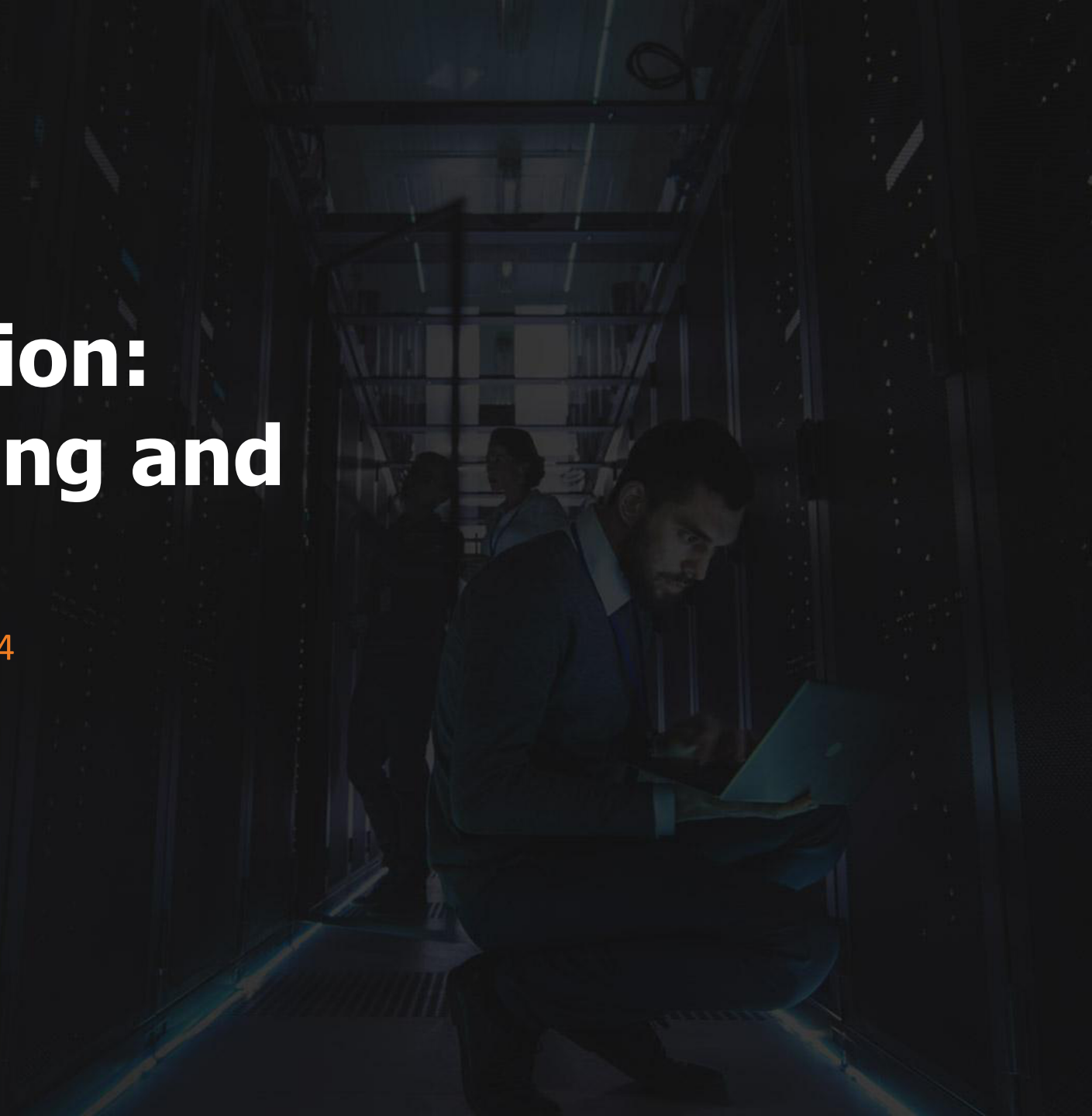




Azure Administration: Resource Monitoring and Protection

Aligned with Microsoft Certification Exam AZ-104

ine.com



Course Topics

Resource Monitoring
Azure Monitor and Log
Analytics
Application Monitoring
Recovery Services
Azure Backup

