



Azure Study Group

AZ-301 - Microsoft Azure Architect Design

Amber Sitko
Partner Technology Strategist



Week 1

Determine Workload Requirements
(10-15%)

Agenda

1

Agenda

2

Speaker
Introduction

3

Feedback
Loop

4

Objective
Review

5

Open Mic

Series Agenda

1	Determine Workload Requirements (10-15%)
2	Design for Identity and Security (20-25%)
3	Design a Data Platform Solution (15-20%)
4	Design a Business Continuity Strategy (15-20%)
5	Design for Deployment, Migration, and Integration (10-15%)
6	Design an Infrastructure Strategy (15-20%)

<https://aka.ms/azurecsg>

Amber Sitko

- Technology Strategist based in the Detroit Area
- 19 years with Microsoft (16 of those years in MCS), 25+ in the industry
- Started with SQL Server 7.0/Sybase

Call is being recorded



Feedback Loop

Exam basics



40-60 questions

- Some questions worth more than 1 point
- Answer all the questions
 - *No penalty for guessing*
 - *Some questions cannot be skipped!*
- Mark items for review if you're not sure of your answer



Plan for 180 minutes

- 150 minutes to answer questions
- 30 minutes for instructions, comments, score reporting, etc.



More than just multiple-choice questions!

- Build list, hot area, active screen, drag and drop, etc.
- *Performance based coming soon!*



Case Studies

- Detailed information on business and technical requirements; existing environment and other background you need to solve problems
- Requires you to understand and integrate information across multiple sources, determine what's important, and make the best decision

- To prep – go through exam objectives
- Carefully read the questions, look for key words
- Write anything that might be helpful to organize thoughts
- docs.Microsoft.com – all exam questions have some type of authoritative answer, typically documentation

- **Labs**
- AZ-300 - <https://github.com/MicrosoftLearning/AZ-300-MicrosoftAzureArchitectTechnologies>
- AZ-301 - <https://github.com/MicrosoftLearning/AZ-301-MicrosoftAzureArchitectDesign>
- <http://aka.ms/CertBlog> - Learning Blog
- <http://aka.ms/az-301> - test link

Introducing performance-based testing

Prove your skills with hands-on labs



Starting with Azure, each job role certification will have performance-based labs



Map to what you do everyday



Demonstrate your skills using the technology



At least one exam in certification will have labs; that exam have at least 2 labs with 7-9 tasks

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation options like 'Create a resource', 'All services', 'FAVORITES', 'Dashboard', 'Resource groups', 'All resources', 'Recent', 'App Services', 'Virtual machines (classic)', 'Virtual machines', 'SQL databases', 'Cloud services (classic)', 'Subscriptions', 'Azure Active Directory', 'Monitor', 'Security Center', 'Cost Management + Bill...', 'Help + support', and 'Advisor'. The main content area shows the 'All resources' page for the 'Netlogon' subscription. It includes a search bar, filters, and a table of resources. The table has columns for NAME, TYPE, RESOURCE GR..., LOCATION, and SUBSCRIPTION. The 'VM1Disk1' resource is selected, and its details are shown in the right pane.

NAME	TYPE	RESOURCE GR...	LOCATION	SUBSCRIPTION
VM1	Virtual machine	RG1lod7290156	East US	Pay-As-You-Go
VM1	Virtual machine	RG1lod7293122	East US	Pay-As-You-Go
VM1	Virtual machine	RG1lod7293312	East US	Pay-As-You-Go
VM1	Virtual machine	RG1lod7294322	East US	Pay-As-You-Go
VM1Disk1	Disk	RG1LOD7289505	East US	Pay-As-You-Go
VM1Disk1	Disk	RG1LOD7289687	East US	Pay-As-You-Go
VM1Disk1	Disk	RG1LOD7290156	East US	Pay-As-You-Go
VM1Disk1	Disk	RG1LOD7293122	East US	Pay-As-You-Go
VM1Disk1	Disk	RG1LOD7293312	East US	Pay-As-You-Go
VM1Disk1	Disk	RG1LOD7294322	East US	Pay-As-You-Go
VM1-NetworkInterface	Network interface	RG1lod7289505	East US	Pay-As-You-Go
VM1-NetworkInterface	Network interface	RG1lod7290667	East US	Pay-As-You-Go

Time remaining 01:54:00

Tasks

Click to expand each objective

- + Task 1
- + Task 2
- + Task 3
- + Task 4
- + Task 5
- + Task 6
- + Task 7



Help



Username/
Password



Next

Objective Review – *Determine workload requirement (10-15%)*

Gather Information and Requirements

- *May include but not limited to:* Identify compliance requirements, identity and access management infrastructure, and service-oriented architectures (e.g., integration patterns, service design, service discoverability); identify accessibility (e.g. Web Content Accessibility Guidelines), availability (e.g. Service Level Agreement), capacity planning and scalability, deploy-ability (e.g., repositories, failback, slot-based deployment), configurability, governance, maintainability (e.g. logging, debugging, troubleshooting, recovery, training), security (e.g. authentication, authorization, attacks), and sizing (e.g. support costs, optimization) requirements; recommend changes during project execution (ongoing); evaluate products and services to align with solution; create testing scenarios

Optimize Consumption Strategy

- *May include but not limited to:* Optimize app service, compute, identity, network, and storage costs

Design an Auditing and Monitoring Strategy

- *May include but not limited to:* Define logical groupings (tags) for resources to be monitored; determine levels and storage locations for logs; plan for integration with monitoring tools; recommend appropriate monitoring tool(s) for a solution; specify mechanism for event routing and escalation; design auditing for compliance requirements; design auditing policies and traceability requirements

