Microsoft

AZ-305T00A Designing Microsoft Azure Infrastructure Solutions

Design a solution to log and monitor Azure resources

Learning Objectives

- Design for Azure Monitor data sources
- Design for Log Analytics
- Design for Azure workbooks and Azure Insights
- Design for Azure Data Explorer
- Case study
- Learning recap

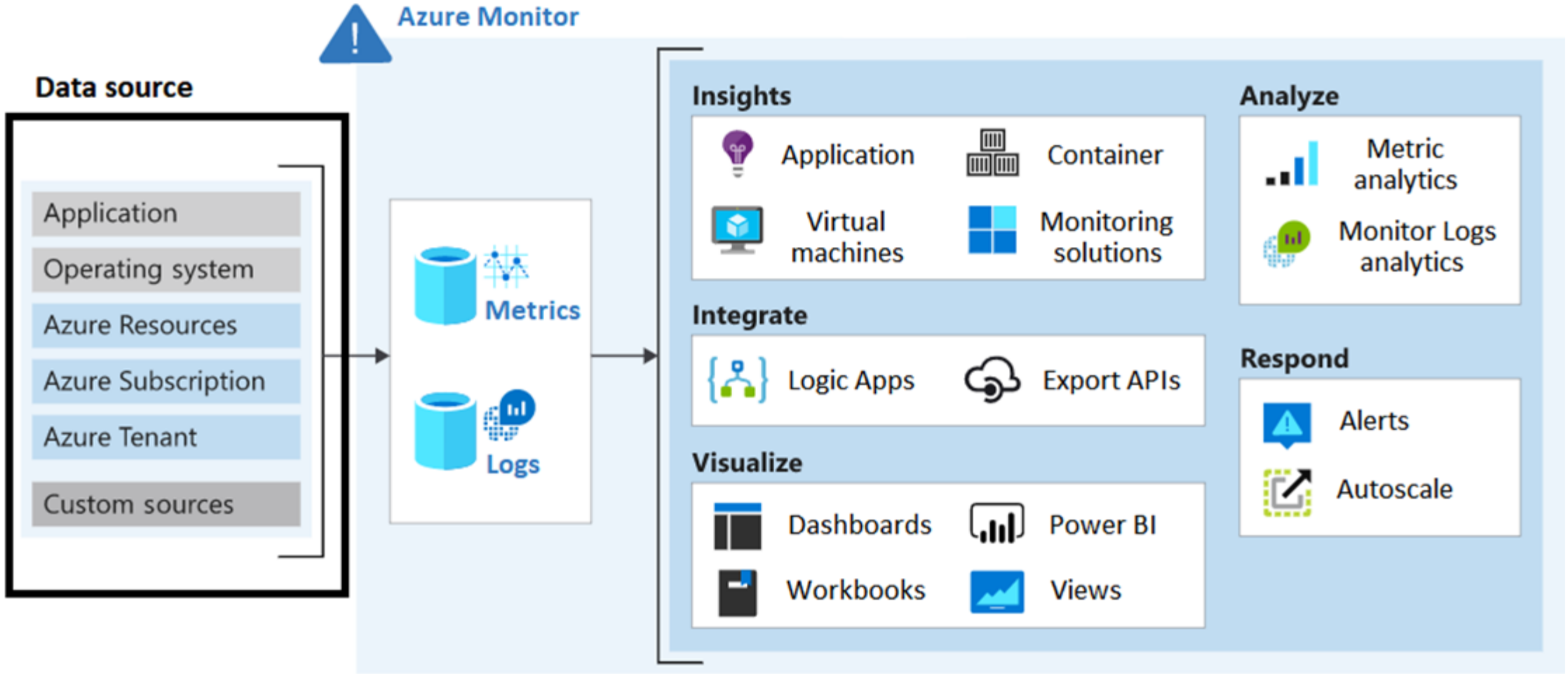
AZ-305: Design Identity, Governance, and Monitoring Solutions (25-30%)

Design a Solution for Logging and Monitoring

- Recommend a logging solution
- Recommend a solution for routing logs
- Recommend a monitoring solution

Design for Azure Monitor data sources

Review Azure Monitor capabilities



Identify data sources and access method

Azure Monitor collects data automatically from a range of components.

