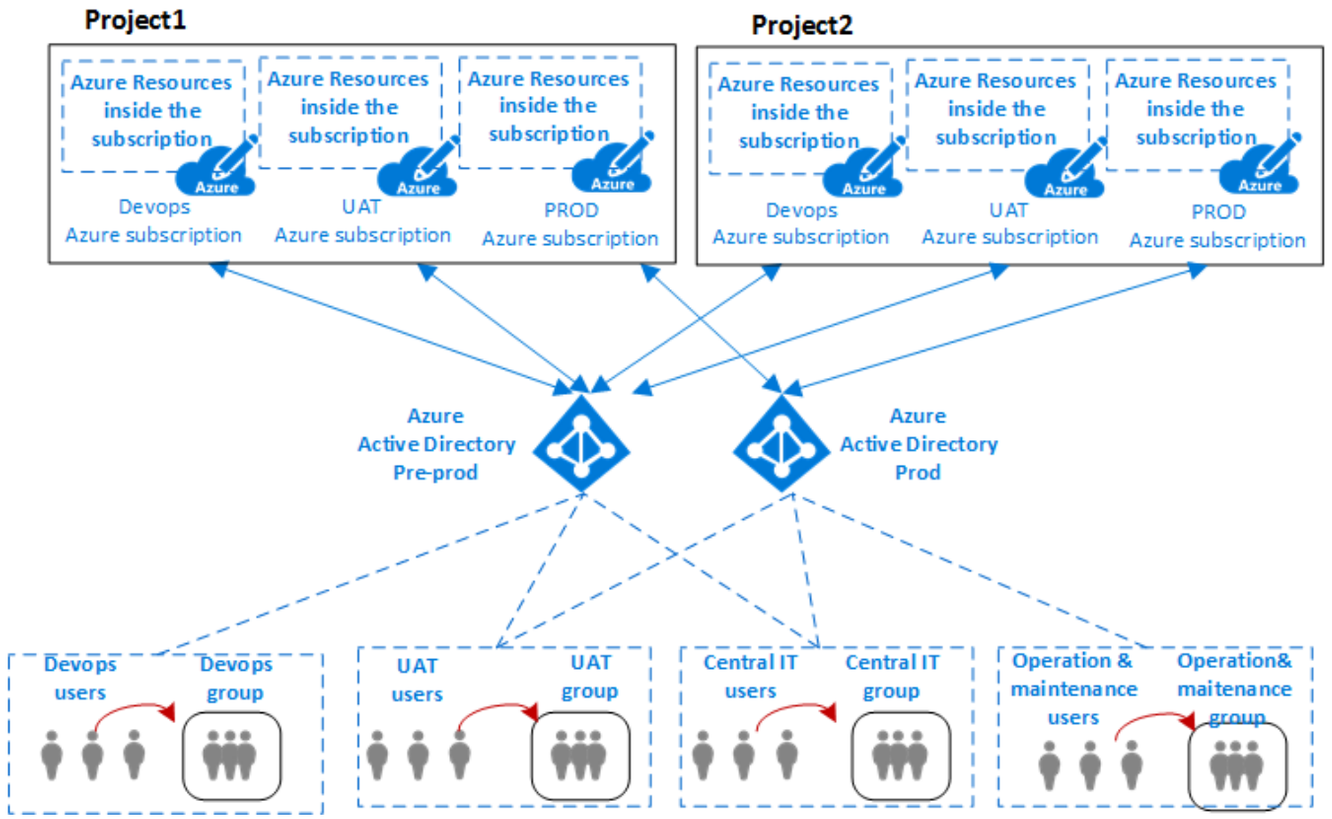
Trust through isolation

Assign roles to users and groups at subscription, resource group, or resource level.

Use built-in roles with pre-configured permissions.

