



Azure Security – Managing Security Operations

Aligned with Microsoft Certification Exam AZ-500

ine.com





Tracy Wallace

Azure Solutions Architect Expert



twallace@ine.com



@TracyWallaceINE



linkedin.com/in/tracy-wallace-746482a



Course Topics

Security Tools
Security Management

AZ-500 Objective Domains

- + Manage identity and access (30 - 35%)
- + Implement platform protection (15 - 20%)
- + **Manage security operations (25 - 30%)**
- + Secure data and applications (20 - 25%)

Exam AZ-500: Microsoft Azure Security Technologies

- + Monitor security by using Azure Monitor services
 - + create and customize alerts
 - + monitor security logs by using Azure Monitor
 - + configure diagnostic logging and log retention
- + Monitor security by using Azure Security Center
 - + evaluate vulnerability scans from Azure Security Center
 - + configure Just in Time VM access by using Azure Security Center
 - + configure centralized policy management by using Azure Security Center
 - + configure compliance policies and evaluate for compliance by using Azure Security center
- + Monitor security by using Azure Sentinel
 - + create and customize alerts
 - + configure data sources to Azure Sentinel
 - + evaluate results from Azure Sentinel
 - + configure a playbook for a security event by using Azure Sentinel
- + Configure security policies
 - + configure security settings by using Azure Policy
 - + configure security settings by using Azure Blueprint

Pre-requisites

Azure Fundamentals
Azure Administrations

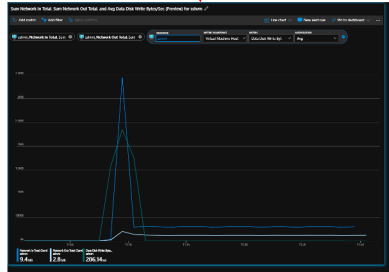


Azure Monitor

Azure Monitor

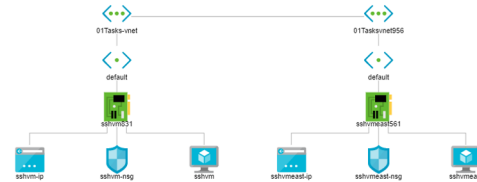
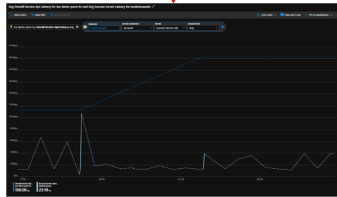
- Azure Monitor
- Demo: Azure Monitor

Azure Monitor



2 items.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION
Action taken as a result of Azure Policy evaluation	Succeeded	6 min ago	Thu Sep 26 ...	INE Demonstrations
Create or Update Virtual Network	Succeeded	16 min ago	Thu Sep 26 ...	INE Demonstrations



First 50 items.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT SEVERITY
Returns Storage Account SAS Token	Failed	2 min ago	Thu Sep 26 ...	INE Demonstrations	Microsoft.EventGrid
Returns Storage Account SAS Token	Failed	2 min ago	Thu Sep 26 ...	INE Demonstrations	Microsoft.EventGrid
Returns Storage Account SAS Token	Failed	2 min ago	Thu Sep 26 ...	INE Demonstrations	Microsoft.EventGrid
Returns Storage Account SAS Token	Failed	2 min ago	Thu Sep 26 ...	INE Demonstrations	Microsoft.EventGrid
Returns Storage Account SAS Token	Failed	2 min ago	Thu Sep 26 ...	INE Demonstrations	Microsoft.EventGrid
Returns Storage Account SAS Token	Failed	2 min ago	Thu Sep 26 ...	INE Demonstrations	Microsoft.EventGrid
Returns Storage Account SAS Token	Failed	2 min ago	Thu Sep 26 ...	INE Demonstrations	Microsoft.EventGrid
Returns Storage Account SAS Token	Failed	2 min ago	Thu Sep 26 ...	INE Demonstrations	Microsoft.EventGrid

Demo: Azure Monitor



Configuring Diagnostics on Resources



Configuring Diagnostics on Resources

- ▶ Demonstration: Virtual machine diagnostics
- ▶ Demonstration: Web app diagnostics
- ▶ Demonstration: Other resources

Resource Diagnostics Take-aways

- Diagnostic sources
 - Diagnostics extensions for VMs
 - Application Insights for Web Apps
 - Save directly to Log Analytics workspace
- Diagnostic destinations
 - Azure Monitor
 - Event Grid
 - Storage Account
 - Log Analytics
 - Direct to Log Analytics
- Diagnostics retention
 - 90 days base for Azure Monitor
 - 30 days base for Log Analytics



Implement Vulnerability Management

Implement Vulnerability Management

- Vulnerability Assessment
- Demo: Vulnerability Assessment

Vulnerability Assessment

- + Integrated with standard tier security center
- + Virtual machines
 - + Feature of Azure security center standard tier
 - + Powered by Qualys
 - + Runs as an extension deployed to the VM
 - + Reports on vulnerabilities at the OS level and above
 - + 3rd party scanners are also supported
- + Container registries
 - + Images are assessed for known vulnerabilities when pushed
- + Available for SQL Server
- + Third party tools recognized by security center

Demo: Vulnerability Assessment



Centralize Security Policy Management


Centralize Security Policy Management

- Central Security Policy
- Custom Policies
- Regulatory Compliance Policy
- Demo: Security Policies

Centralize Security Policy

- Manage policy from security center
- Apply policies to management groups and subscriptions
- Define default policy
- Over 90 specific policies