- Data tiers go from Azure applications (highest tier) to Azure platform components (lowest tier)
- The method of accessing data from each tier varies – for example, installing an agent
- Each data tier can stream to different external systems
- Prioritize and be deliberate on what data sources you need

- Windows events
- Linux syslog
- Client performance data
- Processes and dependencies (VM Insights)
- Application text logs
- IIS logs
- SNMP traps
- Management pack data (SCOM)

Design for Log Analytics

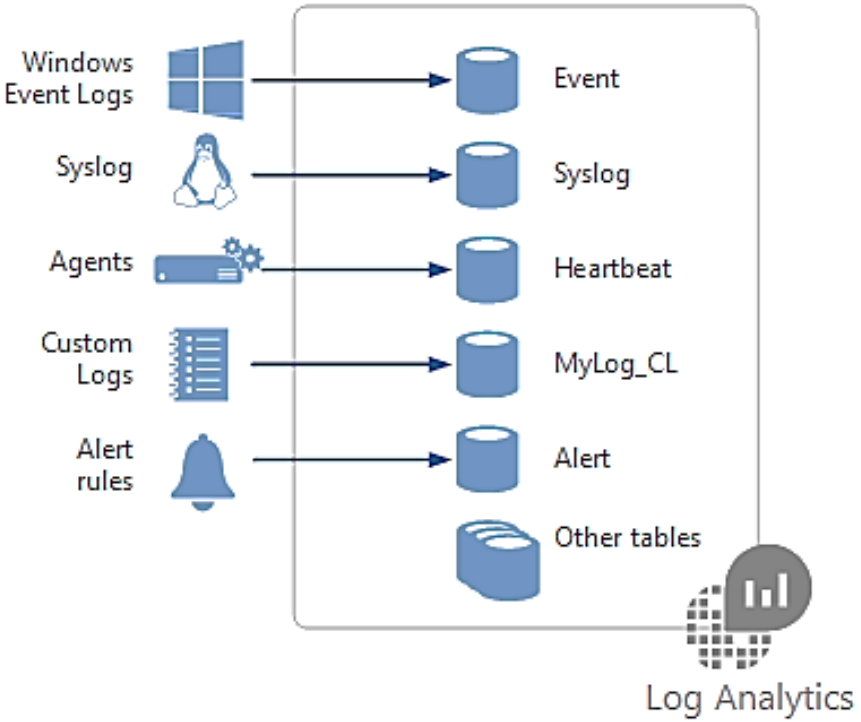
What is Log Analytics?

Log Analytics is a service in that helps you collect and analyze data.

- Azure Monitor stores log data in the workspace
- Data in a workspace is organized into tables with properties you can query

A Log Analytics workspace provides:

- A geographic location for data storage.
- Data isolation by granting different users access rights following one of our recommended design strategies.
- Scope for configuration of settings like pricing tier, retention, and data capping.



