TOLUWANI ADEFISOYE (2023)

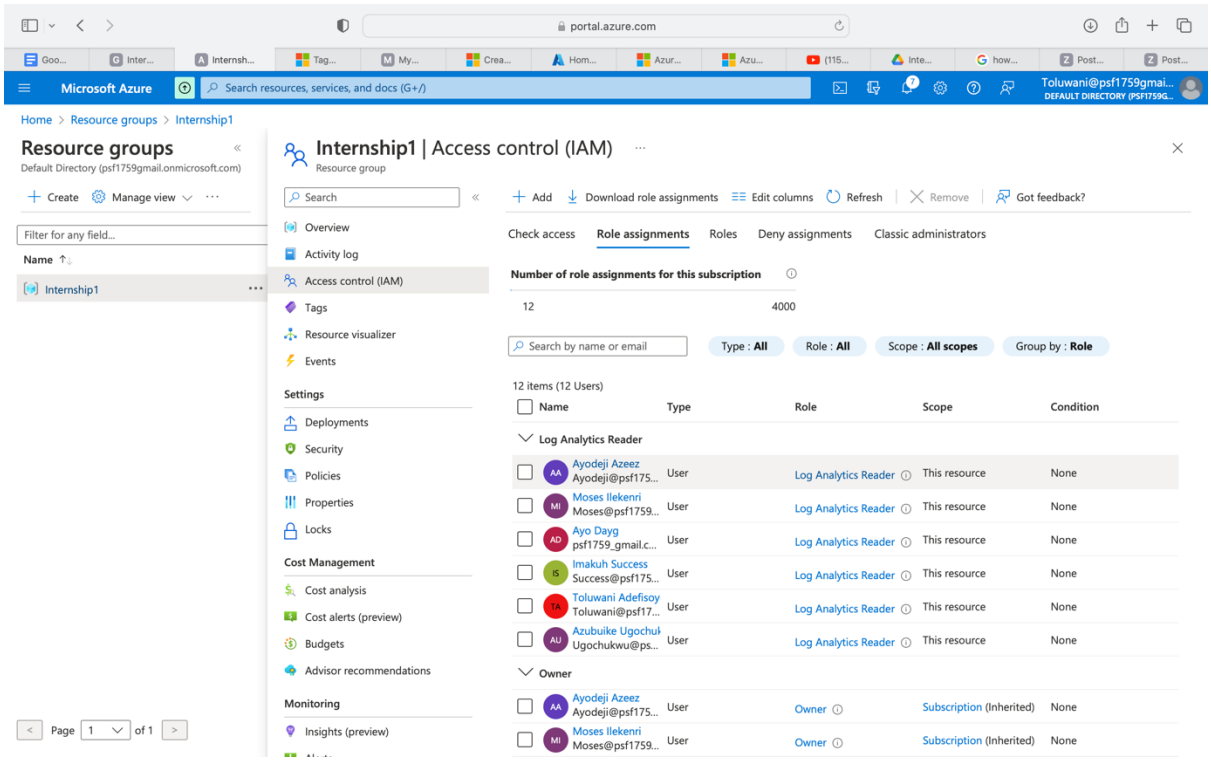
AUDIT, MONITORING AND LOGGING ON CLOUD – AUDIT LOGS/ AZURE SENTINEL

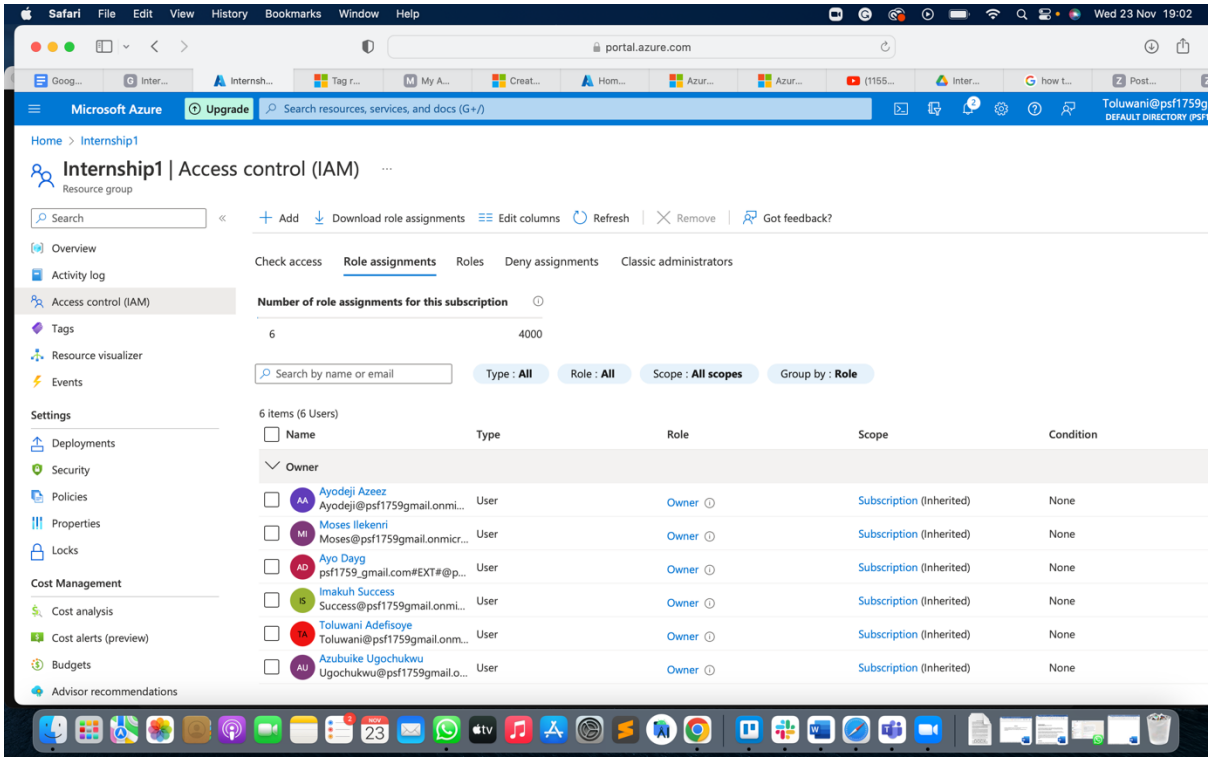
An audit log comprises the consecutive records of data that are important and/or necessary to uphold the system's security.

