AZ-305T00A Designing Microsoft Azure Infrastructure Solutions

Design a solution to log and monitor Azure resources

https://learn.microsoft.com/training/modules/design-solution-to-log-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%)

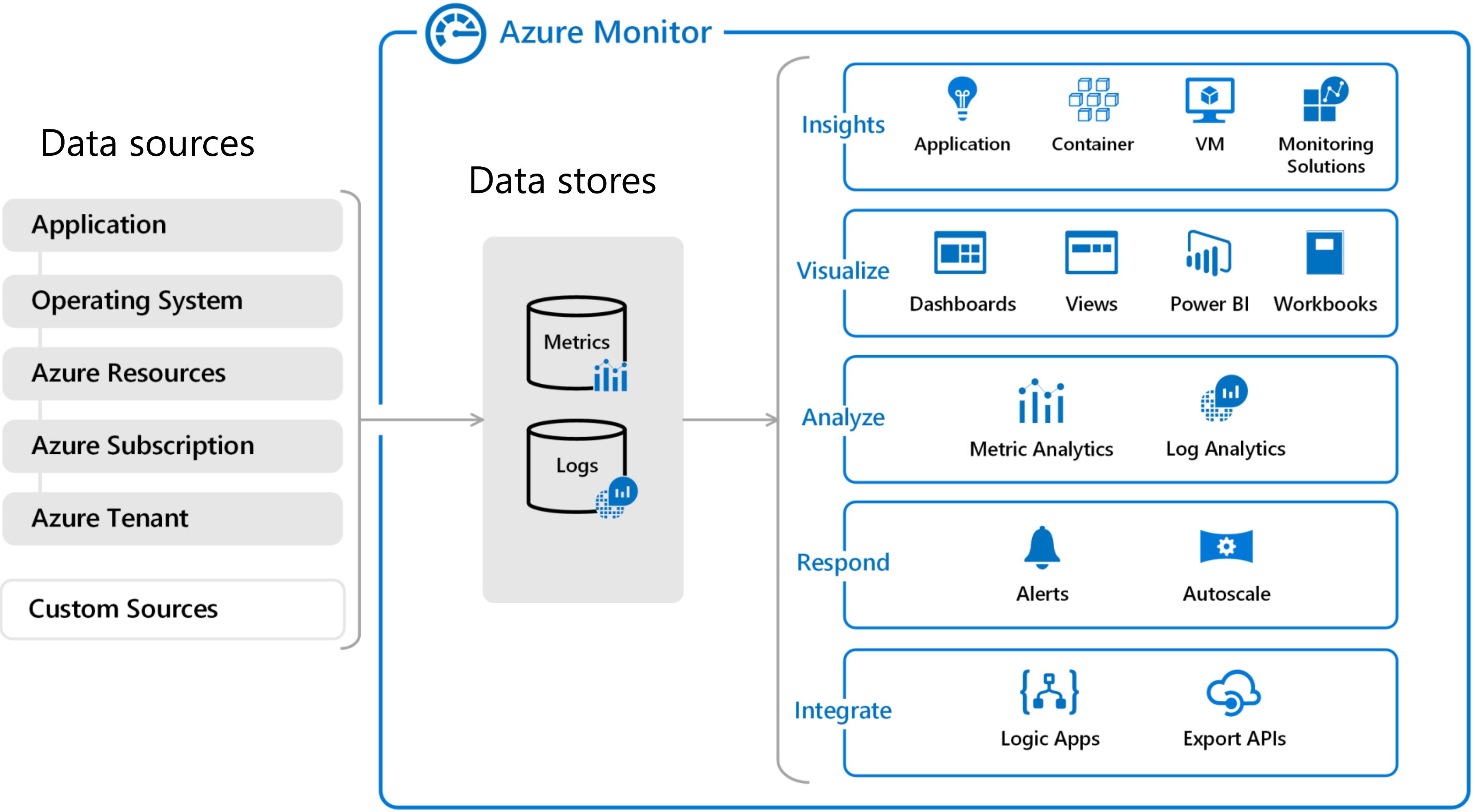
Design a Solution for Logging and Monitoring

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

Design for Azure Monitor data sources

Review Azure Monitor capabilities

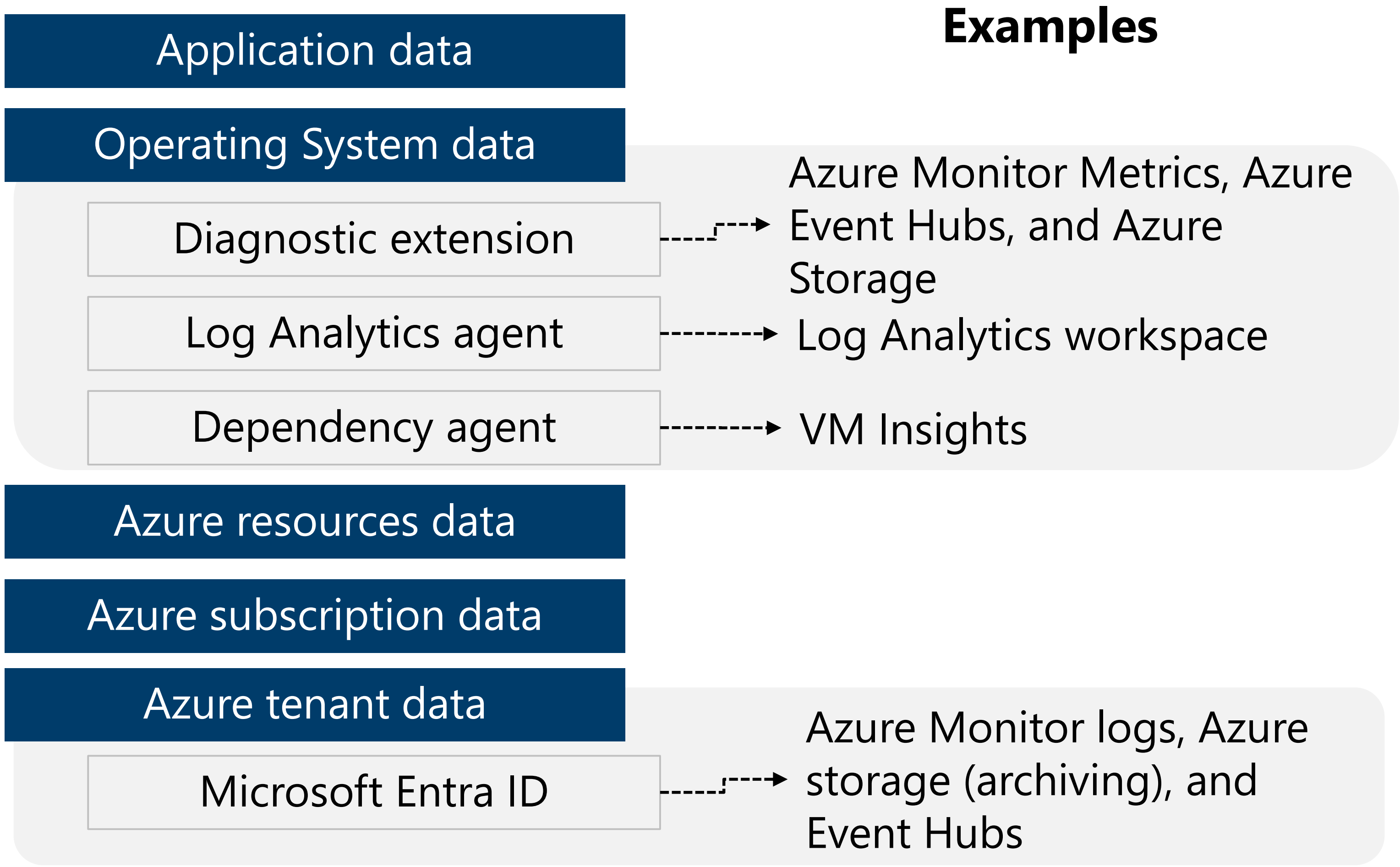
Analysis, alerting, and streaming to external systems



