Log Analytics Workspace

A Log Analytics Workspace in Azure is a centralized data storage and analysis platform where logs and telemetry data from various Azure resources, on-premises systems, and other environments are collected, stored, and analyzed. It is a key component of Azure Monitor, allowing users to query, analyze, and visualize logs from different sources.

The workspace supports structured and unstructured data, enabling users to gain insights into system performance, troubleshoot issues, and monitor applications. It uses Kusto Query Language (KQL) for powerful querying, helping to identify trends, detect anomalies, and generate reports. The workspace is also integrated with other Azure services for a comprehensive monitoring and security solution.

Key features include:

1. **Data Collection:** Collects logs and metrics from Azure resources, virtual machines, containers, and custom applications.
2. **Advanced Querying**: Utilizes KQL for detailed analysis and complex queries on logs.
3. **Visualization:** Create dashboards and charts to track trends and system health.
4. **Alerting and Automation:** Set up alerts based on log data to trigger notifications or automated actions.
5. **Security and Compliance:** Supports security monitoring, auditing, and compliance tracking, making it useful for regulatory purposes like GDPR or HIPAA.

Use cases of Log Analytics Workspace

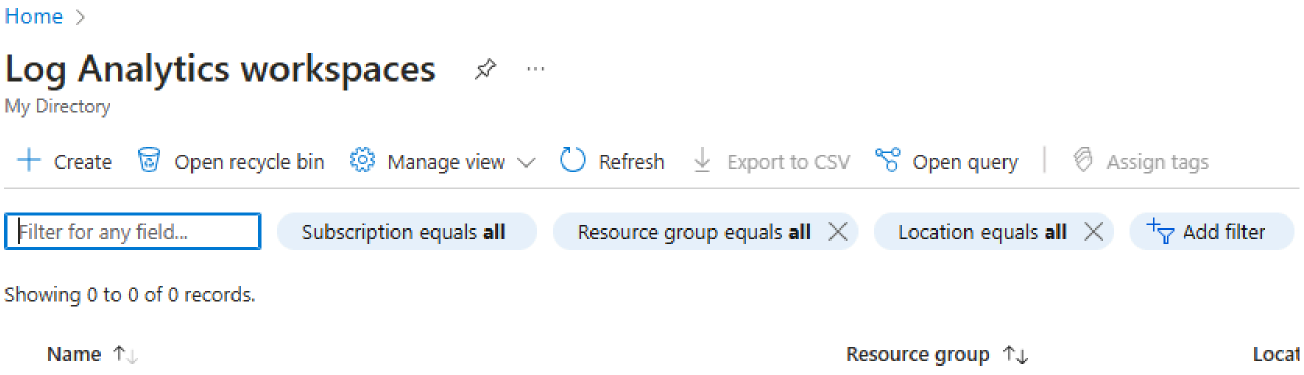
1. **Operational Insights**: Helps organizations gain a deeper understanding of the performance and health of their Azure environment and on-premises infrastructure by collecting logs from virtual machines, applications, and servers. This allows users to troubleshoot issues, identify bottlenecks, and optimize resource usage.
2. **Security Monitoring and Threat Detection**: Collects and analyzes security logs from Azure resources, network appliances, and security solutions to identify malicious activities and threats in real-time. It helps in investigating and responding to security incidents, improving overall security posture.
3. **Compliance and Audit**: Centralizes log data to support compliance efforts. It tracks user activities, monitors access to sensitive data, and generates audit logs for regulatory requirements like **GDPR**, **HIPAA**, and **PCI DSS**, helping businesses ensure they meet legal and regulatory standards.
4. **Application Monitoring and Troubleshooting**: Developers use Log Analytics Workspace to track application logs, performance metrics, and errors. It enables proactive troubleshooting and optimization, improving the application's reliability and user experience.

5. **Infrastructure Optimization**: Analyzes resource utilization, helping organizations identify inefficiencies in infrastructure. It can track underutilized resources, recommend cost optimizations, and ensure that infrastructure is properly sized for business needs.
6. **DevOps and Continuous Monitoring**: Integrates with **DevOps** practices, enabling continuous monitoring and feedback loops. It allows teams to track the health of application deployments, identify performance issues, and automate corrective actions to ensure smooth continuous delivery and deployment.
7. **Predictive Analytics and Anomaly Detection**: Using machine learning, Log Analytics can perform predictive analytics and anomaly detection on log data, identifying abnormal patterns and predicting future trends. This helps in proactive management and prevention of potential operational issues.

The end goal of this lab is to configure a Log Analytics Workspace in Azure and set up data collection rules to centralize logs and telemetry data from a Windows Virtual Machine. This enables efficient monitoring and analysis of performance metrics, event logs, and system behaviors. By collecting and visualizing this data in the Log Analytics Workspace, users can gain actionable insights, identify and troubleshoot issues, monitor compliance with security standards, and optimize resource utilization. Ultimately, this lab empowers users to enhance operational efficiency, improve security posture, and ensure proactive management of their Azure environment.