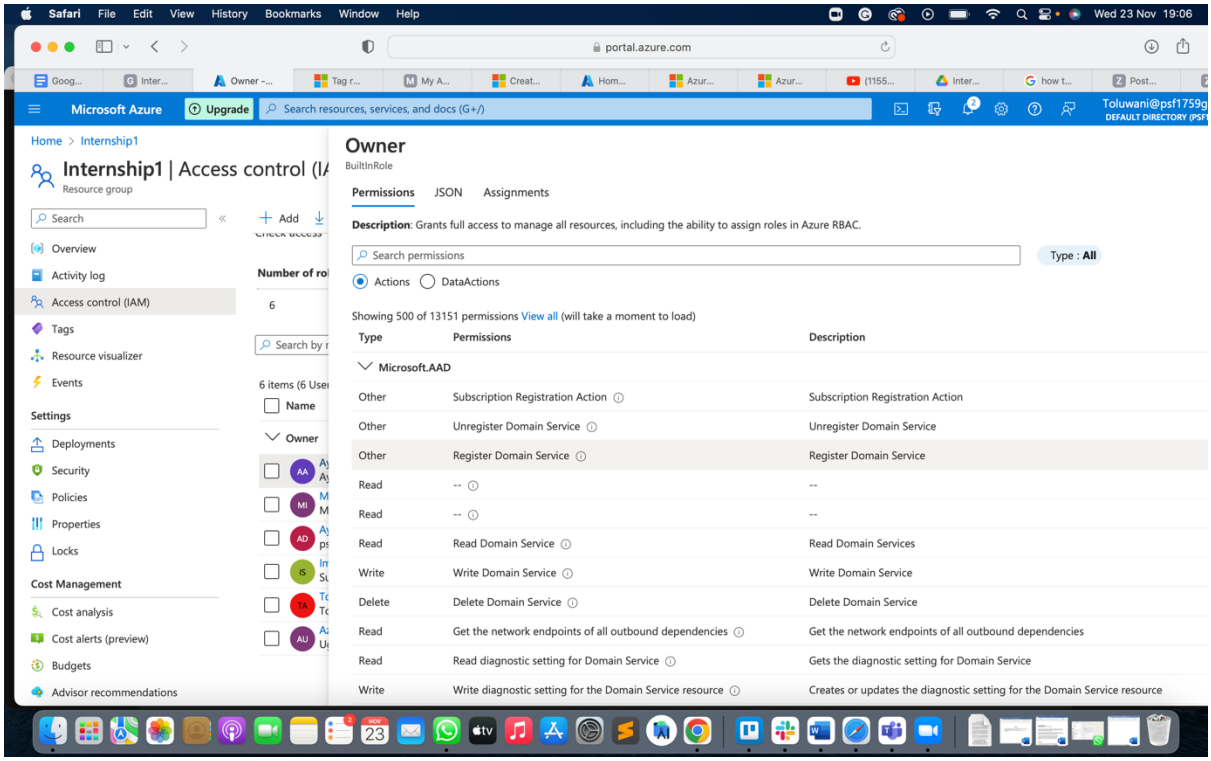
These records contain comprehensive information on the modifications or actions that affected a certain system operation, event, or process. We had to build a virtual machine for this task, give members Log Reader Permission, and keep an eye on the resource's behaviour.