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



Examples

Application data

Operating System data

Diagnostic extension → Azure Monitor Metrics, Azure Event Hubs, and Azure Storage

Log Analytics agent → Log Analytics workspace

Dependency agent → VM Insights

Azure resources data

Azure subscription data

Azure tenant data

Microsoft Entra ID → Azure Monitor logs, Azure storage (archiving), and Event Hubs

Design for Log Analytics

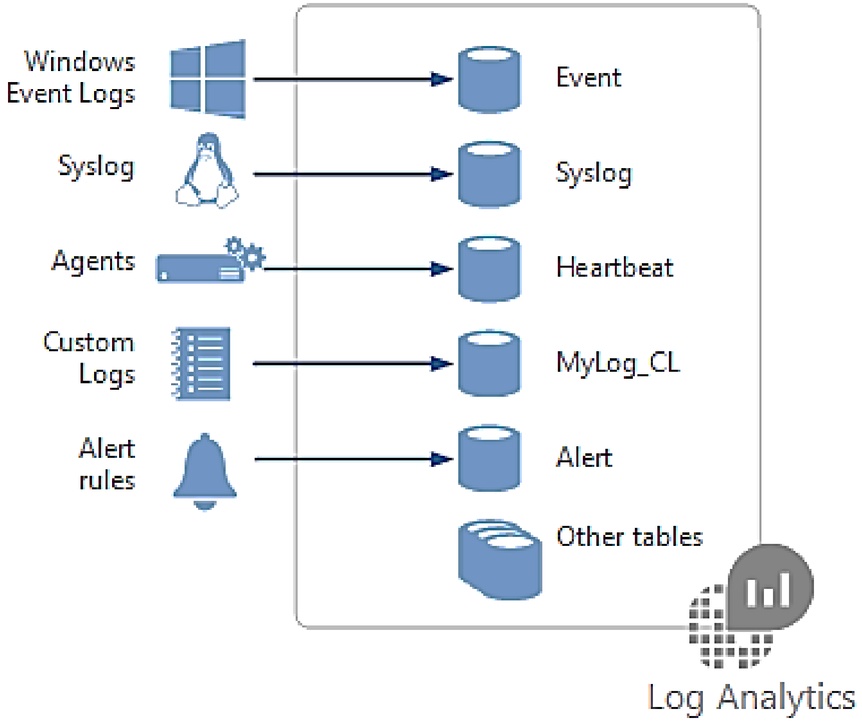
What is Log Analytics?

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.



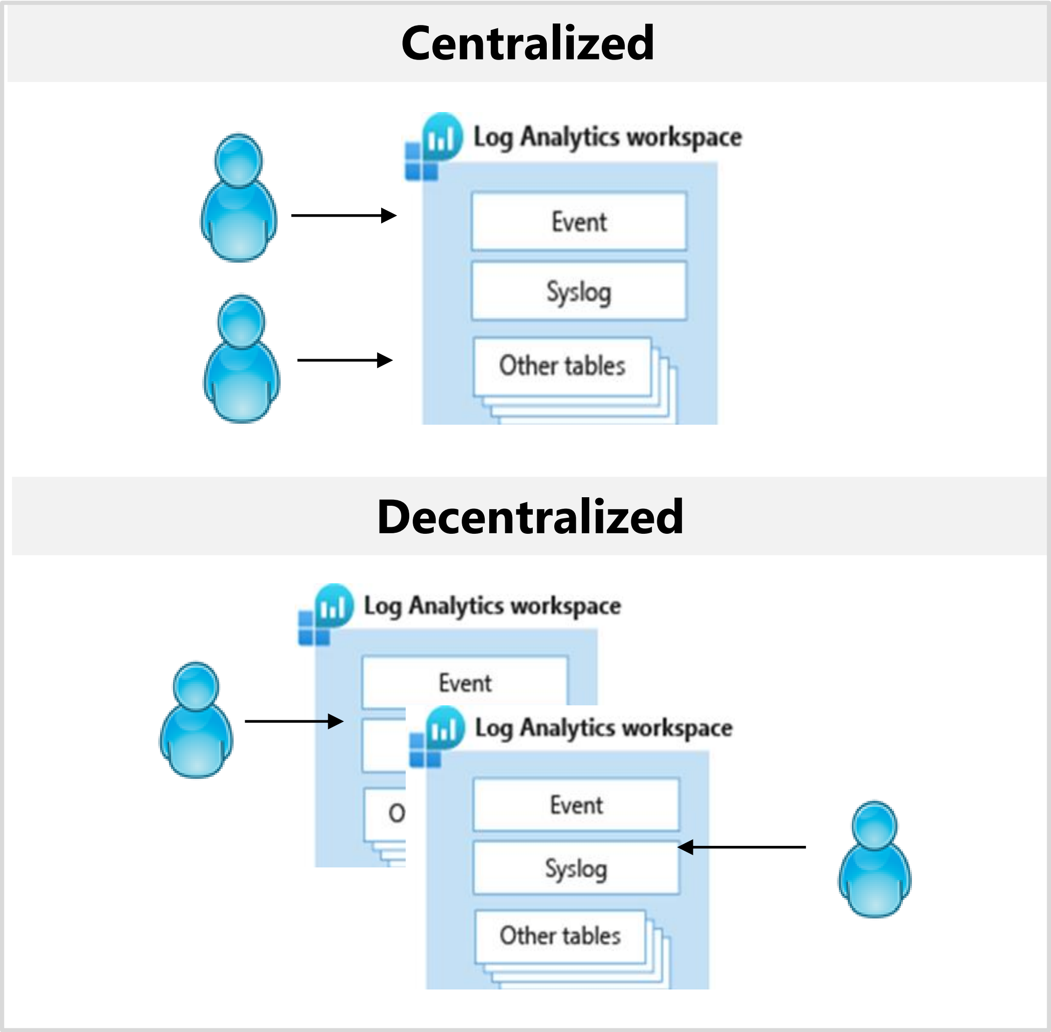
Considerations for workspace access control

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.

