Cloud Security Detection Engineering –Project Report

This report presents a fully refined, professionally rewritten documentation of the Log4j Exploit Detection and Azure Virtual Machine Availability Monitoring project. The goal is to demonstrate hands-on security engineering capability, SIEM detection logic implementation, cloud monitoring, and automation-driven incident response workflows within Microsoft Azure.

Executive Summary

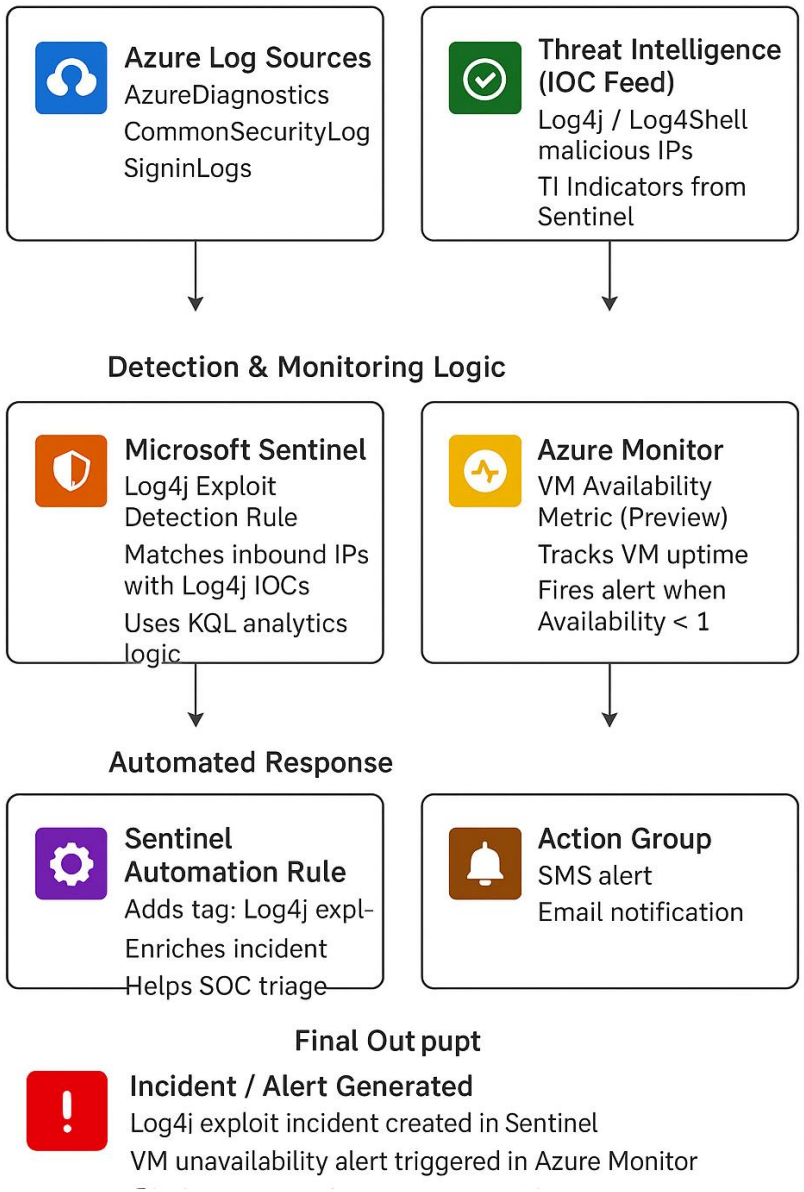
This project delivers two core cloud security capabilities:
- Proactive detection of Log4j (Log4Shell) exploitation attempts using Microsoft Sentinel
- Real-time monitoring of Azure VM availability using Azure Monitor and Action Groups

Through the deployment of analytics rules, threat intelligence correlation, automation workflows, and alerting pipelines, this implementation showcases operational security engineering principles, practical SIEM usage, and cloud observability best practices.

Cloud Detection & Monitoring Architecture

The following diagram illustrates the end-to-end flow of data ingestion, threat detection, monitoring, automated responses, and incident generation across Microsoft Sentinel and Azure Monitor.

Cloud Detection & Monitoring Flow



Part 1 — Log4j Exploit Detection Using Microsoft Sentinel

Objective

Detect potential Log4j exploitation attempts by operationalizing the Log4j Vulnerability Detection solution within Microsoft Sentinel and enabling an analytics rule that correlates inbound IP activity with known Log4Shell-related threat intelligence indicators.

Tools & Technologies

- Microsoft Sentinel
- Azure Log Sources (AzureDiagnostics, SigninLogs, CommonSecurityLog)
- Threat Intelligence Indicators (Log4j IOC Feed)
- Scheduled Analytics Rules
- KQL (Kusto Query Language)
- Sentinel Automation Rules

