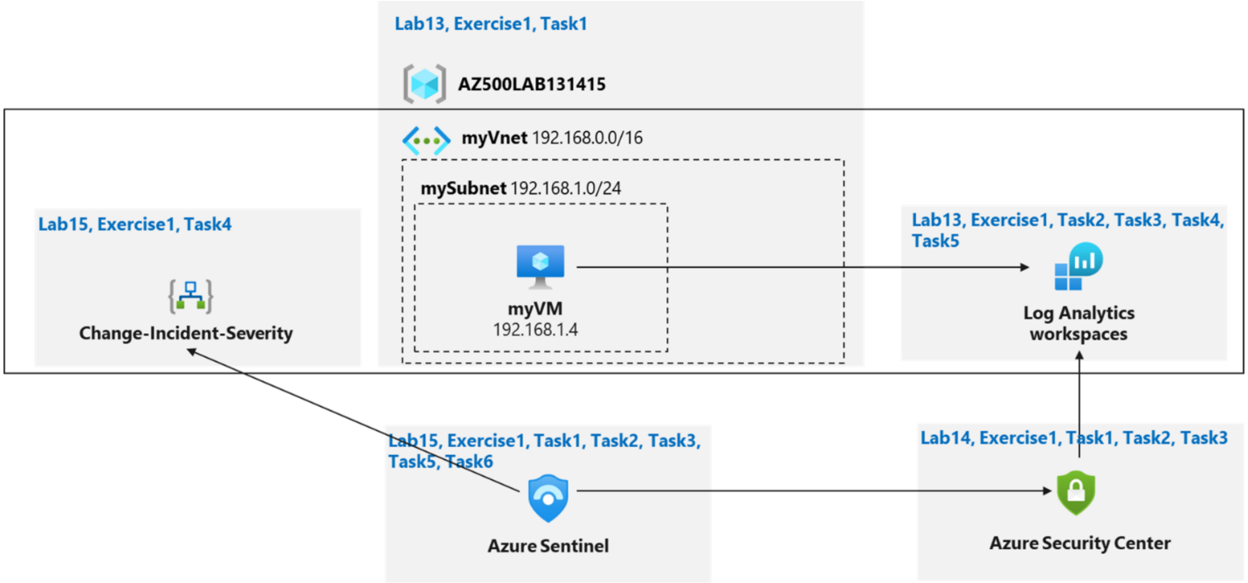
Lab 15: Microsoft Sentinel



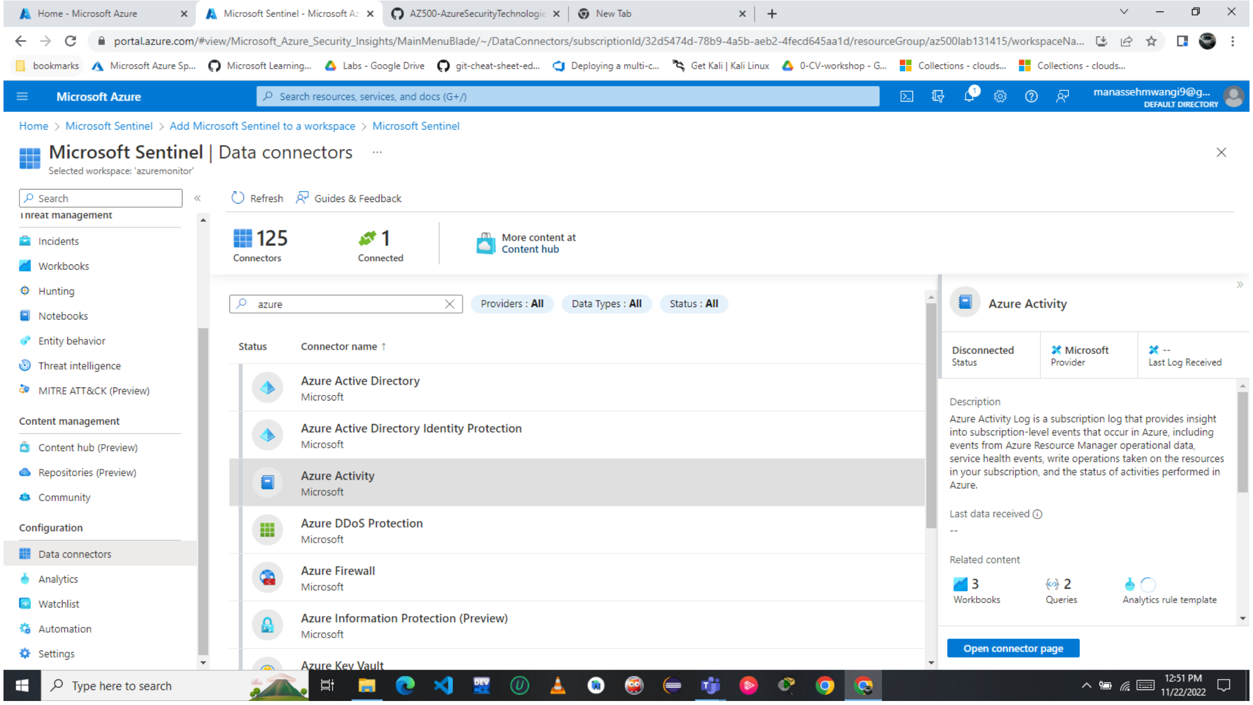
Task 1: On-board Azure Sentinel

If this is your first attempt to action Microsoft Sentinel in the Azure dashboard complete the following step(s): In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Microsoft Sentinel** and press the **Enter** key.
Select **Microsoft Sentinel** from the **Services** view.

On the Add Microsoft Sentinel to a workspace blade, select the Log Analytics workspace you created in the Azure Monitor lab and click Add**.**

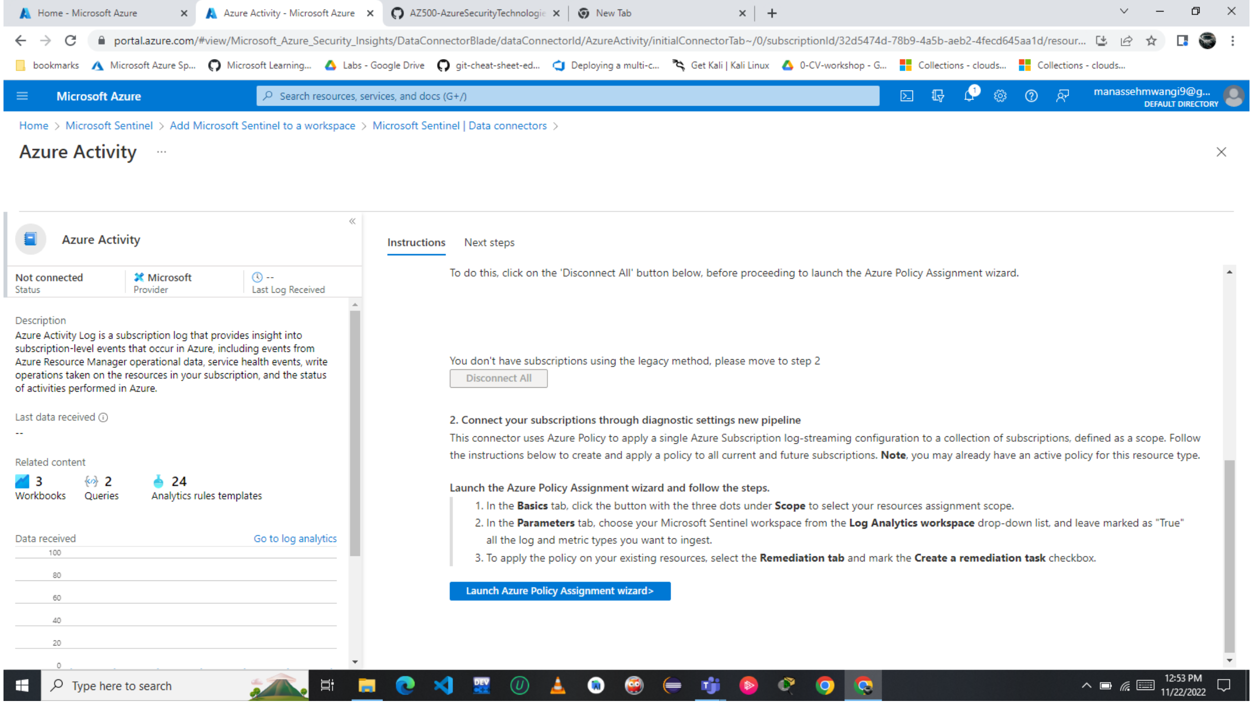
Task 2: Configure Microsoft Sentinel to use the Azure Activity data connector.

select the entry representing the Azure Activity connector then click Open connector page.



Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.

review the "Launch the Azure Policy Assignment wizard and follow the steps" instructions then click Launch the Azure Policy Assignment wizard


portal.azure.com/#view/Microsoft_Azure_Security_Insights/DataConnectorBlade/dataConnectorId/AzureActivity/initialConnectorTab~/0/subscriptionId/32d5474d-78b9-4a5b-aeb2-4fecd645aa1d/resour...
Microsoft Azure
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Data connectors >
Azure Activity
Azure Activity
Not connected
Status
Microsoft
Provider
--
Last Log Received
Description
Last data received
--
Related content
3 Workbooks
2 Queries
24 Analytics rules templates
Data received
Go to log analytics
100
80
60
40
20
0
Instructions
Next steps
Disconnect All
Launch Azure Policy Assignment wizard>
Type here to search
12:53 PM
11/22/2022

Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.

To do this, click on the 'Disconnect All' button below, before proceeding to launch the Azure Policy Assignment wizard.

You don't have subscriptions using the legacy method, please move to step 2

2. Connect your subscriptions through diagnostic settings new pipeline

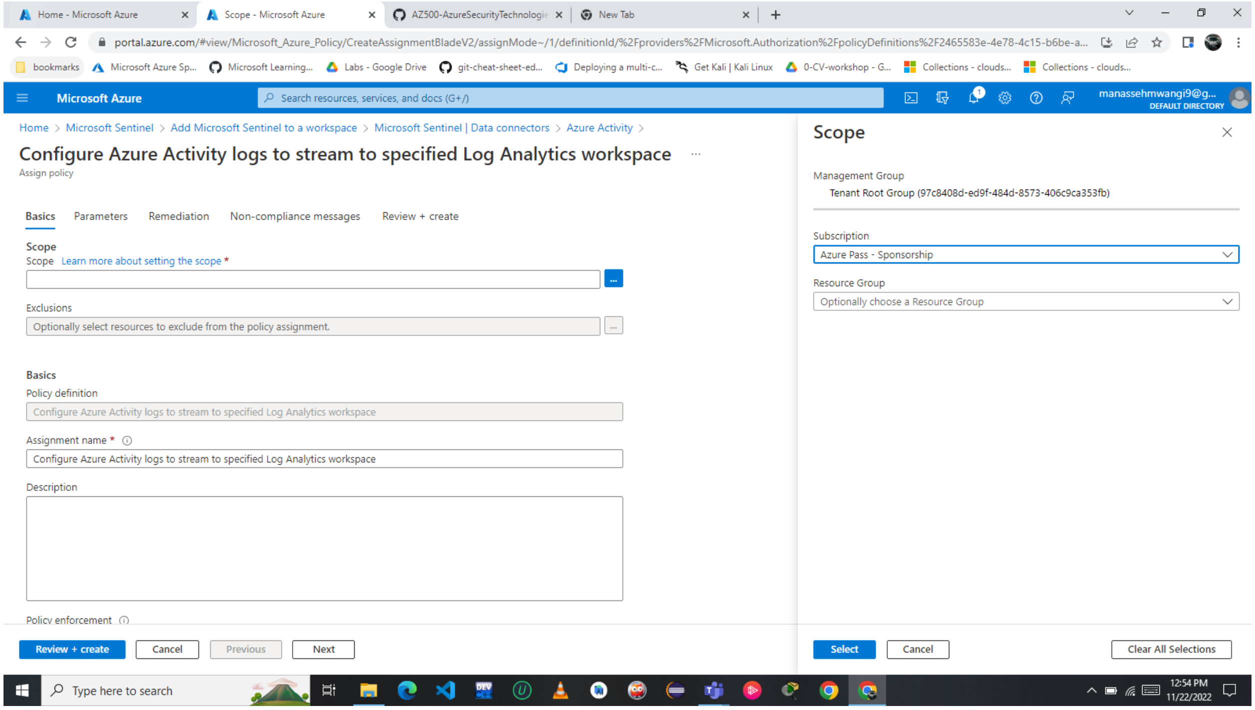
This connector uses Azure Policy to apply a single Azure Subscription log-streaming configuration to a collection of subscriptions, defined as a scope. Follow the instructions below to create and apply a policy to all current and future subscriptions. **Note**, you may already have an active policy for this resource type.

Launch the Azure Policy Assignment wizard and follow the steps.

1. In the **Basics** tab, click the button with the three dots under **Scope** to select your resources assignment scope.
2. In the **Parameters** tab, choose your Microsoft Sentinel workspace from the **Log Analytics workspace** drop-down list, and leave marked as "True" all the log and metric types you want to ingest.
3. To apply the policy on your existing resources, select the **Remediation tab** and mark the **Create a remediation task** checkbox.

On the Configure Azure Activity logs to stream to specified Log Analytics workspace

hoose your Azure Pass subscription from the drop-down



Home - Microsoft Azure
Scope - Microsoft Azure
AZ500-AzureSecurityTechnologie
New Tab
portal.azure.com/#view/Microsoft_Azure_Policy/CreateAssignmentBladeV2/assignMode~/1/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F2465583e-4e78-4c15-b6be-a...
Microsoft Azure
Search resources, services, and docs (G+/)
manassehmwangi9@g...
DEFAULT DIRECTORY

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Data connectors > Azure Activity >

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assign policy

Basics | Parameters | Remediation | Non-compliance messages | Review + create

Scope

Scope Learn more about setting the scope *

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition: Configure Azure Activity logs to stream to specified Log Analytics workspace

Assignment name *: Configure Azure Activity logs to stream to specified Log Analytics workspace

Description

Policy enforcement

Review + create | Cancel | Previous | Next

Scope

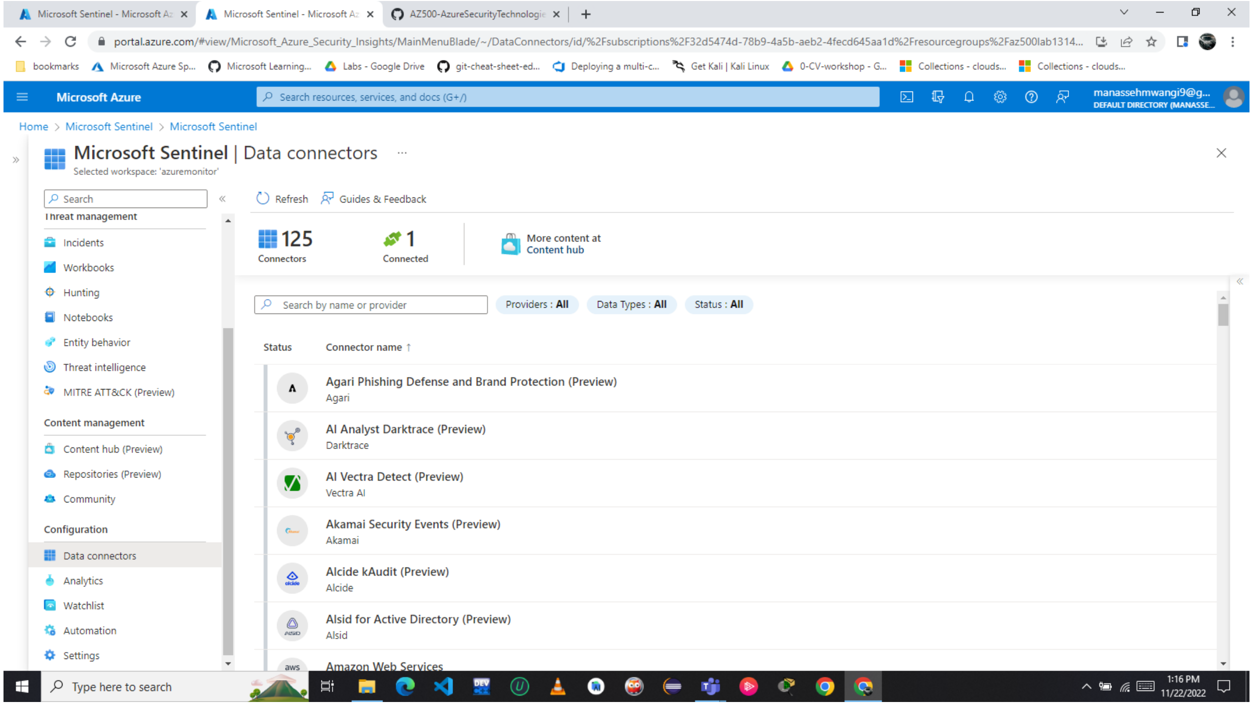
Management Group: Tenant Root Group (97c8408d-ed9f-484d-8573-406c9ca353fb)

Subscription: Azure Pass - Sponsorship

Resource Group: Optionally choose a Resource Group

Select | Cancel | Clear All Selections

the Status shows "Connected"



Microsoft Sentinel - Microsoft Az
Microsoft Sentinel - Microsoft Az
AZ500-AzureSecurityTechnologie
portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/DataConnectors/id/%2Fsubscriptions%2F32d5474d-78b9-4a5b-aeb2-4fecd645aa1d%2Fresourcegroups%2Faz500lab1314...
Microsoft Azure
Search resources, services, and docs (G+/)
manassehmwangi9@g...
DEFAULT DIRECTORY (MANASSE...