AZ-104 Objective Domains

- Manage Azure Identities and Governance (15-20%)
- Implement and Manage Storage (10-15%)
- Deploy and Manage Azure Compute Resources (25-30%)
- Configure and Manage Virtual Networking (30-35%)
- **Monitor and back up Azure resources (10-15%)**

Exam AZ-104: Microsoft Certified Azure Administrator Associate

- Monitor resources by using Azure Monitor
 - + configure and interpret metrics
 - + analyze metrics across subscriptions
 - + configure Log Analytics
 - + implement a Log Analytics workspace
 - + configure diagnostic settings
 - + query and analyze logs
 - + create a query
 - + save a query to the dashboard
 - + interpret graphs
 - + set up alerts and actions
 - + create and test alerts
 - + create action groups
 - + view alerts in Azure Monitor
 - + analyze alerts across subscriptions
 - + configure Application Insights
- Implement backup and recovery
 - + configure and review backup reports
 - + perform backup and restore operations by using Azure Backup Service
 - + create a Recovery Services Vault
 - + use soft delete to recover Azure VMs
 - + create and configure backup policy
 - + perform site-to-site recovery by using Azure Site Recovery

Pre-requisites

- **Azure Fundamentals**



Resource Diagnostics

Resource Diagnostics

- ❓ Azure Diagnostic Tools
- ❓ Demo: Configure Diagnostics
- ❓ Demo: View Diagnostics

Diagnostic Tools

- + Built-in
 - + Activity log
 - + Performance
- + Resource specific
 - + Storage
 - + App service
 - + Virtual machine
- + Azure monitor
 - + Diagnostics page
 - + Activity log
 - + Performance
 - + Log analytics

A man with glasses and a beard is shown in profile, looking at a computer screen. The screen displays lines of code, likely in a programming language like Python or JavaScript. The background is dark, and the overall tone is professional and technical.

Demo: Configure Diagnostics Demo: View Diagnostics



Alerts

Alerts

- ☐ Azure Alerts
- ☐ Demo: Set Alerts
- ☐ Advanced Alerts
- ☐ Demo: Set A Budget Alert
- ☐ Alert Takeaways

Azure Alerts

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

Demo: Set A Performance Alert

Advanced Alerts

- + Budget Alerts
- + Azure AD
 - + Password reset
 - + Users at risk
 - + Privileged identity management