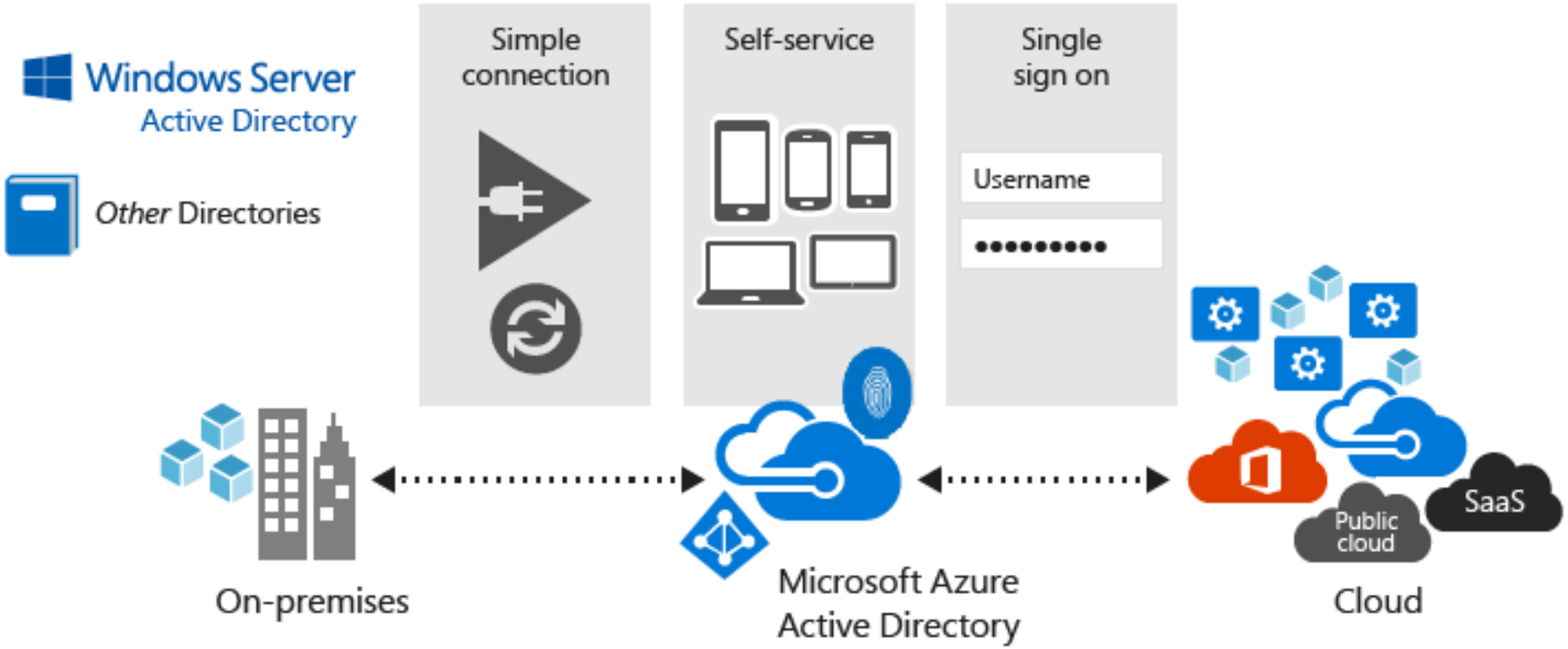


A VDC can be partitioned to securely host multiple projects.

