



## Azure Application Security

Protect Your Applications in the Cloud



# Introduction

# Reza Salehi

Cloud Consultant and Trainer



@zaalion





# Course Repository

<https://github.com/zaalion/oreilly-azure-app-security>



master

2 branches

0 tags

Go to file

Add file

<> Code



### Your master branch isn't protected

Protect this branch from force pushing, deletion, or require status checks before merging



clean up



.gitattributes

Initial checkin



.gitignore

slide deck



resources.txt

references

Help people interested in this repository understand your project by adding a

Local

Codespaces New

Clone



HTTPS

SSH

GitHub CLI

<https://github.com/zaalion/oreilly-azure-app->




Use Git or checkout with SVN using the web URL.

Open with GitHub Desktop

Open with Visual Studio

Download ZIP

# Azure Well-architected Framework

 Filter by title

Microsoft Azure Well-Architected Framework

## Overview


- > Reliability
- > Security
- > Cost Optimization
- > Operational Excellence
- > Performance Efficiency
- > Workloads
- > Services

Implementing Recommendations

 Download PDF

# Microsoft Azure Well-Architected Framework

Article • 03/27/2023 • 9 contributors

 Feedback

## In this article

Overview

Reliability

Security

Cost optimization

Show 3 more

The Azure Well-Architected Framework is a set of guiding tenets that you can use to improve the quality of a workload. The framework consists of five pillars of architectural excellence:

- Reliability
- Security
- Cost optimization
- Operational excellence
- Performance efficiency

# Microsoft Azure Well-Architected Framework: Security

- Identity management
- Protect your infrastructure
- Application security
- Data sovereignty and encryption
- Security resources





---

# Microsoft Azure Well-Architected Framework: Application Security

- Encrypt data in-transit with the latest supported TLS versions
- Protect against CSRF and XSS attacks
- Prevent SQL injection attacks
- Consider storing application secrets in Azure Key Vault



# Azure Security Controls V2

# Overview of Azure security controls (v2)

Article • 11/14/2022 • 4 minutes to read • 2 contributors

👉 Feedback

The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure.

This benchmark is part of a set of holistic security guidance that also includes:

- **Cloud Adoption Framework** – Guidance on security, including [strategy](#), [roles and responsibilities](#), [Azure Top 10 Security Best Practices](#), and [reference implementation](#).
- **Azure Well-Architected Framework** – Guidance on [securing your workloads](#) on Azure.
- **Microsoft Security Best Practices** – [recommendations](#) with examples on Azure.

The Azure Security Benchmark focuses on cloud-centric control areas. These controls are consistent with well-known security benchmarks, such as those described by the Center for Internet Security (CIS) Controls Version 7.1 and National Institute of Standards and Technology (NIST) SP 800-53. The following controls are included in the Azure Security Benchmark:



# Azure Security Controls (v2): ASB Control Domains

- Network security (NS)
- Identity Management (IM)
- Privileged Access (PA)
- Data Protection (DP)
- Asset Management (AM)
- Logging and Threat Detection (LT)



# Azure Security Controls (v2): ASB Control Domains

- Incident Response (IR)
- Posture and Vulnerability Management (PV)
- Endpoint Security (ES)
- Backup and Recovery (BR)
- Governance and Strategy (GS)



# Network Security (NS)

# Network Security (NS)

- NS-1: Implement security for internal traffic
- NS-2: Connect private networks together
- NS-3: Establish private network access to Azure services
- NS-4: Protect applications and services from external network attacks
- NS-5: Deploy intrusion detection/intrusion prevention systems (IDS/IPS)
- NS-6: Simplify network security rules
- NS-7: Secure Domain Name Service (DNS)