Demo: Set A Performance Alert

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

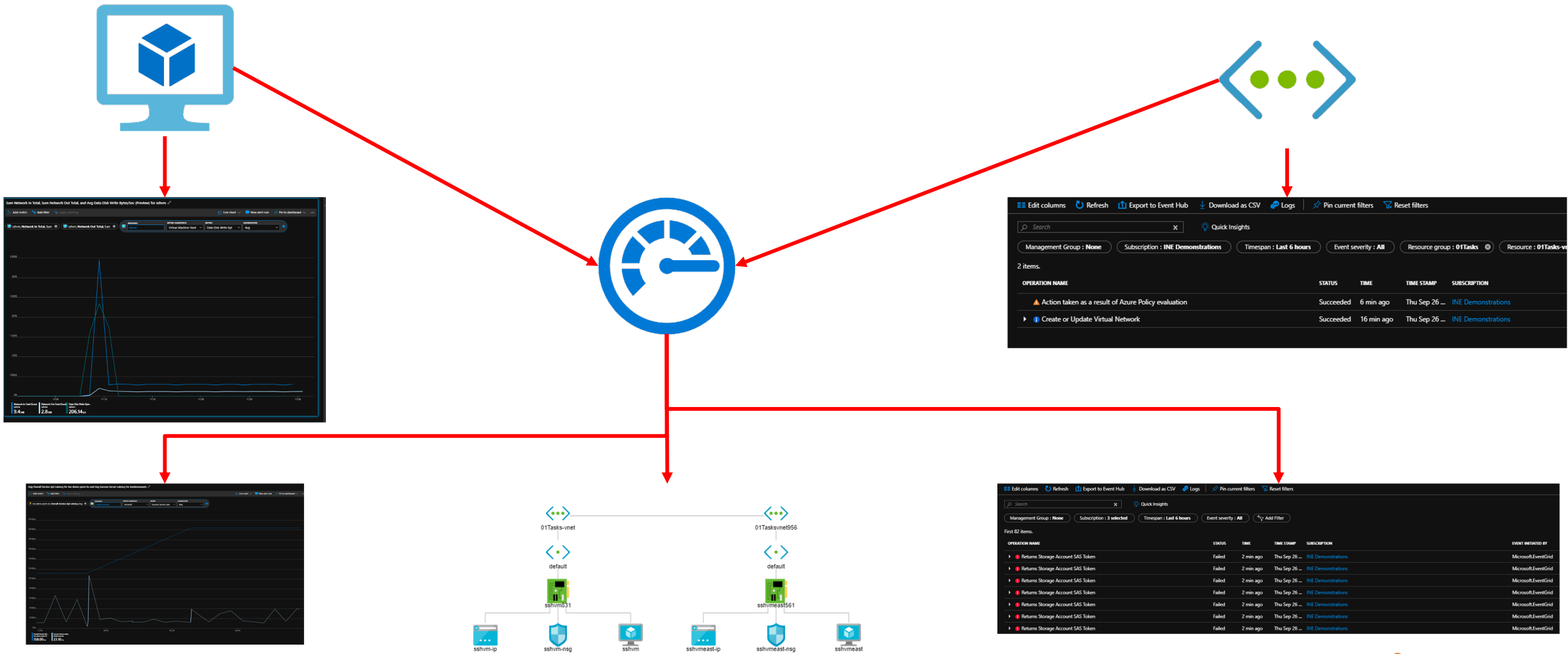


Azure Monitor

Azure Monitor

- ❓ Azure Monitor
- ❓ Demo: Azure Monitor

Azure Monitor



Demo: Azure Monitor



Log Analytics

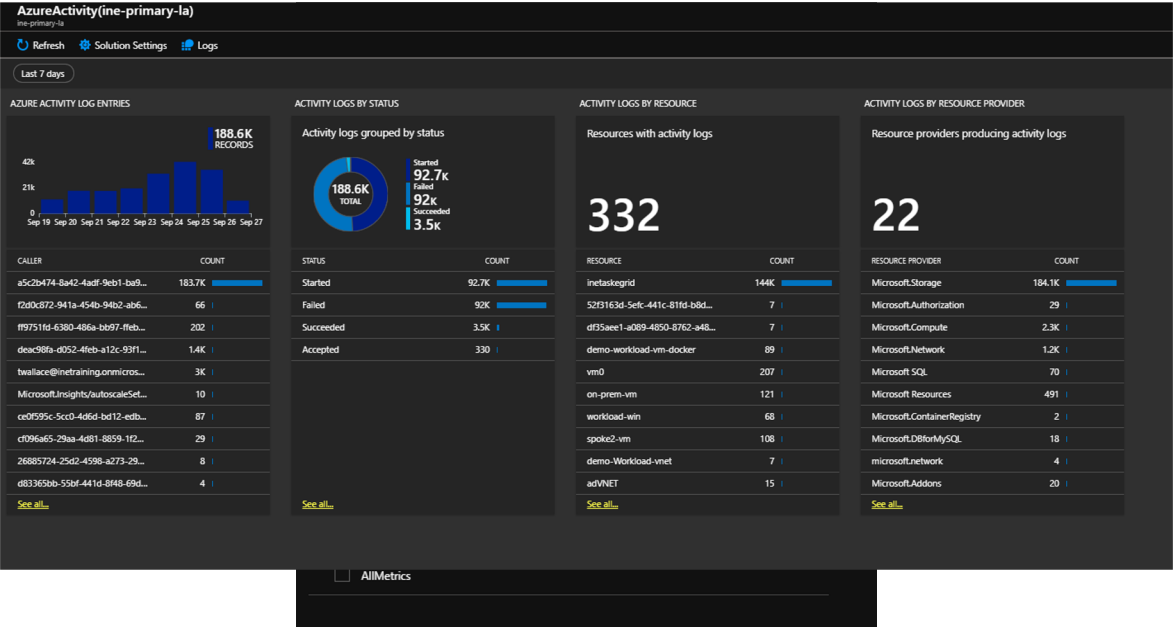
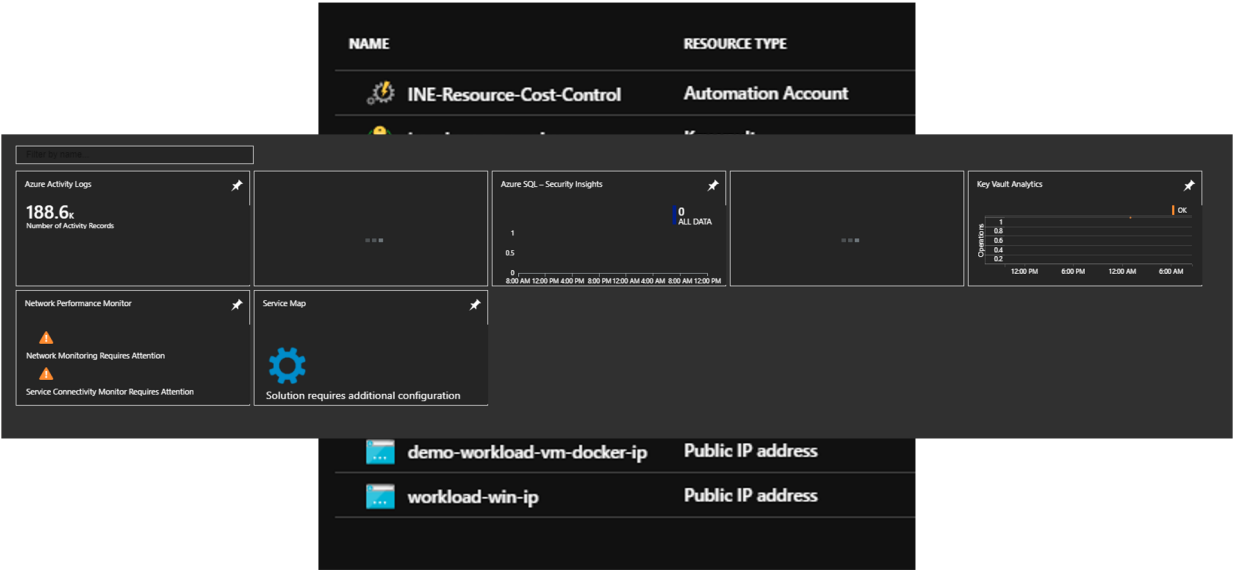
Log Analytics

- ❑ Log Analytics
- ❑ Log Analytics Sources
- ❑ Log Analytics Solutions
- ❑ Demo: Log Analytics

Log Analytics

Log Analytics Sources

Log Analytics Solutions



Demo: Log Analytics



Log Analytics Queries

Log Analytics Queries

- ❑ Query Elements
- ❑ Data Sources
- ❑ Query Examples
- ❑ Demo: Log Analytics Queries

Query Elements

Query Sources

Query Examples

source | operator1 | operator2 | operator n | render instruction

source – origin of diagnostics data (i.e. Logs)

operator – transform data (where, join, project, etc.)

render instructions – display instructions (areachart, table, timechart, etc.)