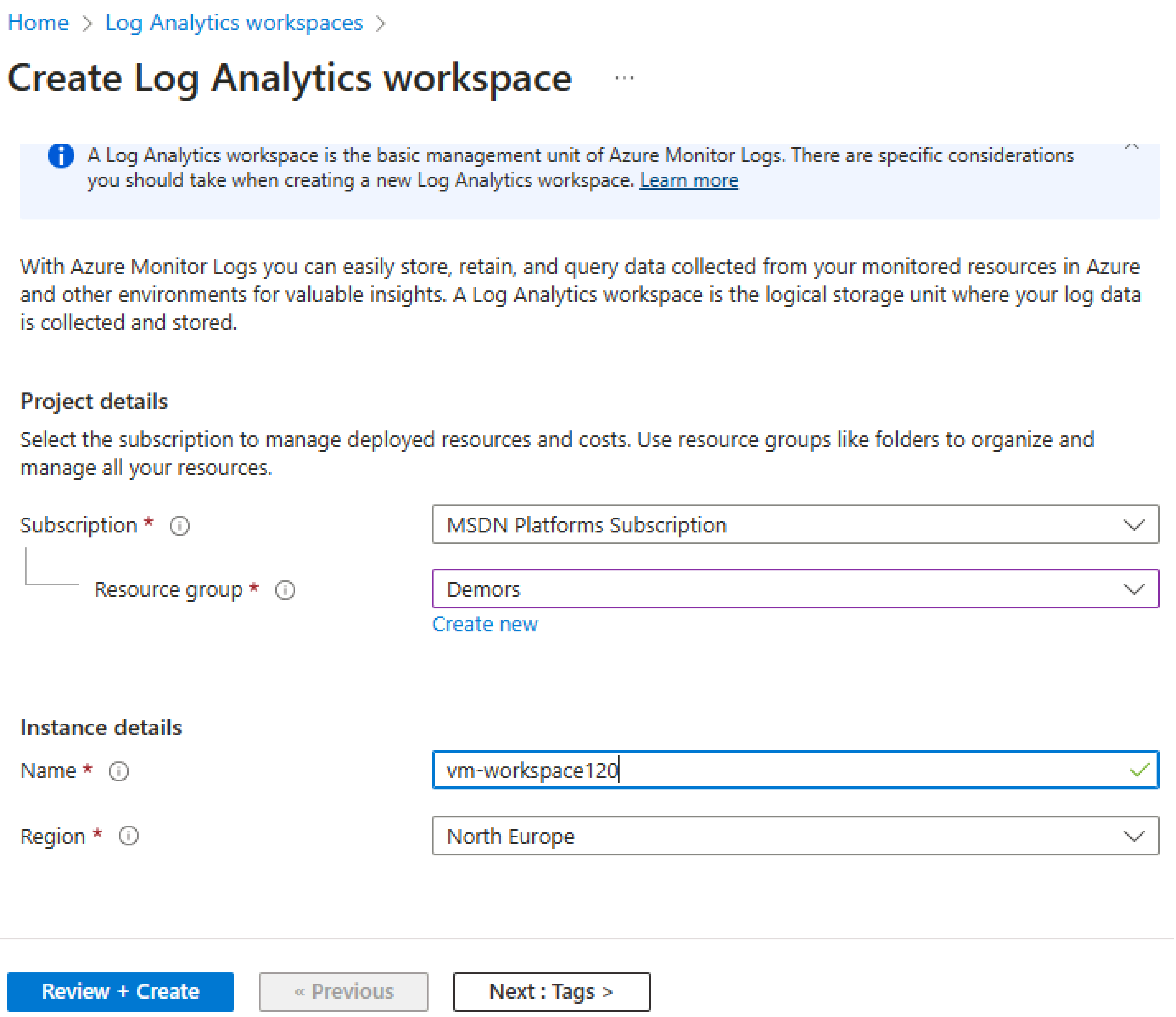
To begin with the lab

1. In the **Azure Portal**, search for **Log Analytics Workspace** and choose the service.



Showing 0 to 0 of 0 records.

2. Select your **resource group**, provide a unique **name** for the workspace. Choose the **North Europe** location. Click **Review + Create** and then click **Create** to deploy the workspace.



Create Log Analytics workspace

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : MSDN Platforms Subscription