Objective Review - #1

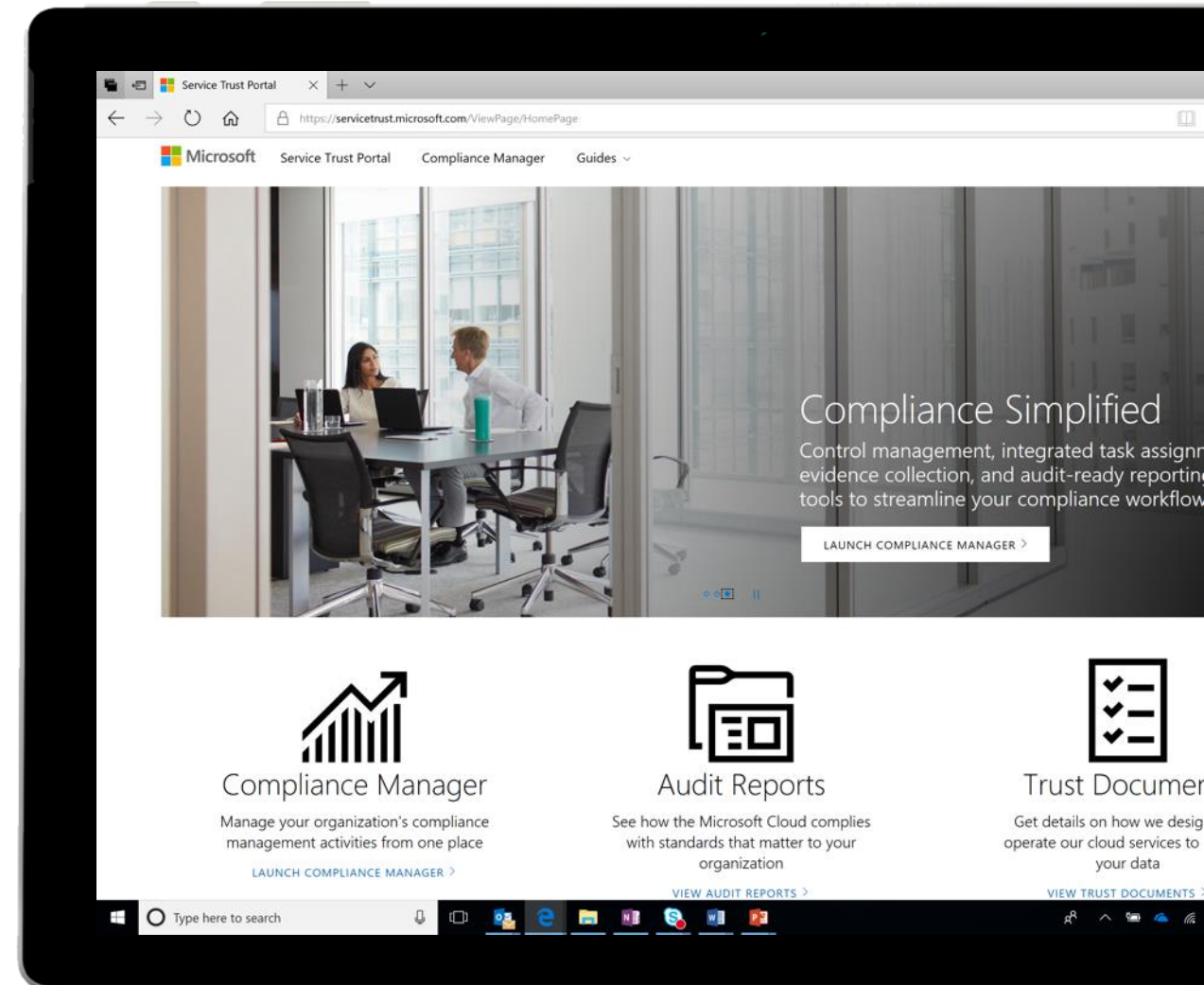
Gather Information and Requirements

- Identify compliance requirements
- Identity and access management infrastructure, and service-oriented architectures (e.g., integration patterns, service design, service discoverability)
- Identify accessibility (e.g. Web Content Accessibility Guidelines), availability (e.g. Service Level Agreement)
- Capacity planning and scalability, deploy-ability (e.g., repositories, failback, slot-based deployment), configurability, governance, maintainability (e.g. logging, debugging, troubleshooting, recovery, training)
- Security (e.g. authentication, authorization, attacks)
- Sizing (e.g. support costs, optimization) requirements; recommend changes during project execution (ongoing)
- Evaluate products and services to align with solution
- Create testing scenarios

Service Trust Portal

Assess Microsoft Cloud with rich resources around security, compliance, and privacy

- **In-depth information**
Access to FedRAMP, ISO, SOC audit reports, data protection white papers, security assessment reports, and more
- **Powerful assessment tools**
Leverage our self-service risk assessment tool, Compliance Manager, to simplify your compliance journey
- **Easy navigation**
Centralized resources around security, compliance, and privacy for all Microsoft Cloud services

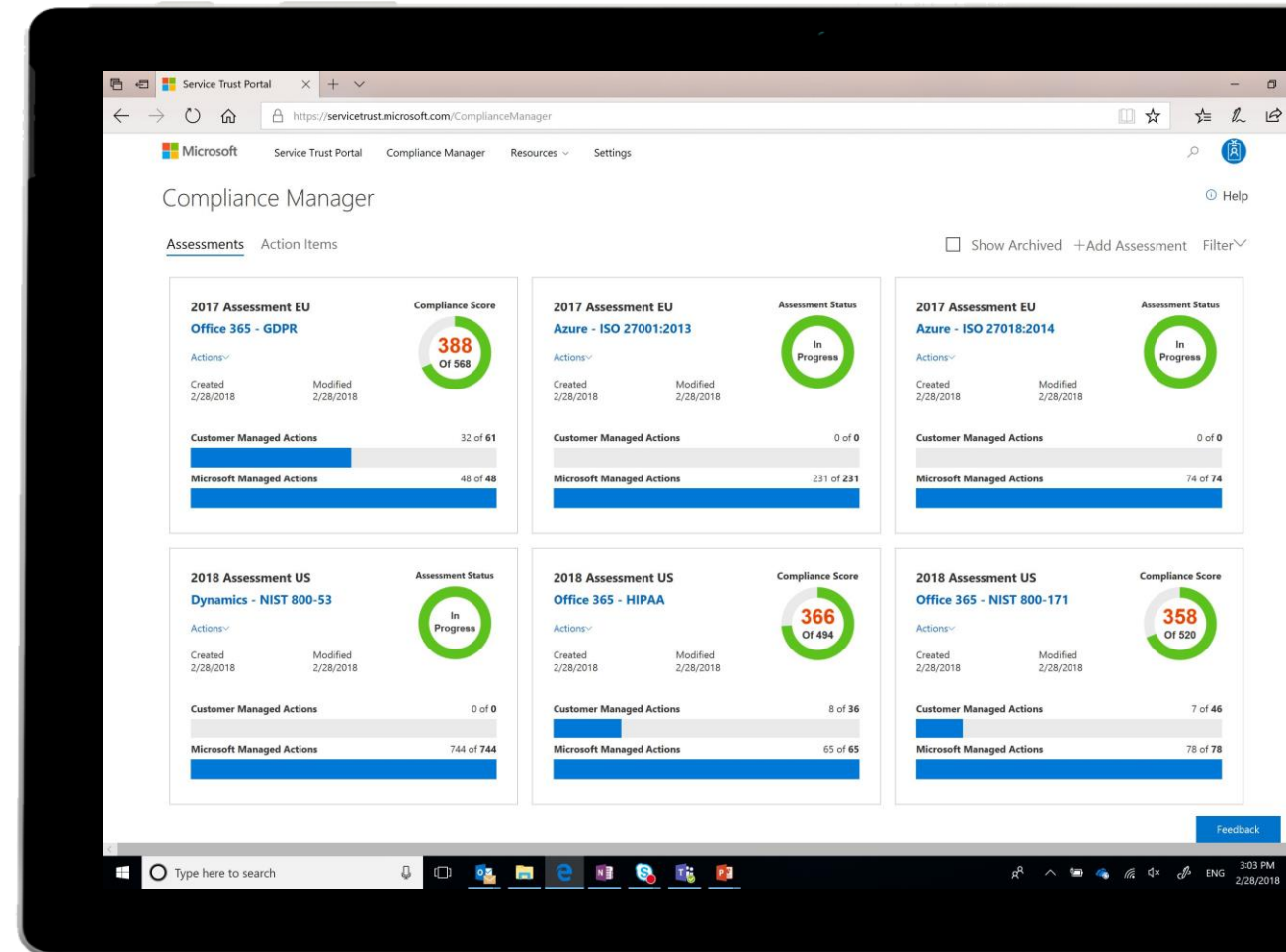


Compliance Manager

Manage your compliance from one place

- Ongoing risk assessment
An intelligent score reflects your compliance posture against regulations or standards
- Actionable insights
Recommended actions to improve your data protection capabilities
- Simplified compliance
Streamlined workflow across teams and richly detailed reports for auditing preparation