Query Elements

Query Sources

Query Examples

- ▼ ine-primary-LA
 - ▼ ContainerInsights
 - ▶ ContainerImageInventory
 - ▶ ContainerInventory
 - ▶ ContainerLog
 - ▶ ContainerNodeInventory
 - ▶ ContainerServiceLog
 - ▶ InsightsMetrics
 - ▶ KubeEvents
 - ▶ KubeHealth
 - ▶ KubeMonAgentEvents
 - ▶ KubeNodeInventory
 - ▶ KubePodInventory
 - ▶ KubeServices
 - ▼ InfrastructureInsights
 - ▶ InsightsMetrics
 - ▶ VMBoundPort
 - ▶ VMConnection
 - ▶ WorkloadMonitoringPerf
 - ▼ LogManagement
 - ▶ AADDomainServicesAccountLogon
 - ▶ AADDomainServicesAccountManagement
 - ▶ AADDomainServicesDirectoryServiceAccess
 - ▶ AADDomainServicesLogonLogoff
 - ▶ AADDomainServicesPolicyChange
 - ▶ AADDomainServicesPrivilegeUse
 - ▶ AADDomainServicesSystemSecurity
 - ▶ ADFActivityRun
 - ▶ ADFPipelineRun
 - ▶ ADFTripleRun

Query Elements

Query Sources

Query Examples

Events logged in the last 24 hours

```
Event | where EventLog == "Application" |  
where TimeGenerated < ago(24h)
```

Diagnostic and metric data that includes 'demo' in any metadata

```
search in (AzureDiagnostics, AzureMetrics)  
'demo'
```

Number of records by type in the last hour in a bar chart.

```
search *  
| where TimeGenerated > ago(1h)  
| summarize CountOfRecords = count() by Type  
| render barchart
```

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples>

Demo: Log Analytics Queries



Monitor Across Subscriptions

Monitoring Across Subscriptions

- ❑ Monitoring Options
- ❑ Demo: Monitor Cross-subscription
- ❑ Take-aways

Monitoring Options

Demo: Monitor Cross-subscription

Cross-subscription Metrics Take-aways

- + Azure monitor is king
 - + Centralized monitoring for multiple subscriptions*
 - + Log analytics is being melted into Azure monitor
- + Understand the importance of log analytics
- + Understand the flow for cross-subscription monitoring of activity log



Monitor Applications with Application Insights

Monitor Application with Application Insights

- + Application Monitoring
- + Application Insights
- + App Insights Telemetry
- + App Insights Reports
- + Integrating App Insights
- + Demo: App Insights