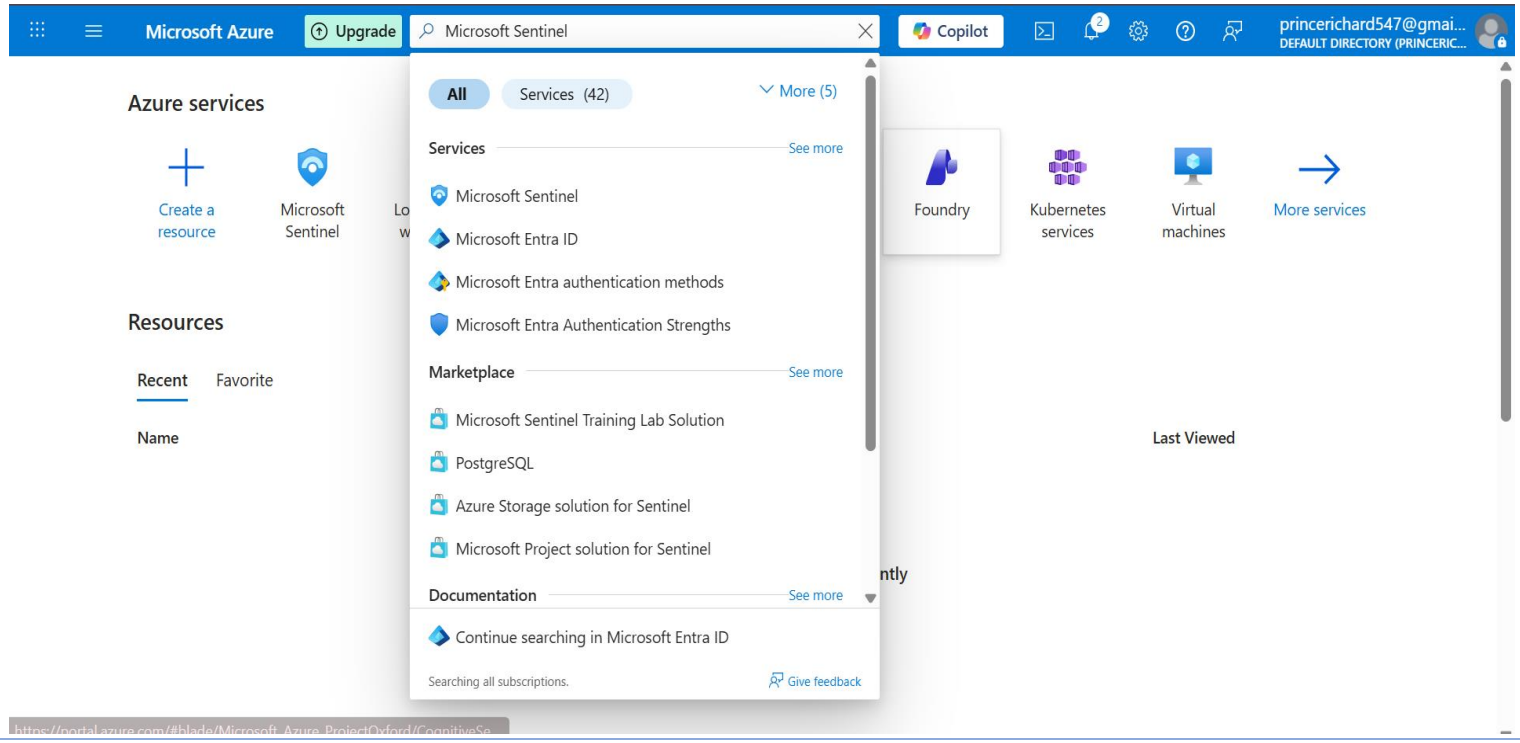
Implementation Summary

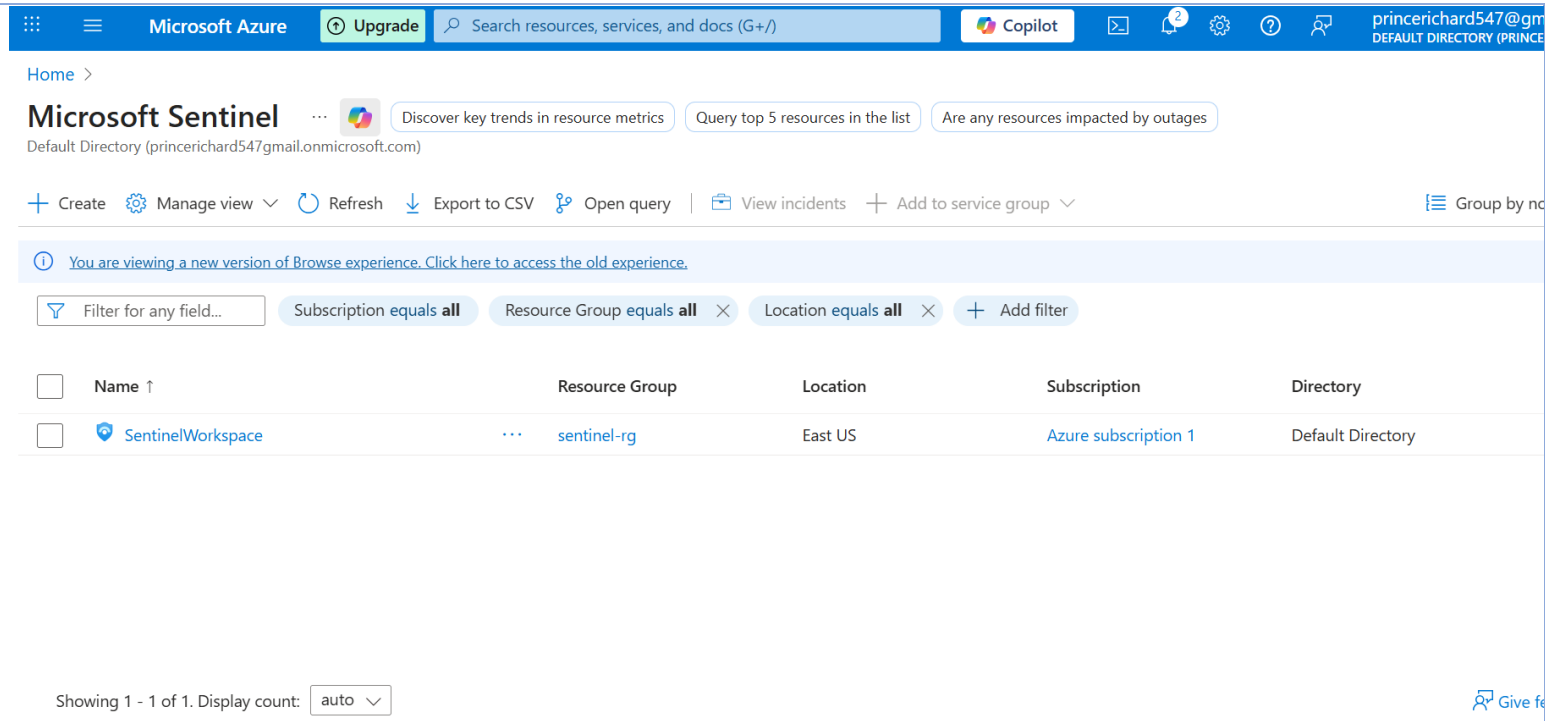
1. Deployed the Log4j Vulnerability Detection solution via Microsoft Sentinel Content Hub.
2. Located and activated the 'Log4j vulnerability exploit aka Log4Shell IP IOC' analytics rule template.
3. Customized rule parameters, added a timestamp field, and enhanced alert naming for clarity.
4. Created an automation rule that tags incidents with 'Log4J exploit' to support structured SOC triage.

Implementation Steps:

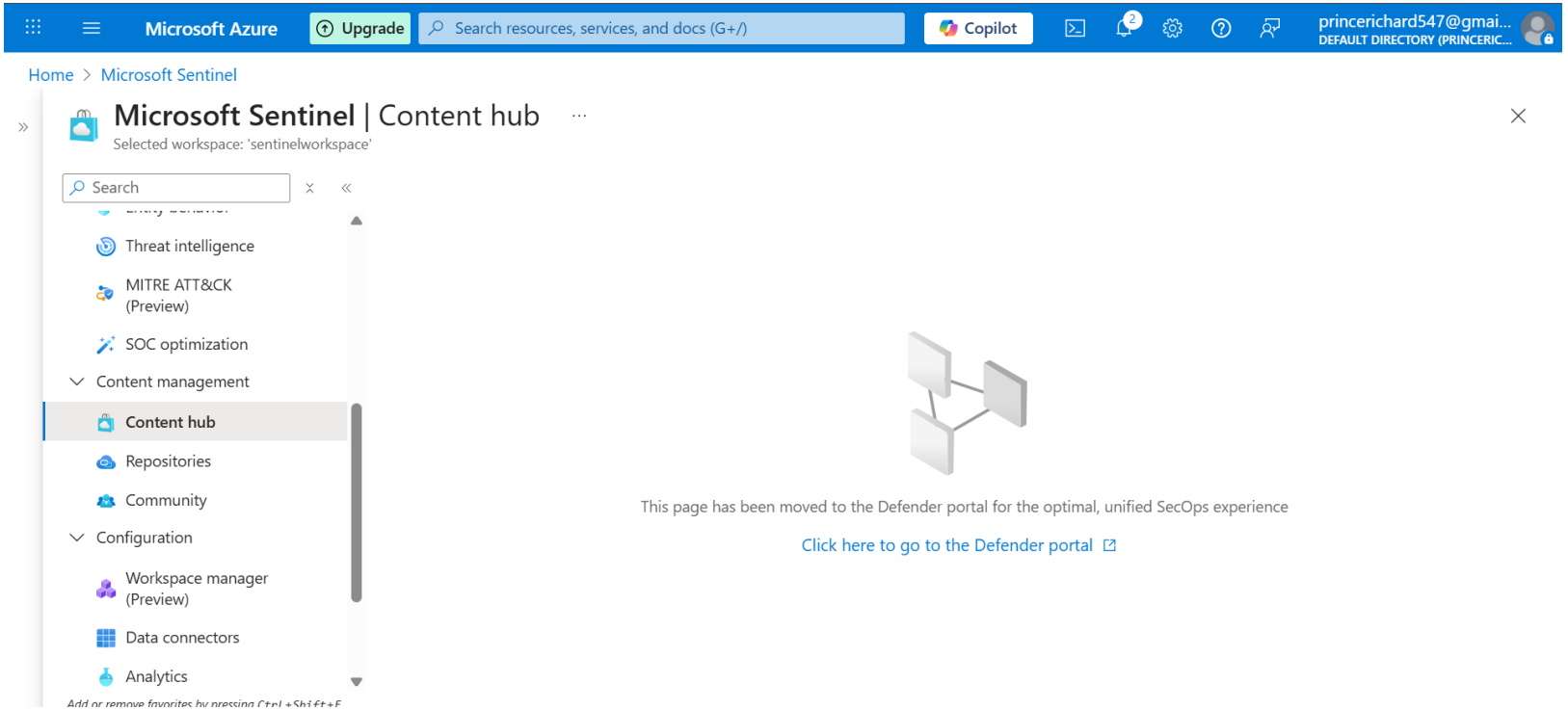
Activity #	Steps
Activity 1: Install the *Log4j Vulnerability Detection* solution from the Content hub.	1. Sign in to the Azure portal with your login credentials. 2. In the global search box, search for and select **Microsoft Sentinel**.