Resource group * : Demors

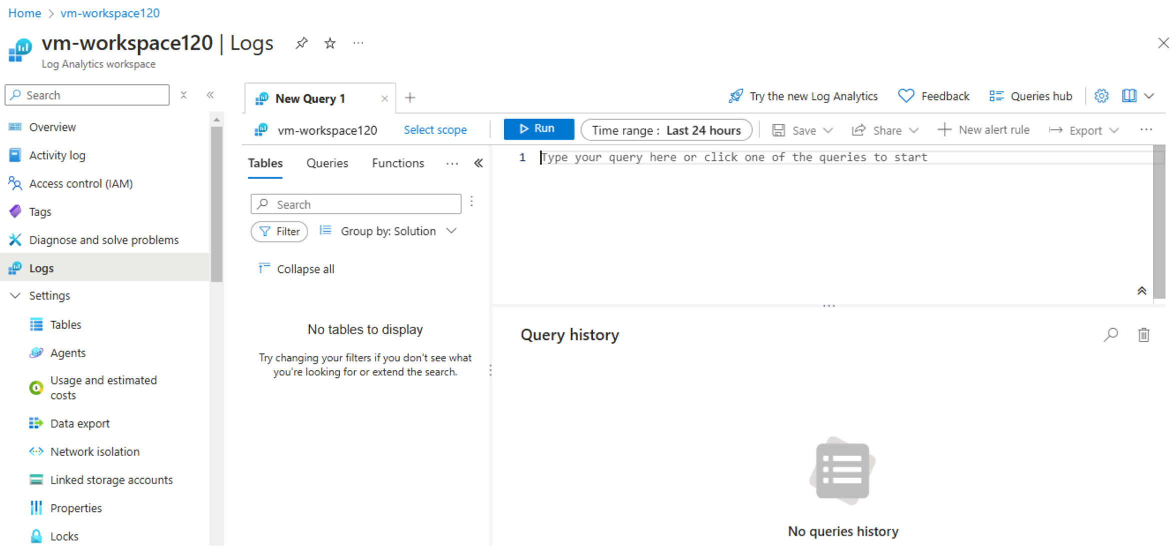
Create new

Instance details

Name * : vm-workspace120

Region * : North Europe

3. Now in your workspace you need to go to logs. You will see that currently your logs are empty.



vm-workspace120 | Logs

Log Analytics workspace

Time range : Last 24 hours

Type your query here or click one of the queries to start

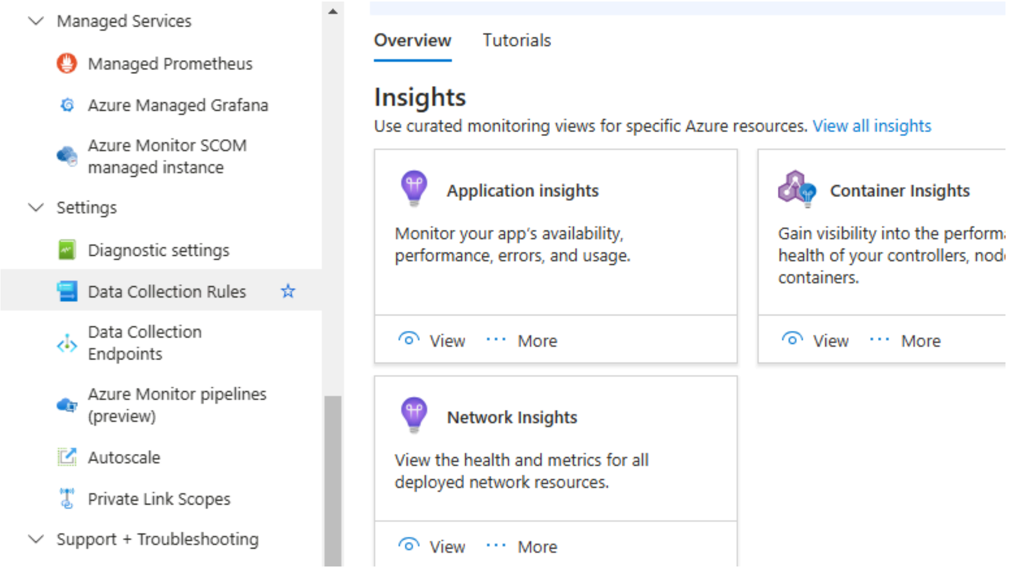
No tables to display

Try changing your filters if you don't see what you're looking for or extend the search.