Application Monitoring

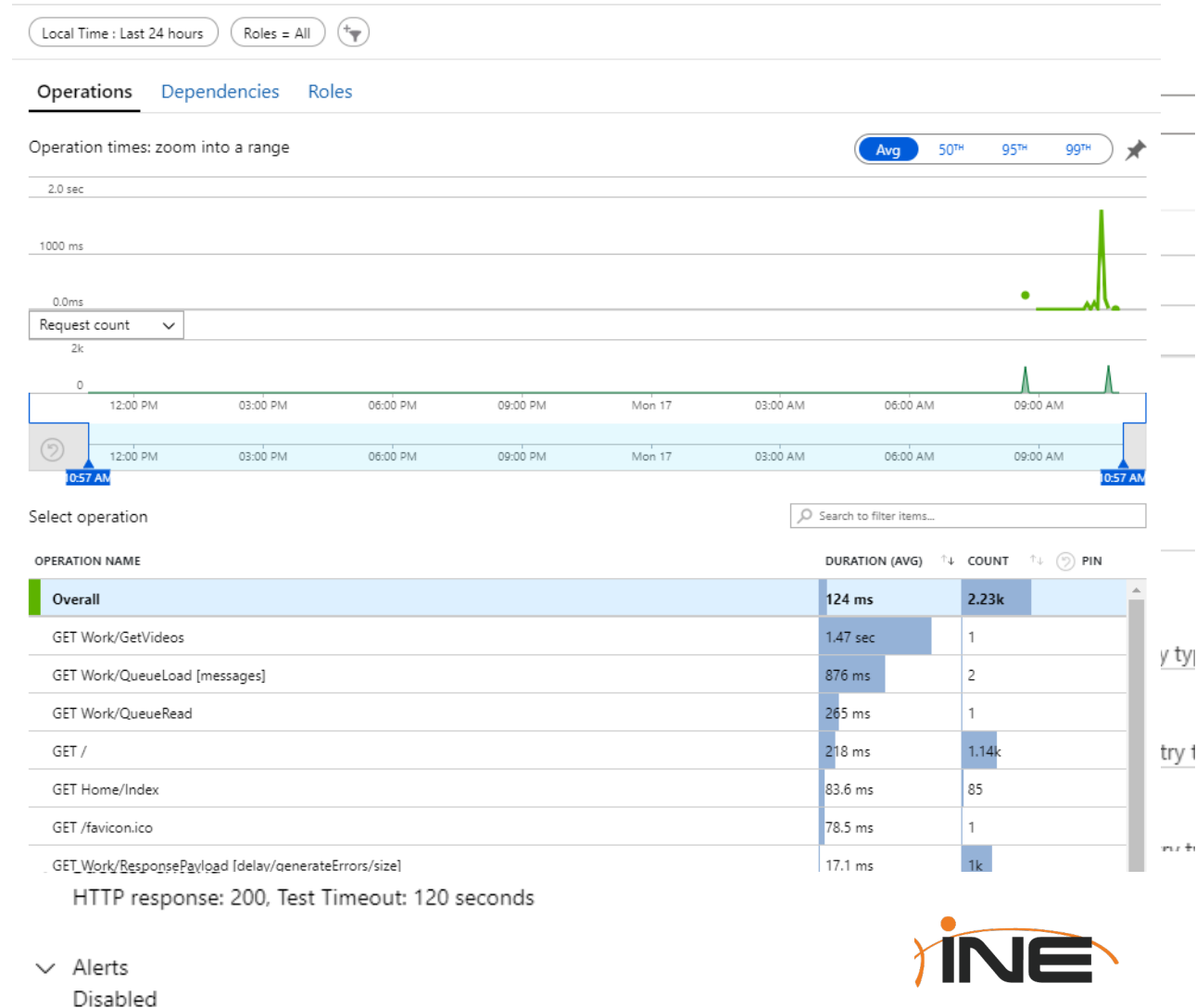
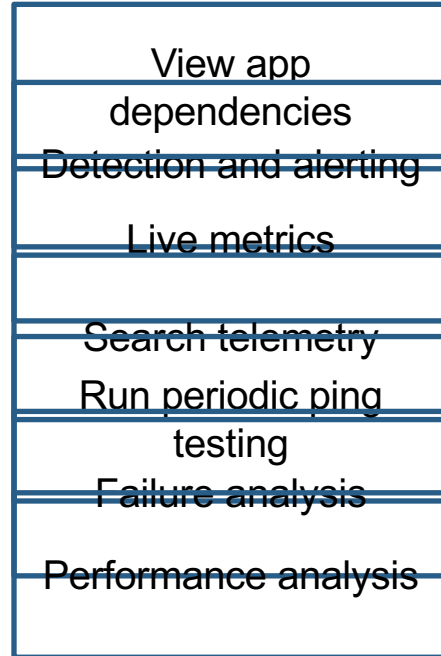
Application Insights

Investigate

- Application map
- Smart Detection
- Live Metrics Stream
- Search
- Availability
- Failures
- Performance
- Troubleshooting guides (pre...

Monitoring

- Alerts
- Metrics
- Logs
- Workbooks











App Insights Telemetry

- Request rates, response times, and failure rates
- Dependency rates, response times, and failure rates
- Exceptions
- Page views and load performance
- AJAX calls from web pages
- Performance counters from your Windows or Linux server machines
- Host diagnostics from Docker or Azure
- Diagnostic trace logs from your app
- Custom events and metrics

App Insights Reports

^ Usage (8)

 Active Users	 Analysis of Page Views	 Engaged Users	 New, Returning and Churned ...	 Usage Calendar
 Usage by hours of the day	 Segmented Funnel	 Authenticated User Timelines		