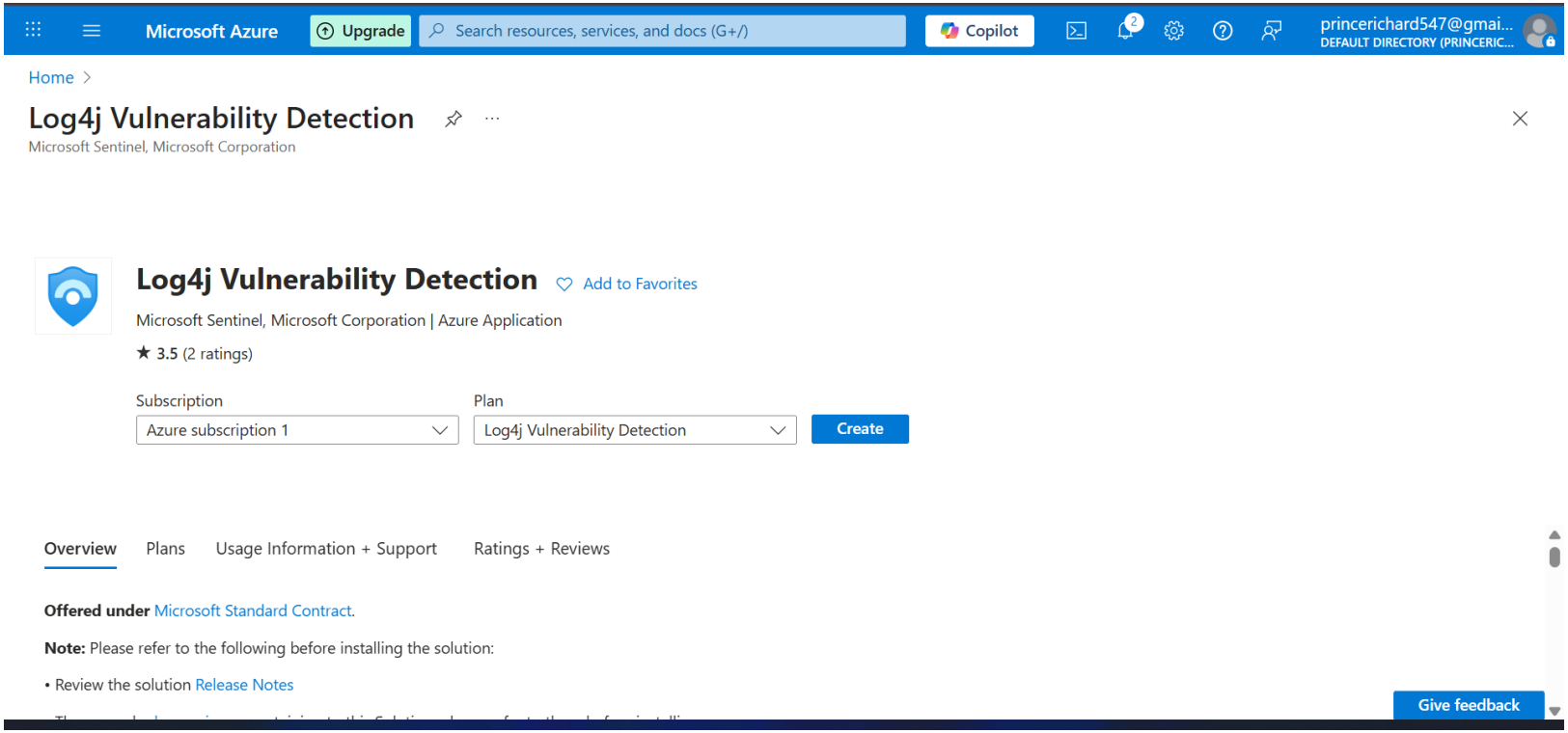
3. **Select** the desired Microsoft Sentinel workspace.