The actions taken to finish this task are listed below;

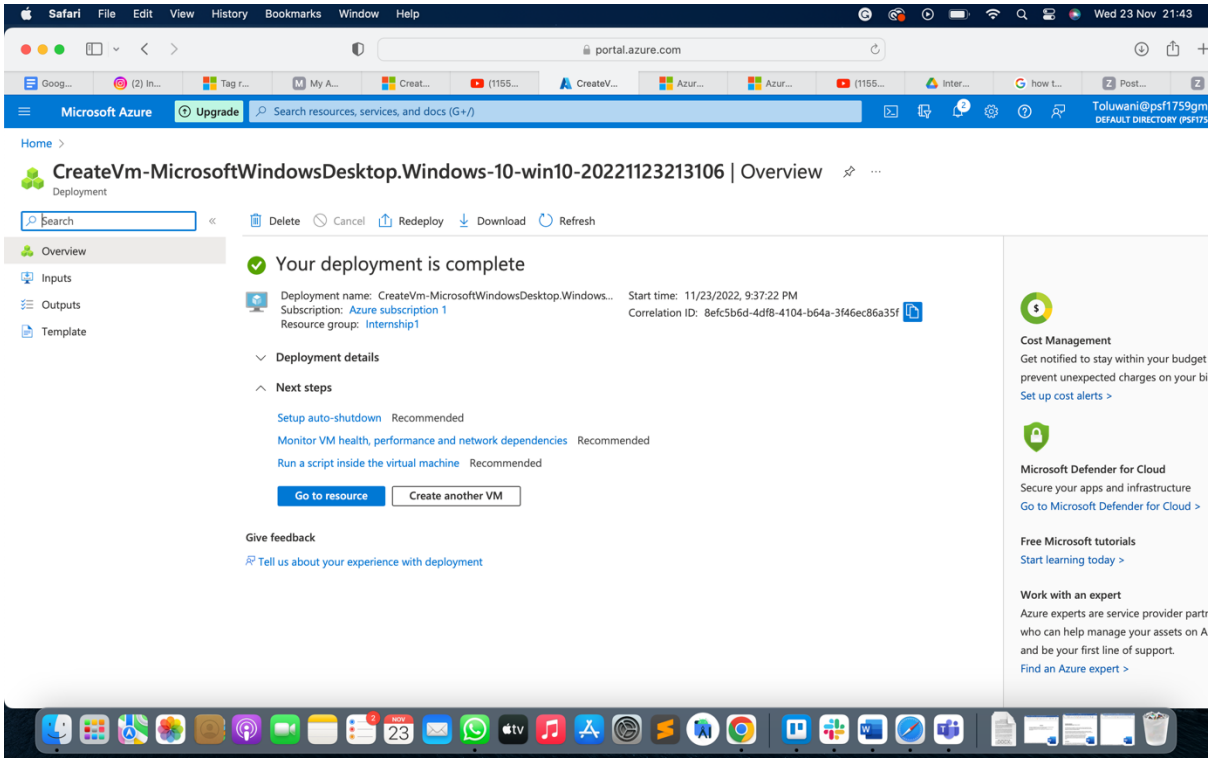
Following the creation of a Resource Group in the same Region, we then deployed a Windows Server Virtual Machine inside of it (UK South). Following that, we gave the resource group's users Log Reader Permissions, as shown in the screenshot below.