- + Security Center
- + Custom Policy
- + Regulatory Compliance

Basics Parameters  Policy Management

Specify parameters for

System updates on vii
AuditIfNotExists

Endpoint protection s
AuditIfNotExists

Vulnerabilities in secu
AuditIfNotExists

System updates shoul
AuditIfNotExists

Vulnerabilities in secu
AuditIfNotExists

Monitor missing Endp
AuditIfNotExists

Disk encryption shoul
AuditIfNotExists

Network Security Gro
Disabled







Choose a subscription or management group from the list below to perform the following tasks:

- View and edit the default ASC policy
- Add a custom policy
- Add regulatory compliance standards to your compliance dashboard

[Click here to learn more >](#)

3 MANAGEMENT GROUPS **3 SUBSCRIPTIONS**

Search by name

Name
▼  Tenant Root Group (3 of 3 subscriptions)
▼  Active (1 of 1 subscriptions)
 INE Demonstrations
▼  Corporate (1 of 1 subscriptions)
 INE Development
 INE Production

- + Security Center
- + Custom Policy
- + Regulatory Compliance

Centralize Security Policy

- Create custom policies
- Create a custom initiative
 - Choose from over 400 policies
 - Create your own custom policies
- Assign the initiative to a management group or subscription

Centralize Security Policy

Add compliance policies through security center
View in the regulatory compliance dashboard

Add regulatory compliance standards



Indu



Download report

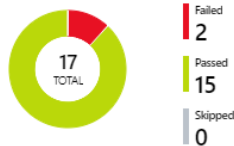


Manage compliance policies

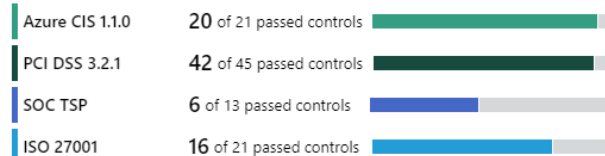


New content is available for the Azure CIS standard. Update your view by clicking on 'Manage compliance policies' above, or click here to learn more. →

Regulatory compliance assessment



Regulatory standards compliance status



Azure Security Benchmark

Track Azure Security

SWIFT CSP CSCF v2020

Track SWIFT CSP

- + Security Center
- + Custom Policy
- + Regulatory Compliance

Demo: Security Policies



Managing Alerts



Managing Alerts

- ▶ Azure alert components
- ▶ Azure alert signals
- ▶ Demonstration: Alerts

Azure Alerts

- Alert Components
 - Alert Rule
 - Resource
 - Condition
 - Action
 - Action Group
 - Communication
 - Function app
 - Logic app
 - Runbook
 - Webhook
 - ITSM
- Alert signals
 - Metrics
 - Activity Logs

Azure Alert Take-aways

- Alert Components
 - Alert Rule – Trigger/filter, Action group, settings
 - Action group – Email/SMS/phone, function app, logic app, runbook, webhook, ITSM
- Alert monitoring
 - Monitoring at the resource level
 - Azure Monitor
 - 3rd party



Configure Security Event Playbooks

Configure Security Event Playbooks

- Security Playbooks
- Demo: Security Center Automation

Security Playbooks

- + Security center workflow automation
- + Automate custom responses to security events
- + Built on Azure logic apps
- + Hundreds of integration providers
- + Triggered by security conditions
 - + Threat detection
 - + Security center recommendation
- + Use cases
 - + Remediation
 - + Auditing / logging
 - + Custom alerting

Demo: Security Center Automation



Azure Security Alerts and Incidents

Azure Security Alerts and Incidents

- Security Alerts
- Security Center Incidents
- Demo: Security Alerts

Security Alerts

- + Require security center standard edition
- + Threat detection
 - + Monitor traffic
 - + Collect logs
 - + Analyze for threats
- + Analytics
 - + Threat intelligence
 - + Behavioral analytics
 - + Anomaly detection
- + Classification
 - + High
 - + Medium
 - + Low
 - + Informational

Security Alerts

- + Sources
 - + Virtual machines
 - + Azure app services
 - + Azure containers
 - + Data
 - + SQL Database and Azure Synapse
 - + Storage
 - + Cosmos DB
 - + Network
 - + ARM*
 - + Key vault*

**Preview as of April 2020*

Security Center Incidents

- + Collection of related alerts
- + Uses Cloud Smart Alert Correlation
- + Based on Fusion Analytics
- + Uses MITRE attack matrix
- + Uses AI to analyze across subscriptions

Demo: Security Incidents



Azure Sentinel

Azure Sentinel

- + Azure Sentinel
- + Data Sources
- + Requirements
- + Demo: Azure Sentinel

Azure Sentinel

- + Security Information Event Management (SEIM)
- + Security Orchestration Automated Response (SOAR)
- + Collect – Users, devices, apps, infrastructure
- + Detect – Microsoft AI and threat intelligence
- + Investigate – deep investigation and hunting tools
- + Respond – Azure monitor workbooks

Data Sources

- + Service to service integration:
 - + Amazon Web Services - CloudTrail
 - + Office 365
 - + Azure AD / Activity / Security Center/ Information Protection / ATP
 - + Windows security events / firewall
- + External solutions via API
 - + Barracuda
 - + Symantec
 - + Citrix Analytics (Security)
- + External solutions via agent
 - + Connect using the Syslog protocol via an agent.

Requirements

- + Log Analytics workspace
- + Subscription contributor role
- + Resource group contributor or reader
- + Paid service

Demo: Azure Sentinel