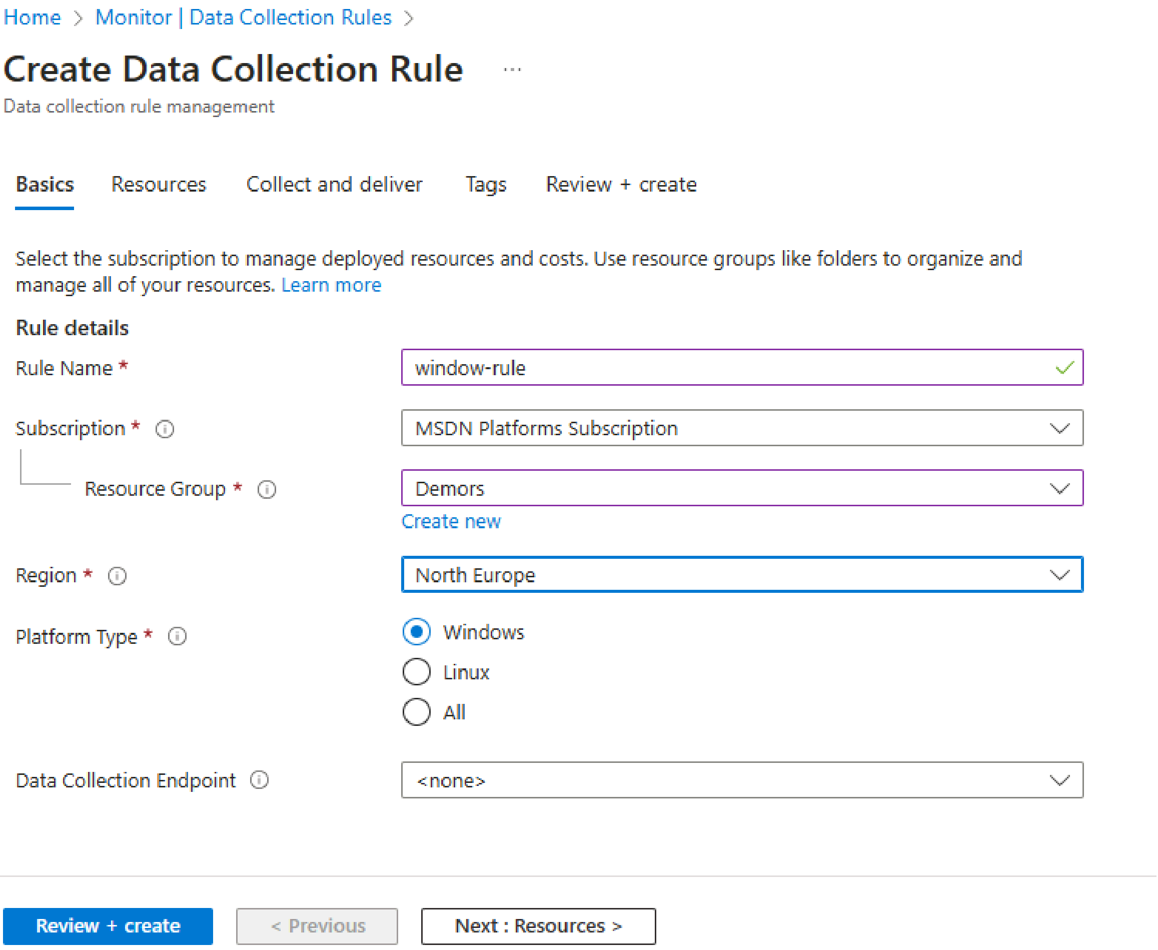
Query history

No queries history

4. Once the workspace is deployed, go to the **Monitor** service in the Azure portal. In the left pane, scroll down and select **Data Collection Rules**.


Managed Services
Managed Prometheus
Azure Managed Grafana
Azure Monitor SCOM managed instance
Settings
Diagnostic settings
Data Collection Rules
Data Collection Endpoints
Azure Monitor pipelines (preview)
Autoscale
Private Link Scopes
Support + Troubleshooting
Overview
Tutorials
Insights
Use curated monitoring views for specific Azure resources. View all insights
Application insights
Monitor your app's availability, performance, errors, and usage.
View
More
Container Insights
Gain visibility into the perform
health of your controllers, nod
containers.
View
More
Network Insights
View the health and metrics for all deployed network resources.
View
More

5. Choose your **resource group**, select **North Europe** as the location and choose **Windows** as the platform type (if your VM is Windows-based).