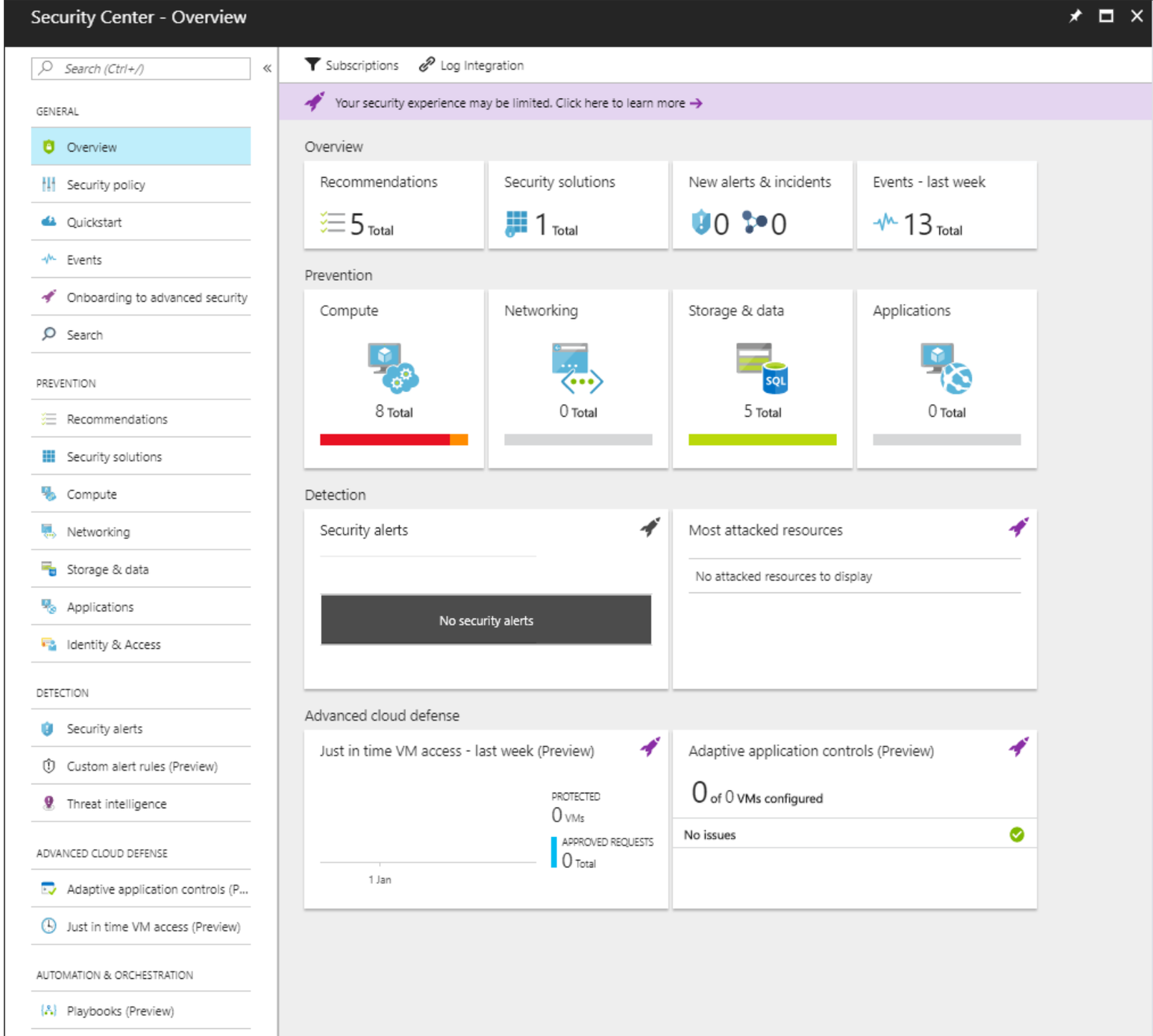


This can be achieved using either subscriptions or resource groups.

Azure AD: a multi-tenant, cloud based directory service.