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Data connectors

Selected workspace: 'azuremonitor'

Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
Refresh
Guides & Feedback

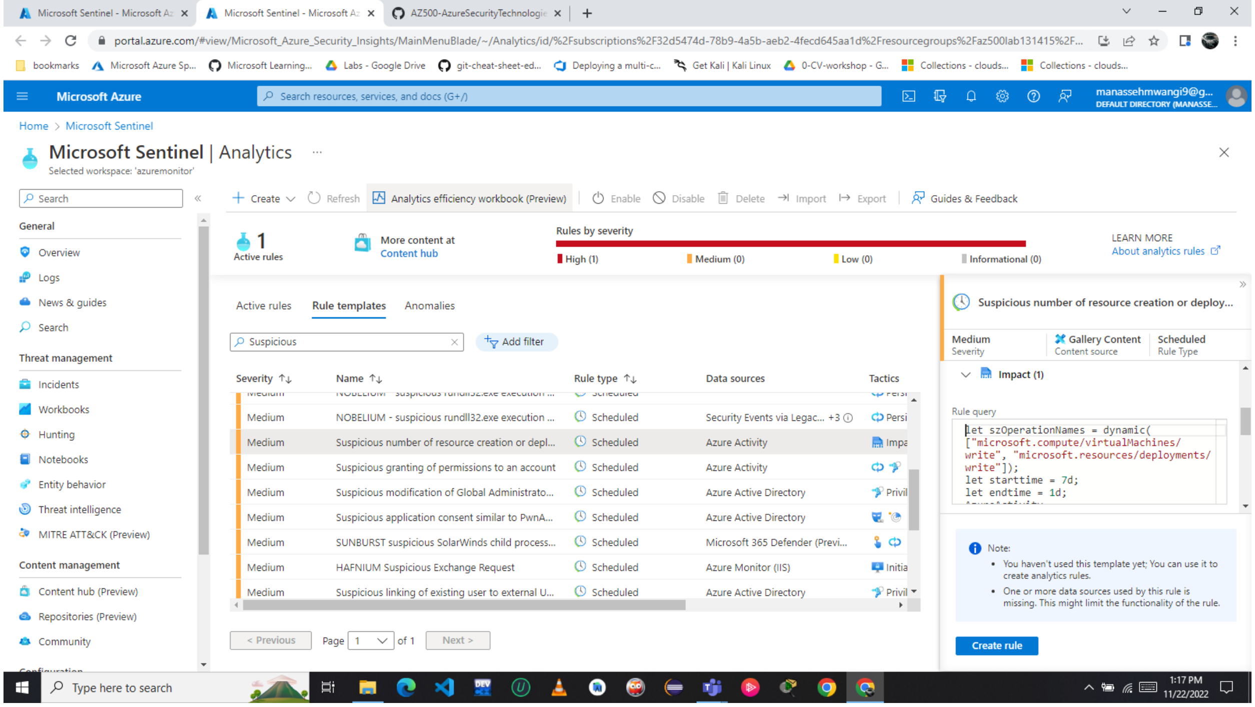
125 Connectors | 1 Connected | More content at Content hub

Search by name or provider | Providers : All | Data Types : All | Status : All

Status	Connector name ↑
	Agari Phishing Defense and Brand Protection (Preview) Agari
	AI Analyst Darktrace (Preview) Darktrace
	AI Vectra Detect (Preview) Vectra AI
	Akamai Security Events (Preview) Akamai
	Alcide kAudit (Preview) Alcide
	Alsid for Active Directory (Preview) Alsid
	Amazon Web Services

Task 3: Create a rule that uses the Azure Activity data connector.

On the Microsoft Sentinel | Configuration blade, click Analytics**.**



Microsoft Sentinel | Analytics

Selected workspace: 'azuremonitor'

1 Active rules

Rules by severity: High (1) Medium (0) Low (0) Informational (0)

Rule templates — search: Suspicious

Severity	Name	Rule type	Data sources	Tactics
Medium	NOBELIUM - suspicious rundll32.exe execution ...	Scheduled	Security Events via Legac... +3	Persi
Medium	Suspicious number of resource creation or depl...	Scheduled	Azure Activity	Impa
Medium	Suspicious granting of permissions to an account	Scheduled	Azure Activity	
Medium	Suspicious modification of Global Administrato...	Scheduled	Azure Active Directory	Privil
Medium	Suspicious application consent similar to PwnA...	Scheduled	Azure Active Directory	
Medium	SUNBURST suspicious SolarWinds child process...	Scheduled	Microsoft 365 Defender (Previ...	
Medium	HAFNIUM Suspicious Exchange Request	Scheduled	Azure Monitor (IIS)	Initia
Medium	Suspicious linking of existing user to external U...	Scheduled	Azure Active Directory	Privil

Suspicious number of resource creation or deploy...

Medium Severity · Gallery Content Content source · Scheduled Rule Type

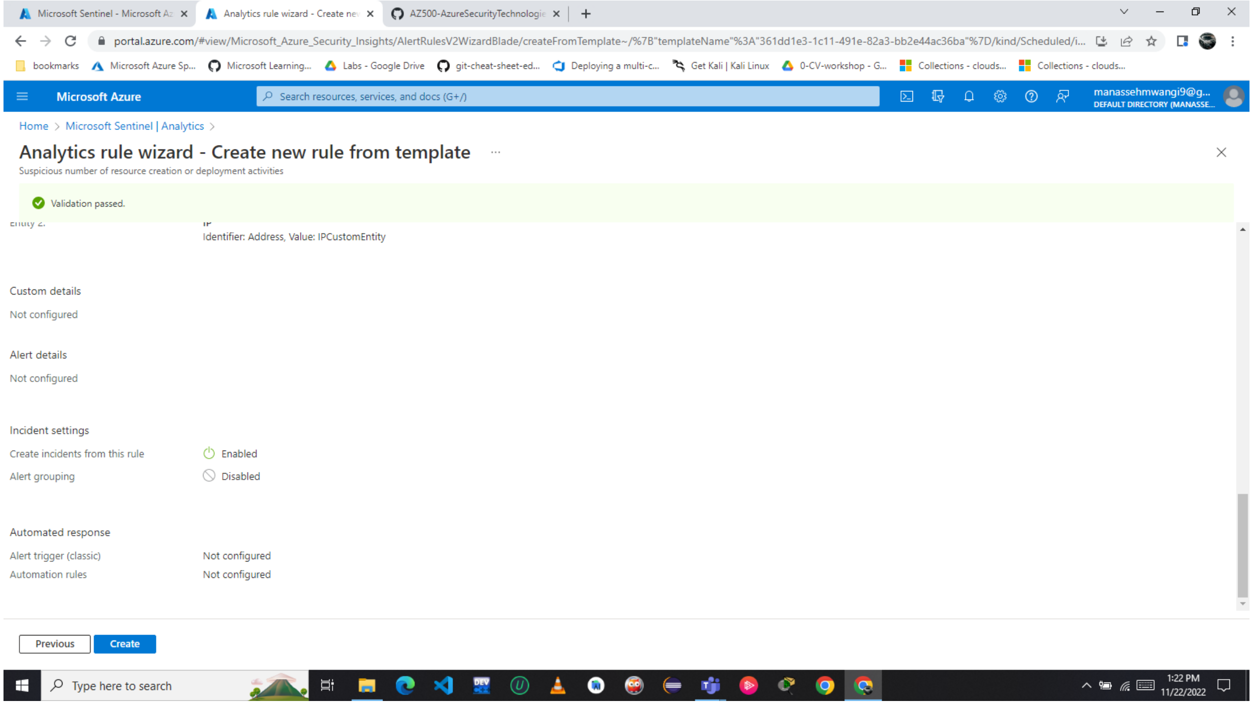
Impact (1)

Rule query

```
let szOperationNames = dynamic(
["microsoft.compute/virtualMachines/
write", "microsoft.resources/deployments/
write"]);
let starttime = 7d;
let endtime = 1d;
```

Note:
- You haven't used this template yet; You can use it to create analytics rules.
- One or more data sources used by this rule is missing. This might limit the functionality of the rule.

On the General tab of the Analytic rule wizard - Create new rule from template blade



Analytics rule wizard - Create new rule from template

Suspicious number of resource creation or deployment activities

Validation passed.