Create Data Collection Rule ···

Data collection rule management

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. Learn more

Rule details

Rule Name * window-rule ✓

Subscription * ⓘ MSDN Platforms Subscription

Resource Group * ⓘ Demors

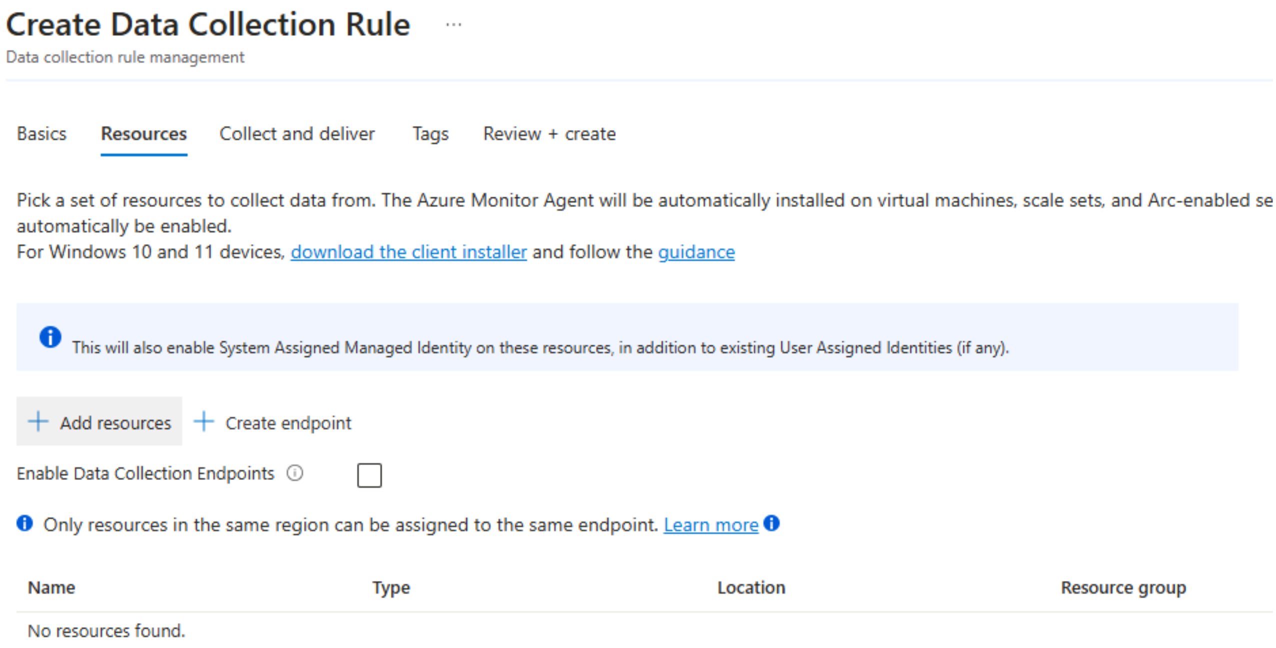
Create new

Region * ⓘ North Europe

Platform Type * ⓘ
● Windows
○ Linux
○ All

Data Collection Endpoint ⓘ <none>

6. Now you have to add resources, to do so click on your virtual machine. Add your **Azure VM** (e.g., **appvm**) to the data collection rule.



Create Data Collection Rule ...

Data collection rule management

Pick a set of resources to collect data from. The Azure Monitor Agent will be automatically installed on virtual machines, scale sets, and Arc-enabled se automatically be enabled.

For Windows 10 and 11 devices, download the client installer and follow the guidance

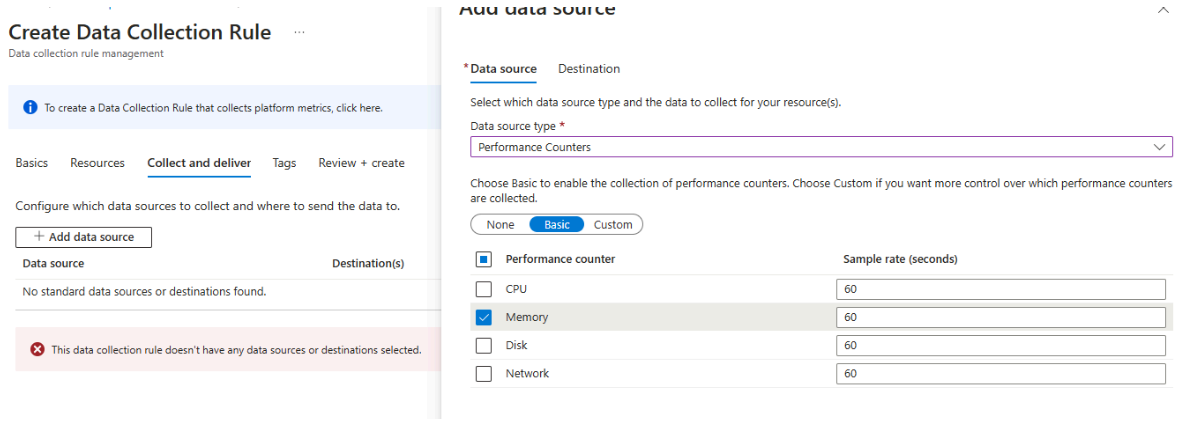
This will also enable System Assigned Managed Identity on these resources, in addition to existing User Assigned Identities (if any).

Enable Data Collection Endpoints ⓘ □

Only resources in the same region can be assigned to the same endpoint. Learn more

Name	Type	Location	Resource group
No resources found.			

7. Now you have to add data source by clicking **Add Data Source**. Select **Performance Counters** to monitor system performance.



Create Data Collection Rule ...

Data collection rule management

To create a Data Collection Rule that collects platform metrics, click here.

Configure which data sources to collect and where to send the data to.

Data source	Destination(s)
No standard data sources or destinations found.	

This data collection rule doesn't have any data sources or destinations selected.

Add data source

Select which data source type and the data to collect for your resource(s).