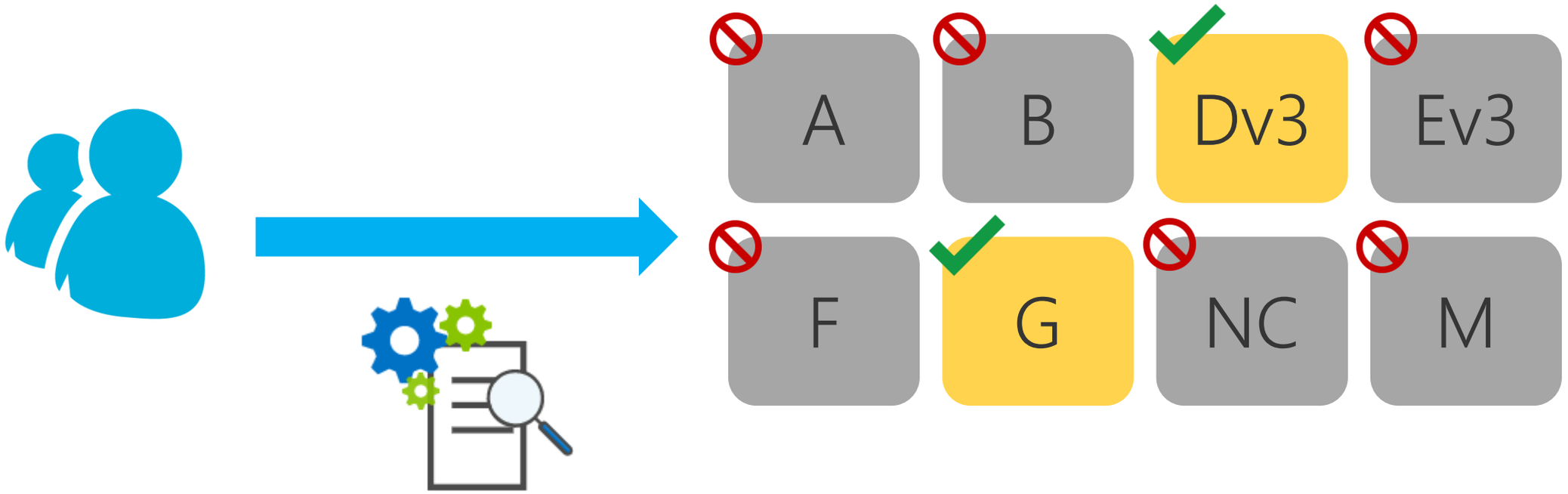


Azure Security Center



Azure Policy

How do I stay compliant in my environment?