Identifier: Address, Value: IPCustomEntity

Custom details

Not configured

Alert details

Not configured

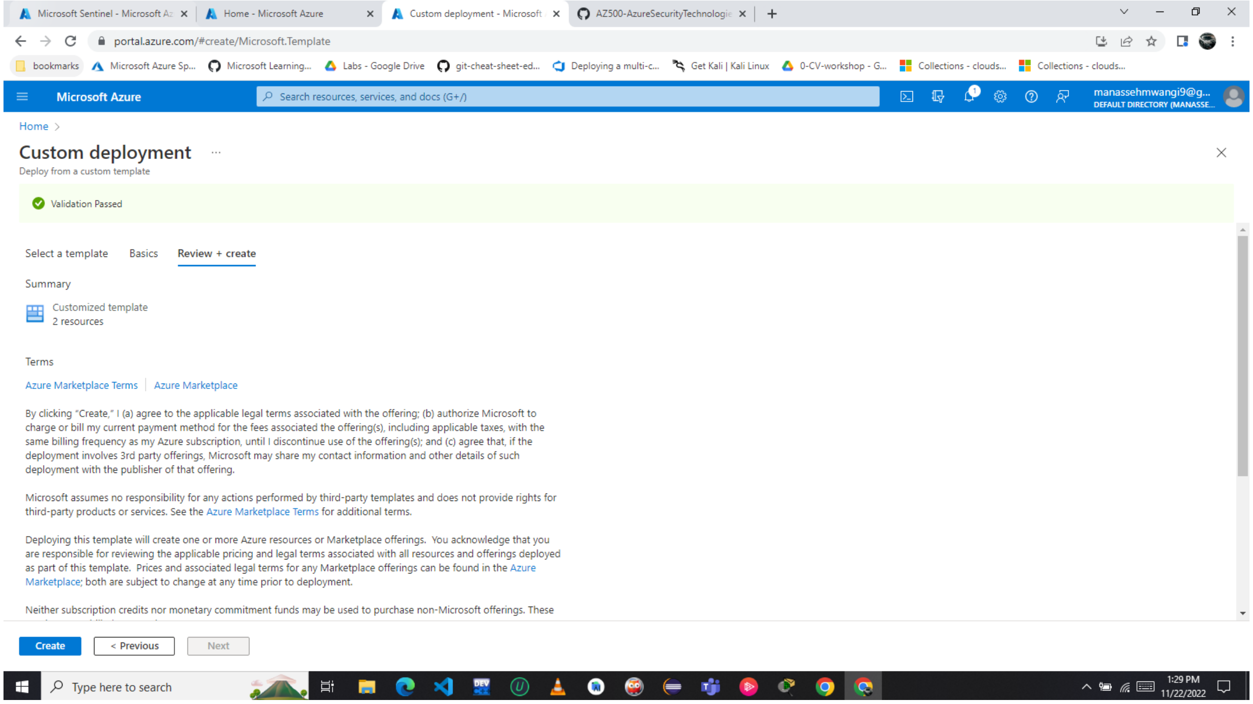
Incident settings

Create incidents from this rule	Enabled
Alert grouping	Disabled

Automated response

Alert trigger (classic)	Not configured
Automation rules	Not configured

You now have an active rule.



Custom deployment

Deploy from a custom template

✓ Validation Passed

Summary

Customized template
2 resources

Terms

Azure Marketplace Terms | Azure Marketplace

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

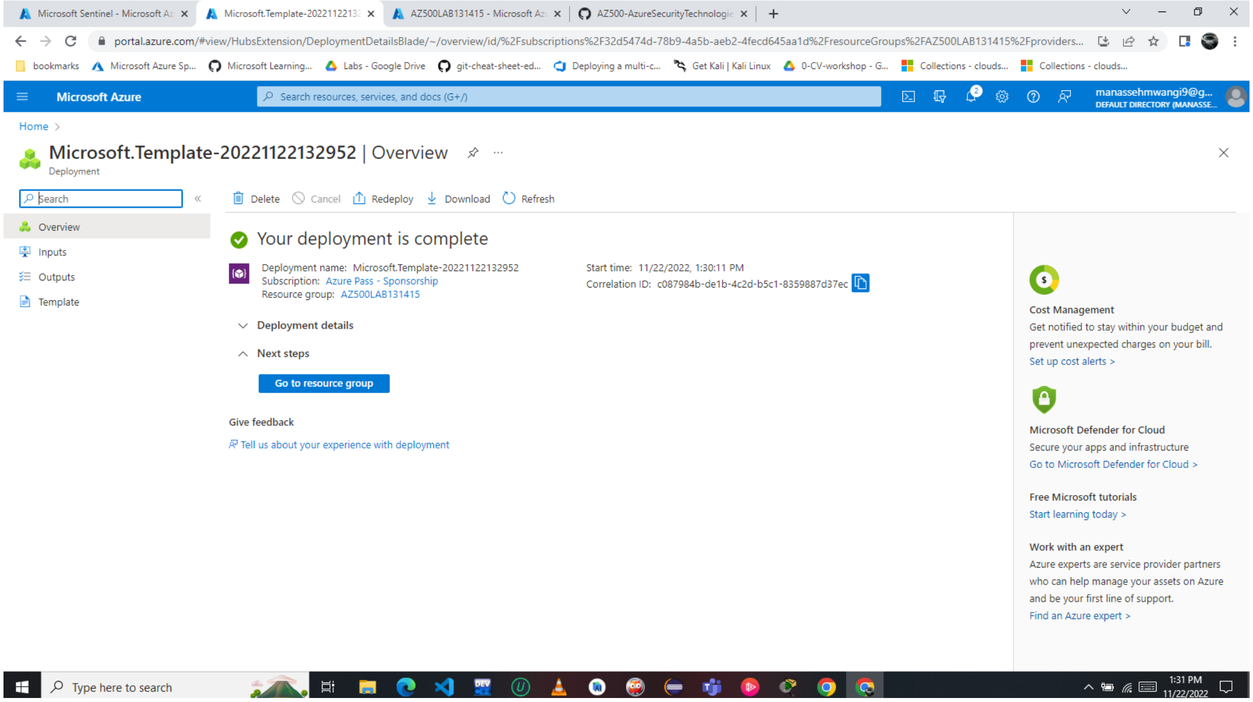
Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the Azure Marketplace Terms for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the Azure Marketplace; both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These

Task 4: Create a playbook

On the Custom deployment blade, Build your own template in the editor option. click Load file, locate \Allfiles\Labs\15\changeincidentseverity.json file



Microsoft Sentinel - Microsoft Az
Microsoft.Template-2022112213
AZ500LAB131415 - Microsoft Az
AZ500-AzureSecurityTechnologie
portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscriptions%2F32d5474d-78b9-4a5b-aeb2-4fecd645aa1d%2FresourceGroups%2FAZ500LAB131415%2Fproviders...
bookmarks
Microsoft Azure Sp...
Microsoft Learning...
Labs - Google Drive
git-cheat-sheet-ed...
Deploying a multi-c...
Get Kali | Kali Linux
0-CV-workshop - G...
Collections - clouds...
Collections - clouds...
Microsoft Azure
Search resources, services, and docs (G+/)
manassehmwangi9@g...
DEFAULT DIRECTORY (MANASSE...
Home >

Microsoft.Template-20221122132952 | Overview

Deployment

Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh

✓ Your deployment is complete

Deployment name: Microsoft.Template-20221122132952
Subscription: Azure Pass - Sponsorship
Resource group: AZ500LAB131415

Start time: 11/22/2022, 1:30:11 PM
Correlation ID: c087984b-de1b-4c2d-b5c1-8359887d37ec

Deployment details
Next steps
Go to resource group

Give feedback

Tell us about your experience with deployment

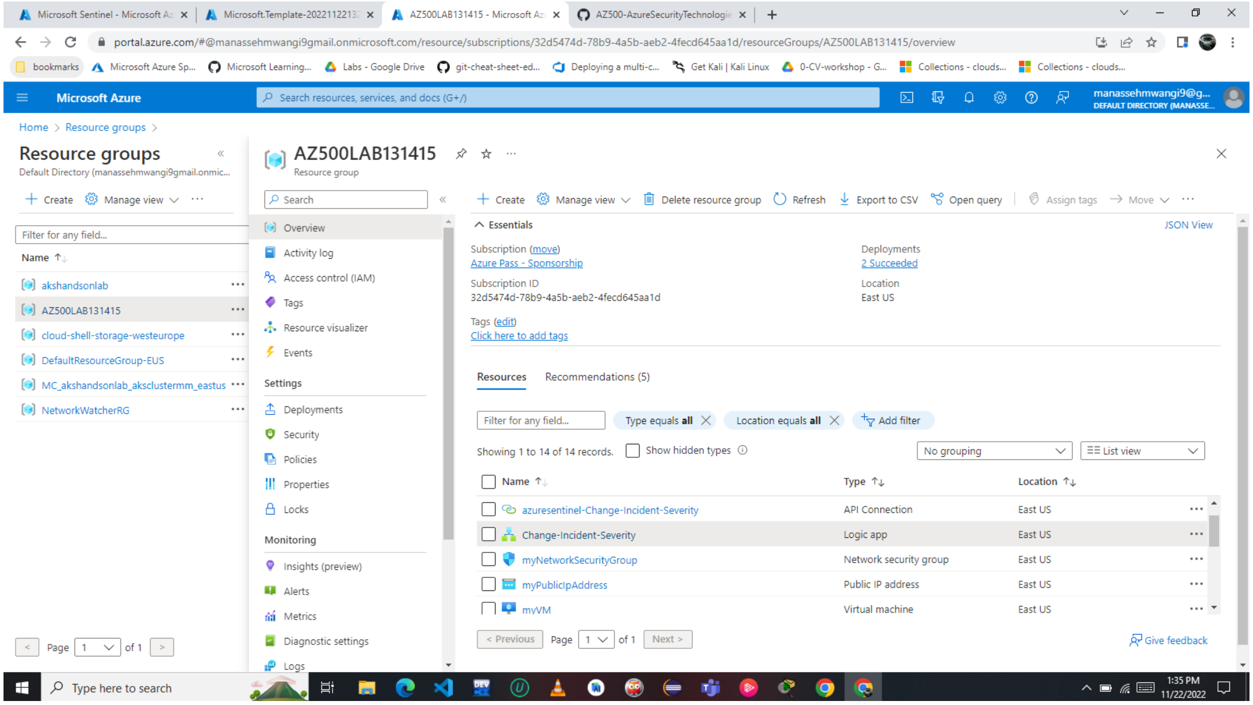
Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >

On the AZ500LAB131415 resource group blade, in the list of resources, click the entry representing the newly created Change-Incident-Severity logic app.