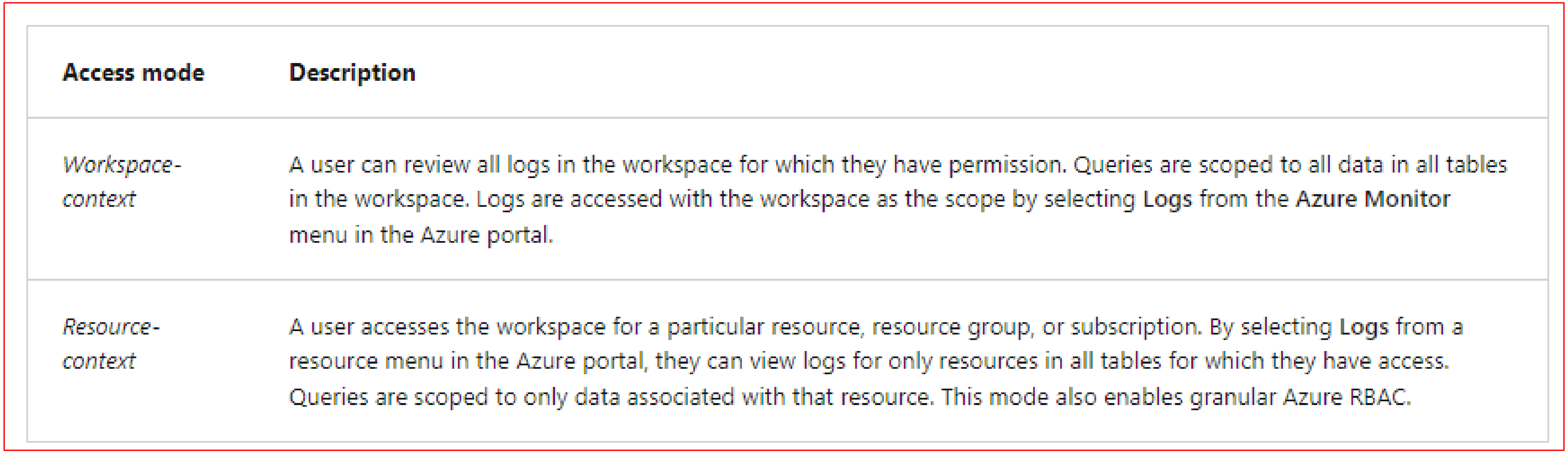
Hybrid: Security audit compliance requirements further complicate this scenario because many organizations implement both deployment models in parallel.



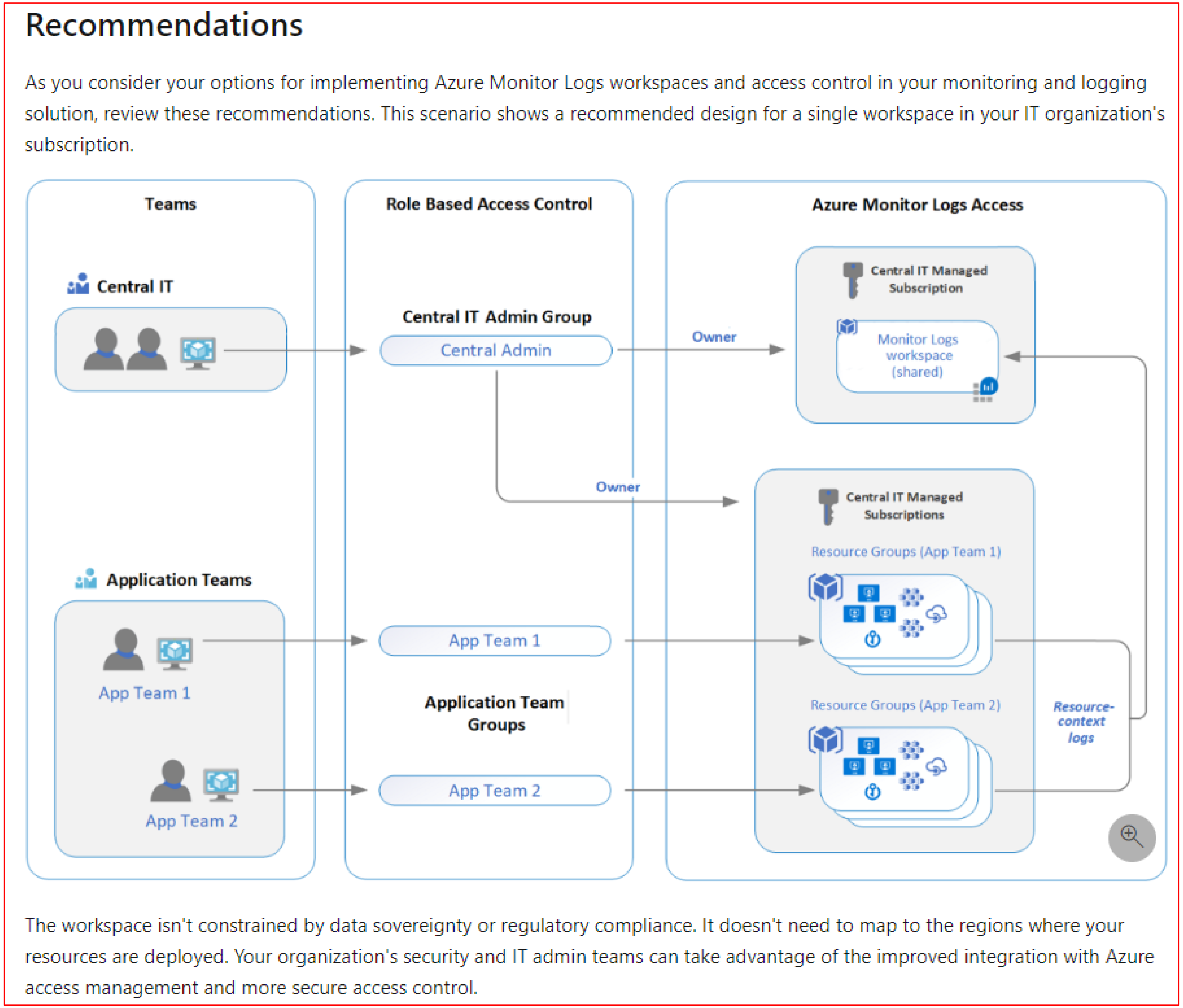
Considerations for access mode

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



Access mode	Description
Workspace-context	A user can review all logs in the workspace for which they have permission. Queries are scoped to all data in all tables in the workspace. Logs are accessed with the workspace as the scope by selecting **Logs** from the **Azure Monitor** menu in the Azure portal.
Resource-context	A user accesses the workspace for a particular resource, resource group, or subscription. By selecting **Logs** from a resource menu in the Azure portal, they can view logs for only resources in all tables for which they have access. Queries are scoped to only data associated with that resource. This mode also enables granular Azure RBAC.



Recommendations

As you consider your options for implementing Azure Monitor Logs workspaces and access control in your monitoring and logging solution, review these recommendations. This scenario shows a recommended design for a single workspace in your IT organization's subscription.