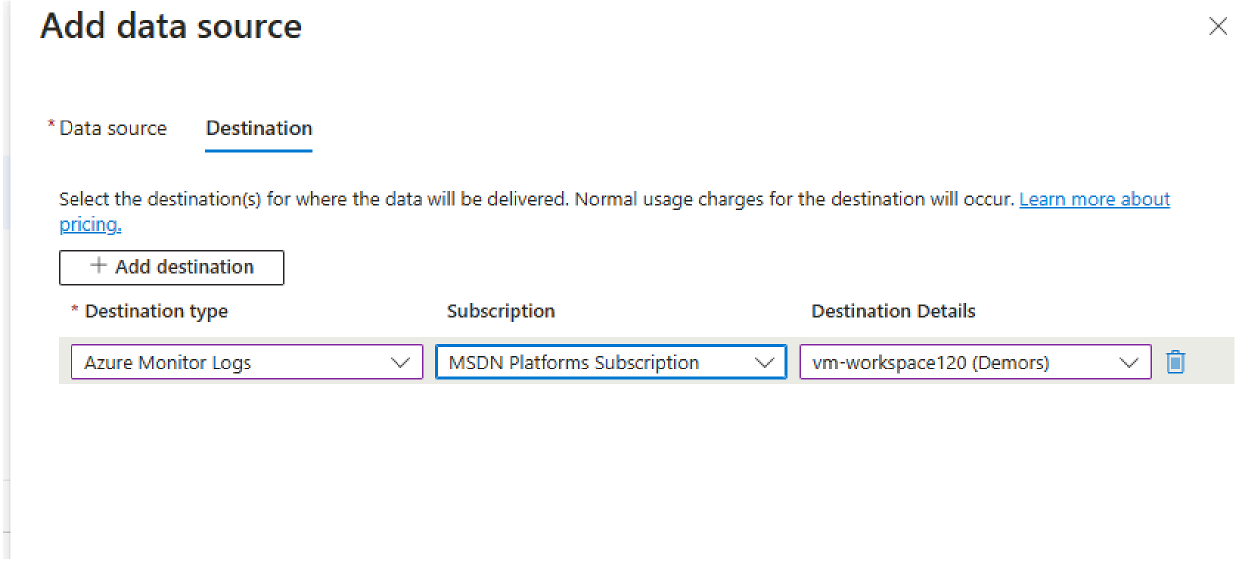
Data source type *

Performance Counters

Choose Basic to enable the collection of performance counters. Choose Custom if you want more control over which performance counters are collected.

None [✓ Basic] Custom

■ Performance counter	Sample rate (seconds)
□ CPU	60
☑ Memory	60
□ Disk	60
□ Network	60

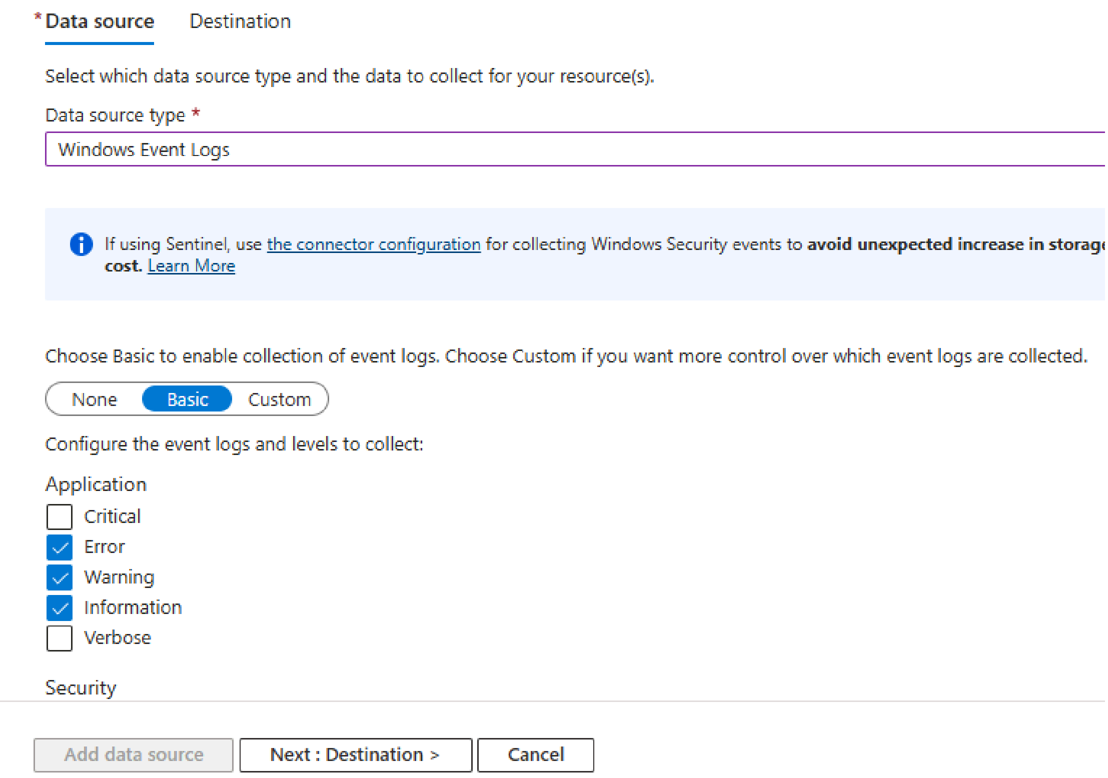


Add data source

Select the destination(s) for where the data will be delivered. Normal usage charges for the destination will occur. Learn more about pricing.

* Destination type	Subscription	Destination Details
Azure Monitor Logs	MSDN Platforms Subscription	vm-workspace120 (Demors)

8. After you have added your initial data source, the next step is to incorporate an additional data source, specifically selecting Windows event logs. Subsequently, you should select the categories of error, warning, and information for the logs.



Select which data source type and the data to collect for your resource(s).

Data source type *: Windows Event Logs

If using Sentinel, use the connector configuration for collecting Windows Security events to **avoid unexpected increase in storag** **cost.** Learn More

Choose Basic to enable collection of event logs. Choose Custom if you want more control over which event logs are collected.