Monitoring

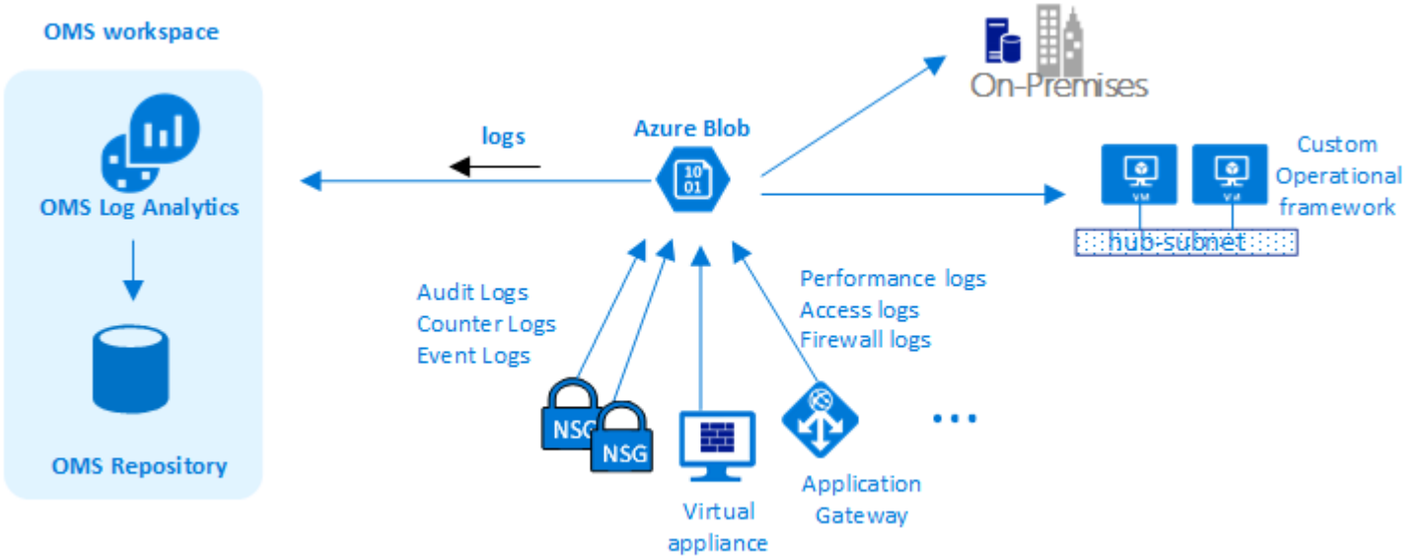
Service Health

Azure Monitor

Network Watcher

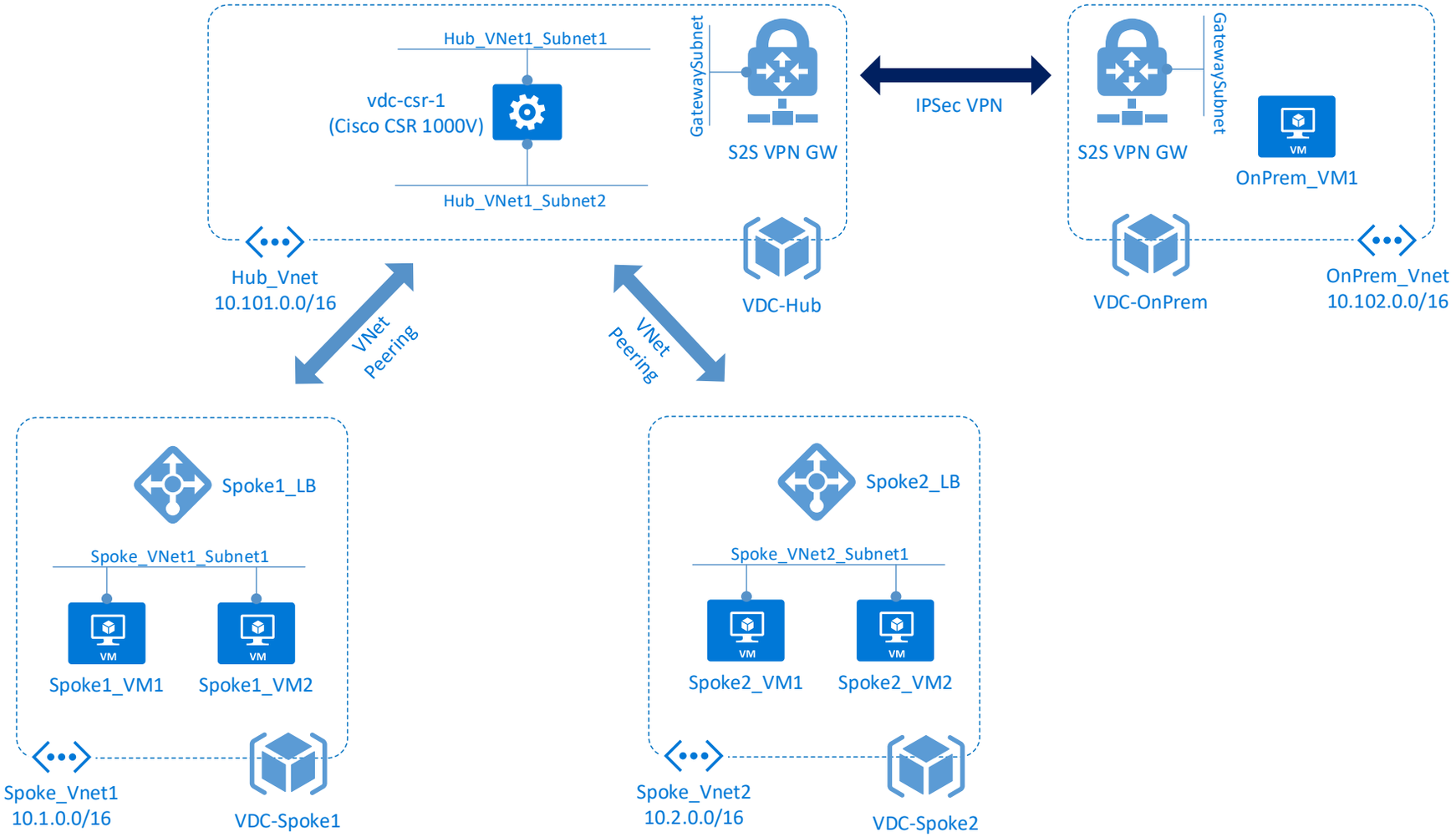
Operations Management Suite

Monitoring is key in a VDC environment – Azure offers many logging and monitoring services.

