

## 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.

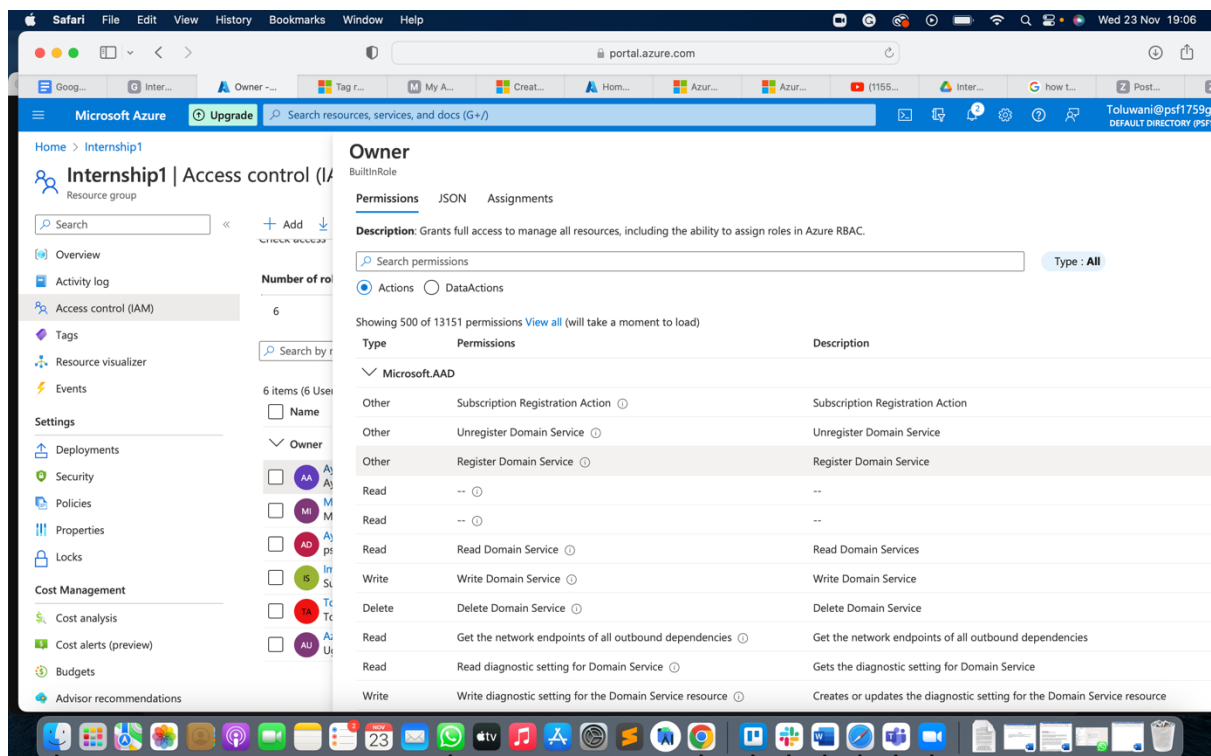
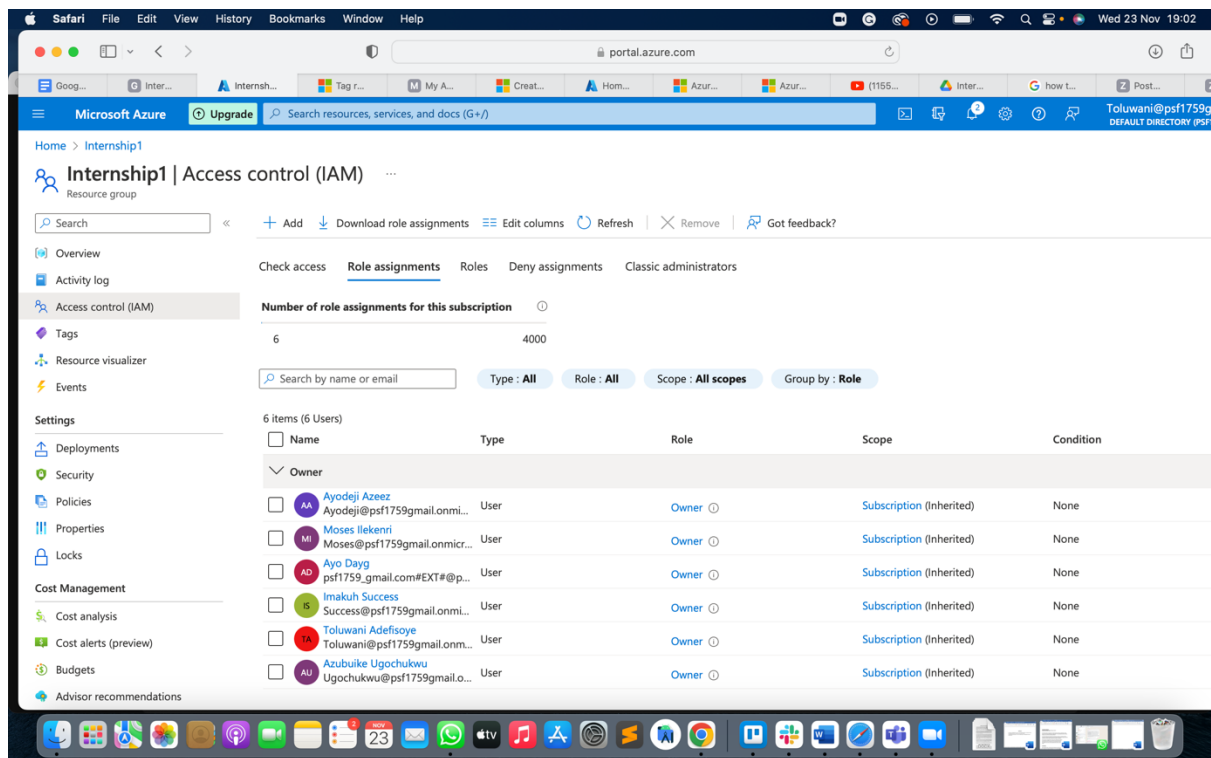
These records contain comprehensive information on the modifications or actions that affected a certain system operation, event, or process. We had to build a virtual machine for this task, give members Log Reader Permission, and keep an eye on the resource's behaviour.