Teams
Role Based Access Control
Azure Monitor Logs Access
Central IT
Central IT Admin Group
Central Admin
Owner
Central IT Managed Subscription
Monitor Logs workspace (shared)
Owner
Central IT Managed Subscriptions
Resource Groups (App Team 1)
Application Teams
App Team 1
App Team 1
Application Team Groups
Resource Groups (App Team 2)
Resource-context logs
App Team 2
App Team 2

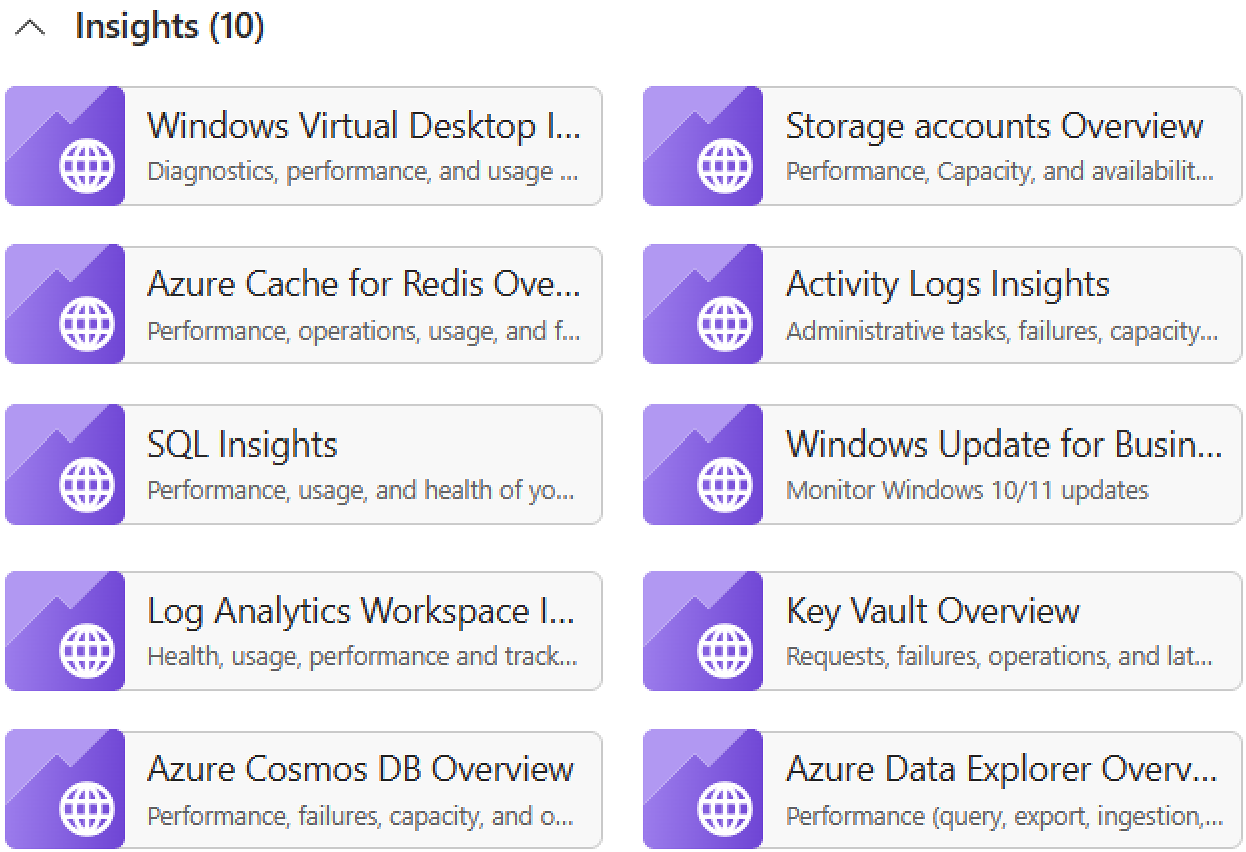
The workspace isn't constrained by data sovereignty or regulatory compliance. It doesn't need to map to the regions where your resources are deployed. Your organization's security and IT admin teams can take advantage of the improved integration with Azure access management and more secure access control.

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



Insights (10)

Windows Virtual Desktop I...
Diagnostics, performance, and usage ...

Storage accounts Overview
Performance, Capacity, and availabilit...

Azure Cache for Redis Ove...
Performance, operations, usage, and f...

Activity Logs Insights
Administrative tasks, failures, capacity...

SQL Insights
Performance, usage, and health of yo...

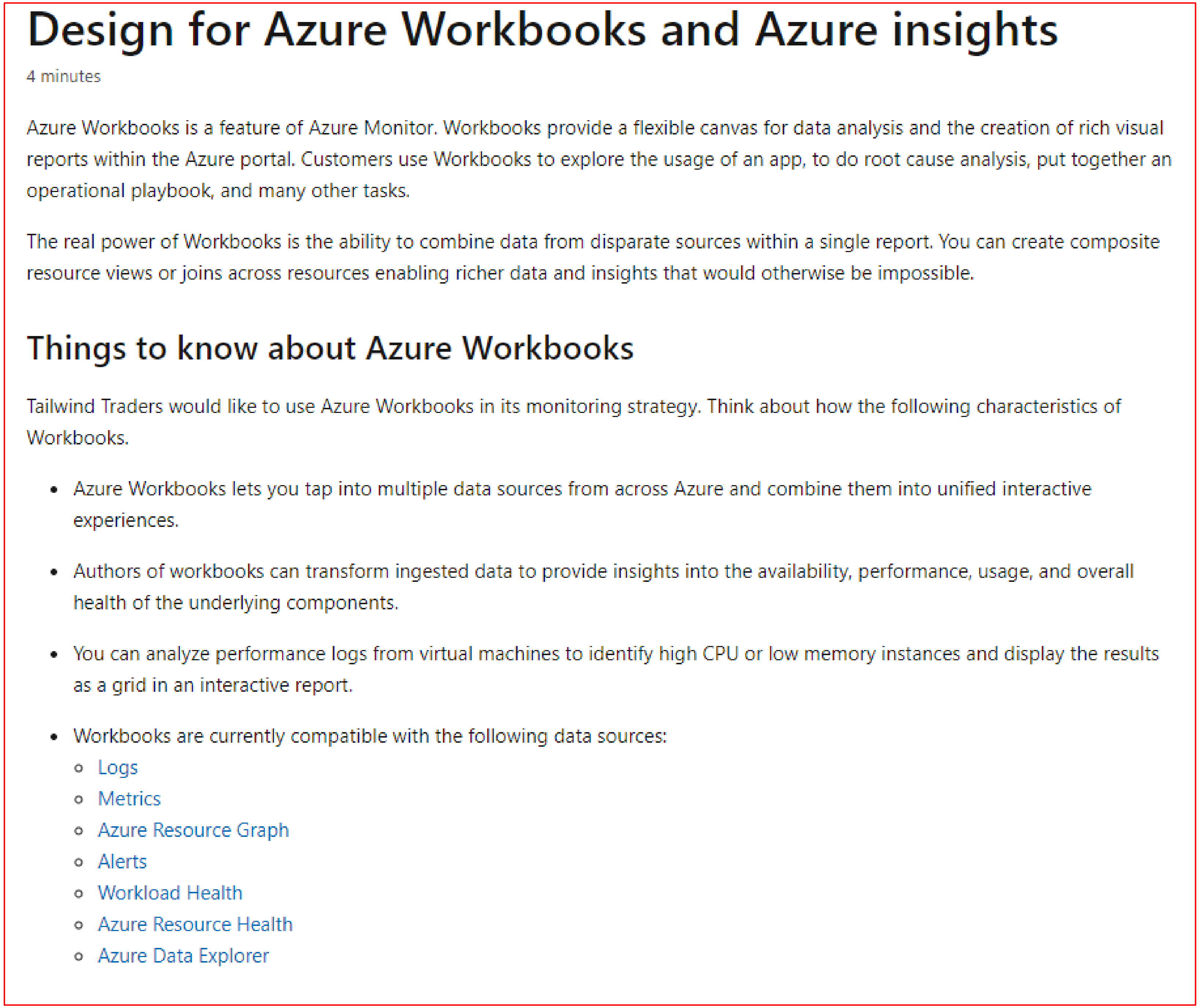
Windows Update for Busin...
Monitor Windows 10/11 updates

Log Analytics Workspace I...
Health, usage, performance and track...