---

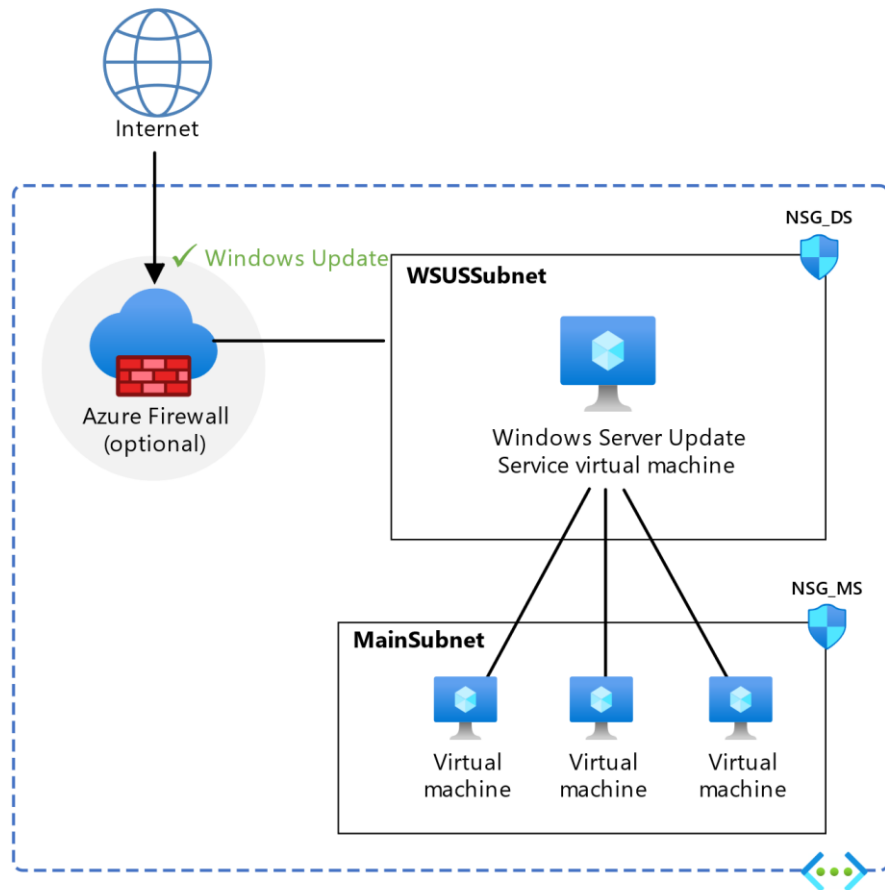
# NS-1: Implement security for internal traffic