The actions taken to finish this task are listed below;

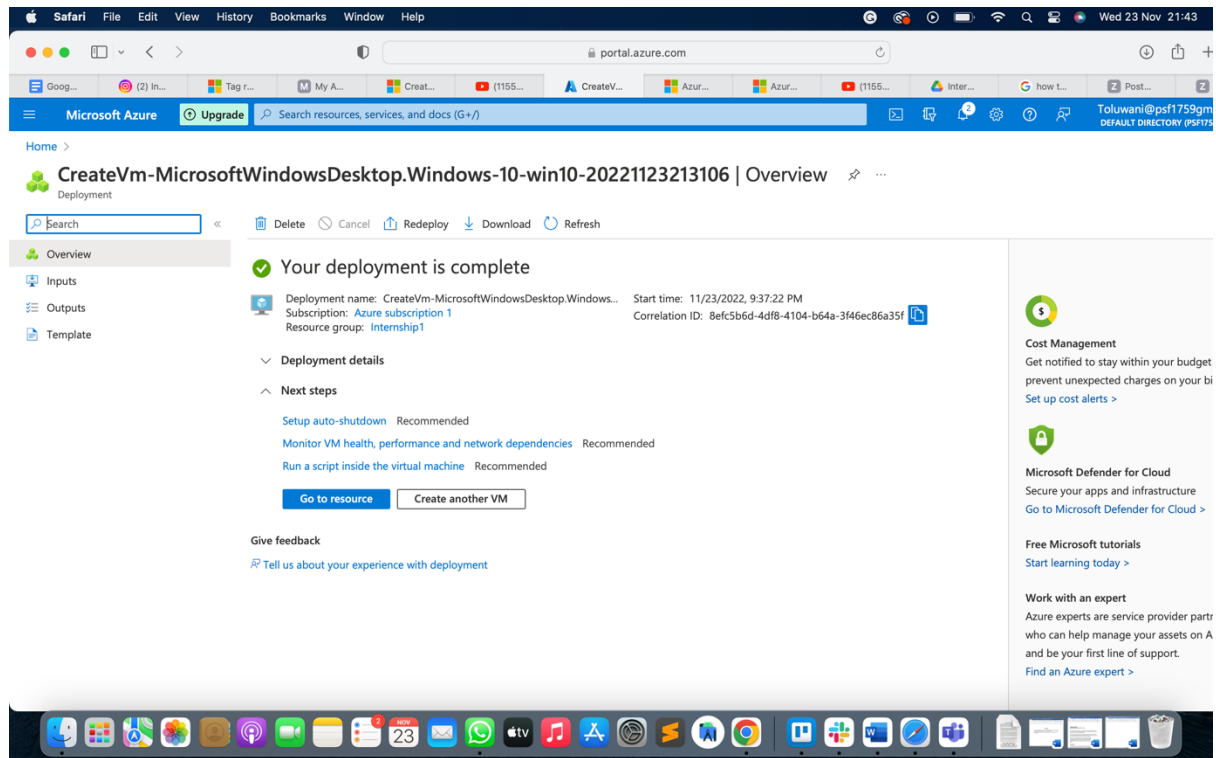
Following the creation of a Resource Group in the same Region, we then deployed a Windows Server Virtual Machine inside of it (UK South). Following that, we gave the resource group's users Log Reader Permissions, as shown in the screenshot below.

The screenshot shows the Microsoft Azure portal interface. The left sidebar displays the 'Resource groups' section with a list of resource groups, including 'Internship1'. The main content area shows the 'Access control (IAM)' page for the 'Internship1' resource group. The page displays the 'Role assignments' tab, showing a list of role assignments for the subscription. The table lists 12 items (12 Users) with columns for Name, Type, Role, Scope, and Condition. The roles assigned are 'Log Analytics Reader' and 'Owner'.

Name	Type	Role	Scope	Condition
<strong>Log Analytics Reader</strong>				
Ayodeji Azeez Ayodeji@psf175...	User	Log Analytics Reader	This resource	None
Moses Ikenri Moses@psf1759...	User	Log Analytics Reader	This resource	None
Ayo Dayg psf1759_gmail.c...	User	Log Analytics Reader	This resource	None
Imakuh Success Success@psf175...	User	Log Analytics Reader	This resource	None
Toluwani Adefisoy Toluwani@psf17...	User	Log Analytics Reader	This resource	None
Azubuikwe Ugochuk Ugochukwu@ps...	User	Log Analytics Reader	This resource	None
<strong>Owner</strong>				
Ayodeji Azeez Ayodeji@psf175...	User	Owner	Subscription (Inherited)	None
Moses Ikenri Moses@psf1759...	User	Owner	Subscription (Inherited)	None



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 > MicrosoftLogAnalyticsOMS | Overview >

## LogAnalytics

Log Analytics workspace

Search

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)

Essentials

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](#)

JSON View

### 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

portal.azure.com

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Internship1 | Deployments > MicrosoftLogAnalyticsOMS | Overview > LogAnalytics > Virtual machines >

## InternshipVM

Virtual machine

[Connect](#) [Disconnect](#) [Refresh](#)