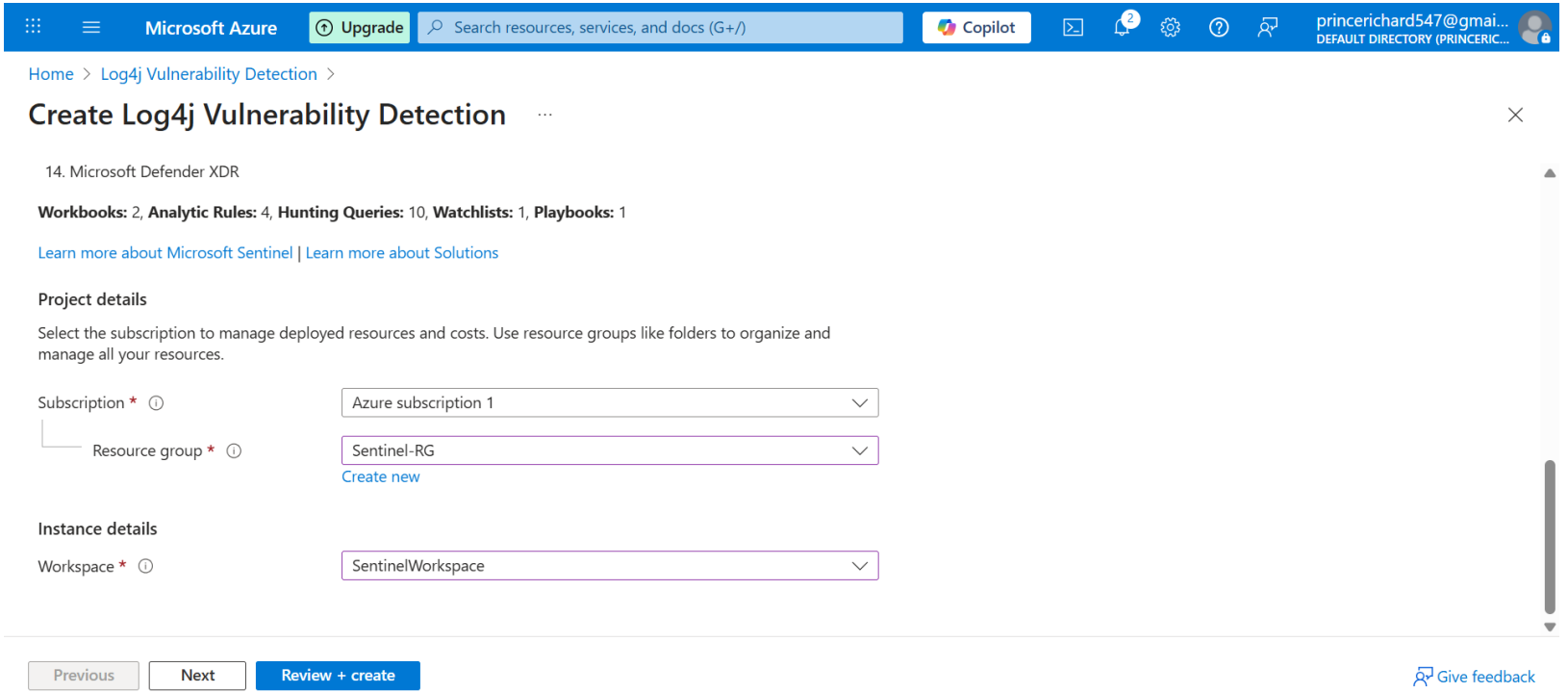


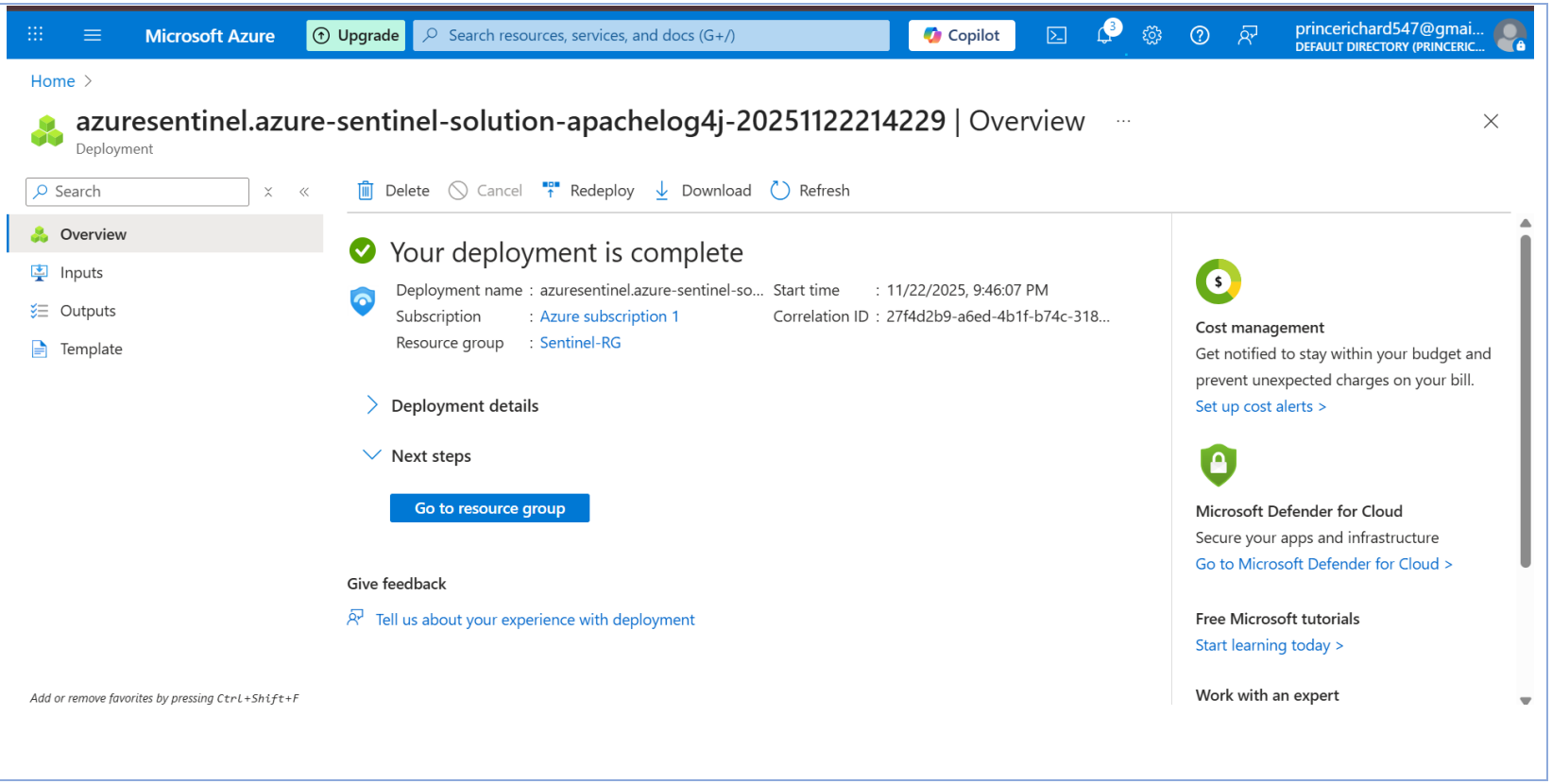


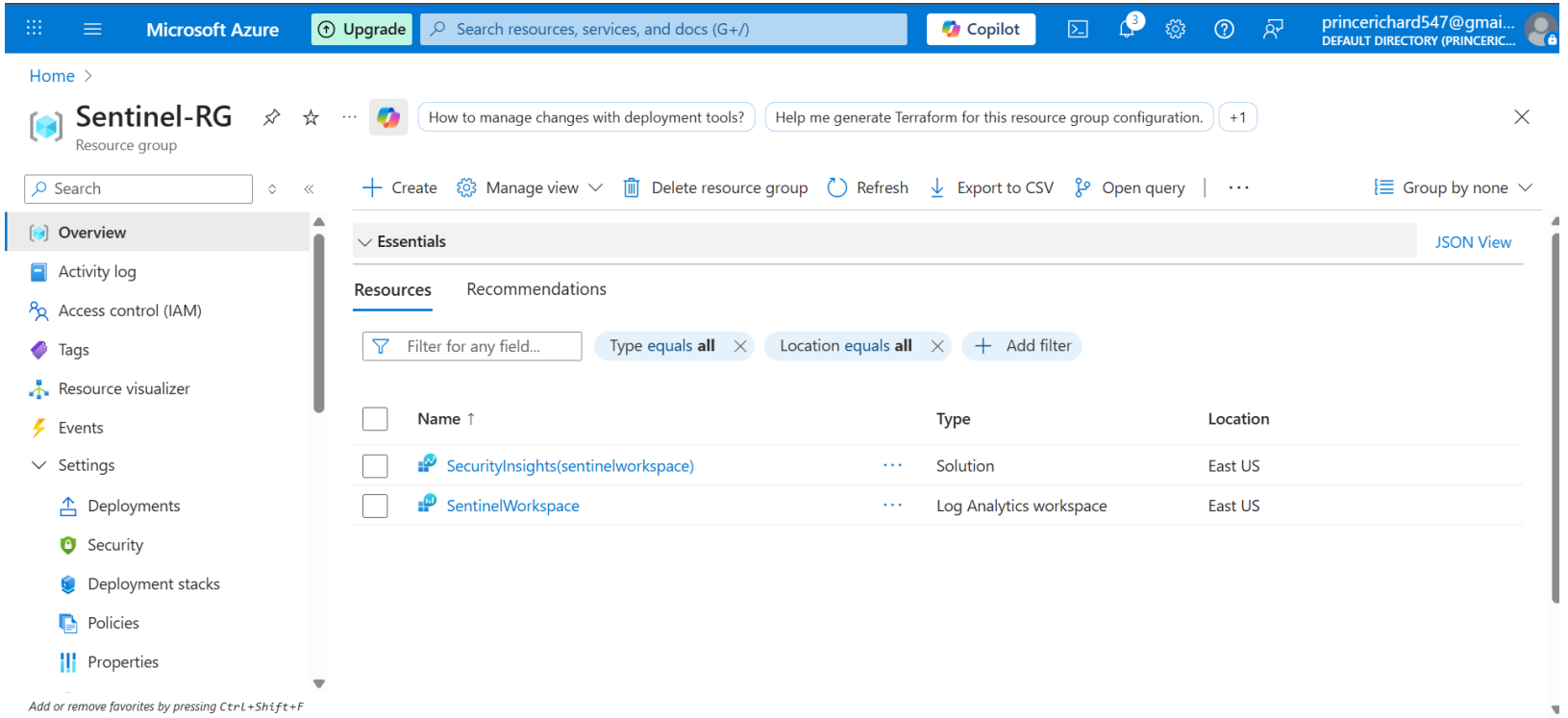
4. On the **Microsoft Sentinel** page, under **Content management**, select **Content hub**.
5. On the **Content hub** page, click on **Go to defender portal**
6. Search and select the **Log4j Vulnerability Detection** solution.
7. On the **Log4j Vulnerability Detection** wizard that appears, select **Install**.


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
princerichard547@gmai...
DEFAULT DIRECTORY (PRINCERIC...
Home > Microsoft Sentinel
Microsoft Sentinel | Content hub
Selected workspace: 'sentinelworkspace'
Search
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