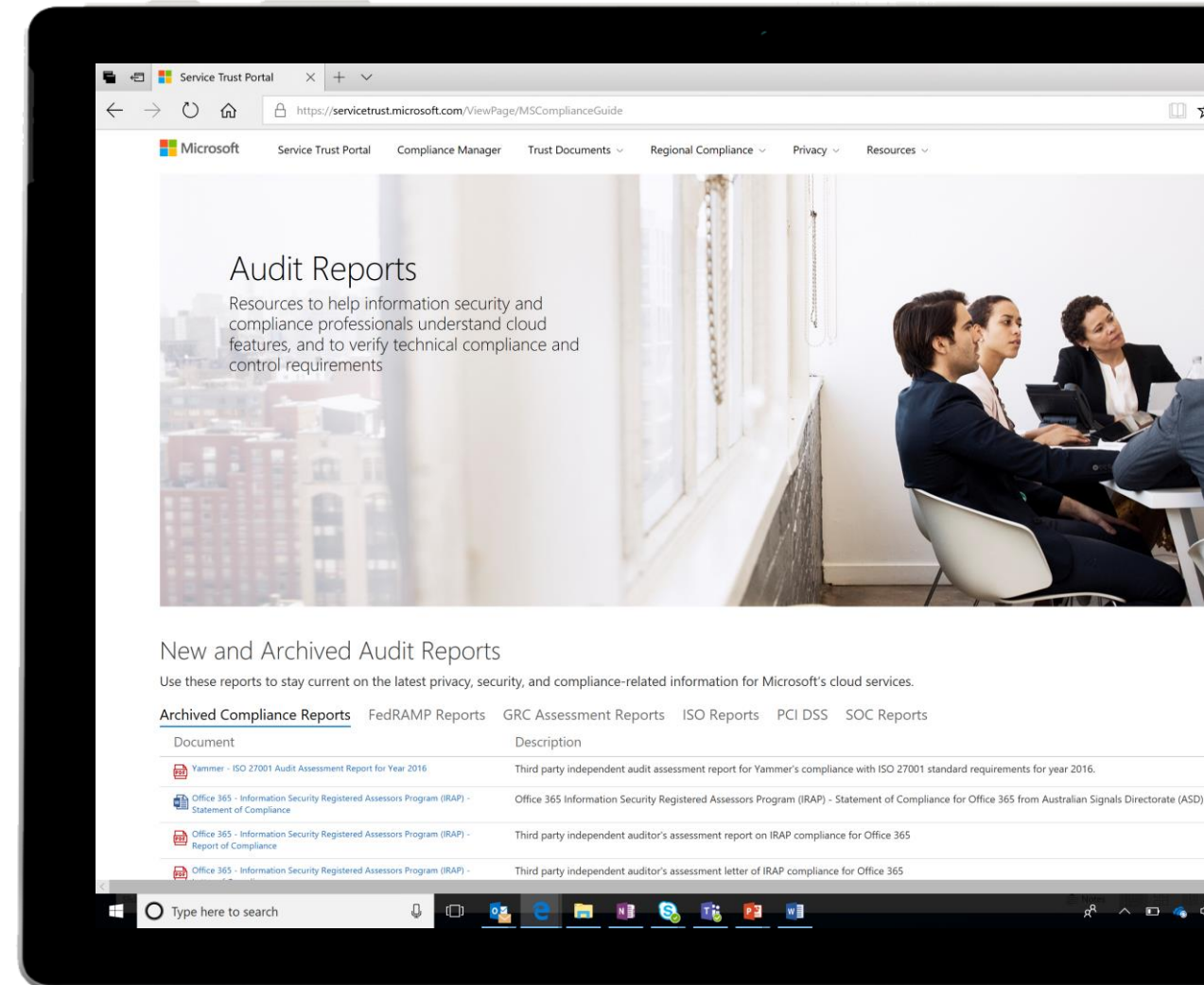
Compliance Manager is a dashboard that provides the Compliance Score and a summary of your data protection and compliance stature as well as recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.



Trust Documents

Build trust with transparency and empowerment

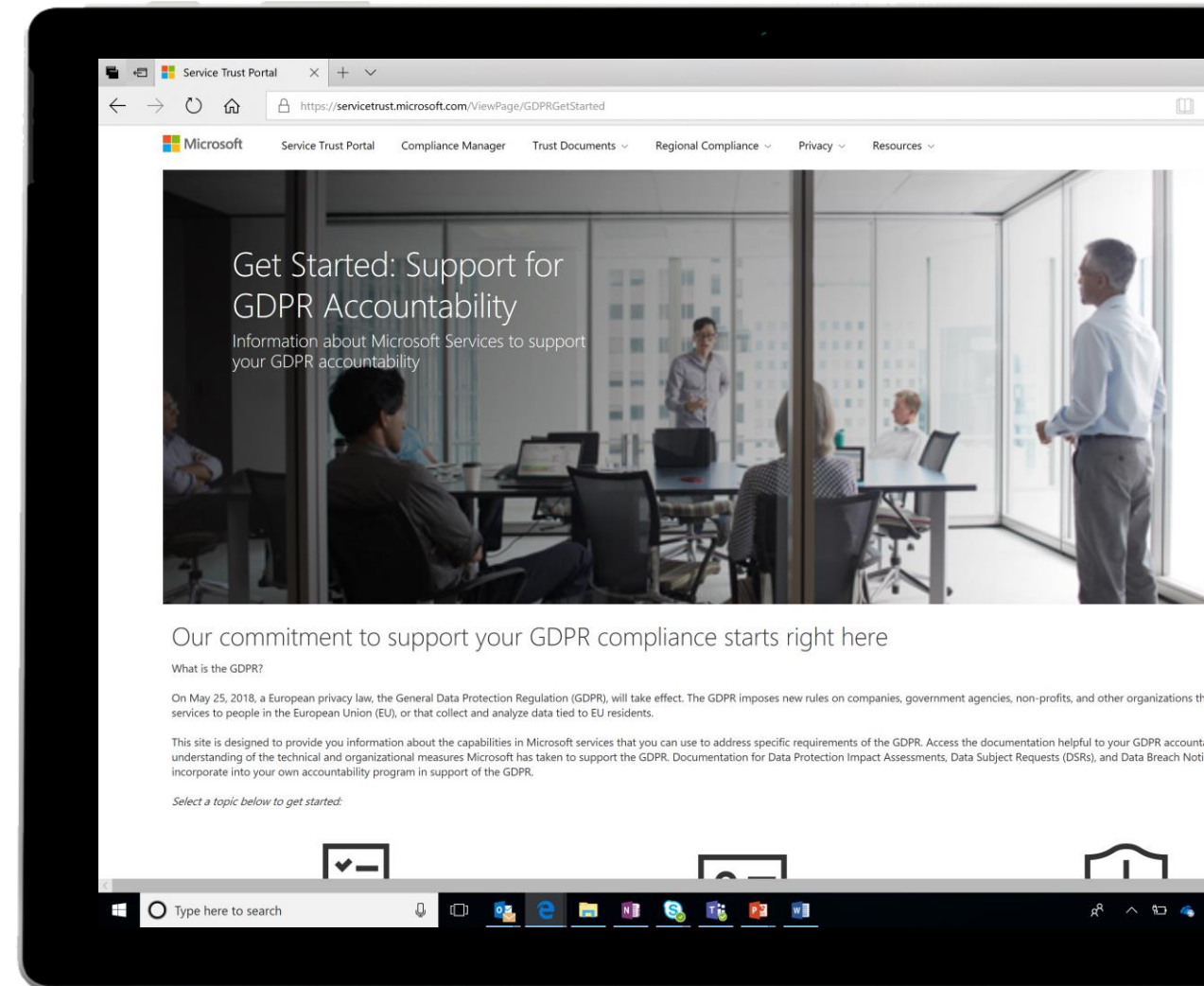
- **Audit reports**
FedRAMP, ISO, SOC, PCI-DSS audit reports and global GRC assessment reports
- **Data protection documents**
Whitepapers, FAQs, security reports, penetration tests, compliance guides, and other resources
- **Azure blueprints**
Resources to assist you in building and launching cloud-powered applications that help you comply with stringent regulations and standards.