Status

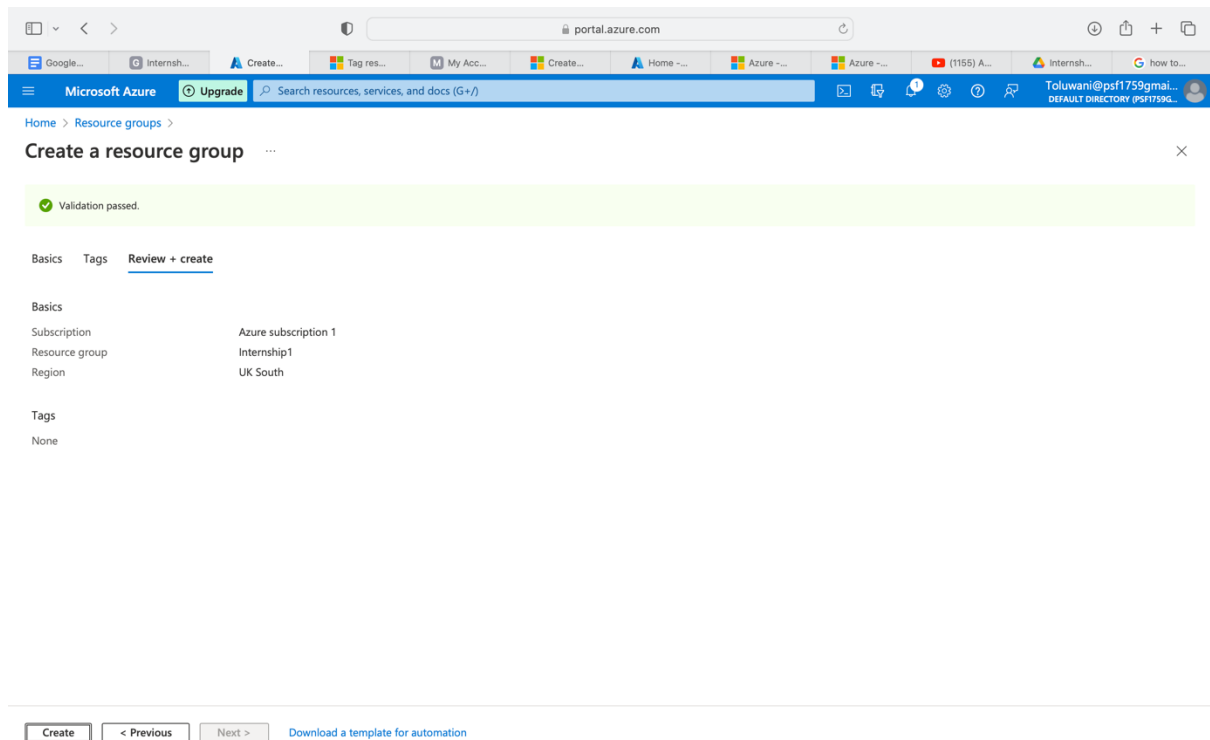
This workspace

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.

[Home](#) > [LogAnalytics](#) > [loganalytics | Agents management](#) > [Data collection rules](#) >

## Create Data Collection Rule ...

Data collection rule management

[Basics](#) [Resources](#) [Collect and deliver](#) [Review + create](#)

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

+ Add data source	
Data source	Destination(s)
<a href="#">Windows Event Logs</a>	Azure Monitor Logs

[Home](#) > [LogAnalytics](#) > [loganalytics | Agents management](#) > [Data collection rules](#) >

## Create Data Collection Rule ...

Data collection rule management

✓ Validation passed

### Basics

Data rule name	Internship1
Subscription	Azure subscription 1
Resource Group	Internship1

### Selected resources

Resources	Type
<a href="#">InternshipVM</a>	Microsoft.Compute/virtualMachines

### Configurations

Data source	Destination(s)
Windows Event Logs	Azure Monitor Logs

### Platform Type

Platform	Windows
----------	---------

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

[Home](#) > [Microsoft Sentinel](#) >

## Add Microsoft Sentinel to a workspace ...

[+ Create a new workspace](#) [Refresh](#)

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...				
Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
LogAnalytics	uksouth	internship1	Azure subscription 1	Default Directory

[Home](#) > [Microsoft Sentinel](#)

## Microsoft Sentinel | Incidents ...

Selected workspace: 'loganalytics'

[+ Create incident \(Preview\)](#) [Refresh](#) [Last 24 hours](#) [Actions](#) [Delete](#) [Security efficiency workbook](#) [Columns](#) [Guides & Feedback](#)