This page has been moved to the Defender portal for the optimal, unified SecOps experience
Click here to go to the Defender portal

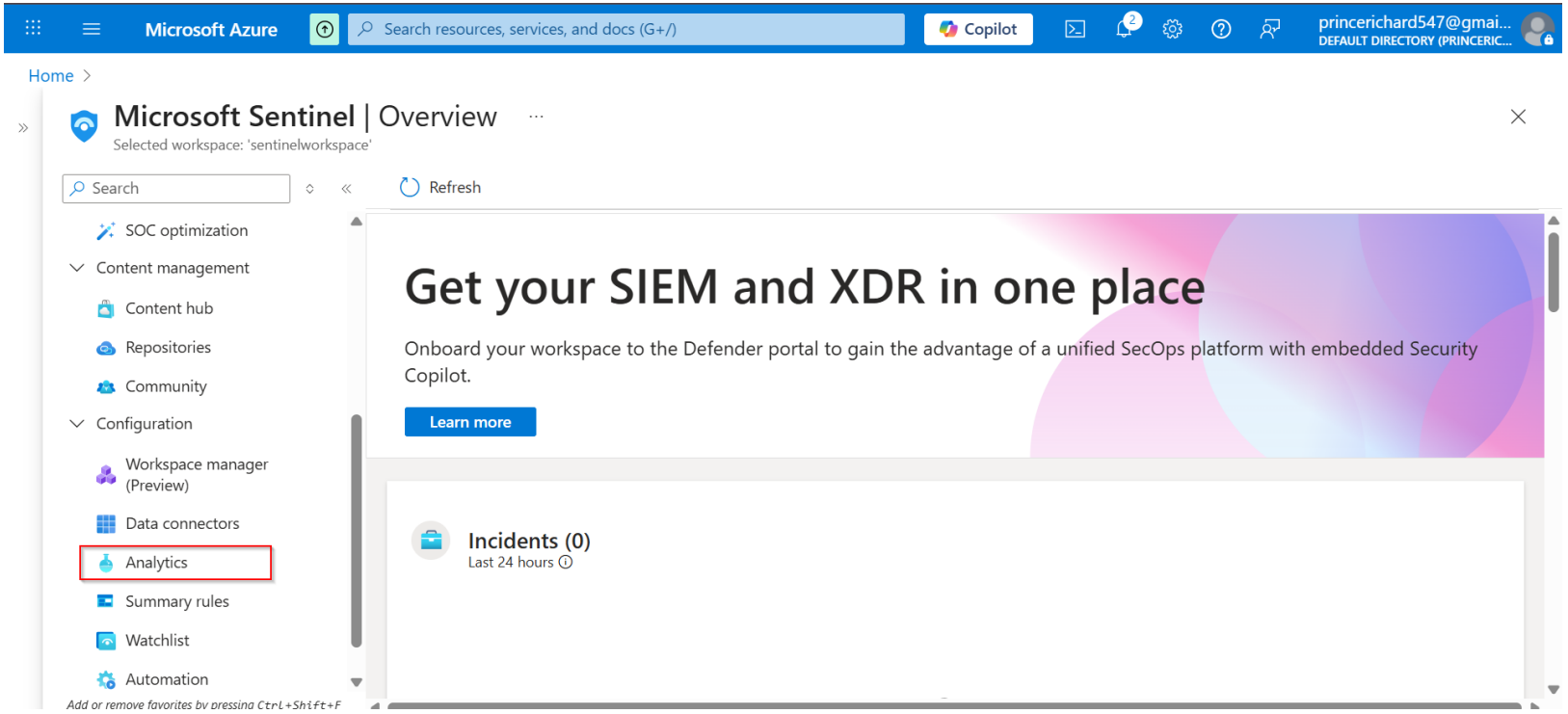

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
princerichard547@gmai...
DEFAULT DIRECTORY (PRINCERIC...
Home
Log4j Vulnerability Detection
Microsoft Sentinel, Microsoft Corporation
Log4j Vulnerability Detection
Add to Favorites
Microsoft Sentinel, Microsoft Corporation | Azure Application
★ 3.5 (2 ratings)
Subscription
Azure subscription 1
Plan
Log4j Vulnerability Detection
Create
Overview
Plans
Usage Information + Support
Ratings + Reviews
Offered under Microsoft Standard Contract.
Note: Please refer to the following before installing the solution:
• Review the solution Release Notes
Give feedback