Key Vault Overview
Requests, failures, operations, and lat...

Azure Cosmos DB Overview
Performance, failures, capacity, and o...

Azure Data Explorer Overv...
Performance (query, export, ingestion,...



Design for Azure Workbooks and Azure insights

4 minutes

Azure Workbooks is a feature of Azure Monitor. Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. Customers use Workbooks to explore the usage of an app, to do root cause analysis, put together an operational playbook, and many other tasks.

The real power of Workbooks is the ability to combine data from disparate sources within a single report. You can create composite resource views or joins across resources enabling richer data and insights that would otherwise be impossible.

Things to know about Azure Workbooks

Tailwind Traders would like to use Azure Workbooks in its monitoring strategy. Think about how the following characteristics of Workbooks.

- Azure Workbooks lets you tap into multiple data sources from across Azure and combine them into unified interactive experiences.
- Authors of workbooks can transform ingested data to provide insights into the availability, performance, usage, and overall health of the underlying components.
- You can analyze performance logs from virtual machines to identify high CPU or low memory instances and display the results as a grid in an interactive report.
- Workbooks are currently compatible with the following data sources:
    - Logs
    - Metrics
    - Azure Resource Graph
    - Alerts
    - Workload Health
    - Azure Resource Health
    - Azure Data Explorer

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:

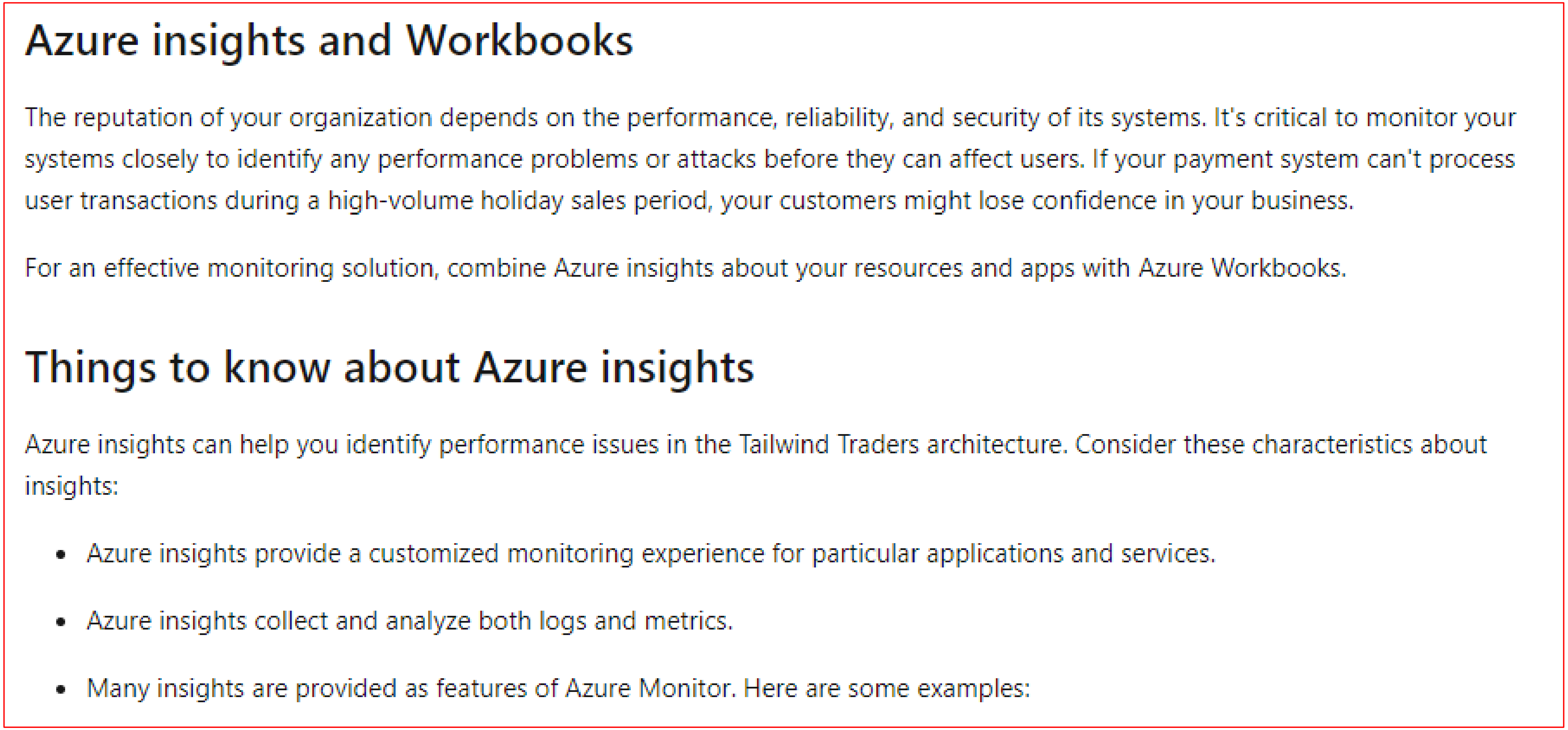
- Analyze and address issues and problems that affect your application's health and performance.
- Improve your application's development lifecycle.
- Measure your user experience and analyze users' behavior.

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.