Privacy resources

Information about Microsoft services to support your GDPR accountability

- **Data Subject Requests**
How Microsoft enable you to respond to Data Subject Requests (DSRs)
- **Data breach notifications**
How Microsoft detects and responds to a breach of personal data, and notifies you under the GDPR
- **Data Protection Impact Assessments**
How Microsoft helps controllers complete GDPR Data Protection Impact Assessments (DPIAs)






Identity

Azure Identity Management and access control security best practices

- Identity as primary security perimeter
- Centralize ID management
- Enable single sign-on
- Conditional Access – device standards
- Enable password management (SSPR – self service password reset)
- Enforce MFA
- RBAC – subscription, resource group, or resource
- Lower exposure of privileged accounts
- Control locations where resources are created
- Actively monitor for suspicious activity

RBAC

Who has access to Azure resources, what they can do with those resources, and what areas they have access to

		Role			
		Reader	Resource-specific or custom role	Contributor	Owner
Scope	 Subscription	Observers	Users managing resources		Admins
	 Resource group				
	 Resource	Automated processes			

RBAC

- [Owner](#) - Has full access to all resources including the right to delegate access to others.
- [Contributor](#) - Can create and manage all types of Azure resources but can't grant access to others.
- [Reader](#) - Can view existing Azure resources.
- [User Access Administrator](#) - Lets you manage user access to Azure resources.

Security

Authentication – Identity

- Azure Active Directory (Azure AD)
- Microsoft account (MSA)
- Active Directory (AD)

Authorization – Permissions

Once we know who you are, do you have permission to access the resource?

Service Level Agreement

- Define SLA's for each workload
- Dependency mapping – include internal/external dependencies
- Identify single point of failure
- Example – workload requires 99.99% but depends on a service that is only 99.9%
- Mean Time To Recover (MTTR) – avg time it takes to restore
- Mean Time Between Failures (MTBF) – time it will last between outages
- Composite SLA's – SQL SLA 99.99% * Web App 99.5% = 99.94%

Objective Review - #2

Optimize Consumption Strategy

- Configure network access to the storage account
- Optimize app service
- Compute, identity, network, and storage costs

Configure Azure Storage firewalls and virtual networks

- Storage – layered security model
- Network rules – only apps requesting data from over specified networks can access
- Requires authorization – AD, valid access key or token
- Deny all traffic and then grant access to specific VNets

Azure App Service

- PaaS Offering
- Service for hosting web applications, REST APIs, and mobile back ends
- Scalability

Compute Options

[Virtual Machines](#) are an IaaS service, allowing you to deploy and manage VMs inside a virtual network (VNet).

[App Service](#) is a managed PaaS offering for hosting web apps, mobile app back ends, RESTful APIs, or automated business processes.

[Service Fabric](#) is a distributed systems platform that can run in many environments, including Azure or on premises. Service Fabric is an orchestrator of microservices across a cluster of machines.

[Azure Container Service](#) lets you create, configure, and manage a cluster of VMs that are preconfigured to run containerized applications.

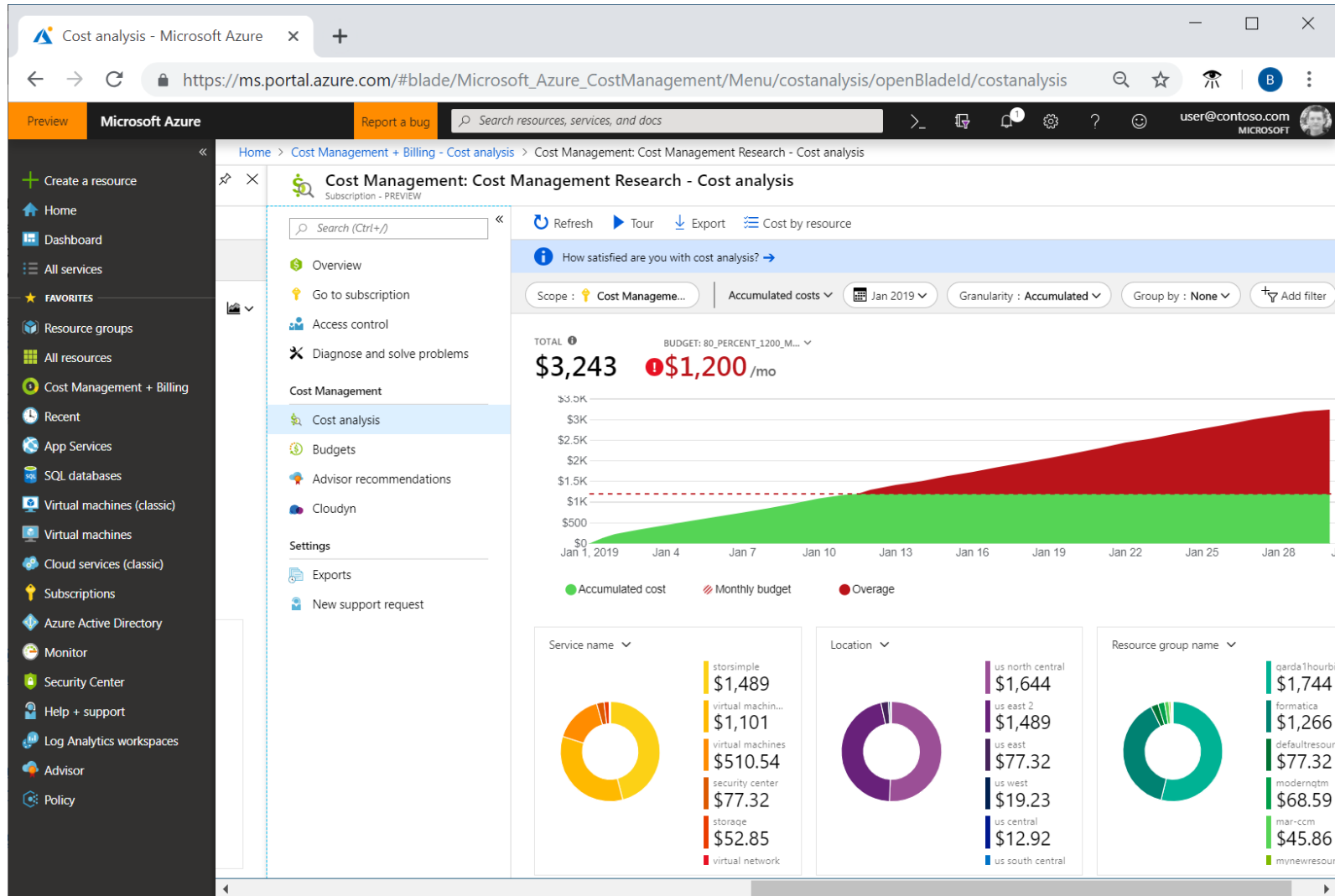
[Azure Container Instances](#) offer the fastest and simplest way to run a container in Azure, without having to provision any virtual machines and without having to adopt a higher-level service.