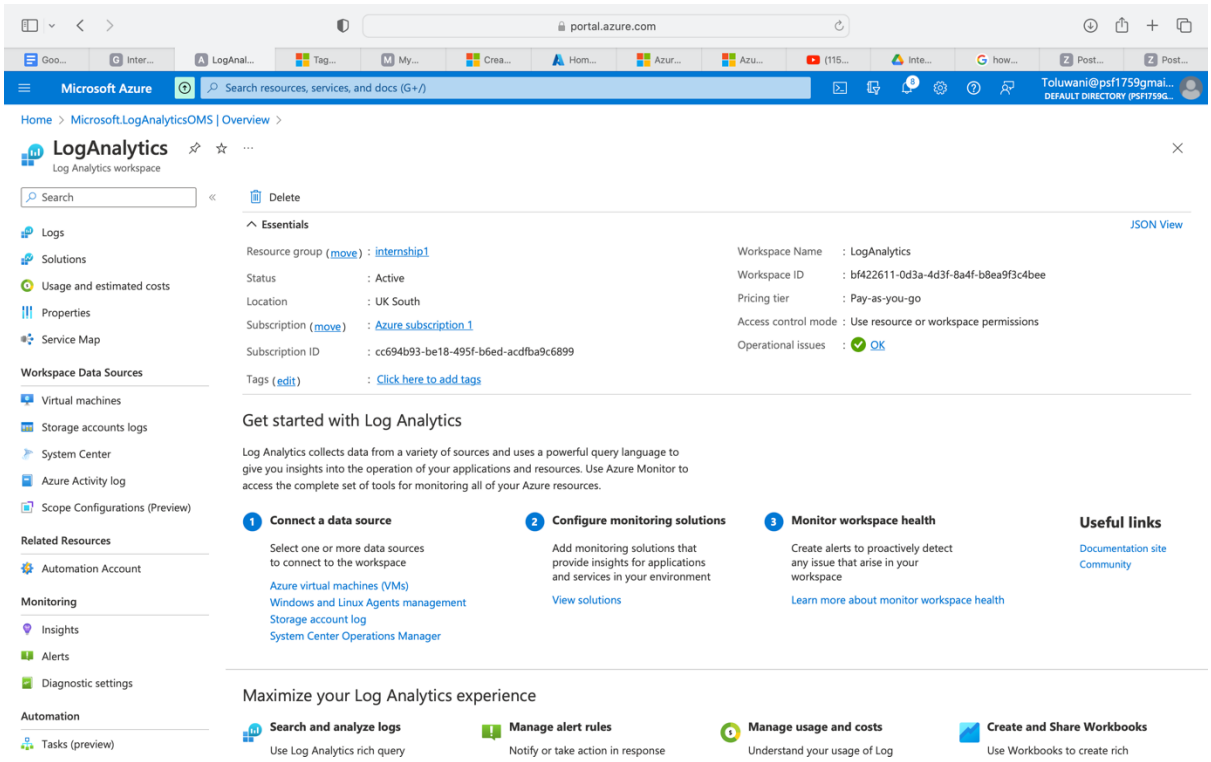
Microsoft Sentinel requires a place to store logs, so we established a Log Analytics Workspace in the same RG and region as the previously established Virtual Machine.