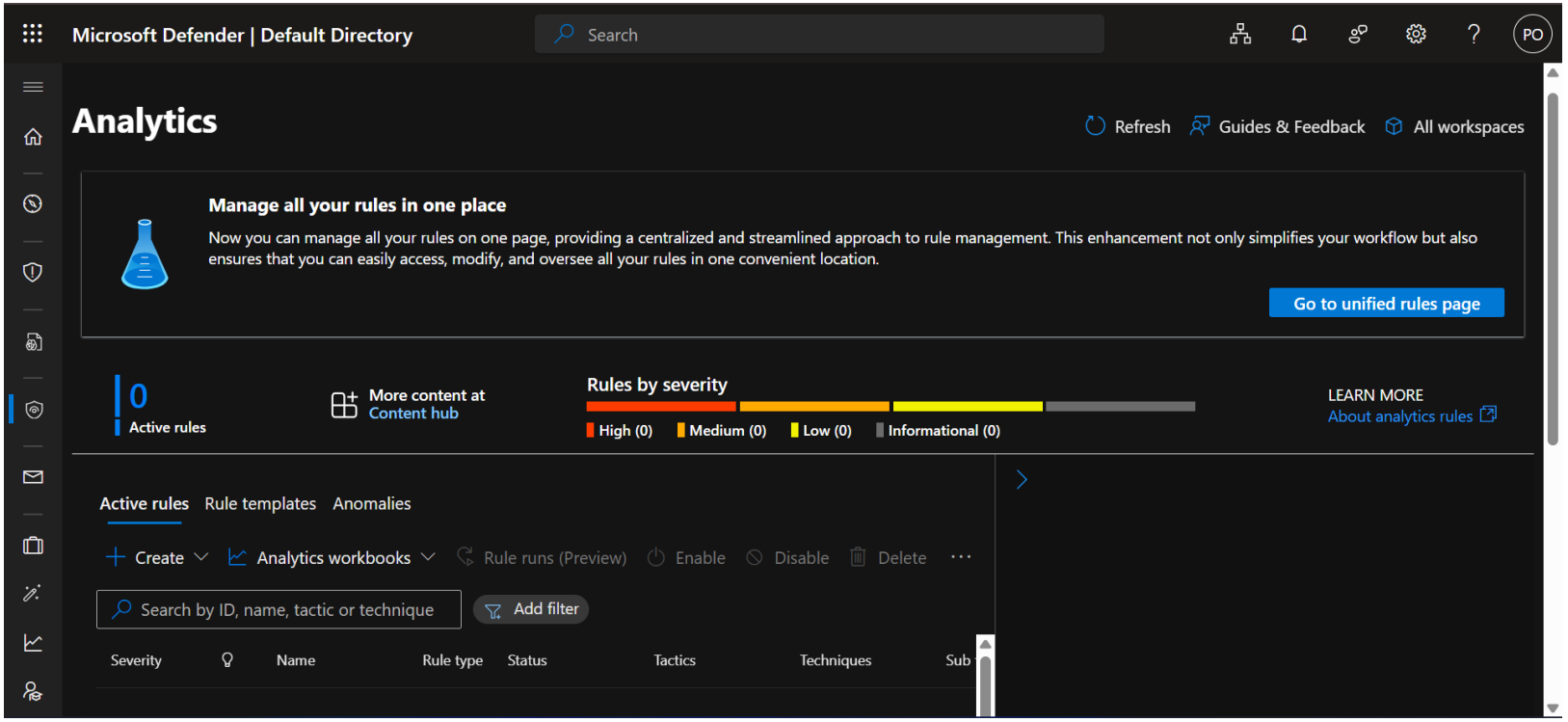

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
princerichard547@gmai...
DEFAULT DIRECTORY (PRINCERIC...
Home > Log4j Vulnerability Detection >
Create Log4j Vulnerability Detection
14. Microsoft Defender XDR
Workbooks: 2, Analytic Rules: 4, Hunting Queries: 10, Watchlists: 1, Playbooks: 1
Learn more about Microsoft Sentinel | Learn more about Solutions
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Azure subscription 1
Resource group *
Sentinel-RG
Create new
Instance details
Workspace *
SentinelWorkspace
Previous
Next
Review + create
Give feedback

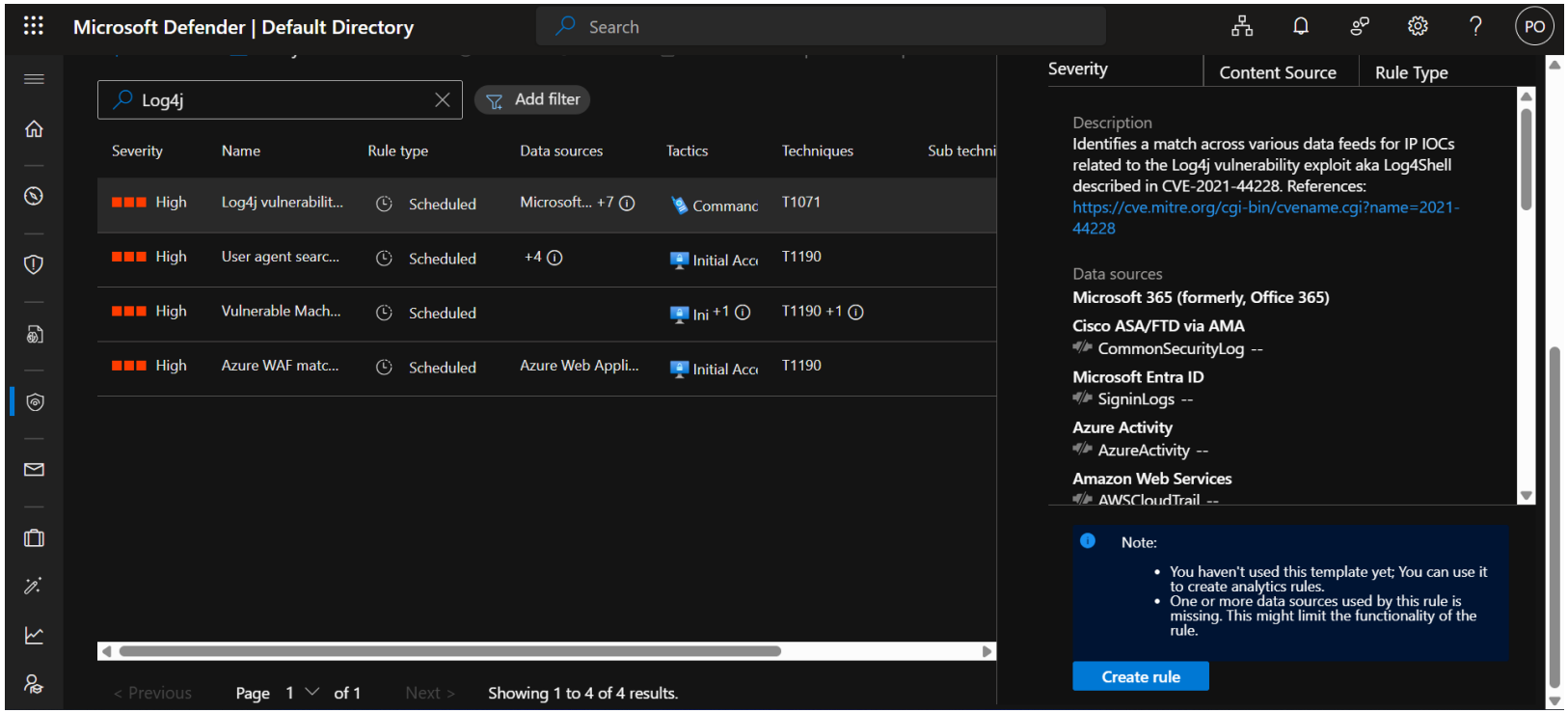

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
princerichard547@gmai...
DEFAULT DIRECTORY (PRINCERIC...
Home
azuresentinel.azure-sentinel-solution-apachelog4j-20251122214229 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name : azuresentinel.azure-sentinel-so...
Subscription : Azure subscription 1
Resource group : Sentinel-RG
Start time : 11/22/2025, 9:46:07 PM
Correlation ID : 27f4d2b9-a6ed-4b1f-b74c-318...
Deployment details
Next steps
Go to resource group
Give feedback
Tell us about your experience with deployment
Add or remove favorites by pressing Ctrl+Shift+F
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