Subscription (move)
Azure Pass - Sponsorship

Subscription ID
32d5474d-78b9-4a5b-aeb2-4fecd645aa1d

Tags (edit)
Click here to add tags

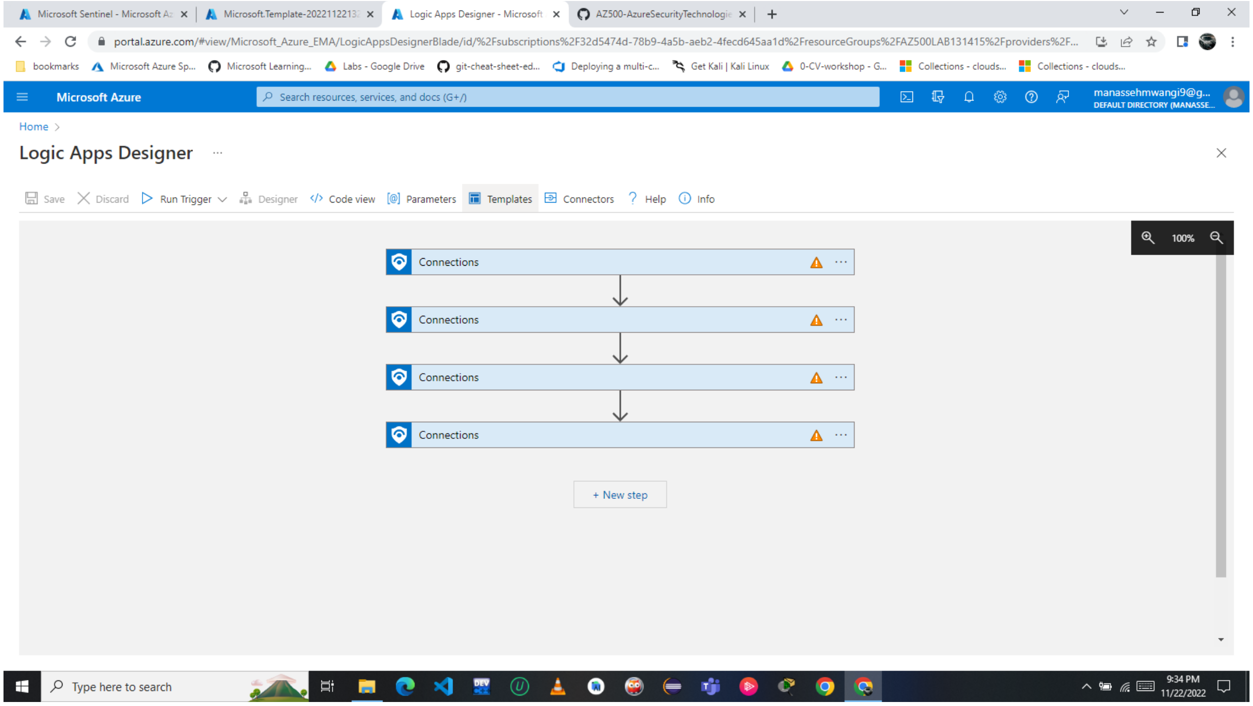
Deployments
2 Succeeded

Location
East US

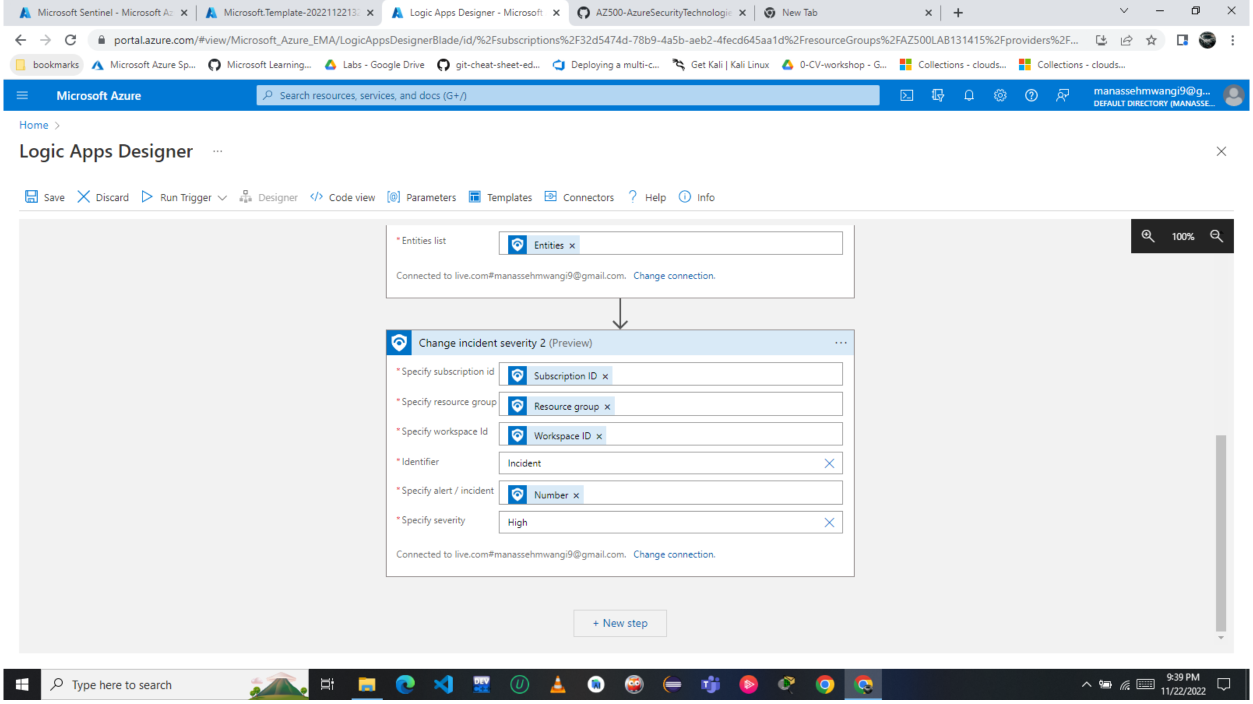
Showing 1 to 14 of 14 records.

Name	Type	Location
azuresentinel-Change-Incident-Severity	API Connection	East US
Change-Incident-Severity	Logic app	East US
myNetworkSecurityGroup	Network security group	East US
myPublicIpAddress	Public IP address	East US
myVM	Virtual machine	East US

On the Logic Apps Designer blade, each of the four connections displays a warning.


Microsoft Sentinel - Microsoft Az
Microsoft.Template-2022112213
Logic Apps Designer - Microsoft
AZ500-AzureSecurityTechnologie
portal.azure.com/#view/Microsoft_Azure_EMA/LogicAppsDesignerBlade/id/%2Fsubscriptions%2F32d5474d-78b9-4a5b-aeb2-4fecd645aa1d%2FresourceGroups%2FAZ500LAB131415%2Fproviders%2F...
Microsoft Azure
Search resources, services, and docs (G+/)
manassehmwangi9@g...
DEFAULT DIRECTORY (MANASSE...
Home >
Logic Apps Designer
Save
Discard
Run Trigger
Designer
Code view
Parameters
Templates
Connectors
Help
Info
100%
Connections
Connections
Connections
Connections
+ New step
Type here to search
9:34 PM
11/22/2022

Ensure that the entry in the Tenant drop down list contains your Azure AD tenant name and click Sign-in. Ensure there are no warnings displayed on any of the steps.



Logic Apps Designer

* Entities list: Entities

Connected to live.com#manassehmwangi9@gmail.com. Change connection.