- NSG
- Azure Firewall





# NSG





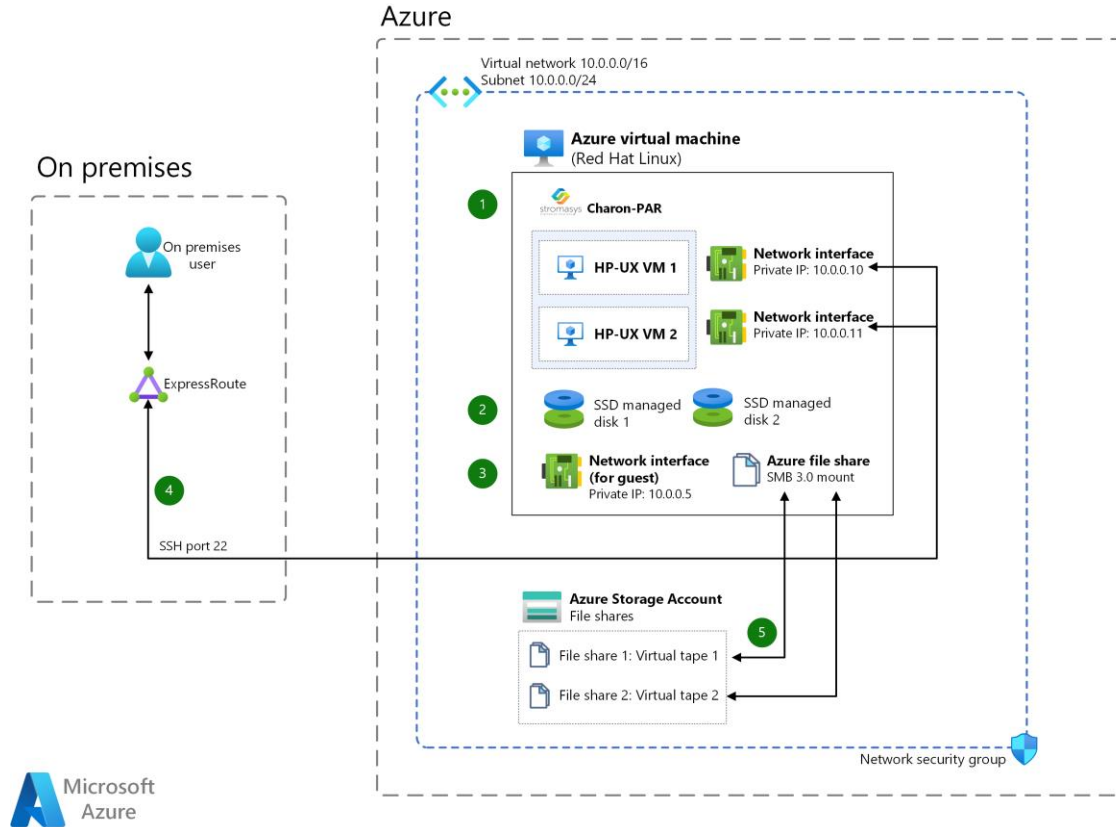
---

# NS-2: Connect private networks together

- Azure ExpressRoute
- Azure VPN
- Azure Network Peering
- Azure Private Link

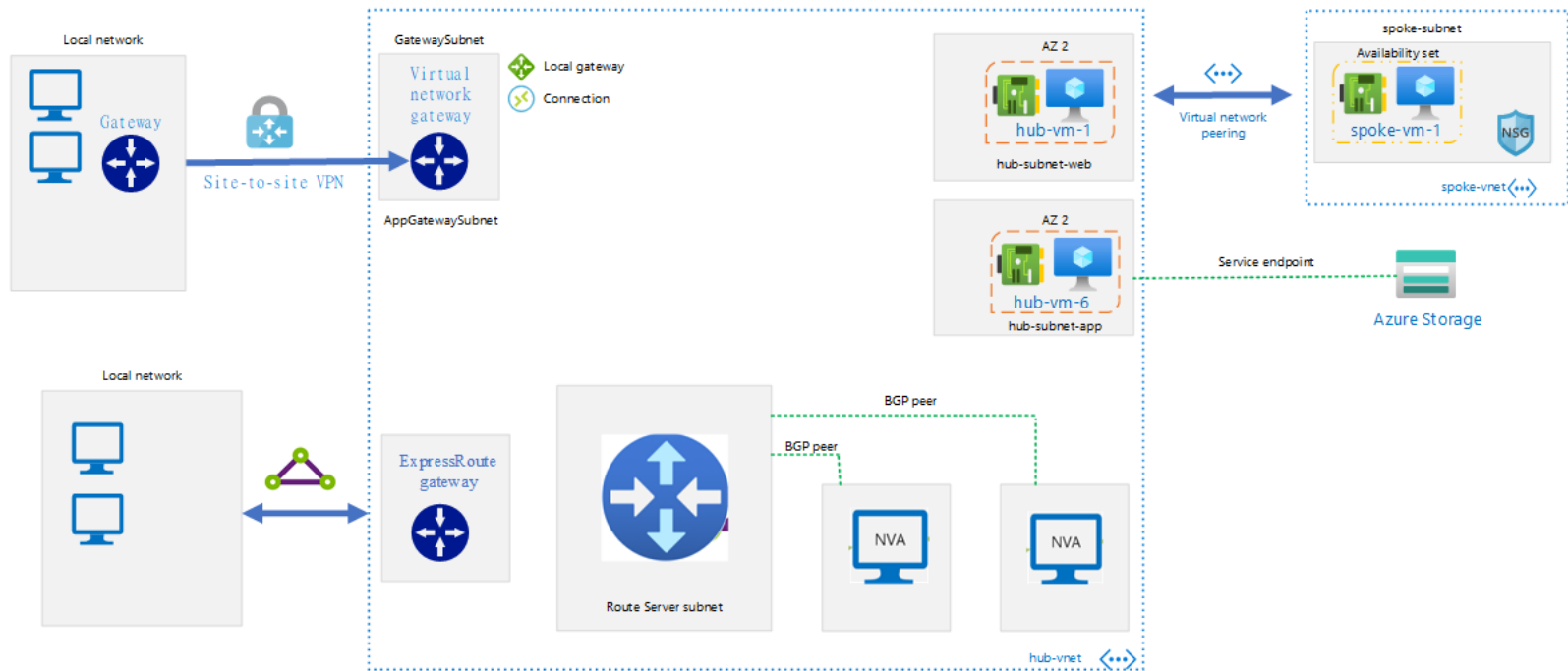


# Azure ExpressRoute

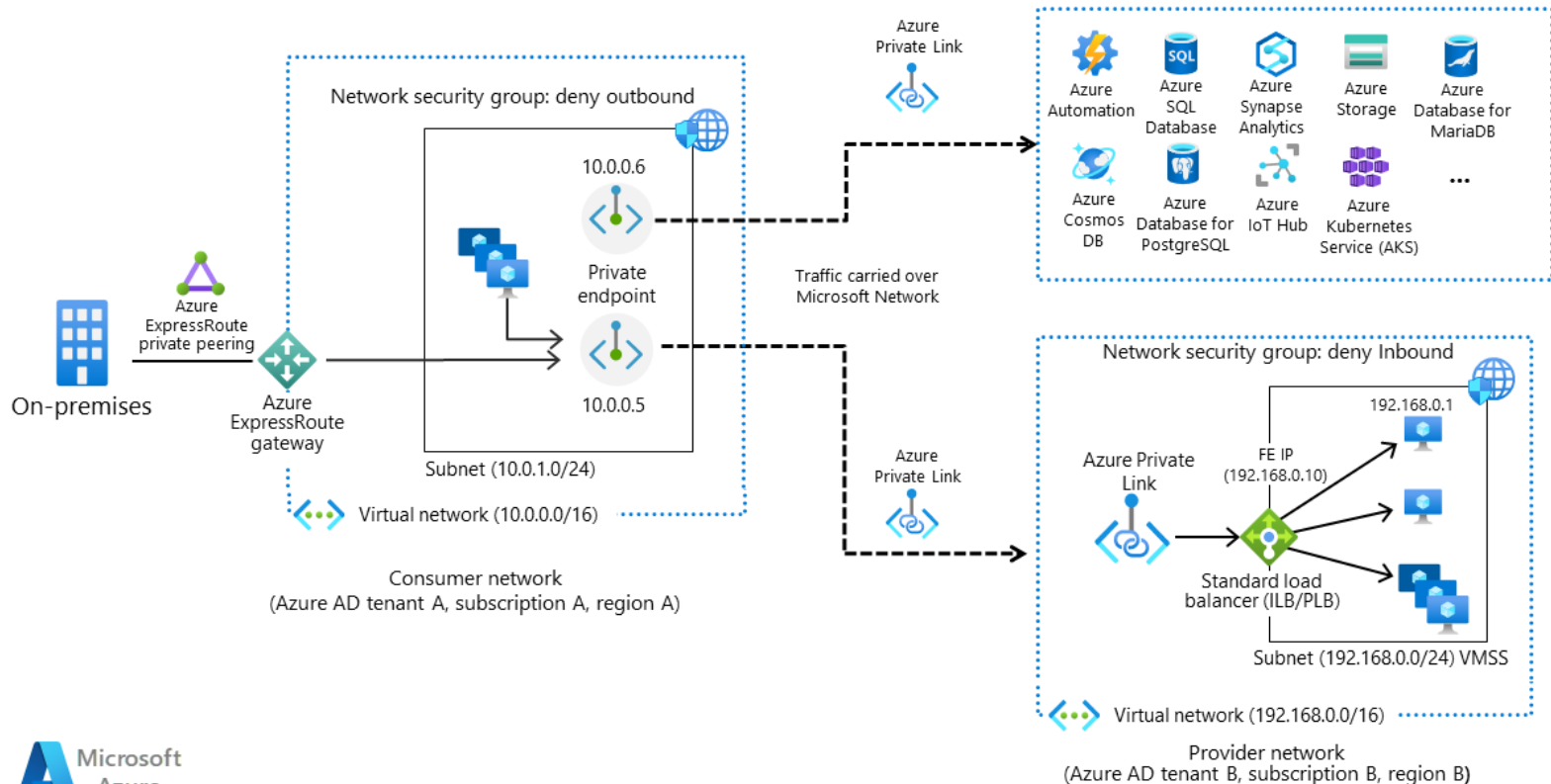




# Azure Network Peering



# Azure Private Link



---

# NS-3: Establish private network access to Azure services

- Azure Private Link
- Azure Service Endpoints





---

# NS-4: Protect applications and services from external network attacks

- Azure Firewall
- Azure WAF
- Azure DDoS Protection



---

# NS-5: Deploy intrusion detection/intrusion prevention systems (IDS/IPS)

- Azure Firewall
- Microsoft Defender for Workload