Azure insights and Workbooks

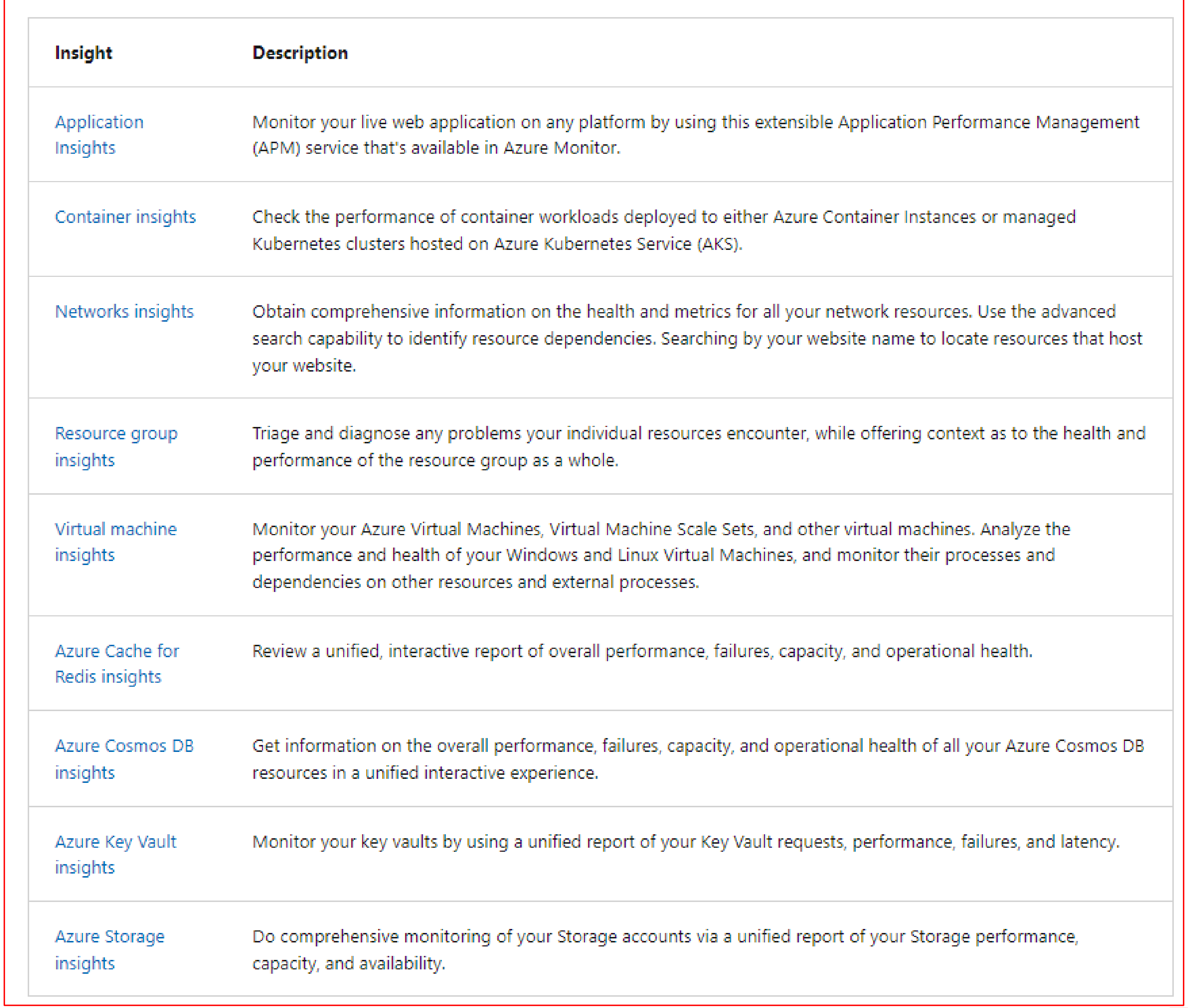
The reputation of your organization depends on the performance, reliability, and security of its systems. It's critical to monitor your systems closely to identify any performance problems or attacks before they can affect users. If your payment system can't process user transactions during a high-volume holiday sales period, your customers might lose confidence in your business.

For an effective monitoring solution, combine Azure insights about your resources and apps with Azure Workbooks.

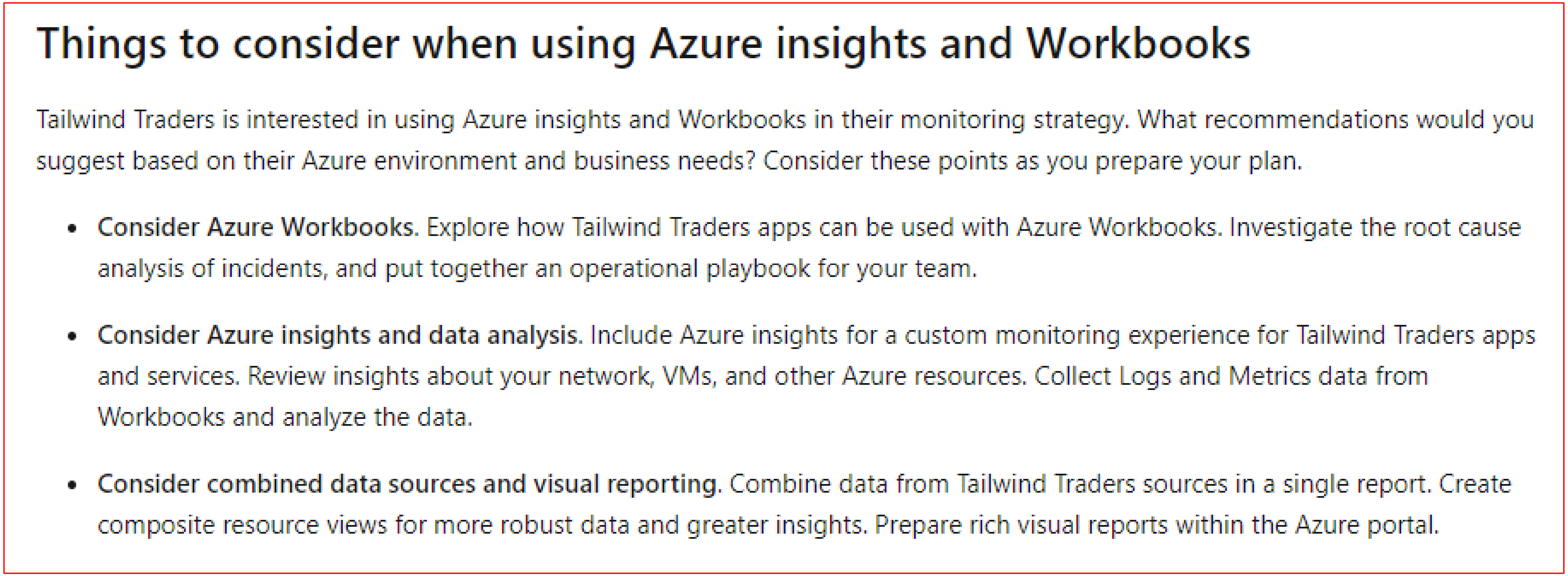
Things to know about Azure insights

Azure insights can help you identify performance issues in the Tailwind Traders architecture. Consider these characteristics about insights:

- Azure insights provide a customized monitoring experience for particular applications and services.
- Azure insights collect and analyze both logs and metrics.
- Many insights are provided as features of Azure Monitor. Here are some examples:



Insight	Description
Application Insights	Monitor your live web application on any platform by using this extensible Application Performance Management (APM) service that's available in Azure Monitor.
Container insights	Check the performance of container workloads deployed to either Azure Container Instances or managed Kubernetes clusters hosted on Azure Kubernetes Service (AKS).
Networks insights	Obtain comprehensive information on the health and metrics for all your network resources. Use the advanced search capability to identify resource dependencies. Searching by your website name to locate resources that host your website.
Resource group insights	Triage and diagnose any problems your individual resources encounter, while offering context as to the health and performance of the resource group as a whole.
Virtual machine insights	Monitor your Azure Virtual Machines, Virtual Machine Scale Sets, and other virtual machines. Analyze the performance and health of your Windows and Linux Virtual Machines, and monitor their processes and dependencies on other resources and external processes.
Azure Cache for Redis insights	Review a unified, interactive report of overall performance, failures, capacity, and operational health.
Azure Cosmos DB insights	Get information on the overall performance, failures, capacity, and operational health of all your Azure Cosmos DB resources in a unified interactive experience.
Azure Key Vault insights	Monitor your key vaults by using a unified report of your Key Vault requests, performance, failures, and latency.
Azure Storage insights	Do comprehensive monitoring of your Storage accounts via a unified report of your Storage performance, capacity, and availability.



Things to consider when using Azure insights and Workbooks

Tailwind Traders is interested in using Azure insights and Workbooks in their monitoring strategy. What recommendations would you suggest based on their Azure environment and business needs? Consider these points as you prepare your plan.