[Azure Functions](#) is a managed FaaS service.

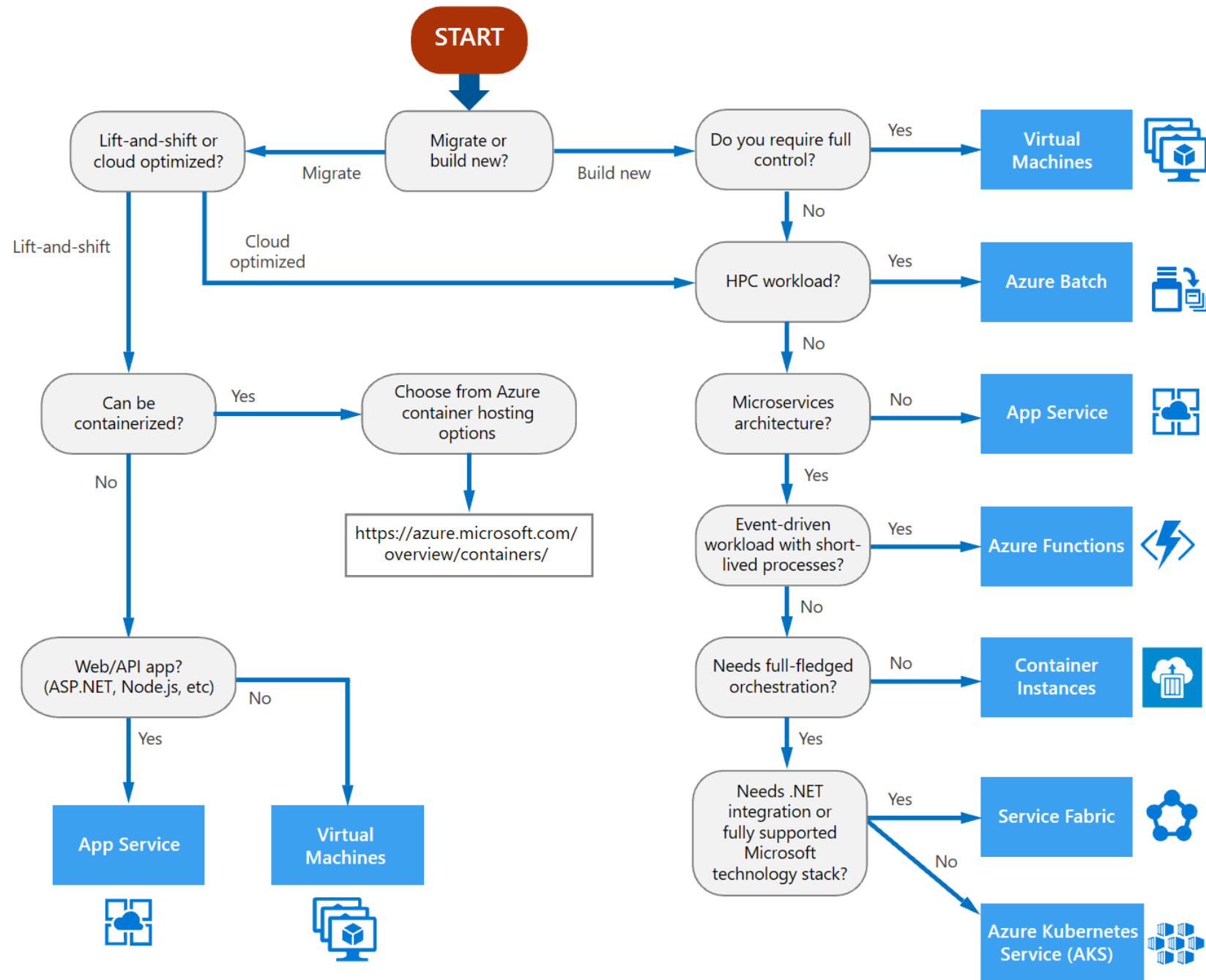
[Azure Batch](#) is a managed service for running large-scale parallel and high-performance computing (HPC) applications.

[Cloud Services](#) is a managed service for running cloud applications. It uses a PaaS hosting model.

Azure Cost Management



Flowchart



Choose the right data store

- RDMS – Azure DB, Managed Instances
- Key/value stores – Redis Cache
- Document databases – Cosmos DB
- Graph Databases – Cosmos DB
- Column-family databases – Cosmos DB
- Data Analytics
- Search engine databases
- Time Series databases
- Object storage
- Shared Files

Design Principles

[Design for self healing](#). In a distributed system, failures happen. Design your application to be self healing when failures occur.

[Make all things redundant](#). Build redundancy into your application, to avoid having single points of failure.

[Minimize coordination](#). Minimize coordination between application services to achieve scalability.

[Design to scale out](#). Design your application so that it can scale horizontally, adding or removing new instances as demand requires.

[Partition around limits](#). Use partitioning to work around database, network, and compute limits.

[Design for operations](#). Design your application so that the operations team has the tools they need.

[Use managed services](#). When possible, use platform as a service (PaaS) rather than infrastructure as a service (IaaS).

[Use the best data store for the job](#). Pick the storage technology that is the best fit for your data and how it will be used.

[Design for evolution](#). All successful applications change over time. An evolutionary design is key for continuous innovation.

[Build for the needs of business](#). Every design decision must be justified by a business requirement.

Sizes for VM Windows Virtual Machine in Azure

Type	Sizes	Description
General purpose	B, Dsv3, Dv3, DSv2, Dv2, Av2, DC	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
Compute optimized	Fsv2, Fs, F	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
Memory optimized	Esv3, Ev3, M, GS, G, DSv2, Dv2	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
Storage optimized	Lsv2, Ls	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.
GPU	NV, NVv2, NC, NCv2, NCv3, ND, Ndv2 (Preview)	Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.
High performance compute	H	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).

Objective Review - #3

Design an Auditing and Monitoring Strategy

- Define logical groupings (tags) for resources to be monitored
- Determine levels and storage locations for logs
- Plan for integration with monitoring tools
- Recommend appropriate monitoring tool(s) for a solution
- Specify mechanism for event routing and escalation
- Design auditing for compliance requirements
- Design auditing policies and traceability requirements

Logical Groupings (tags)

- Tags – name/value pairs
- Allows to retrieve related resources
- Billing/Management
- Develop a self-service metadata tagging strategy
- User must have write access

Storage Levels and locations

Blob

- Premium (preview) – high performance hardware
- Hot – frequent access
- Cool – 30 days, infrequent access, lower availability but high durability and time to access/throughput as hot
- Archive – 180 days, offline, highest access costs but most cost effective for infrequently accessed data