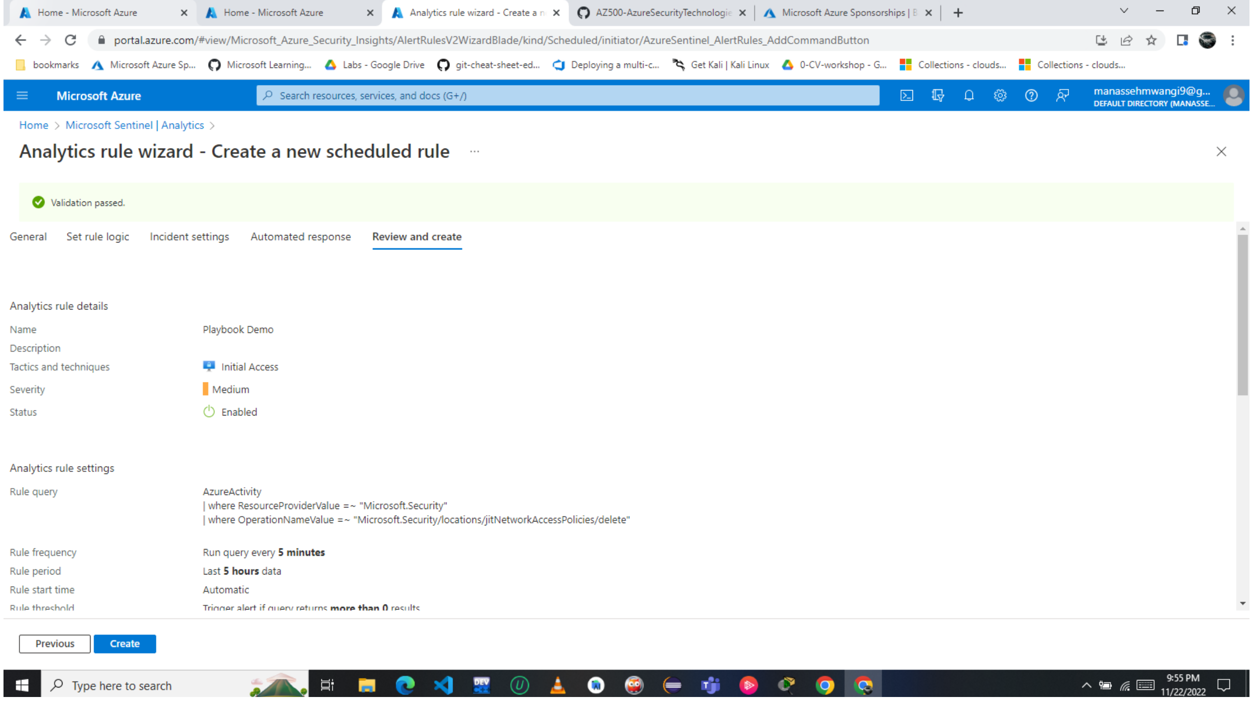
Change incident severity 2 (Preview)

- * Specify subscription id: Subscription ID
- * Specify resource group: Resource group
- * Specify workspace Id: Workspace ID
- * Identifier: Incident
- * Specify alert / incident: Number
- * Specify severity: High

Connected to live.com#manassehmwangi9@gmail.com. Change connection.

Task 5: Create a custom alert and configure a playbook as an automated response

specify the following settings



Analytics rule wizard - Create a new scheduled rule

Validation passed.

Analytics rule details

Name	Playbook Demo
Description	
Tactics and techniques	Initial Access
Severity	Medium
Status	Enabled

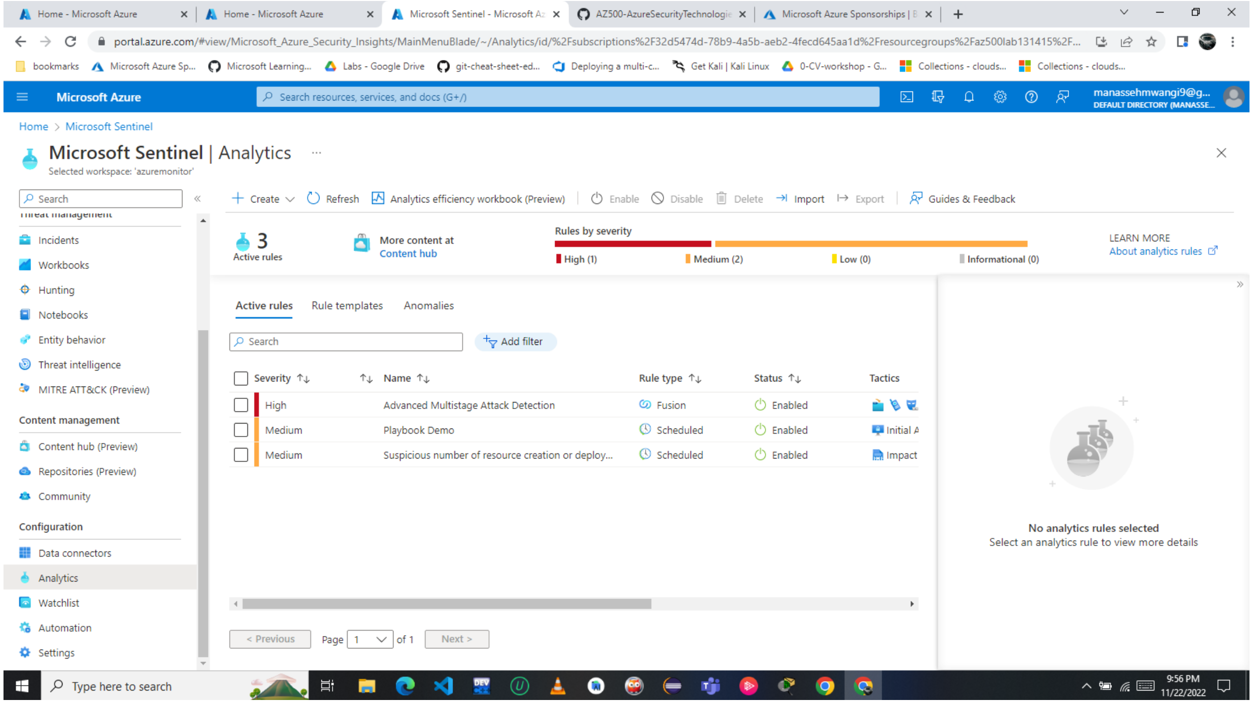
Analytics rule settings

Rule query

```
AzureActivity
| where ResourceProviderValue =~ "Microsoft.Security"
| where OperationNameValue =~ "Microsoft.Security/locations/jitNetworkAccessPolicies/delete"
```

Rule frequency	Run query every **5 minutes**
Rule period	Last **5 hours** data
Rule start time	Automatic
Rule threshold	Trigger alert if query returns **more than 0** results

You now have a new active rule called **Playbook Demo**.



Home > Microsoft Sentinel

Microsoft Sentinel | Analytics

Selected workspace: 'azuremonitor'

3 Active rules

More content at Content hub

Rules by severity: High (1) Medium (2) Low (0) Informational (0)

LEARN MORE About analytics rules

Active rules | Rule templates | Anomalies

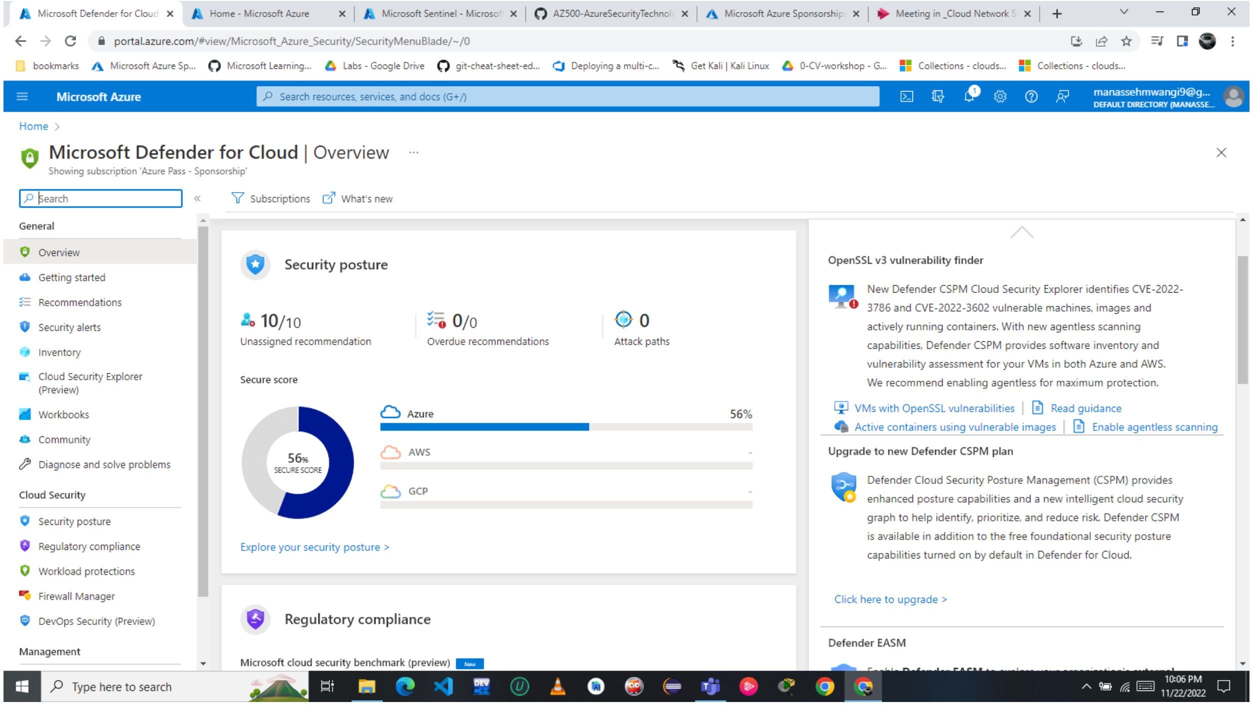
Severity	Name	Rule type	Status	Tactics
High	Advanced Multistage Attack Detection	Fusion	Enabled	
Medium	Playbook Demo	Scheduled	Enabled	Initial A
Medium	Suspicious number of resource creation or deploy...	Scheduled	Enabled	Impact

No analytics rules selected

Select an analytics rule to view more details

Task 6: Invoke an incident and review the associated actions.