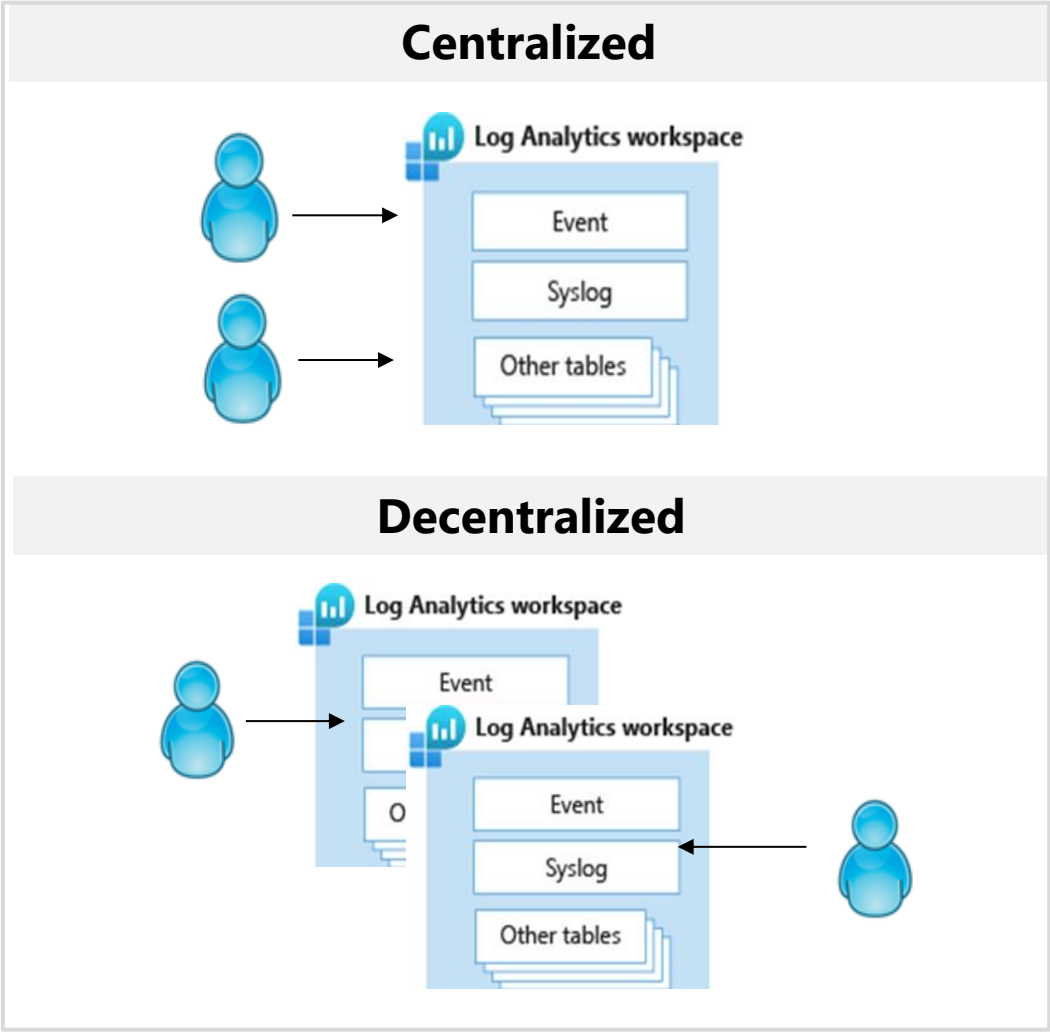
Considerations for workspace access control

Workspace deployment models include centralized, decentralized, and hybrid.

Centralized: All logs are stored in a central workspace and administered by a single team, with Azure Monitor providing differentiated access per-team.

Decentralized: Each team has their own workspace created in a resource group they own and manage, and log data is segregated per resource.

Hybrid: Security audit compliance requirements further complicate this scenario because many organizations implement both deployment models in parallel.



Considerations for access mode

The access mode is how a user accesses the workspace and what data they can access.

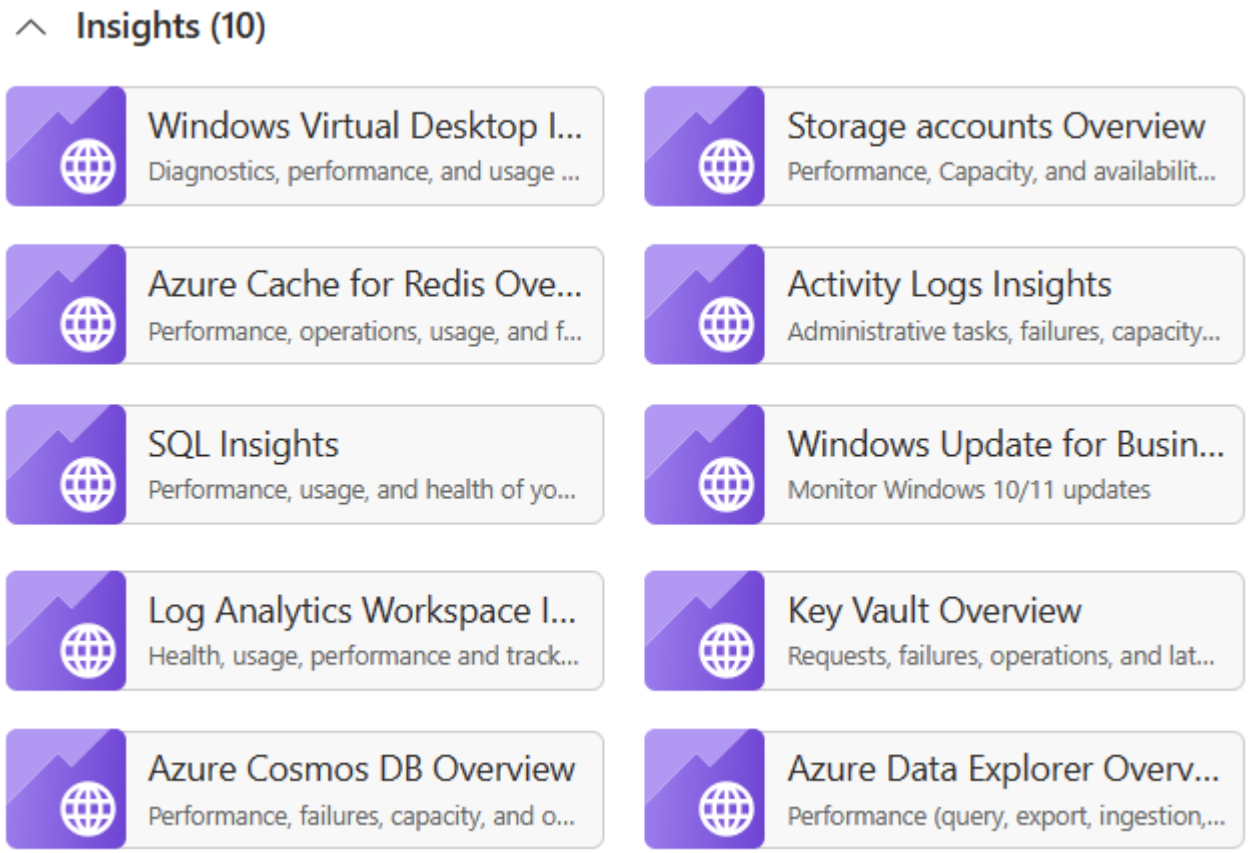
Issue	Workspace-context	Resource-context
How does the access mode work?	• You can view all logs in the workspace you have permission to. • Queries in this mode are scoped to all data in all tables in the workspace. • This is the access mode used when logs are accessed with the workspace as the scope.	• When you access the workspace for a particular resource, resource group, or subscription. • You can view logs for only resources in all tables that you have access to. • Queries in this mode are scoped to only data associated with that resource.
Who is each model intended for?	Central administration	Application teams
What does a user require to view logs?	Permissions to the workspace	Read access to the resource
What is the scope of permissions?	Workspace	Azure resource