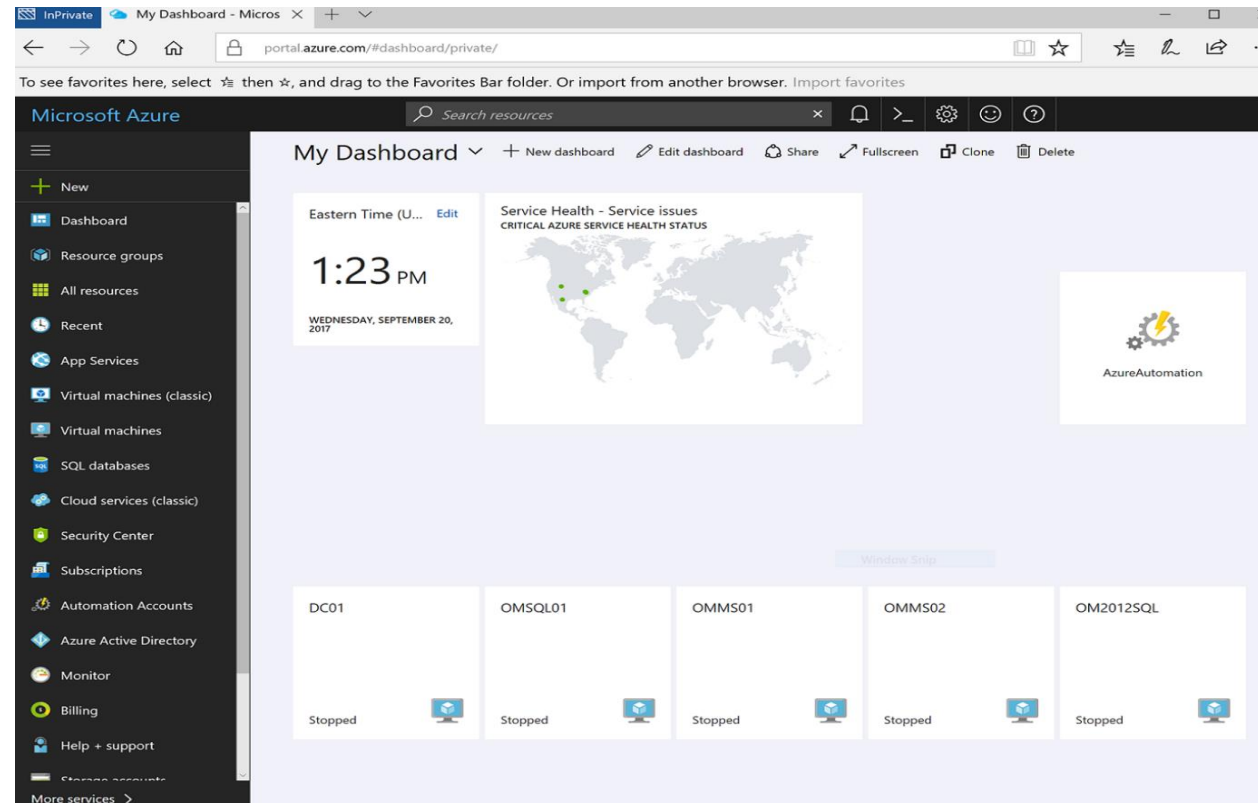
Metrics and Logs

Metrics – numerical, lightweight, point in time

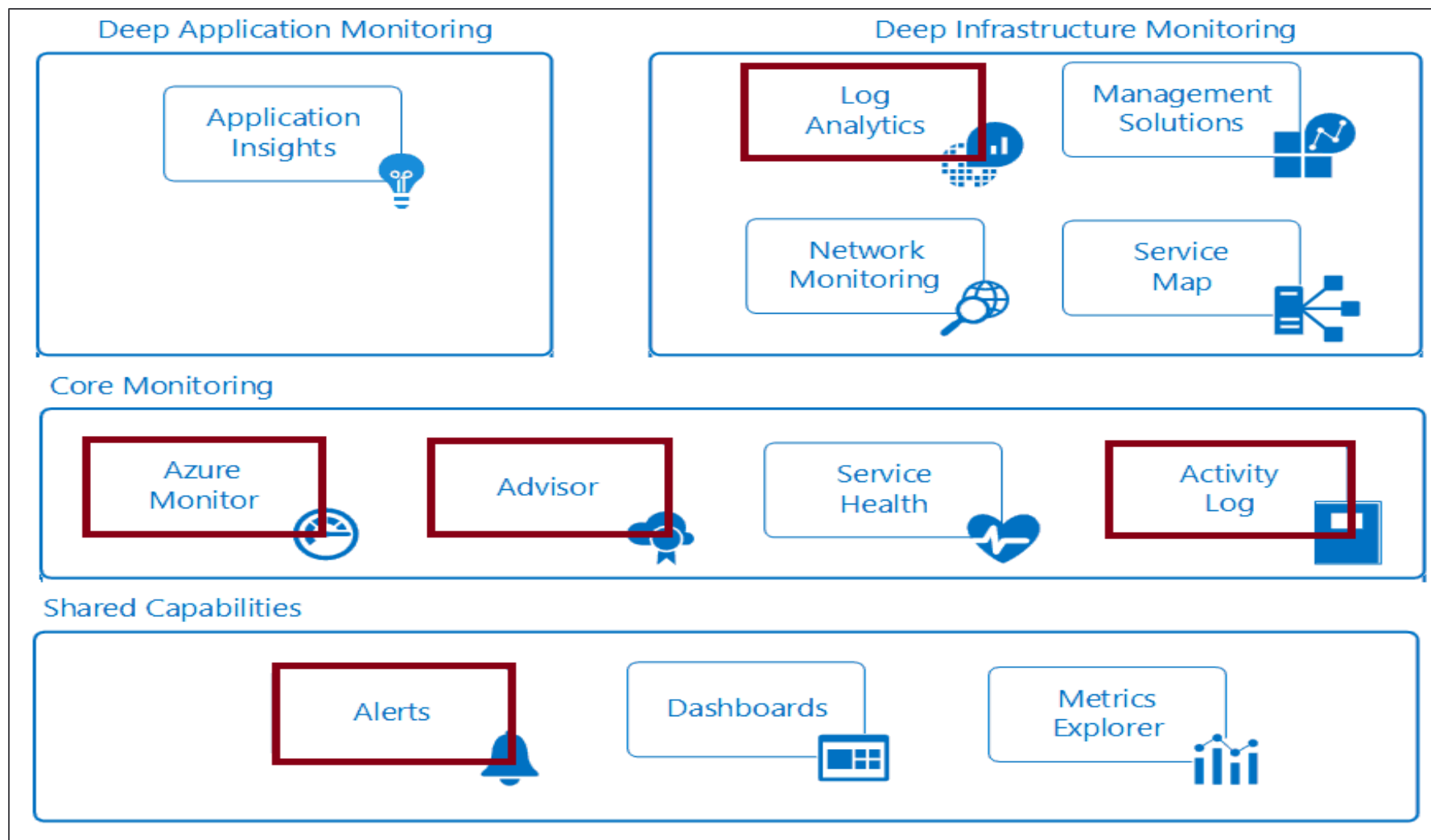
Logs – analyze with queries

Azure Monitor uses Kusto query language. Can do aggregations, joins, etc.