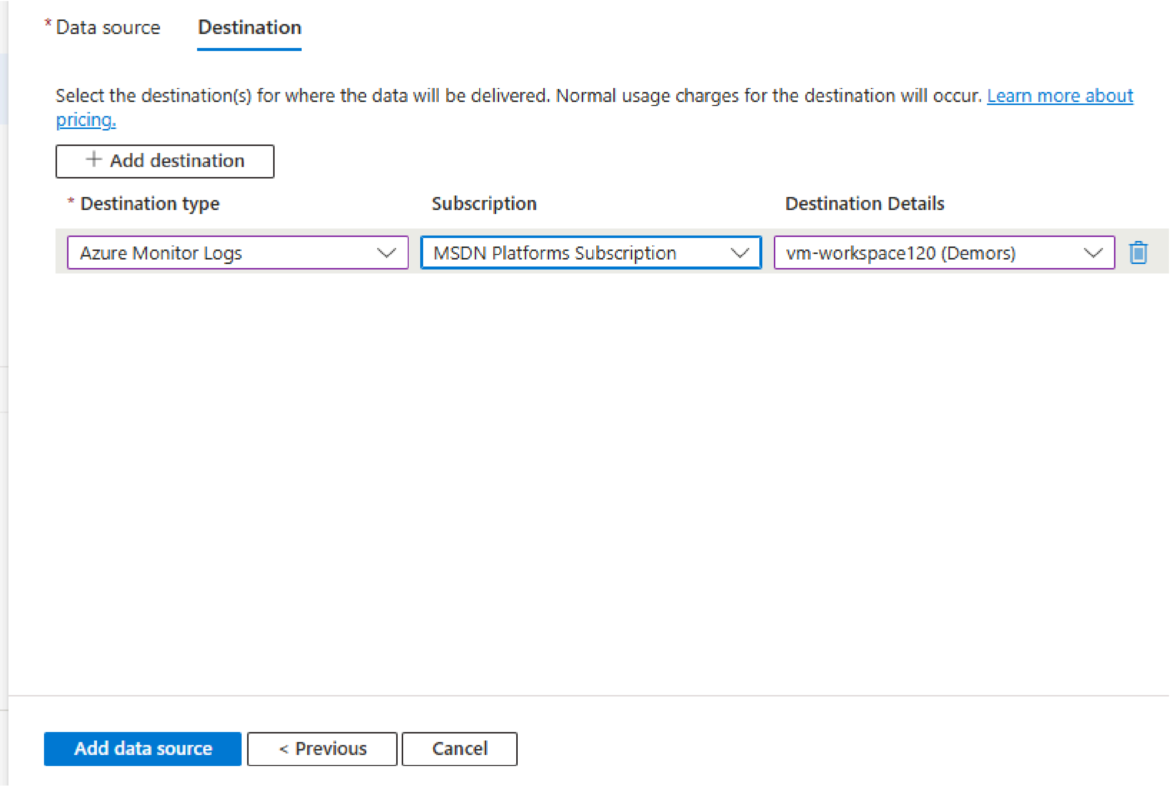
None | [✓ Basic] | Custom

Configure the event logs and levels to collect:

Application

- □ Critical
- ☑ Error
- ☑ Warning
- ☑ Information
- □ Verbose

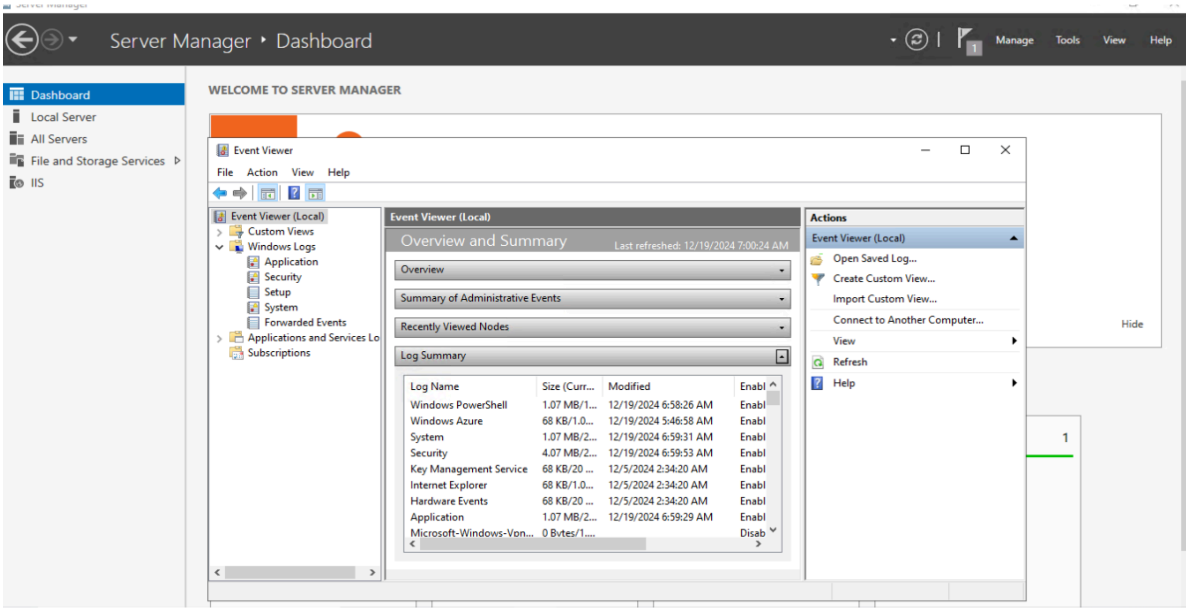
Security



Select the destination(s) for where the data will be delivered. Normal usage charges for the destination will occur. Learn more about pricing.