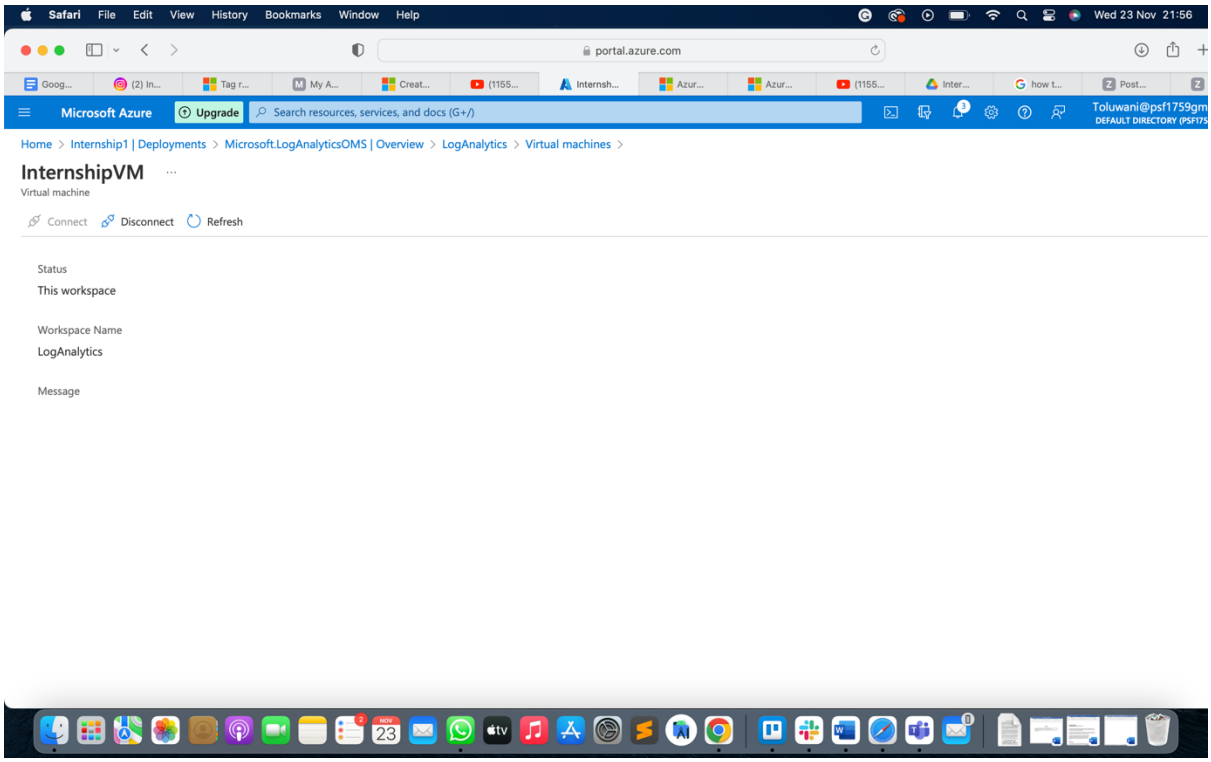


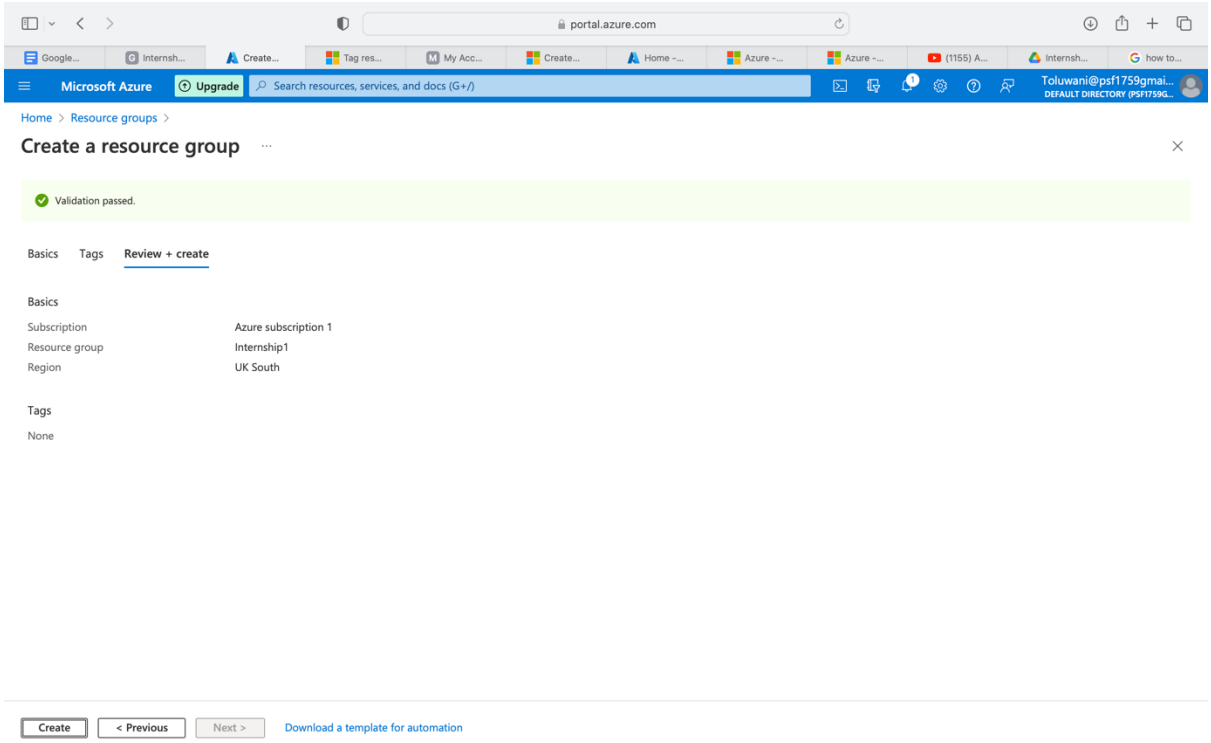
The last step is to link the VM to the Log Analytics Workspace, which we did in two steps using Windows Agent Management and Azure Virtual Machines Connect (to gather Heartbeat Logs) (to collect Windows Event Logs). And as can be seen in the screenshot below, this is located on the overview page of the Log Analytics Workspace.

We choose the VM that required authentication on the Azure Virtual Machines connect page.