Check your secure score. By now it should have updated.



Home >

Microsoft Defender for Cloud | Overview

Showing subscription 'Azure Pass - Sponsorship'

Security posture

10/10 Unassigned recommendation

0/0 Overdue recommendations

0 Attack paths

Secure score

56% SECURE SCORE

Azure 56%

AWS -

GCP -

Explore your security posture >

Regulatory compliance

Microsoft cloud security benchmark (preview)

OpenSSL v3 vulnerability finder

New Defender CSPM Cloud Security Explorer identifies CVE-2022-3786 and CVE-2022-3602 vulnerable machines, images and actively running containers. With new agentless scanning capabilities, Defender CSPM provides software inventory and vulnerability assessment for your VMs in both Azure and AWS. We recommend enabling agentless for maximum protection.

VMs with OpenSSL vulnerabilities | Read guidance

Active containers using vulnerable images | Enable agentless scanning

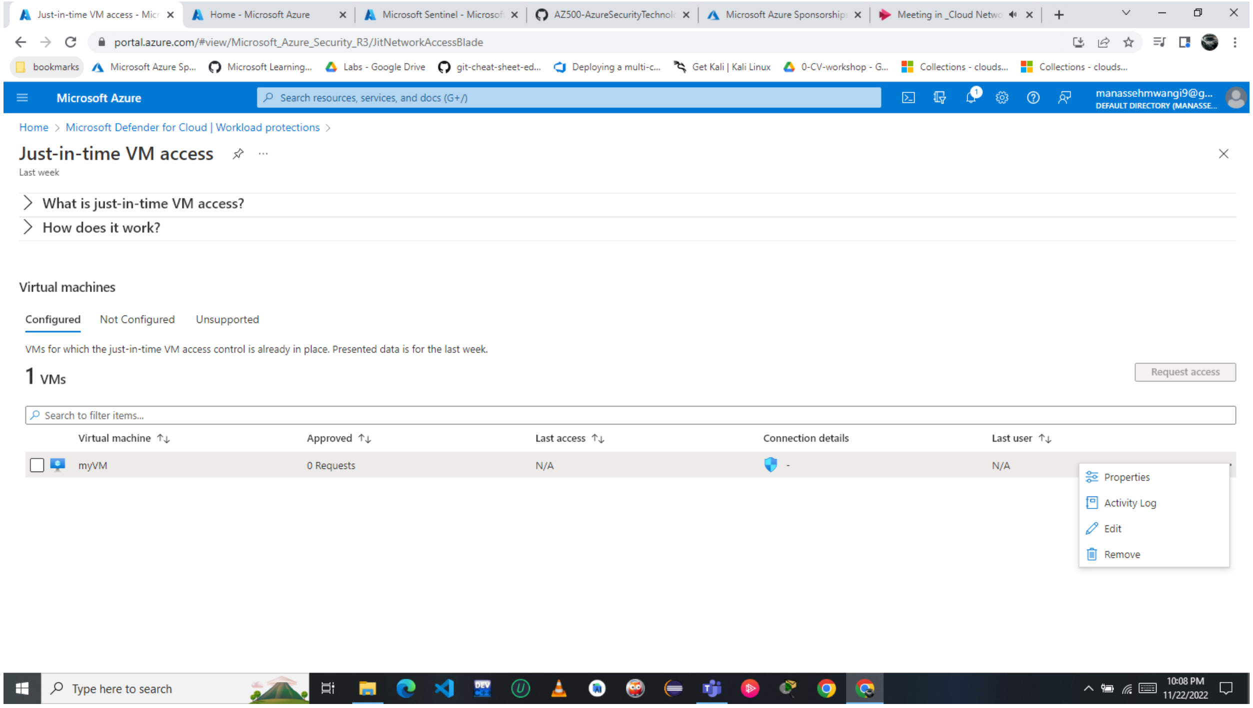
Upgrade to new Defender CSPM plan

Defender Cloud Security Posture Management (CSPM) provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize, and reduce risk. Defender CSPM is available in addition to the free foundational security posture capabilities turned on by default in Defender for Cloud.

Click here to upgrade >

Defender EASM

Navigate to the Activity log blade, note and Delete JIT Network Access Policies entry.



portal.azure.com/#view/Microsoft_Azure_Security_R3/JitNetworkAccessBlade

Home > Microsoft Defender for Cloud | Workload protections >

Just-in-time VM access

Last week

> What is just-in-time VM access?

> How does it work?

Virtual machines

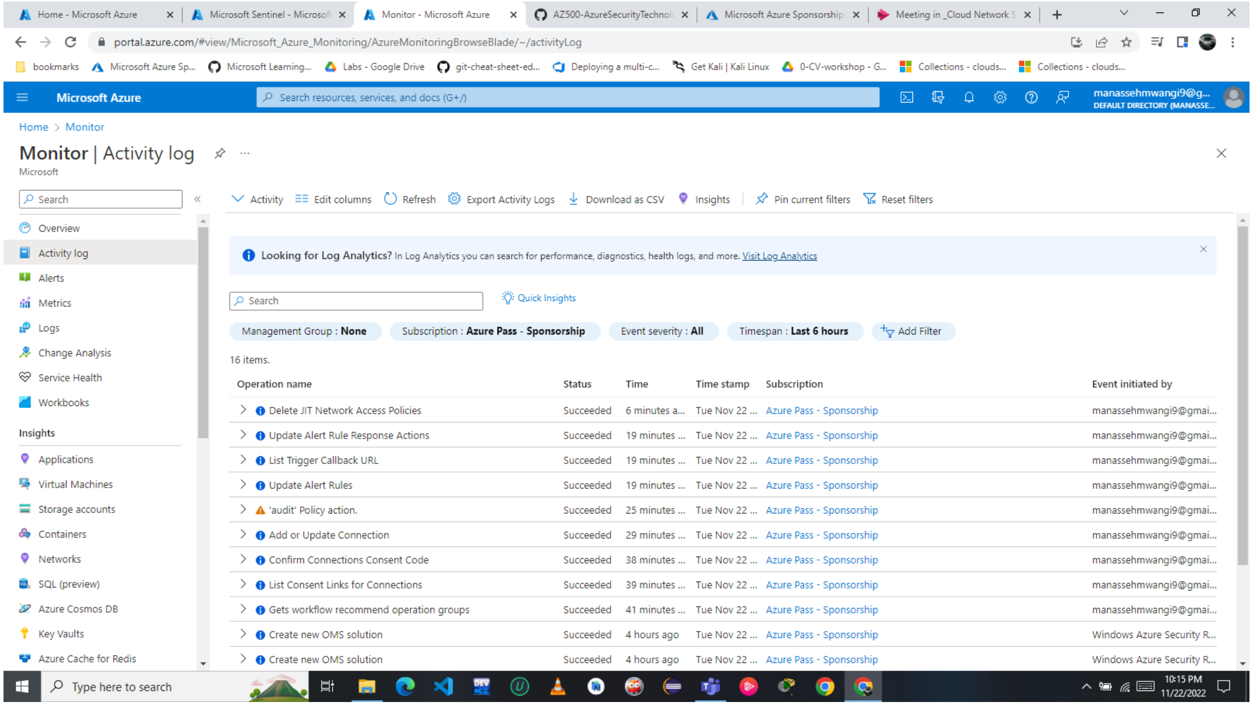
Configured | Not Configured | Unsupported

VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.