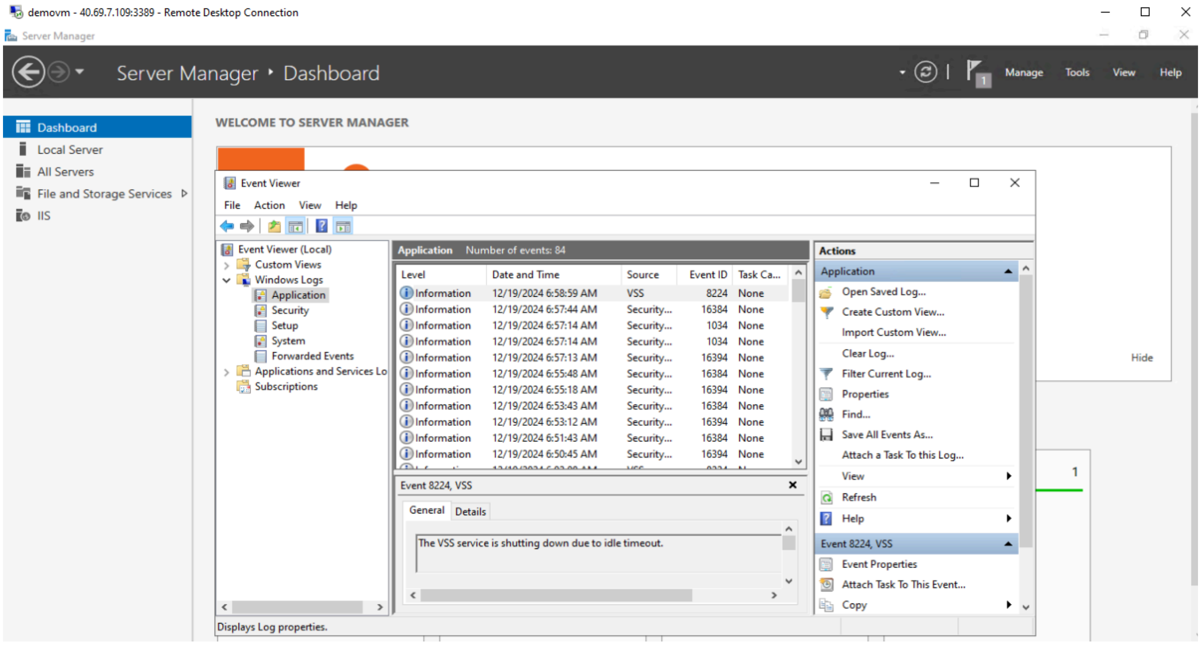
* Destination type	Subscription	Destination Details
Azure Monitor Logs	MSDN Platforms Subscription	vm-workspace120 (Demors)

9. Review the data collection settings and Click **Create** to finalize the data collection rule.
10. To begin, access the Event Viewer on your Windows virtual machine. Expand the Windows Logs section to examine both the Application and Security logs. These logs will be gathered and transmitted to the Log Analytics workspace. To verify the logs in the Log Analytics Workspace:



Log Name	Size (Curr...	Modified	Enabl
Windows PowerShell	1.07 MB/1...	12/19/2024 6:58:26 AM	Enabl
Windows Azure	68 KB/1.0...	12/19/2024 5:46:58 AM	Enabl
System	1.07 MB/2...	12/19/2024 6:59:31 AM	Enabl
Security	4.07 MB/2...	12/19/2024 6:59:53 AM	Enabl
Key Management Service	68 KB/20 ...	12/5/2024 2:34:20 AM	Enabl
Internet Explorer	68 KB/1.0...	12/5/2024 2:34:20 AM	Enabl
Hardware Events	68 KB/20 ...	12/5/2024 2:34:20 AM	Enabl
Application	1.07 MB/2...	12/19/2024 6:59:29 AM	Enabl
Microsoft-Windows-Vpn...	0 Bytes/1....		Disab

11. Allow approximately 10 minutes for the data to be collected and sent to the workspace. Return to the Log Analytics workspace within the Azure portal. Proceed to the Logs section.
12. In the Log Management tables, find the Event table. Execute a query on the Event table to review the logs from your Windows virtual machine, which will include both security and application logs.
13. Now if you want to see that logs you just need to write the name of the log and click on run then you'll able to see the logs.



Application Number of events: 84

Level	Date and Time	Source	Event ID	Task Ca...
Information	12/19/2024 6:58:59 AM	VSS	8224	None
Information	12/19/2024 6:57:44 AM	Security...	16384	None
Information	12/19/2024 6:57:14 AM	Security...	1034	None
Information	12/19/2024 6:57:14 AM	Security...	1034	None
Information	12/19/2024 6:57:13 AM	Security...	16394	None
Information	12/19/2024 6:55:48 AM	Security...	16384	None
Information	12/19/2024 6:55:18 AM	Security...	16394	None
Information	12/19/2024 6:53:43 AM	Security...	16384	None
Information	12/19/2024 6:53:12 AM	Security...	16394	None
Information	12/19/2024 6:51:43 AM	Security...	16384	None
Information	12/19/2024 6:50:45 AM	Security...	16394	None

Event 8224, VSS

General Details

The VSS service is shutting down due to idle timeout.