Shared dashboard



Azure Monitor Service





Azure Monitor

Application

Operating System

Azure Resources

Azure Subscription

Azure Tenant

Custom Sources



Insights



Application



Container



VM



Monitoring
Solutions

Visualize



Dashboards



Views



Power BI



Workbooks

Analyze



Metric Analytics



Log Analytics

Respond



Alerts



Autoscale

Integrate



Event Hubs

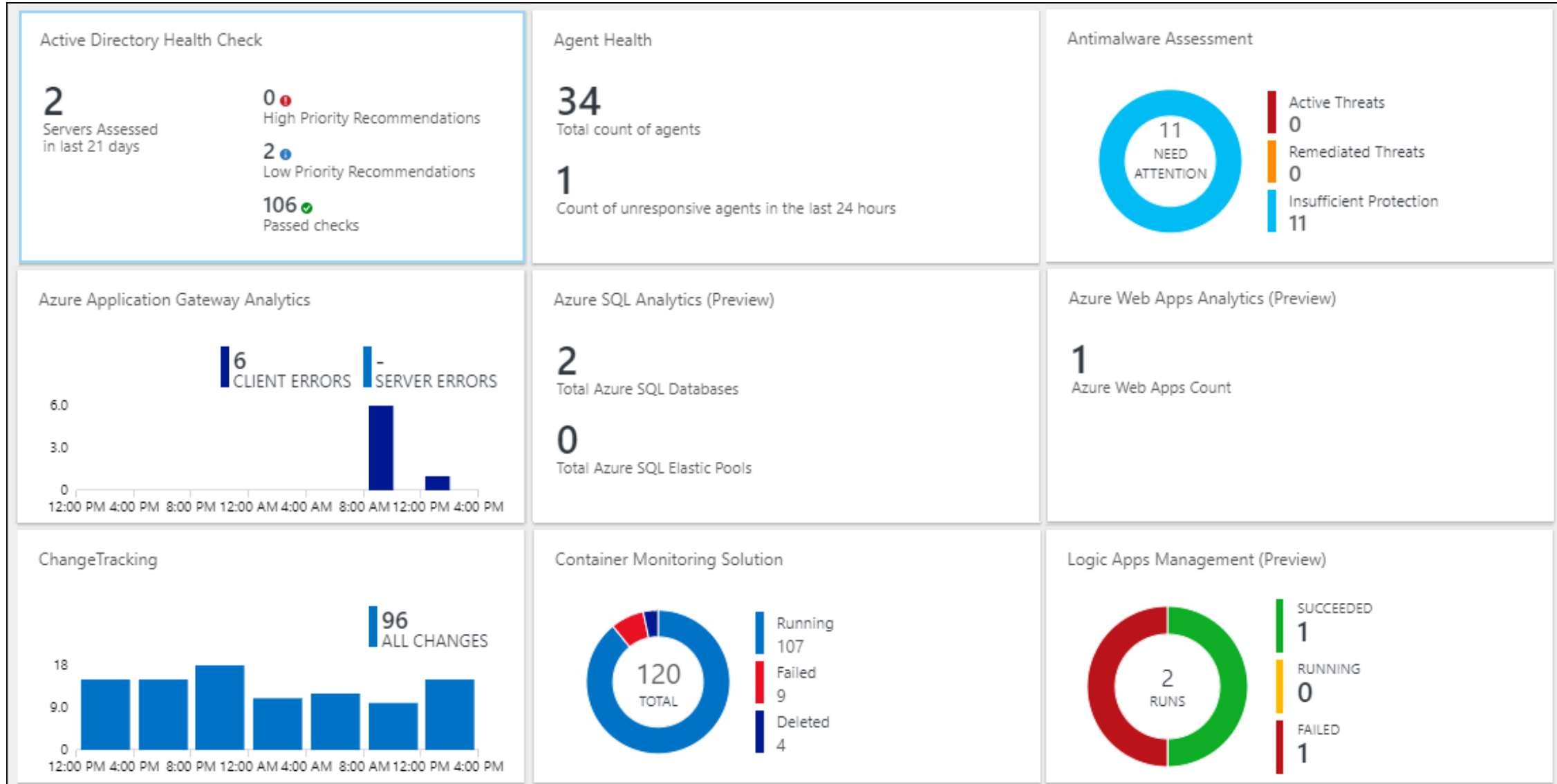


Logic Apps



Ingest &
Export APIs

Video: Log Analytics



Log Analytics Scenarios

Example 1 - Assessing updates

- IT Administrators assess systems update requirements
- Must be able to accurately schedule updates
- OMS/Log Analytics collects data from all customers performing updates
- Uses "Crowd-sourced" data to provide an average time to help meet strict SLAs

Example 2 - Change tracking

- Troubleshooting operational incidents is a complex process
- OMS/Log Analytics let you perform analysis from multiple angles, using a variety of sources
- Everything correlated through a single interface
- Track issues such as unexpected system reboots or shutdowns

Practice: Collect and Analyze Data

Part 1

Collect data about virtual machines

Create a workspace

Enable Log Analytics on virtual machines

Collect event and performance data

View the data collected

Part 2

View or analyze data collected with Log Analytics search

Search, modify, and filter event data

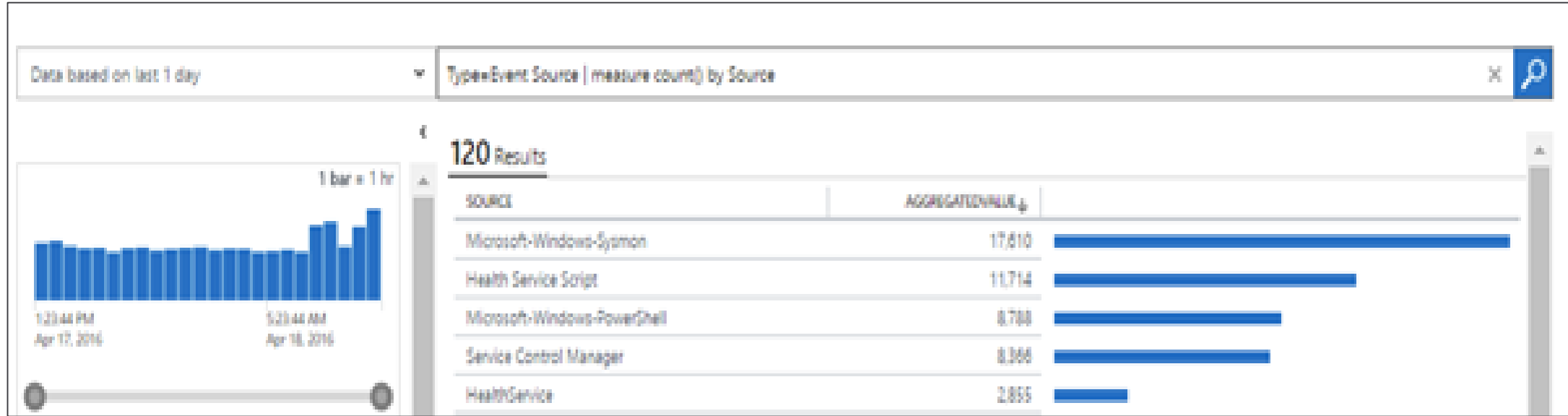
Work with performance data

Practice: Analysis with Log Analytics

Microsoft Online Labs has a self-paced **Deep Analysis with Microsoft Azure Log Analytics** exercise.