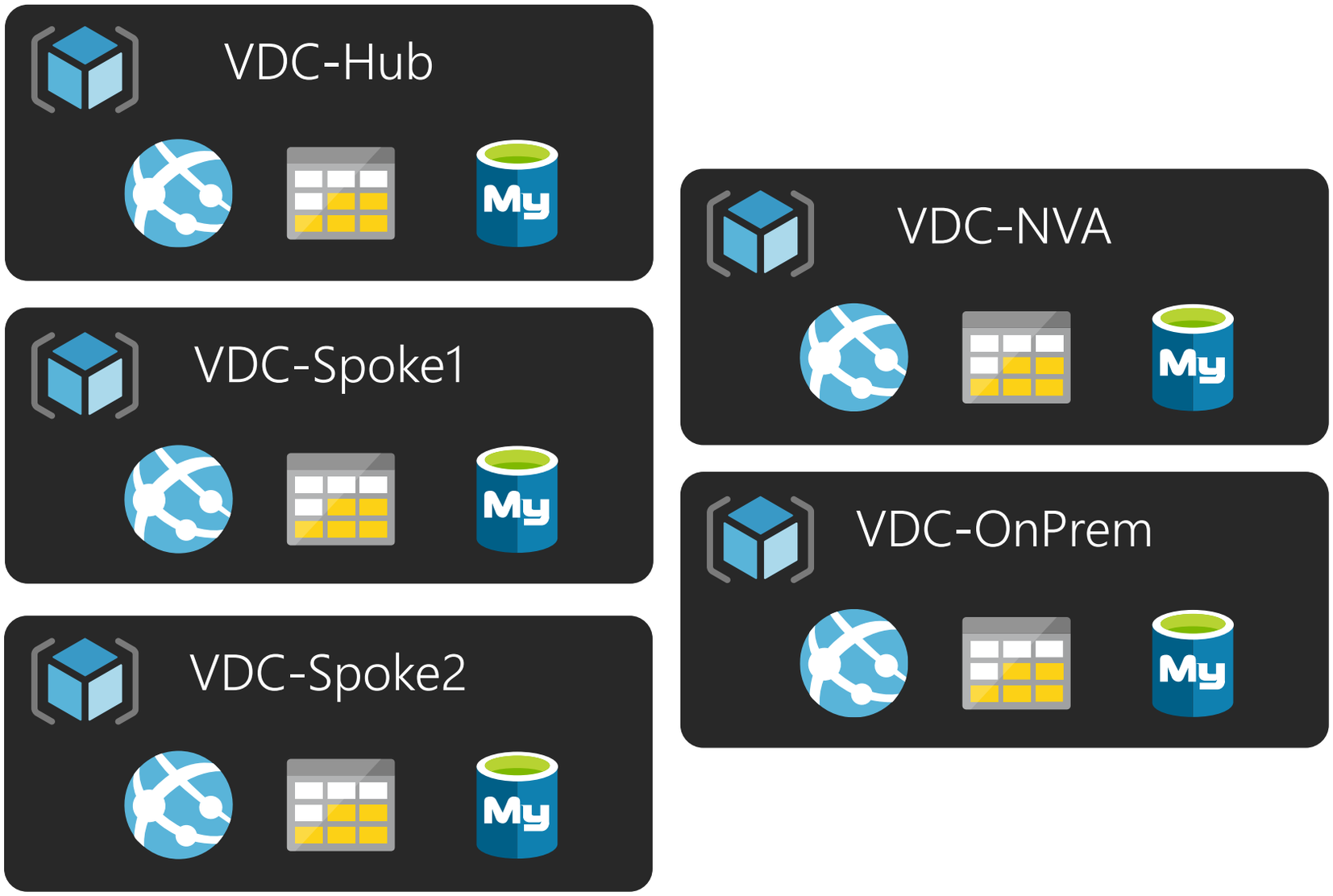


Logs can be sent to Azure storage or to OMS (log analytics).

What's covered in the lab?