---

# NS-6: Simplify network security rules

- Azure Service Tags
- Application Security Groups



---

# NS-7: Secure Domain Name Service (DNS)

- Azure DNS



# Data Protection (DP)

# Data Protection (DP)

- DP-1: Discovery, classify and label sensitive data
- DP-2: Protect sensitive data
- DP-3: Monitor for unauthorized transfer of sensitive data
- DP-4: Encrypt sensitive information in transit
- DP-5: Encrypt sensitive data at rest



---

# DP-1: Discovery, classify and label sensitive data

- Azure Information Protection
- Azure SQL Data Discovery





# DP-2: Protect sensitive data

- Azure role-based access control (Azure RBAC)
- Customer data protection in Azure





---

# DP-3: Monitor for unauthorized transfer of sensitive data

- Azure Defender for SQL
- Azure Defender for Storage



---

# DP-4: Encrypt sensitive information in transit

- Encryption in transit with Azure
- TLS Security
- Double encryption for Azure data in transit



# DP-5: Encrypt sensitive data at rest

- Encryption at rest in Azure
- Data at rest double encryption in Azure



# Application Security

---

# Azure Log Analytics Workspace

- “A Log Analytics workspace is a unique environment for log data from Azure Monitor and other Azure services, such as Microsoft Sentinel and Microsoft Defender for Cloud.”



---

# Azure Virtual Networks

- What is Azure Virtual Network?
- Azure best practices for network security
- Azure network security overview



