Managing Microsoft Azure Subscriptions

CONFIGURING MICROSOFT AZURE POLICIES

Dan Lachance
linkedin.com/in/danlachance

Topics

1. Configuring Microsoft Azure Policies

2. Configure Cost Center Spending Limits and Tagging

3. Assign Role-based Access Control

4. Manage Microsoft Azure Resource Providers

Introduction

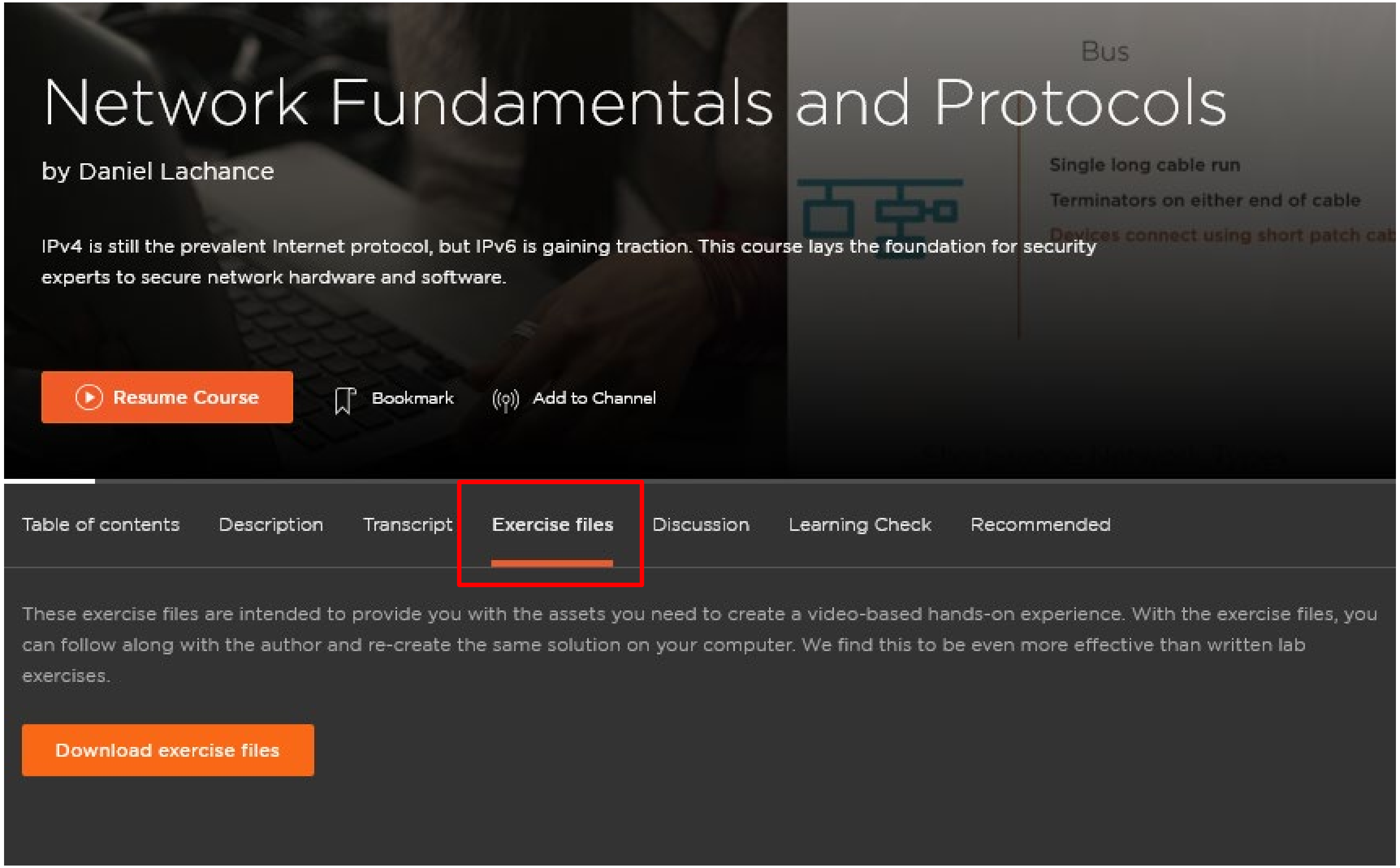
Resource Tagging

- Purpose
- How to tag resources

Microsoft Azure Policies

- Purpose
- Policy initiative definitions
- Exclusion scopes
- Built-in and custom policies

Downloadable Exercise Files



Network Fundamentals and Protocols

by Daniel Lachance

IPv4 is still the prevalent Internet protocol, but IPv6 is gaining traction. This course lays the foundation for security experts to secure network hardware and software.