Design for Azure workbooks and Azure Insights

Design for Azure Workbooks

Flexible canvas for data analysis and the creation of rich visual reports

- Tap into multiple data sources and combine them into unified interactive experiences
- Provide insights into the availability, performance, usage, and health of resources
- Enable rich data and insights through composite views and joins



Design for Azure Insights

It's critical to monitor your systems closely to identify any performance problems or attacks before they can affect users. Designing insights as a part of your overall architecture will help identify performance issues.

Use Application Insights to:

- Analyze and address issues and problems that affect your application's health and performance.
- Improve your application's development lifecycle.
- Measure your user experience and analyze users' behavior.

Use Azure Monitor VM insights to:

- View the health and performance of your VMs.
- Monitor your VMs at-scale across multiple subscriptions and resource groups.
- Want a topology view that shows the processes, and network connection details of your VMs and scale sets.

Use Azure Monitor container insights to:

- View the health and performance of your Kubernetes workloads at-scale across multiple subscriptions and resource groups.
- Want visibility into memory and processor performance metrics from controllers, nodes, and containers.
- Want view and store container logs for real time and historical analysis.

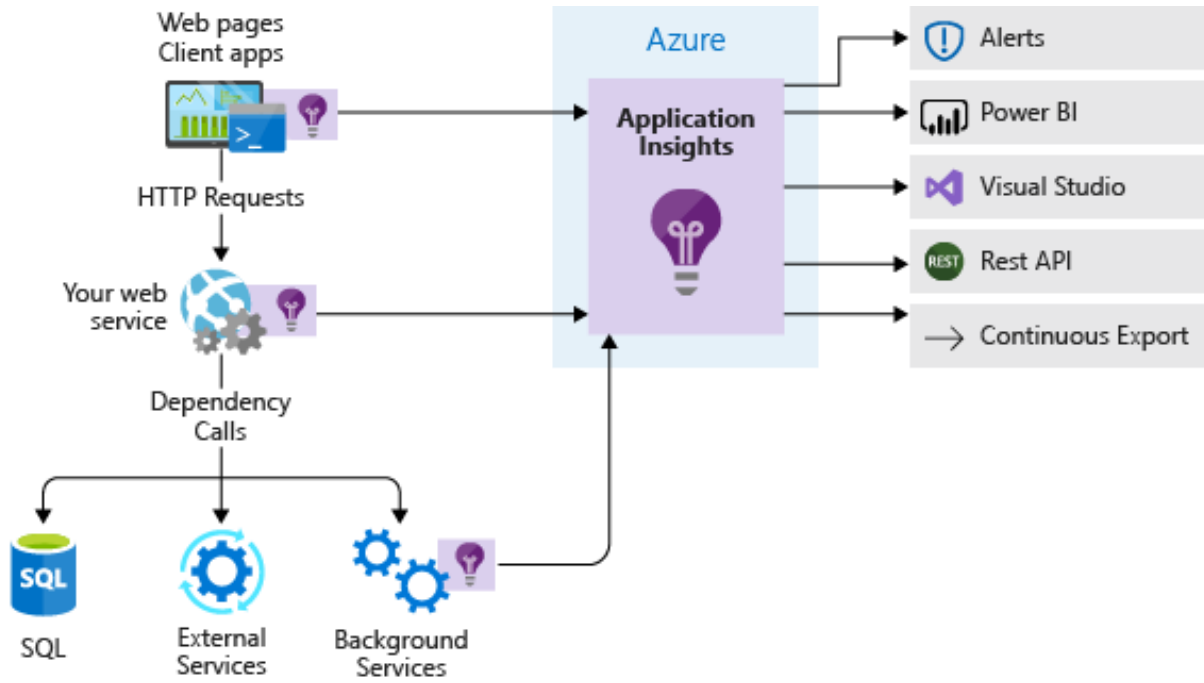
Select Application Insights

You want to understand how your app is performing and how it's being used.

You need usage information on request rates, response times, and failure rates.

You need transaction diagnostics and performance statistics (client and server).

You want to automatically collect a snapshot of a live application to analyze it at a later stage.

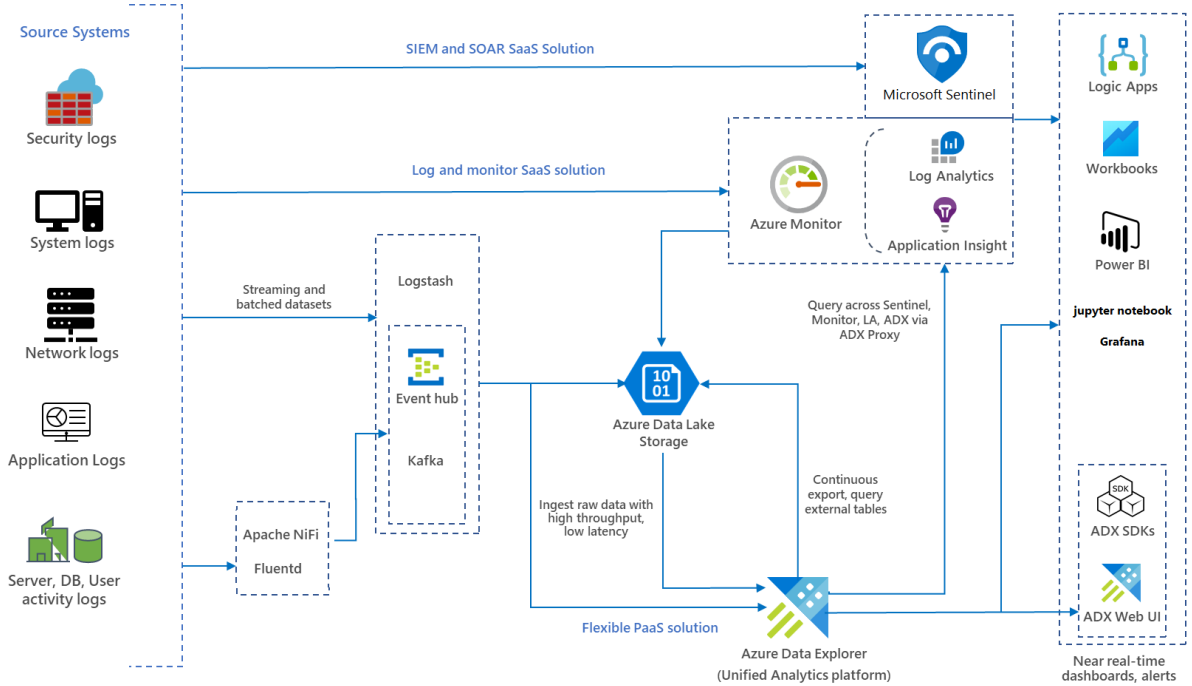


Design for Azure Data Explorer

When to use Azure Data Explorer

Azure Data Explorer is a fast and highly scalable data exploration service for log and telemetry data.