---

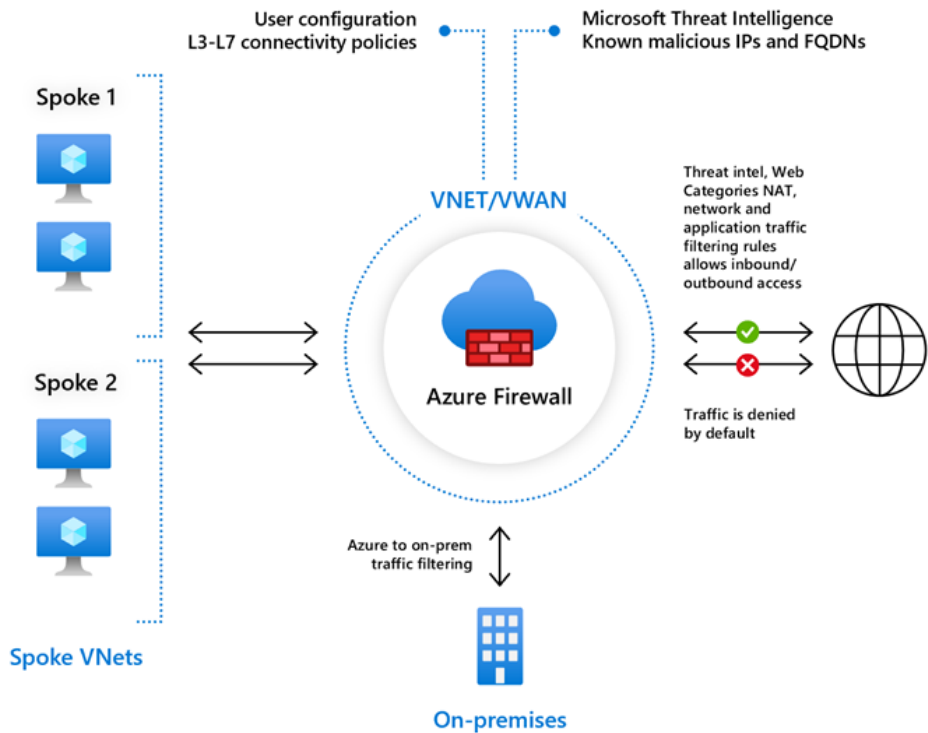
# Azure NSG

- Network security groups



# Azure Firewall

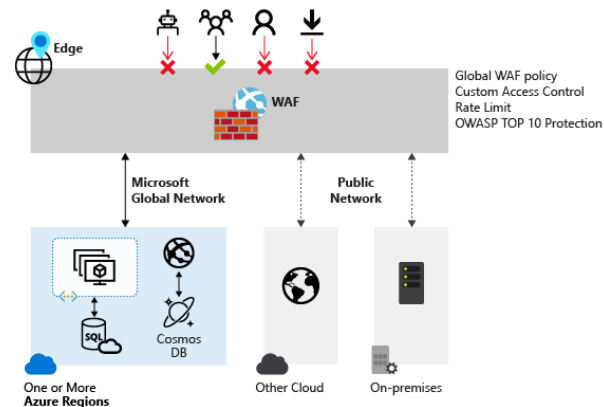
- What is Azure Firewall?





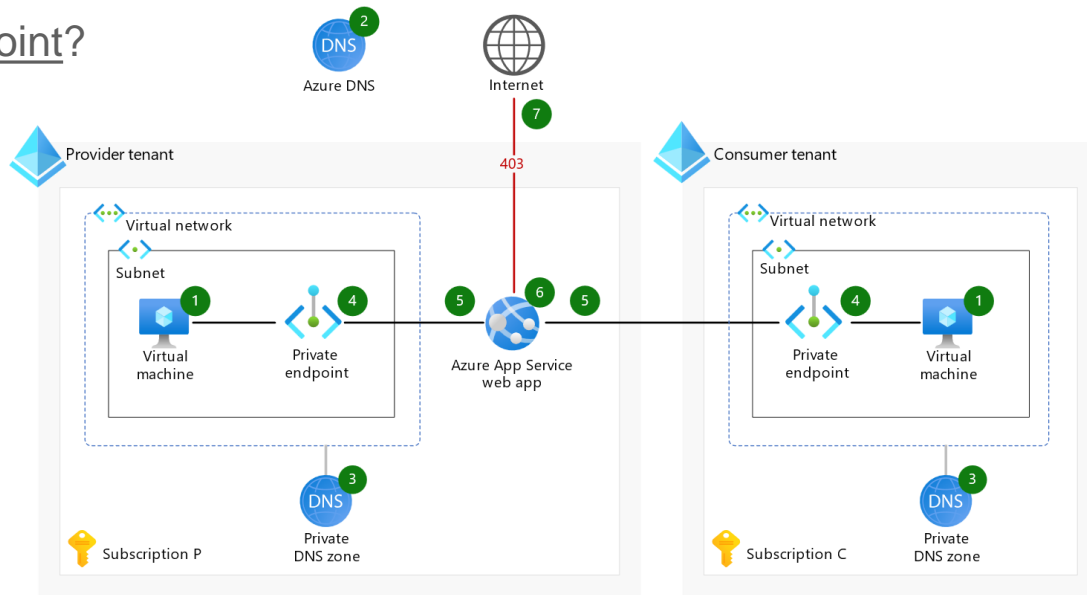
# Azure Web Application Firewall

- Azure Web Application Firewall on Azure Application Gateway
- Azure Web Application Firewall on Azure Front Door
- Azure Web Application Firewall on Azure Content Delivery Network



# Azure Private Endpoint

- What is a private endpoint?





# Azure Managed Identity

- What are managed identities for Azure resources?



---

# Azure Key Vault

- Azure Key Vault



---

# Securing Azure App Services/Functions

- Security in Azure App Service
- Encryption for data in transit
- Limiting the incoming traffic
- Limiting the outgoing traffic
- Key Vault References
- Private Endpoints
- Authentication/Authorization



---

# Securing Azure Storage Account

- Encryption at rest in Azure
- Data at rest double encryption in Azure





# Securing Azure SQL

- Azure SQL Database and SQL Managed Instance security capabilities
- Azure SQL Firewall





# Securing Azure Cosmos DB

- [Overview of database security in Azure Cosmos DB](#)
- [Cosmos DB Firewall](#)
- [Encryption for data at rest](#)
- [Private Endpoints](#)





---

# Azure Messaging Services

- Securing Azure Storage Queues
- Securing Azure Service Bus
- Securing Azure Event Hubs
- Securing Azure IoT Hub



# O'REILLY<sup>®</sup>

## Thank you!

Reza Salehi

@zaalion