1 VMs

Virtual machine	Approved	Last access	Connection details	Last user
myVM	0 Requests	N/A	-	N/A

Navigate to the Activity log blade, note an Delete JIT Network Access Policies entry



portal.azure.com/#view/Microsoft_Azure_Monitoring/AzureMonitoringBrowseBlade/~/activityLog

Home > Monitor

Monitor | Activity log

Microsoft

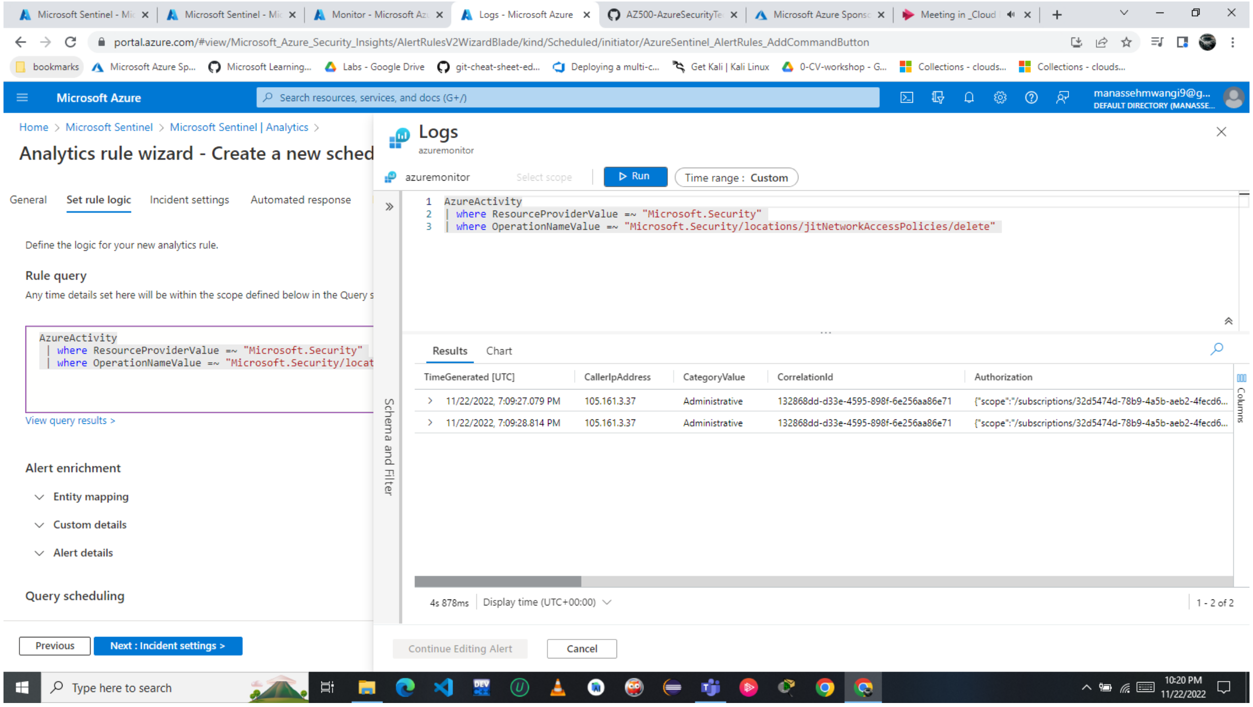
Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. Visit Log Analytics

Management Group : None | Subscription : Azure Pass - Sponsorship | Event severity : All | Timespan : Last 6 hours

16 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Delete JIT Network Access Policies	Succeeded	6 minutes a...	Tue Nov 22 ...	Azure Pass - Sponsorship	manassehmwangi9@gmai...
Update Alert Rule Response Actions	Succeeded	19 minutes ...	Tue Nov 22 ...	Azure Pass - Sponsorship	manassehmwangi9@gmai...
List Trigger Callback URL	Succeeded	19 minutes ...	Tue Nov 22 ...	Azure Pass - Sponsorship	manassehmwangi9@gmai...
Update Alert Rules	Succeeded	19 minutes ...	Tue Nov 22 ...	Azure Pass - Sponsorship	manassehmwangi9@gmai...
'audit' Policy action.	Succeeded	25 minutes ...	Tue Nov 22 ...	Azure Pass - Sponsorship	manassehmwangi9@gmai...
Add or Update Connection	Succeeded	29 minutes ...	Tue Nov 22 ...	Azure Pass - Sponsorship	manassehmwangi9@gmai...
Confirm Connections Consent Code	Succeeded	38 minutes ...	Tue Nov 22 ...	Azure Pass - Sponsorship	manassehmwangi9@gmai...
List Consent Links for Connections	Succeeded	39 minutes ...	Tue Nov 22 ...	Azure Pass - Sponsorship	manassehmwangi9@gmai...
Gets workflow recommend operation groups	Succeeded	41 minutes ...	Tue Nov 22 ...	Azure Pass - Sponsorship	manassehmwangi9@gmai...
Create new OMS solution	Succeeded	4 hours ago	Tue Nov 22 ...	Azure Pass - Sponsorship	Windows Azure Security R...
Create new OMS solution	Succeeded	4 hours ago	Tue Nov 22 ...	Azure Pass - Sponsorship	Windows Azure Security R...

This rule identifies removal of Just in time VM access policies.



Analytics rule wizard - Create a new sched

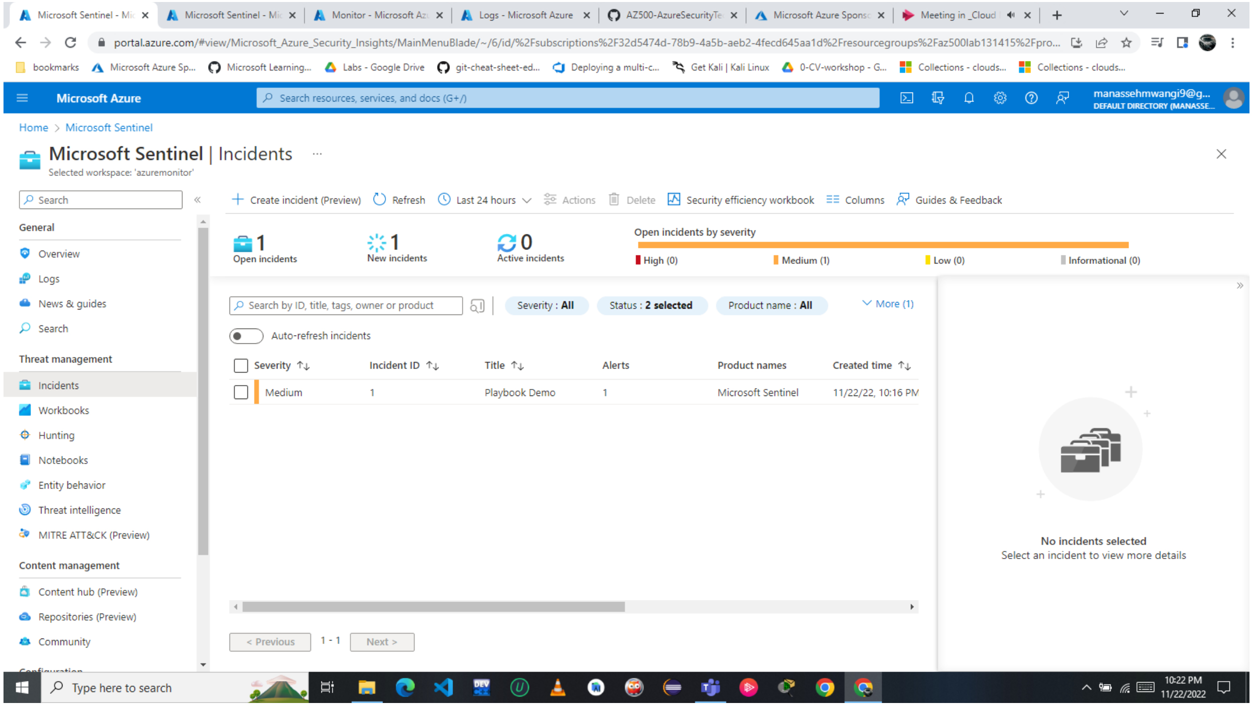
Logs — azuremonitor

```
AzureActivity
| where ResourceProviderValue =~ "Microsoft.Security"
| where OperationNameValue =~ "Microsoft.Security/locations/jitNetworkAccessPolicies/delete"
```

TimeGenerated [UTC]	CallerIpAddress	CategoryValue	CorrelationId	Authorization
11/22/2022, 7:09:27.079 PM	105.161.3.37	Administrative	132868dd-d33e-4595-898f-6e256aa86e71	{"scope":"/subscriptions/32d5474d-78b9-4a5b-aeb2-4fecd6...
11/22/2022, 7:09:28.814 PM	105.161.3.37	Administrative	132868dd-d33e-4595-898f-6e256aa86e71	{"scope":"/subscriptions/32d5474d-78b9-4a5b-aeb2-4fecd6...

4s 878ms Display time (UTC+00:00) 1 - 2 of 2

Review the dashboard and verify that it displays an alert corresponding to the deletion of the Just in time VM access policy.



Microsoft Sentinel | Incidents

Selected workspace: 'azuremonitor'

1 Open incidents · 1 New incidents · 0 Active incidents

Open incidents by severity: High (0) · Medium (1) · Low (0) · Informational (0)

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

Severity	Incident ID	Title	Alerts	Product names	Created time
Medium	1	Playbook Demo	1	Microsoft Sentinel	11/22/22, 10:16 PM

No incidents selected
Select an incident to view more details