- Focus on the basics of Azure Insight and Analytics
- Explore Log Analytics, log searches, analysis of Service Map and Network Performance Monitor solutions

Log Analytics Querying



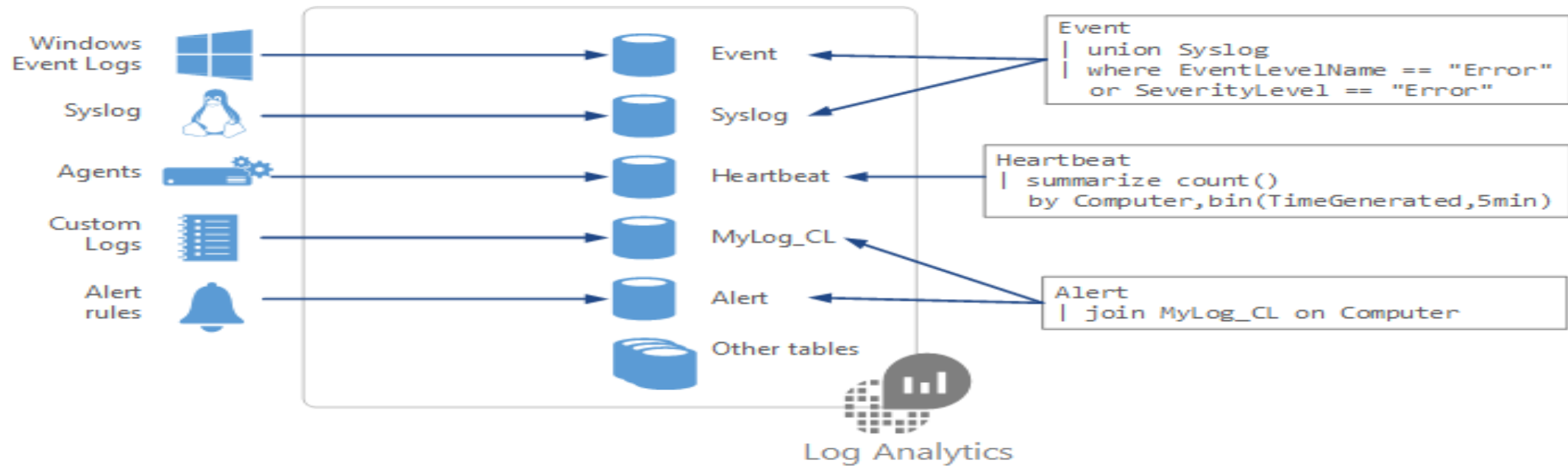
Log Analytics provides a query syntax

Quickly retrieve and consolidate data in the repository

Save or have log searches run automatically to create an alert

Export the data to Power BI or Excel

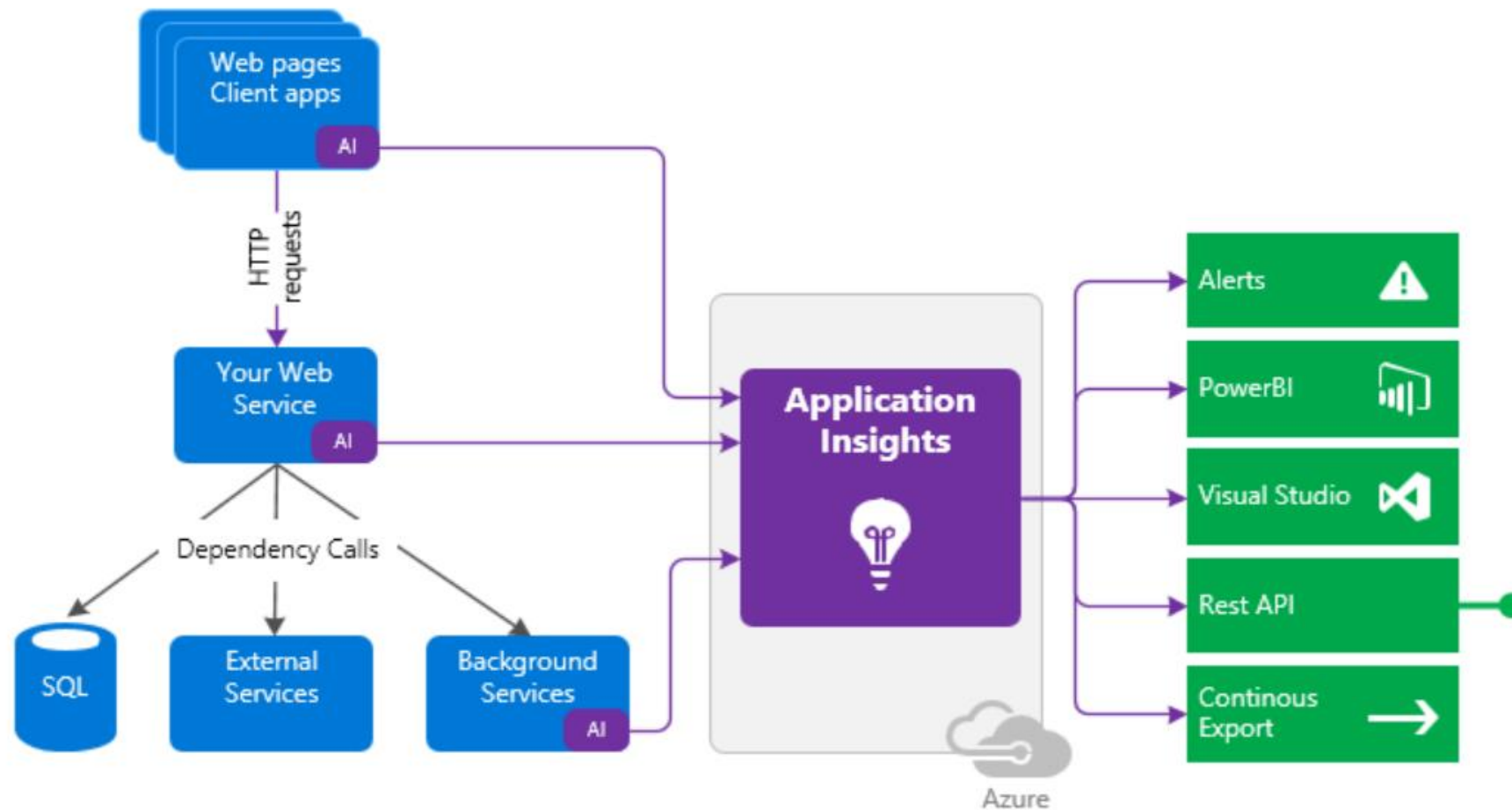
Query Language Syntax



Event

```
| where (EventLevelName == "Error")  
| where (TimeGenerated > ago(1days))  
| summarize ErrorCount = count() by Computer  
| top 10 by ErrorCount desc
```

Application Insights - instrumentation monitors your app and sends telemetry data to the portal



Application Insights

- Smart detection and manual alerts
- Application Maps – bottlenecks/failure spots for distributed apps (triage)
- Profiles
- Usage analysis
- Diagnostic search for instance data
- Metrics explorer for aggregated data
- Dashboards
- Live Metrics stream
- Analytics
- Visual Studio
- Snapshot Debugger

Azure Policies

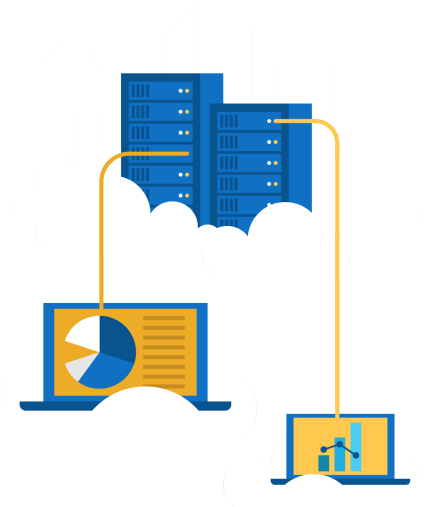
- Focus on deployment & existing resources
- Controls properties like types or locations of resources
- Examples –
 - Require SQL Server 12.0 (denies servers that don't)
 - Allowed VM SKU's
 - Enforce required tag and value on a resource
- Can use PowerShell, Azure CLI or Portal
- Enforced during policy assignment or policy update & [more](#)
- Scope – resource groups, subscription or management groups



Questions?

Homework Assignment

<https://aka.ms/az301asg>



Open Mic