^ Retention (4)

 Cohort Analysis	 N-Period Retention	 Unbounded Retention	 Bracket Retention
--	--	---	---

^ Business Hypotheses (2)

 Improving User Retention	 Increasing Active Users
---	---

Integrating App Insights

- Instrument at runtime:
 - + ASP.NET and ASP.NET core on Azure web apps
 - + ASP.NET on IIS
- Integrate into application:
 - + ASP.NET
 - + ASP.NET Core
 - + .NET (and .NET core) Console
 - + Java
 - + Node.JS
 - + REST API
 - + Web pages
- Visual Studio App Center
- Log Analytics

Demo: App Insights



Overview of Recovery Services

Overview of Recovery Services

- Azure Recovery Services
- Azure Backup Options
- Azure Site Recovery Options

Azure Recovery Services

Azure Backup Options

- Azure
 - + Virtual machine backups
 - + File service backups
 - + SQL Server on an Azure virtual machine
- On-premises
 - + File and folder
 - + Virtual machine*
 - + Physical machine*
 - + Workloads – SQL Server, SharePoint, Exchange*

* - Requires Azure Backup Server

Azure Site Recovery Options

- Architectures
 - + Hyper-V standalone server
 - + Hyper-V SCVMM cloud
 - + VMWare stand-alone server
 - + VMWare vCenter
 - + Physical servers
- Failover
 - + Test failover
 - + On-premises to Azure
 - + On-premises to on-premises
- Failback



Provision and Configure Recovery Services Vault

Provision and Configure Recovery Services Vault

- Provision Recovery Services Vault
- Backup Infrastructure
- Restore Options
- Demo: Provision and Configure Recovery Services Vault

Provision Recovery Services Vault

Project Details

Select the subscription and the resource group in which you want to create the vault.

Subscription * ⓘ

Resource group * ⓘ

[Create new](#)

Instance Details

Vault name * ⓘ

Region * ⓘ

```
New-AzRecoveryServicesVault -Name DemoVault  
-ResourceGroupName 01Tasks -Location EastUS
```

Backup Infrastructure

Demo: Provision and Configure Recovery Services Vault



Backup and Restore Files and Folders

Backup and Restore Files and Folders

- File and Folder Backup
- Demo: File and Folder Backup

File and Folder Backup

- Install MARS agent
- Register MARS agent with service credentials file
- Set passphrase
- Schedule backup (up to 3 per day)
- Restrictions
 - + Windows only
 - + Windows Server 2008 R2 +, Windows 8 +
 - + No read-only volume
 - + No offline volumes
 - + No network shares
 - + No BitLocker protection
 - + No removable media

Demo: File and Folder Backup



Virtual Machine Backup

Configure VM Backup

- VM Backup Options
- VM Restore Options
- Soft Delete
- Demo: Manage VM Backups
- Demo: Restore a VM
- Demo: Soft Delete

VM Backup Options

- Backup frequency (max daily)
- Backup time
- Backup retention

Restore Options

- Azure VM
 - + Create a new VM
 - + Restore a disk
 - + Replace a disk
 - + Restore files*
 - * This is really the "restore a disk option" with a script to attach the disk.
- File and folder
 - + MARS agent
- On-prem
 - + Restore from Data Protection Manager or Azure Backup Server

Soft Delete

- 14-day automatic backup retention after delete
- No extra cost
- Can be disabled

Demo: Manage VM Backups

Demo: Restore a VM

Demo: Soft Delete



Configure and Review Backup Reports

Configure and Review Backup Reports

- Backup Reports
- Demo: Backup Reports

Backup Reports

- Based on diagnostics settings
- Available through PowerBI

Demo: Backup Reports



VM Recovery with ASR

VM Recovery with ASR

- + ASR Recovery Options
- + VM Recovery Requirements
- + Demo: Azure VM Recovery

ASR Recovery Options

VM Recovery Requirements

- Recovery Vault
- Network(s)
- Storage Account
- Administrative Account

Demo: Azure VM Recovery