- **Consider Azure Workbooks.** Explore how Tailwind Traders apps can be used with Azure Workbooks. Investigate the root cause analysis of incidents, and put together an operational playbook for your team.
- **Consider Azure insights and data analysis.** Include Azure insights for a custom monitoring experience for Tailwind Traders apps and services. Review insights about your network, VMs, and other Azure resources. Collect Logs and Metrics data from Workbooks and analyze the data.
- **Consider combined data sources and visual reporting.** Combine data from Tailwind Traders sources in a single report. Create composite resource views for more robust data and greater insights. Prepare rich visual reports within the Azure portal.

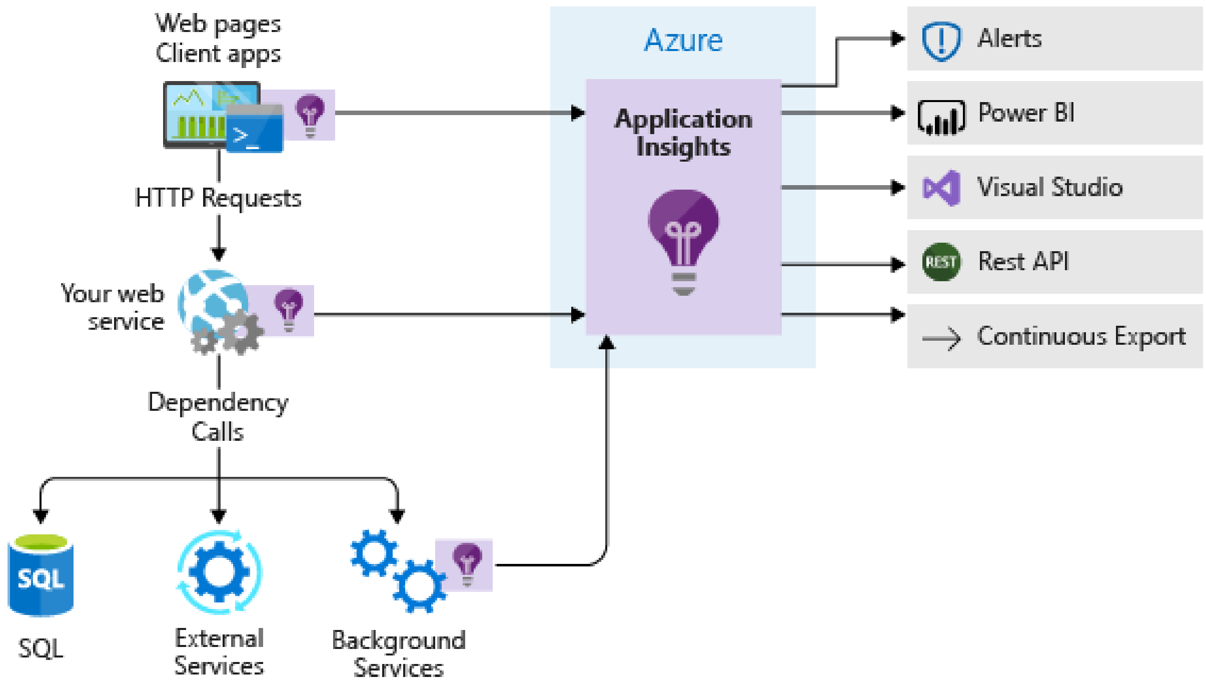
Select Application Insights

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.

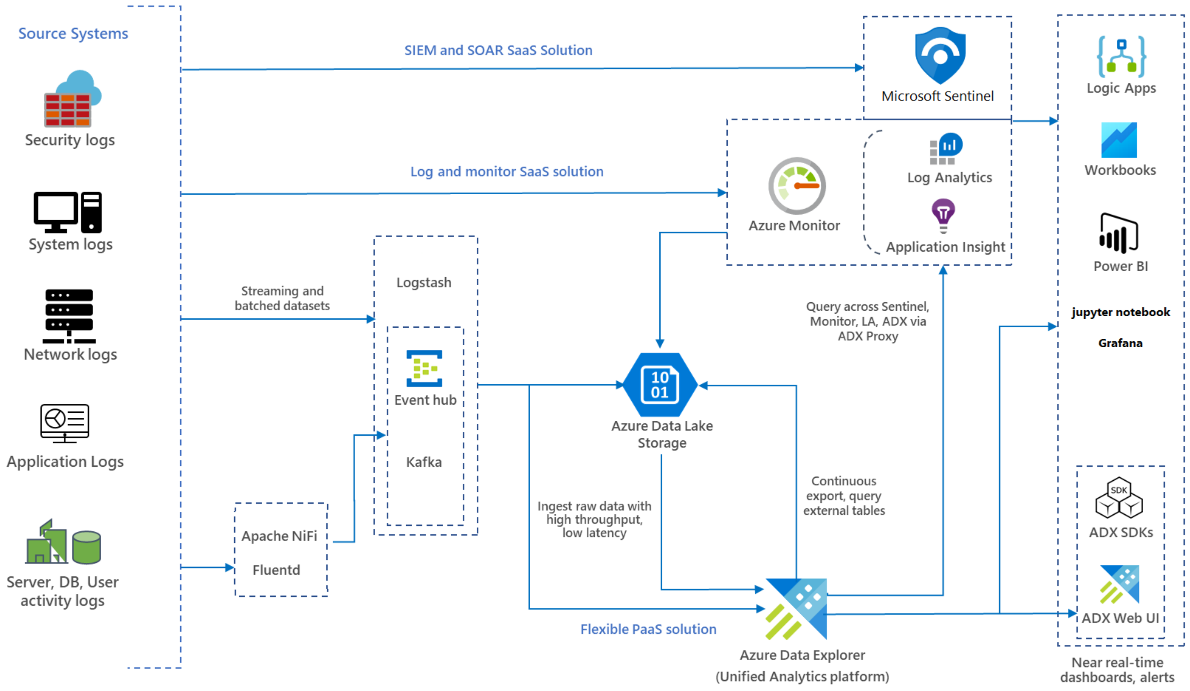


Design for Azure Data Explorer

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.


Source Systems
Security logs
System logs
Network logs
Application Logs
Server, DB, User activity logs
SIEM and SOAR SaaS Solution
Microsoft Sentinel
Log and monitor SaaS solution
Azure Monitor
Log Analytics
Application Insight
Streaming and batched datasets
Logstash
Event hub
Kafka
Apache NiFi
Fluentd
Azure Data Lake Storage
Query across Sentinel, Monitor, LA, ADX via ADX Proxy
Ingest raw data with high throughput, low latency
Continuous export, query external tables
Flexible PaaS solution
Azure Data Explorer (Unified Analytics platform)
Logic Apps
Workbooks
Power BI
jupyter notebook
Grafana
ADX SDKs
ADX Web UI
Near real-time dashboards, alerts

Case study

Use Case Scenarios (activity)