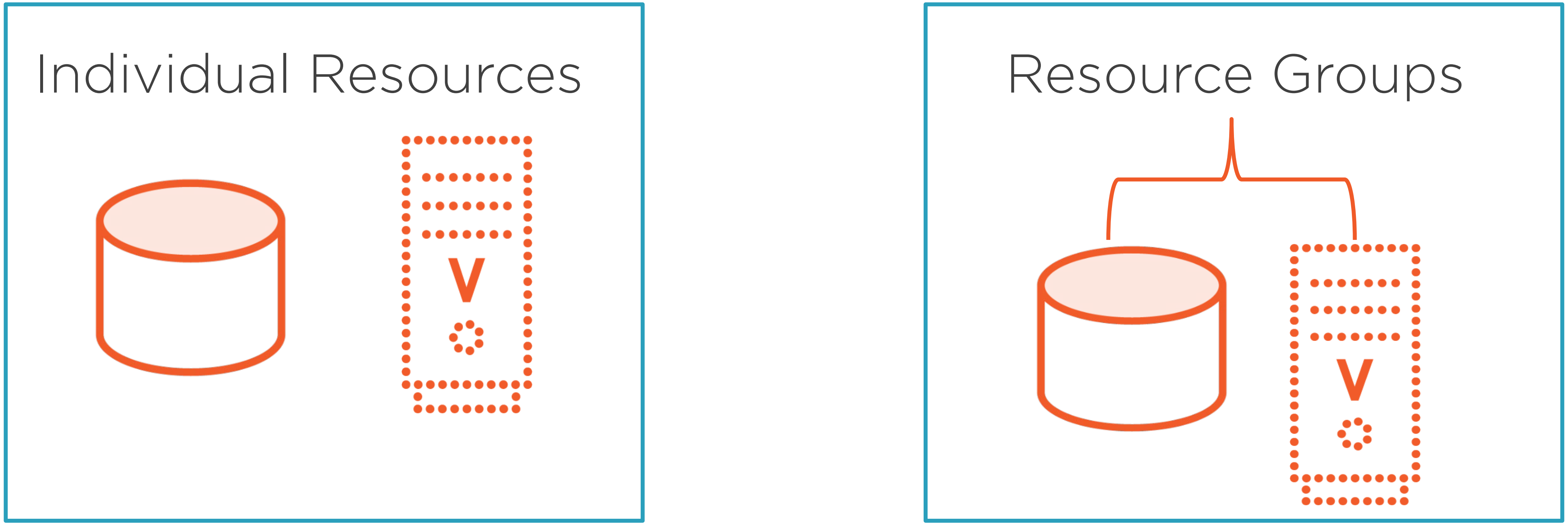
These exercise files are intended to provide you with the assets you need to create a video-based hands-on experience. With the exercise files, you can follow along with the author and re-create the same solution on your computer. We find this to be even more effective than written lab exercises.

Resource Tagging

Tags are additional *metadata* associated with Microsoft Azure ARM resources.

Tag Assignment

Azure Subscription



Individual Resources

Resource Groups

Tag Examples

Tag Key	Tag Value
Project	XYZ
Department	Sales-East
CostCenter	YHZ
LifeCyclePhase	Testing

Why Tag Resources?