The last step is to link the VM to the Log Analytics Workspace, which we did in two steps using Windows Agent Management and Azure Virtual Machines Connect (to gather Heartbeat Logs) (to collect Windows Event Logs). And as can be seen in the screenshot below, this is located on the overview page of the Log Analytics Workspace.

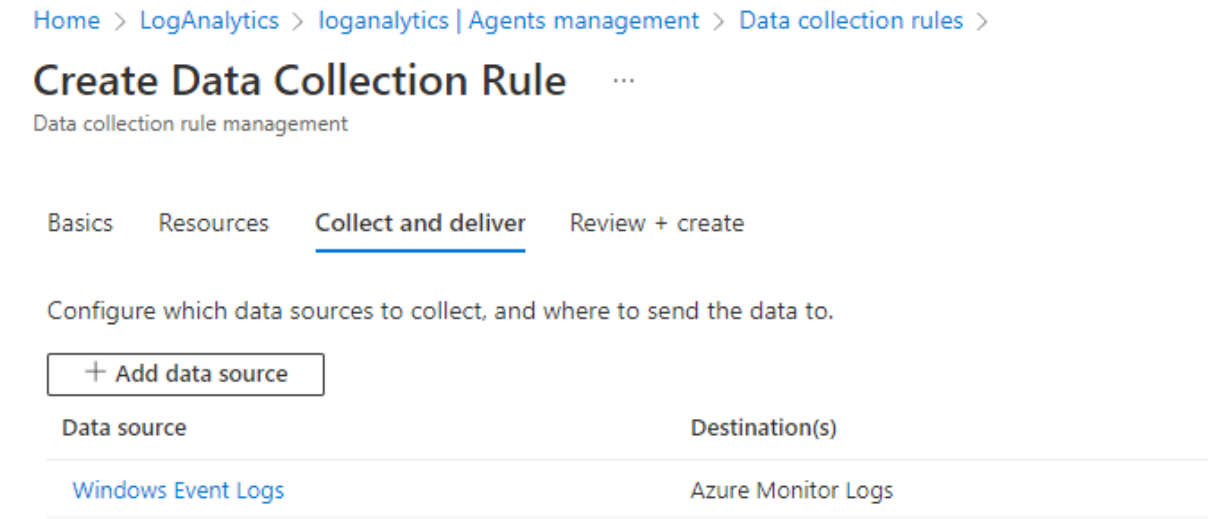
We choose the VM that required authentication on the Azure Virtual Machines connect page.