### General

- [Overview \(Preview\)](#)
- [Logs](#)
- [News & guides](#)
- [Search](#)
- Threat management**
  - Incidents**
  - [Workbooks](#)
  - [Hunting](#)
  - [Notebooks](#)
  - [Entity behavior](#)
  - [Threat intelligence](#)
  - [MITRE ATT&CK \(Preview\)](#)
- Content management**

**0** Open incidents **0** New incidents **0** Active incidents **Open incidents by severity** **High (0)** **Medium (0)** **Low (0)** **Informational (0)**

[Severity: All](#) [Status: 2 selected](#) [Product name: All](#) [Owner: All](#)

☐ Auto-refresh incidents



### No incidents were found

#### What is it?

Microsoft Sentinel incidents are containers of threats in your organization – alerts, entities and any additional related evidence. An incident is created based on alerts that you have defined in the security analytics page. The properties related to the alerts, such as severity and status are set at the incident level.

#### How does it work?

Incidents are automatically created as a result of alerts triggered based on detections defined in 'Security analytics'. The incidents page provide a full view of all the context required for triage, investigation and response. For each incident, you can see the time it was generated and its status.

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.

Home > Microsoft Sentinel

Microsoft Sentinel | Incidents ...

Selected workspace: 'loganalytics'

Search

Create incident (Preview) Refresh Last 24 hours Actions Delete Security efficiency workbook Columns Guides & Feedback

General

- Overview (Preview)
- Logs
- News & guides
- Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Content management

0 Open incidents 0 New incidents 0 Active incidents

Open incidents by severity

High (0) Medium (0) Low (0) Informational (0)

Search by ID, title, tags, owner or product

Severity: All Status: 2 selected Product name: All Owner: All

Auto-refresh incidents

**No incidents were found**

**What is it?**

Microsoft Sentinel incidents are containers of threats in your organization – alerts, entities and any additional related evidence. An incident is created based on alerts that you have defined in the security analytics page. The properties related to the alerts, such as severity and status are set at the incident level.

**How does it work?**

Incidents are automatically created as a result of alerts triggered based on detections defined in 'Security analytics'. The incidents page provide a full view of all the context required for triage, investigation and response. For each incident, you can see the time it was generated and its status.

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

All services > Virtual machines > InternshipVM

Virtual machines

Default Directory (psf1759gmail@microsoft.com)

Create Switch to classic

Filter for any field...

Name ↑

- InternshipVM

Updates

- Inventory
- Change tracking
- Automanage
- Configuration management (Preview)
- Policies
- Run command

Monitoring

- Insights
- Alerts
- Metrics
- Diagnostics settings
- Logs
- Connection monitor (classic)
- Workbooks

Automation

- Tasks (preview)
- Export template

InternshipVM | Logs ...

Virtual machine

New Query 1\*

Select scope

Run Time range: Custom Save Share New alert rule

Tables Queries Functions

Search

Filter Group by: Resource t...

Collapse all

**Favorites**

You can add favorites by clicking on the star icon

**Virtual machines**

- Event
  - AzureDeploymentID (string)
  - Computer (string)
  - EventCategory (int)
  - EventData (string)
  - EventID (int)
  - EventLevel (int)
  - EventLevelName (string)
  - EventLog (string)
  - ManagementGroupName (st...

1 Event

2 | where EventID == 4624

3

4

5 // Virtual Machine available memory

6 // Chart the VM's available memory over time.

7 // To create an alert for this query, click '+ New alert rule'

8 Perf

9 | where ObjectName == "Memory" and

10 (CounterName == "Available MBytes Memory" // the name used in Linux records

11 CounterName == "Available MBytes") // the name used in Windows records

**Results** Chart

1.25

1

0.75

0.5

0.25

0

14532.717 PM

TimeGenerated [UTC]

bf422611-0d3a-4d3f-8a4f-b8ea9f3c4bee

0s 711ms Display time (UTC+00:00) Query details 1 records

Chart formatting