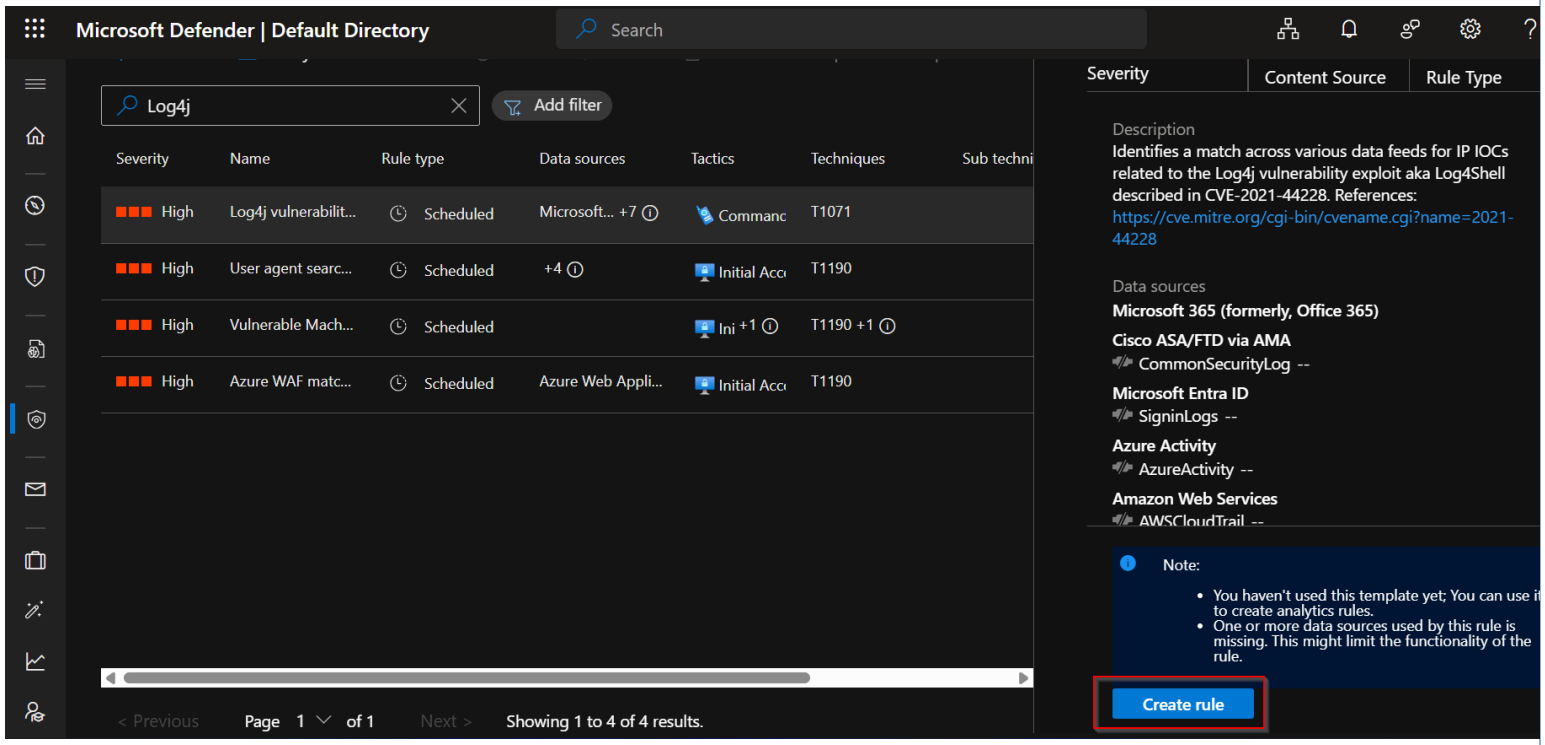


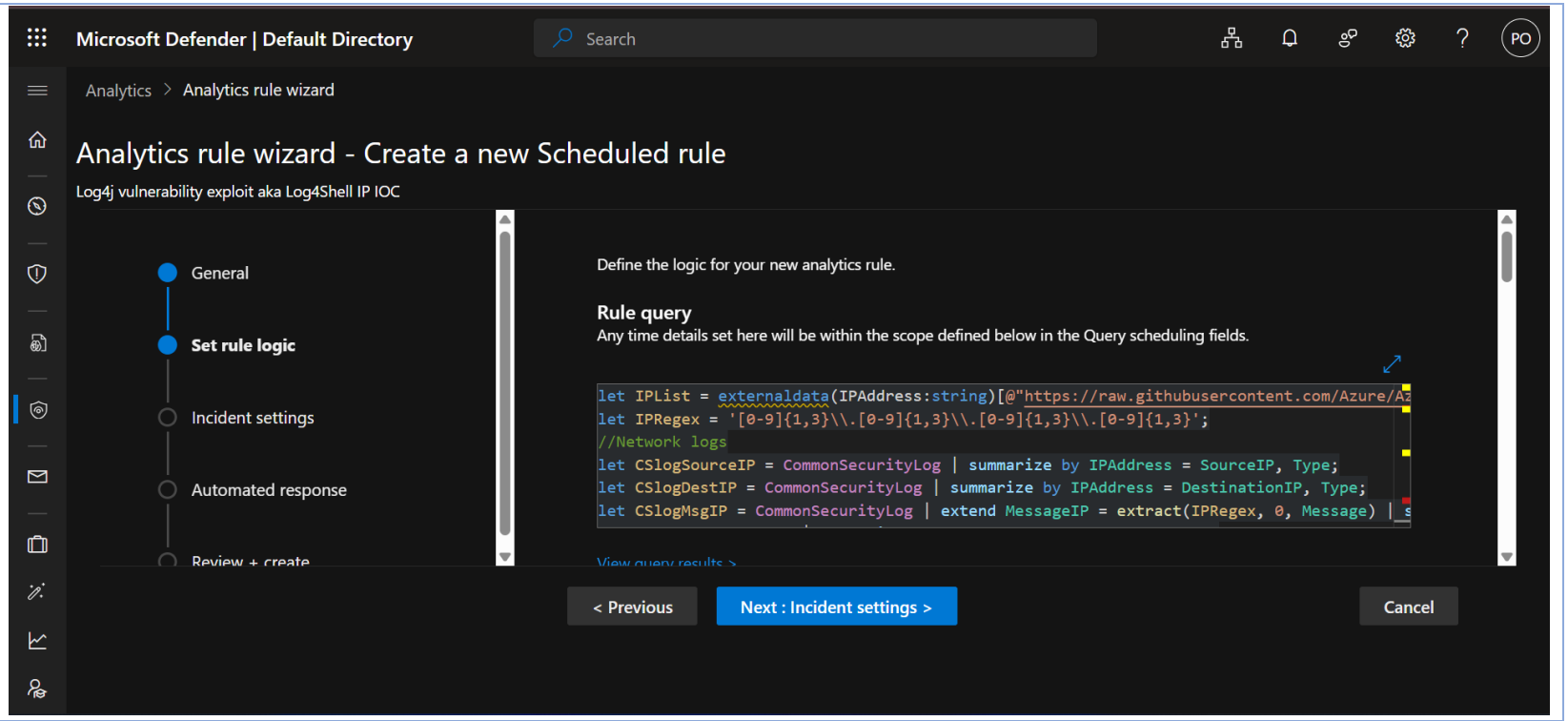
Activity 2: Navigate to the *Log4j vulnerability exploit aka Log4Shell IP IOC* scheduled analytics rule from the Rule templates tab.	1. On the **Microsoft Sentinel** page, under **Configuration**, select **Analytics**. 2. On the **Analytics** page, select the **Rule templates** tab. 3. In the search box, enter **log4j**. 4. From the filtered list of templates displayed, select **Log4j vulnerability exploit aka Log4Shell IP IOC**.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
princerichard547@gmai...
DEFAULT DIRECTORY (PRINCERIC...
Home
Microsoft Sentinel | Overview
Selected workspace: 'sentinelworkspace'
Search
Refresh
SOC optimization
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
Watchlist
Automation
Add or remove favorites by pressing Ctrl+Shift+F
Get your SIEM and XDR in one place
Onboard your workspace to the Defender portal to gain the advantage of a unified SecOps platform with embedded Security Copilot.
Learn more
Incidents (0)
Last 24 hours