Organize deployed Azure resources

Search by tag

Facilitates viewing related resources

Facilitates billing and cost management

Tag Management

Microsoft Azure portal

Microsoft Azure PowerShell

Microsoft Azure CLI

ARM template

Azure Policy “Modify” effect

Demo

Tag resources using the Microsoft Azure portal

Demo

Tag resources using Microsoft Azure PowerShell cmdlets

Demo

Tag resources using the Microsoft Azure CLI

Demo

Use a custom modify policy to ensure tags are present

Microsoft Azure Policy

Microsoft Azure Policies ensure proper cloud governance by controlling resource deployment and usage.

Microsoft Azure Built-In Policies

Policy Name	Description
SQL server TDE protector should be encrypted with your own key	TDE with a customer managed key
Allowed Storage Account SKUs	Controls Storage Account SKU sizes
Allowed Resource Types	Controls which types of resources can be deployed
Allowed Locations	Controls which locations that resources can be deployed into

Microsoft Azure Built-in Policies

Policy Name	Description
Disk encryption should be applied on virtual machines	Ensure VM disks are encrypted
Encrypt unused disks	Ensure managed disks are encrypted even if not attached to a VM
Require a tag and its value on resources	Ensures that resources are tagged with a specific key-value pair

Custom Policies

JSON format

Used for granular resource control

- Deploy Network Security Group security rules

Custom policies can be created

- Manually
- Copy existing policy
- GitHub

Policy Parameters

- Variable values are passed to the policy
- Enables policy reuse
    - Fewer policies are required
- String or array data type

Policy Assignment

Built-in and custom policies can be assigned

- Microsoft Azure portal
- PowerShell cmdlets
- Microsoft Azure CLI
- ARM template

Policy permissions

- Microsoft.Authorization
- Microsoft.PolicyInsights

Policy Effects

Effect	Description
Append	Resource property additions including tags
Audit	Logging only; generates a warning
AuditIfNotExists	Auditing enabled if properties are absent
Deny	Existing non-compliant resources are marked as non-compliant, but not deleted
DeployIfNotExists	If the resource does not already exist, deploy it Supports remediation tasks

Policy Effects

Modify	Add, modify, delete tags, supports remediation tasks
Disabled	Disable a single policy assignment, or within the policy “if” statement Resources are not evaluated for compliance
Modify	Add, modify, delete tags Supports remediation tasks
EnforceOPAContraint	Rules are applied to a Kubernetes cluster

Policy Evaluation Order

1 – Create, update resources

2 – Disabled

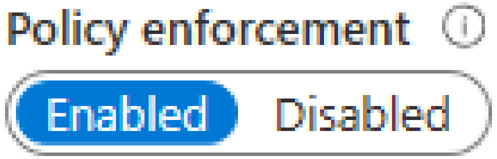
3 – Append, Modify

4 – Deny

5 – Audit

6 – AuditIfNotExists, DeployIfNotExists

Policy Assignment Enforcement Mode



Policy enforcement

[✓ Enabled] Disabled

- **Enabled**: Policy assignment is enforced
- **Disabled**: Policy assignment is not enforced, compliance results will be available

Policy Assignment – Management Groups

- Used to organize Microsoft Azure subscriptions
- Up to 6 hierarchical levels can be created
- Subscriptions inherit settings
- Facilitates role-based access control (RBAC)
- Subscriptions can be moved to other parts of the hierarchy

Policy Assignment

- Subscription
  - Exclusions can apply to child items such as resource groups

- Resource group
  - Exclusions can apply to child items such as virtual machines