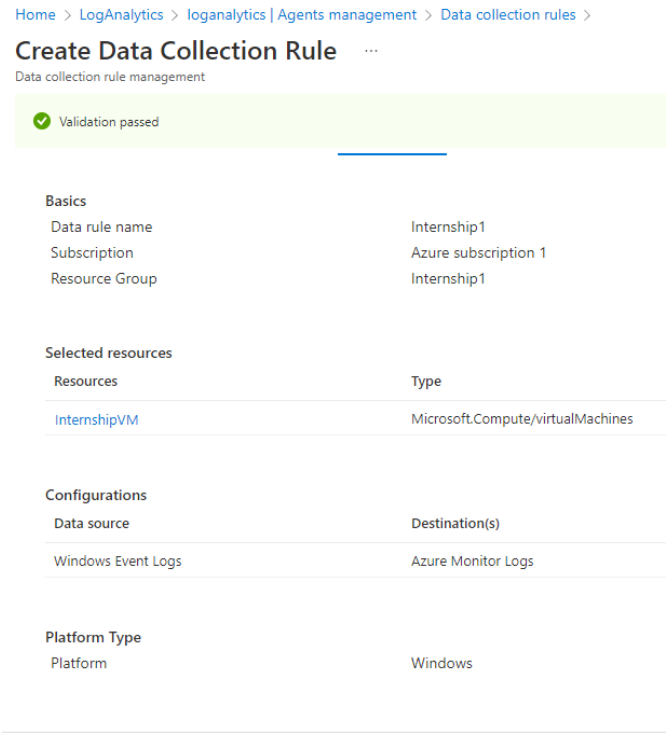

portal.azure.com
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft.LogAnalyticsOMS | Overview >
LogAnalytics
Log Analytics workspace
Search
Logs
Solutions
Usage and estimated costs
Properties
Service Map
Workspace Data Sources
Virtual machines
Storage accounts logs
System Center
Azure Activity log
Scope Configurations (Preview)
Related Resources
Automation Account
Monitoring
Insights
Alerts
Diagnostic settings
Automation
Tasks (preview)
Delete
Essentials
JSON View
Resource group (move) : internship1
Status : Active
Location : UK South
Subscription (move) : Azure subscription 1
Subscription ID : cc694b93-be18-495f-b6ed-acdfba9c6899
Tags (edit) : Click here to add tags
Workspace Name : LogAnalytics
Workspace ID : bf422611-0d3a-4d3f-8a4f-b8ea9f3c4bee
Pricing tier : Pay-as-you-go
Access control mode : Use resource or workspace permissions
Operational issues : OK
Get started with Log Analytics
Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.
1 Connect a data source
Select one or more data sources to connect to the workspace
Azure virtual machines (VMs)
Windows and Linux Agents management
Storage account log
System Center Operations Manager
2 Configure monitoring solutions
Add monitoring solutions that provide insights for applications and services in your environment
View solutions
3 Monitor workspace health
Create alerts to proactively detect any issue that arise in your workspace
Learn more about monitor workspace health
Useful links
Documentation site
Community
Maximize your Log Analytics experience
Search and analyze logs
Use Log Analytics rich query
Manage alert rules
Notify or take action in response
Manage usage and costs
Understand your usage of Log
Create and Share Workbooks
Use Workbooks to create rich