- Helps you handle the many data streams emitted by modern software, so you can collect, store, and analyze data.
- Azure Data Explorer is ideal for analyzing large volumes of diverse data from any data source, such as websites, applications, IoT devices, and more.
- This data is used for diagnostics, monitoring, reporting, machine learning, and additional analytics capabilities.
- Can combine with Microsoft Sentinel and Azure Monitor.



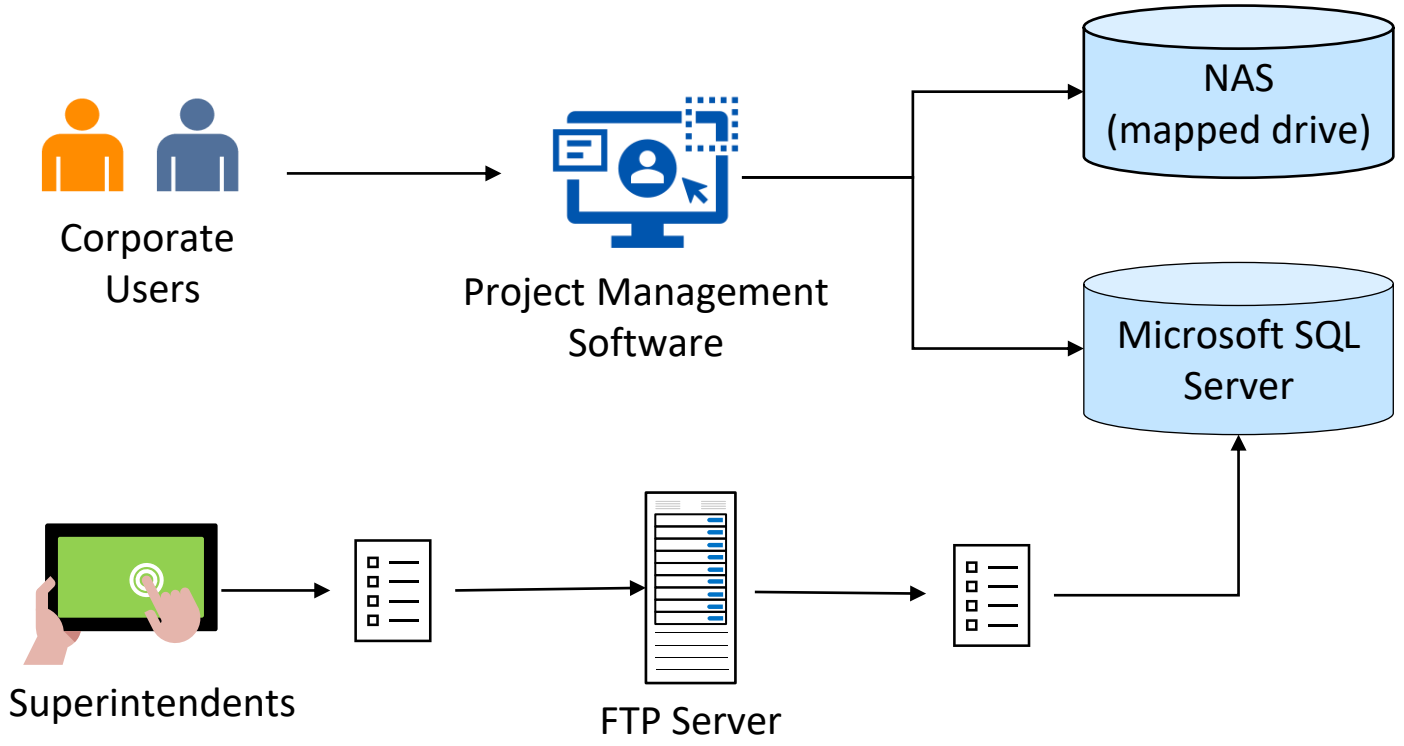
Case study

Use Case Scenarios (activity)