- Azure Monitor
- Application Insights
- Azure workbooks
- Log Analytics

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

You need to edit and run log queries

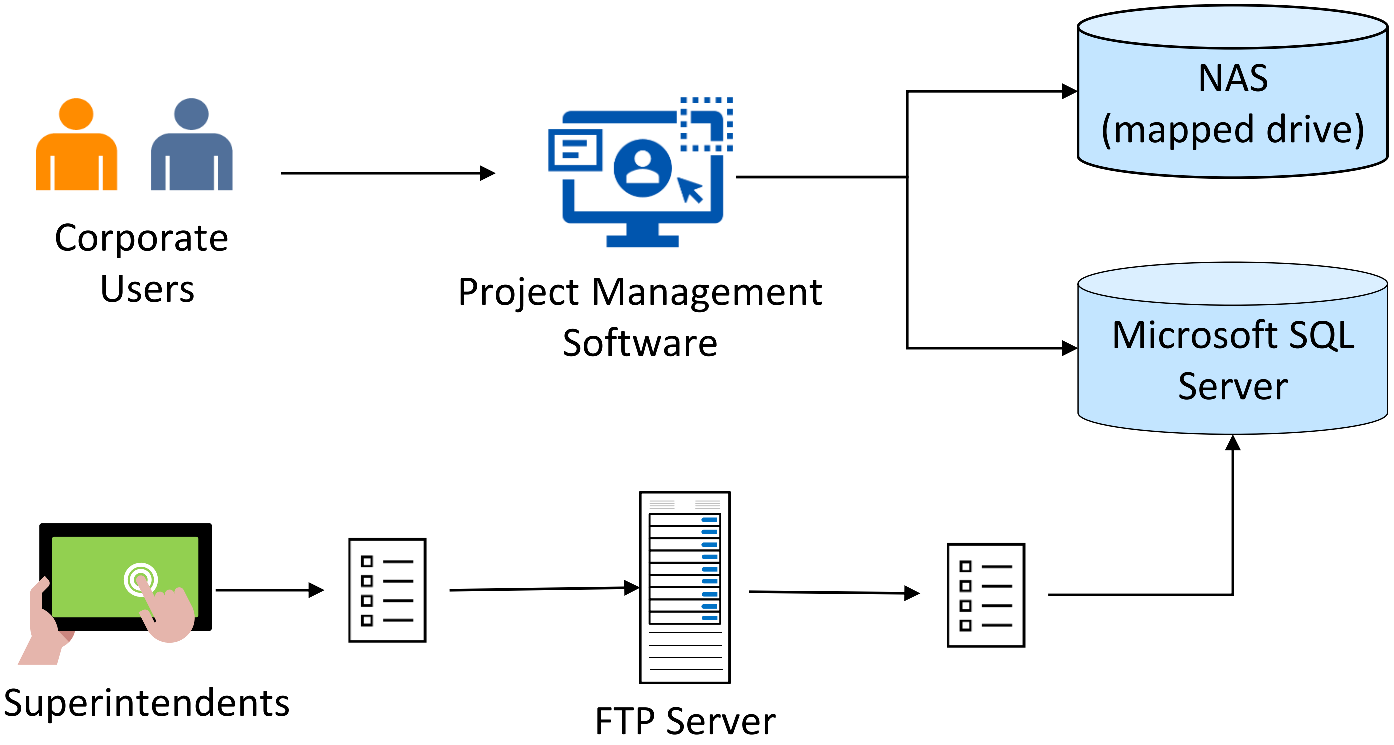
You need transaction diagnostics and performance statistics (client and server).

You need data analysis and the creation of rich visual reports

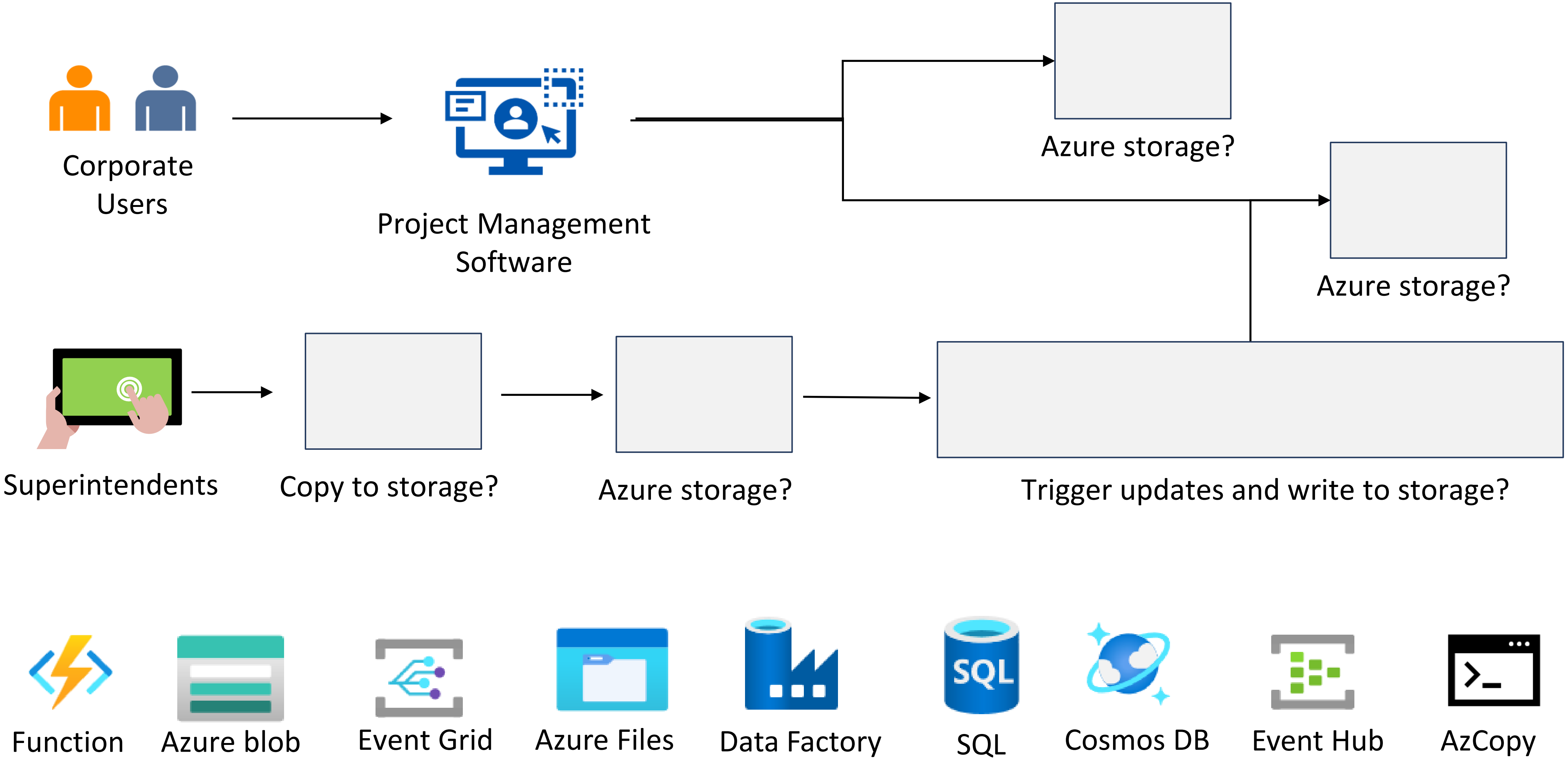
You need usage information on request rates, response times, and failure rates of an application

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



Solution - Fabrikam Residences PM software



Corporate Users

Project Management Software

Azure storage?

Azure storage?

Superintendents

Copy to storage?

Azure storage?

Trigger updates and write to storage?

Function

Azure blob

Event Grid

Azure Files

Data Factory

SQL

Cosmos DB

Event Hub

AzCopy