Safari File Edit View History Bookmarks Window Help
Wed 23 Nov 21:56
portal.azure.com
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Home > Internship1 | Deployments > Microsoft.LogAnalyticsOMS | Overview > LogAnalytics > Virtual machines >
InternshipVM
Virtual machine
Connect
Disconnect
Refresh
Status
This workspace
Workspace Name
LogAnalytics
Message

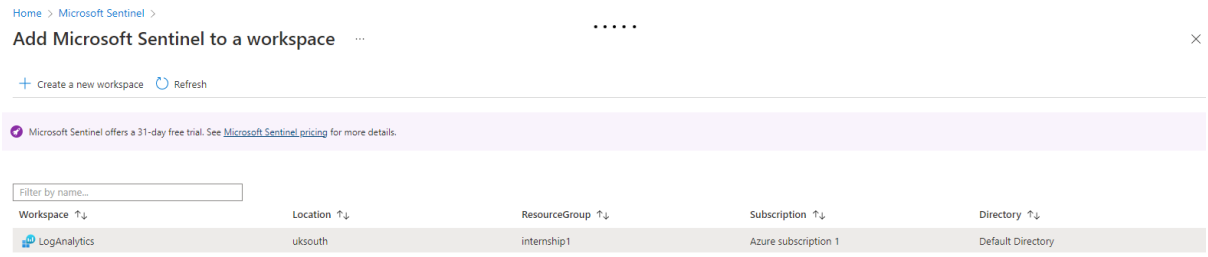


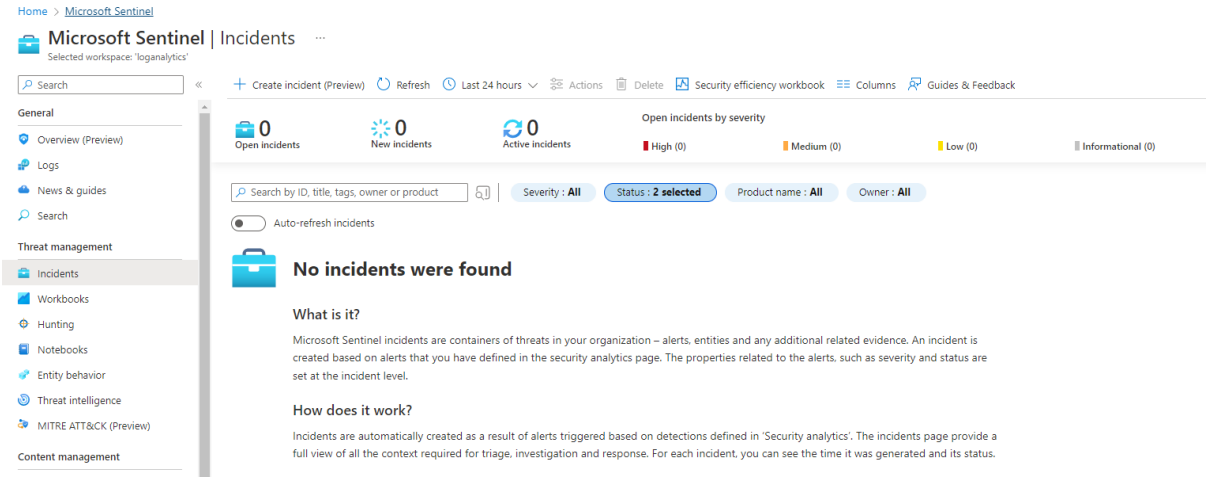
On the Windows Agent management page, we chose Windows Server > Data connection rules > Create and then added Windows Event Logs as the data source.





We next went to Microsoft Sentinel, added the earlier-created Log Analytics Workspace, and watched Logs being collected.





A monitoring technology called Azure Sentinel was employed to efficiently record the operations of cloud-based services. This keeps track of audit logs for significant system modifications crucial to the system's security.

We were able to obtain some recorded activities after constructing a resource group containing virtual machines and successfully coupling them to the log analytics workspace where the logs are actually stored.

In order to track the events and activity that would be created, we logged into the Windows Server VM. After that, we created a straightforward KQL query in Microsoft Sentinel's Logs section to filter the logs to only contain successful Logon attempts.