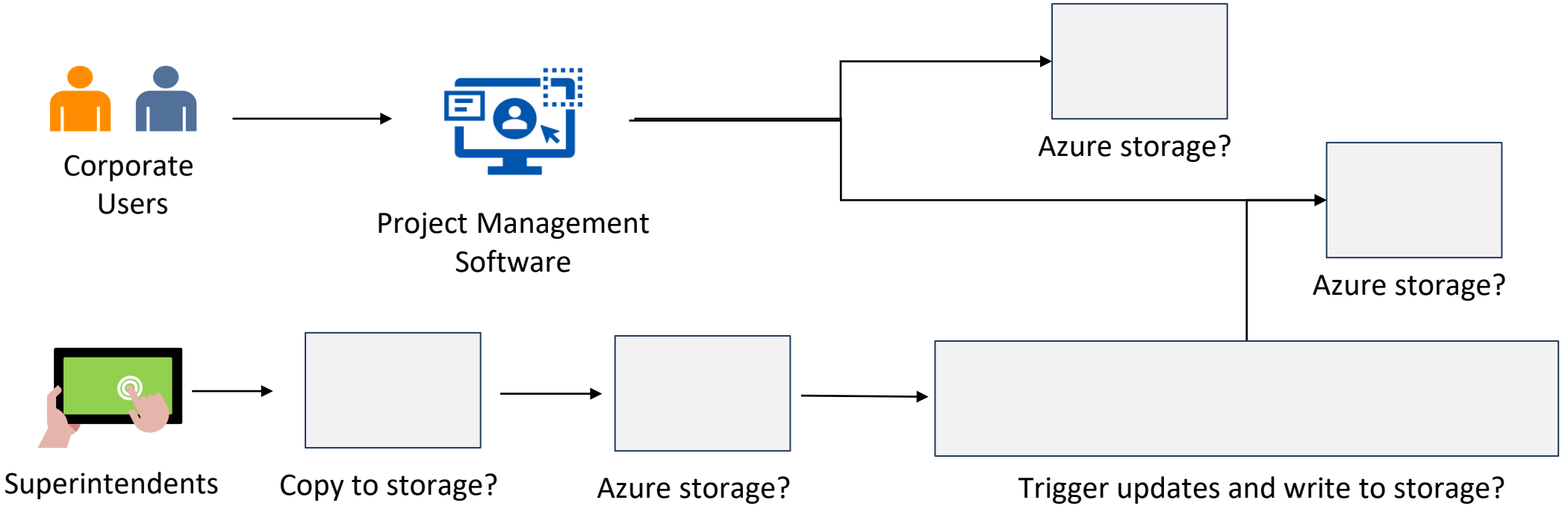
Azure Monitor	Measure user experience and analyze users' behavior for all external facing applications	Solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments
Application Insights	You need to edit and run log queries	You need transaction diagnostics and performance statistics (client and server).
Azure workbooks	You need data analysis and the creation of rich visual reports	You need usage information on request rates, response times, and failure rates of an application
Log Analytics		

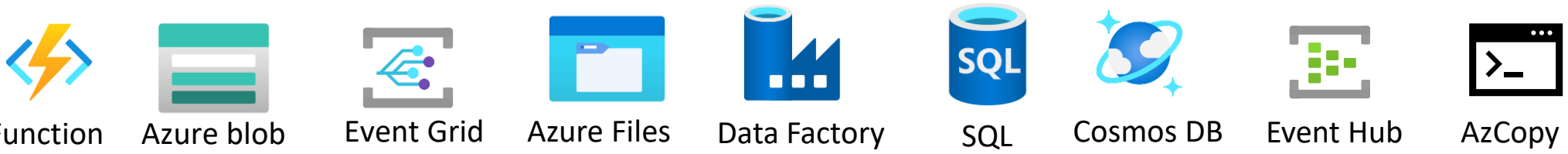
Fabrikam Residences case study – PM software

- Third party Windows application
- 2 node cluster with SQL backend
- Images and documents stored on NAS device
- Corporate provides data on schedules and orders
- Superintendents record daily progress

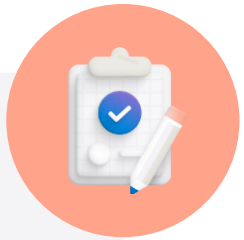


Instructor solution - Fabrikam Residences PM software





Learning Recap – Log and monitor solutions



Check your knowledge questions and review

Reference modules

- Design a full-stack monitoring strategy on Azure
- Analyze your Azure infrastructure by using Azure Monitor logs
- Monitor your Azure virtual machines with Azure Monitor
- Monitor app performance

Optional exercises

- Monitor, diagnose, and troubleshoot your Azure storage

End of presentation