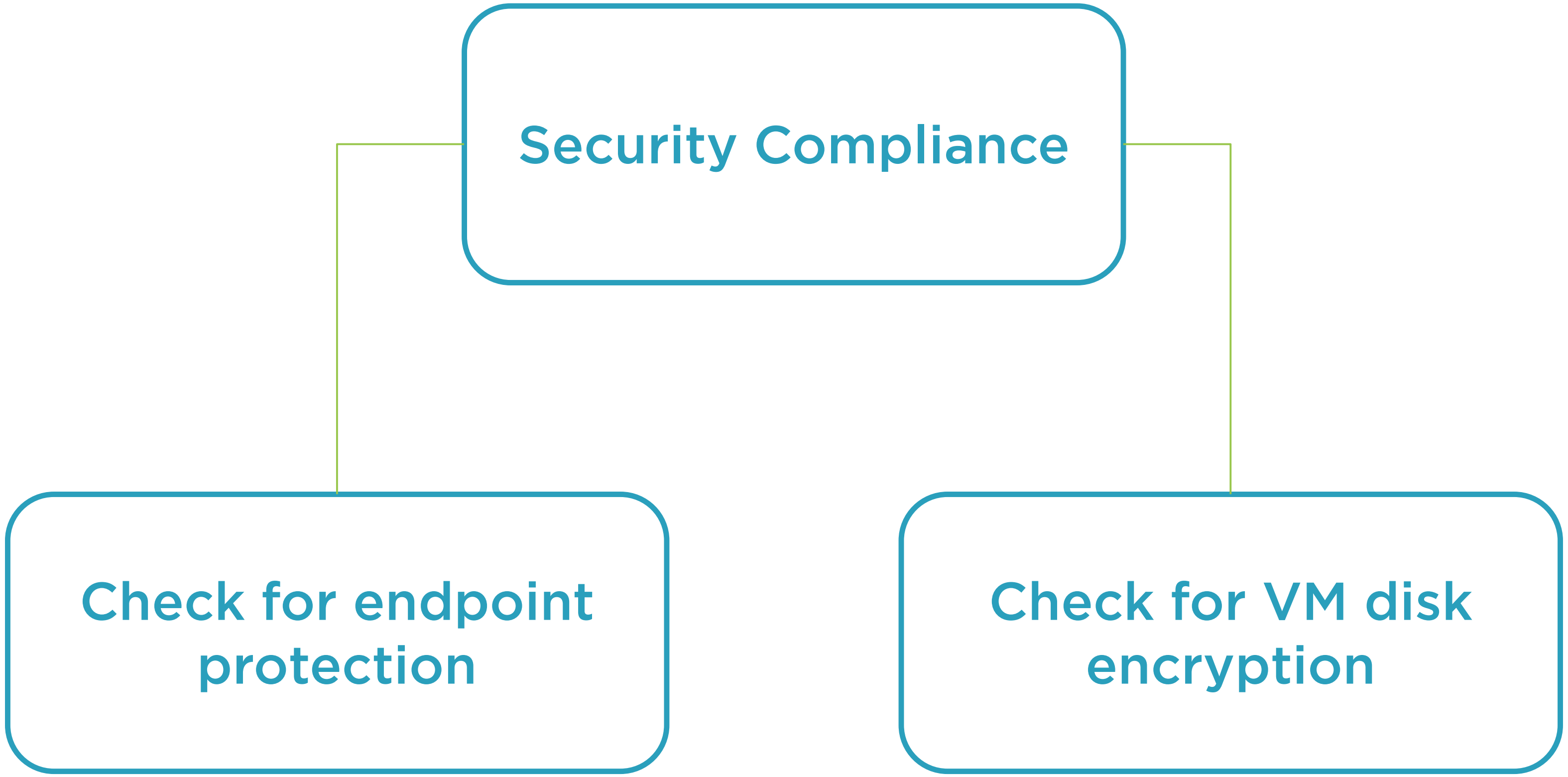
Policy Initiative Definitions

Policy Initiative Definitions

- Groups policies into a single unit
- Used when a single Azure governance goal consists of multiple checks
    - Example:
        - Initiative Definition: Security Compliance

Assign Policy **Assign Initiative**

Policy Initiative Definition Example



Microsoft Azure Policy Compliance

Policies apply to new and existing resources

Azure runs delta scans against resources are to ensure policy compliance

Geo-compliance

- “Allowed Locations” built-in policy

Demo

Assign policies using the Microsoft Azure portal

Demo

Assign policies using Microsoft Azure PowerShell cmdlets

Demo

View policies and assignments using the Microsoft Azure CLI

Demo

Create and assign a custom policy

Demo

Assign a built-in remediation policy

Summary

Resource Tagging

- Purpose
- How to tag resources

Microsoft Azure Policy

- Purpose
- Policy initiative definitions
- Exclusion scopes
- Built-in and custom policies