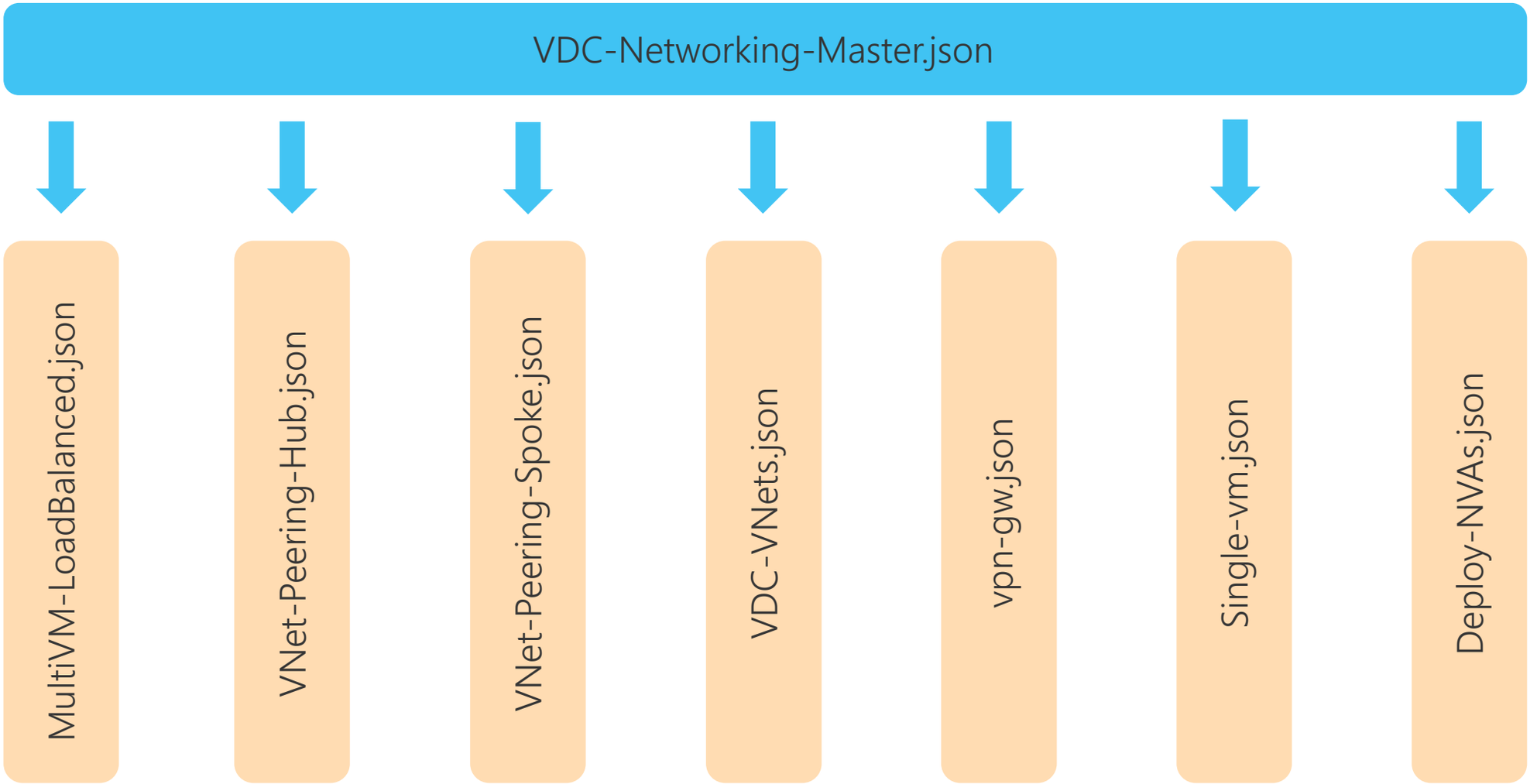
You'll be building a full VDC environment, covering networking, security, monitoring and identity.



Resources deployed into multiple resource groups.

ARM templates are used to build out the initial ‘base’ environment.

```
"resources": [
    {
        "comments": "Create Hub VNet",
        "name": "hubVnet",
        "type": "Microsoft.Resources/deployments",
        "apiVersion": "2017-05-10",
        "properties": {
            "mode": "Incremental",
            "templateLink": {
                "uri": "[variables('hubVnetTemplateURL')]",
                "contentVersion": "1.0.0.0"
            },
            "parameters": "[variables('hubVnetTemplate')]"
        }
    },
    {
        "comments": "Create OnPremises VNet",
        "name": "onPremVnet",
        "type": "Microsoft.Resources/deployments",
        "resourceGroup": "[parameters('onPremRG')]",
        "apiVersion": "2017-05-10",
        "properties": {
            "mode": "Incremental",
            "templateLink": {
                "uri": "[variables('hubVnetTemplateURL')]",
                "contentVersion": "1.0.0.0"
            },
            "parameters": "[variables('onPremVnetTemplate')]"
        }
    },
    {
        "comments": "Create Spoke1 VNet",
        "name": "spoke1Vnet",
        "type": "Microsoft.Resources/deployments",
        "resourceGroup": "[parameters('spoke1RG')]",
        "apiVersion": "2017-05-10",
        "properties": {
            "mode": "Incremental",
            "templateLink": {
                "uri": "[variables('spokeVnetTemplateURL')]",
                "contentVersion": "1.0.0.0"
            },
            "parameters": "[variables('spoke1VnetTemplate')]"
        }
```



A ‘master’ ARM template runs which in turn calls a number of other templates.

Part 1: Explore the Lab

Part 2: Networking

Site-to-Site VPN
Cisco CSR1000V Configuration
User Defined Routes

Network Security Groups
Azure Security Center
Azure Resource Policies

Part 3: Security

Part 4: Monitoring

Network Watcher
NSG Flow Logs
Metrics, Alerts & Diagnostics with Azure Monitor

Users and Groups
Role Based Access Control

Part 5: Identity

Microsoft