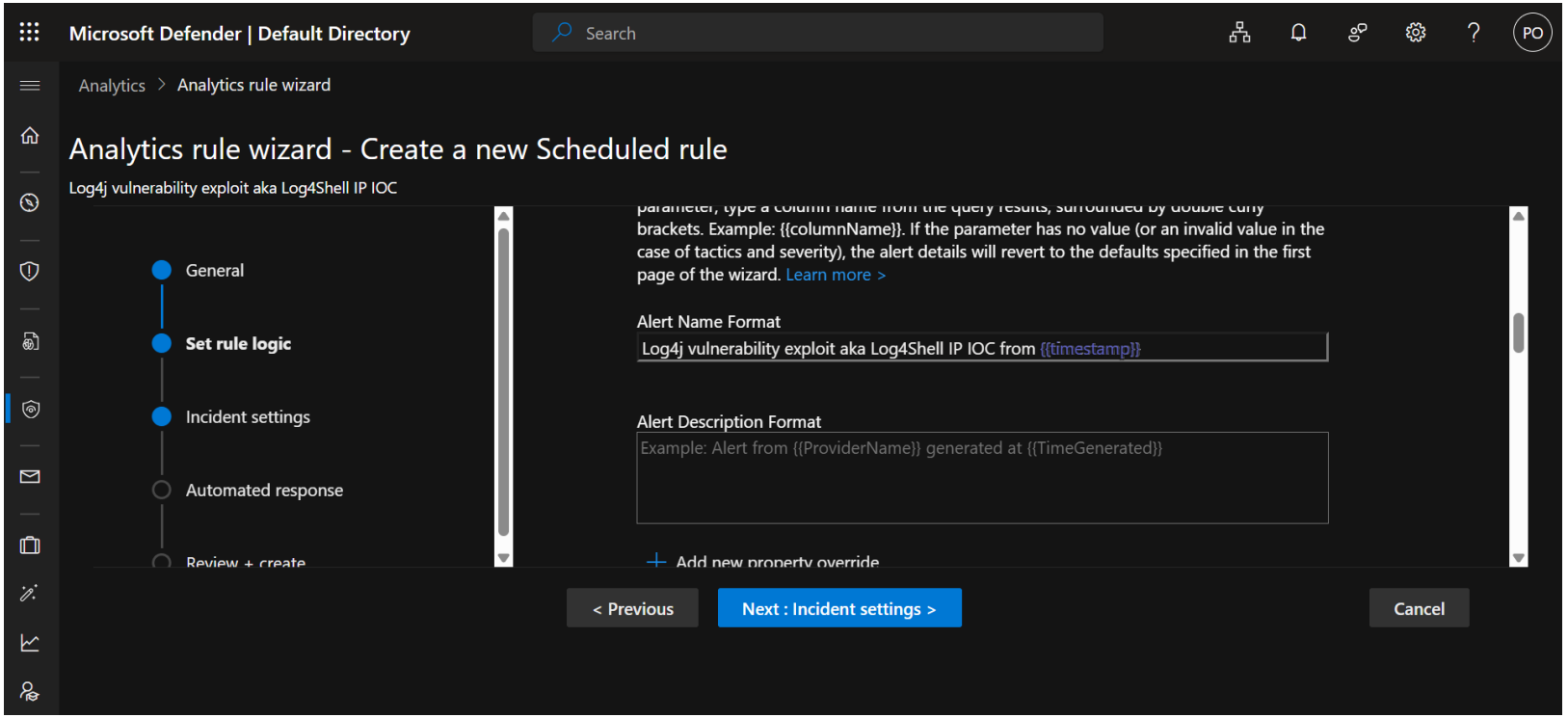

Microsoft Defender | Default Directory
Search
PO
Analytics
Refresh
Guides & Feedback
All workspaces
Manage all your rules in one place
Now you can manage all your rules on one page, providing a centralized and streamlined approach to rule management. This enhancement not only simplifies your workflow but also ensures that you can easily access, modify, and oversee all your rules in one convenient location.
Go to unified rules page
0
Active rules
More content at
Content hub
Rules by severity
High (0)
Medium (0)
Low (0)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Create
Analytics workbooks
Rule runs (Preview)
Enable
Disable
Delete
Search by ID, name, tactic or technique
Add filter
Severity
Name
Rule type
Status
Tactics
Techniques
Sub


Microsoft Defender | Default Directory
Search
PO
Log4j
Add filter
Severity
Name
Rule type
Data sources
Tactics
Techniques
Sub techni
High
Log4j vulnerabilit...
Scheduled
Microsoft... +7
Commanc
T1071
High
User agent searc...
Scheduled
+4
Initial Acc
T1190
High
Vulnerable Mach...
Scheduled
Ini +1
T1190 +1
High
Azure WAF matc...
Scheduled
Azure Web Appli...
Initial Acc
T1190
< Previous
Page 1 of 1
Next >
Showing 1 to 4 of 4 results.
Severity
Content Source
Rule Type
Description
Identifies a match across various data feeds for IP IOCs related to the Log4j vulnerability exploit aka Log4Shell described in CVE-2021-44228. References: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228
Data sources
Microsoft 365 (formerly, Office 365)
Cisco ASA/FTD via AMA
CommonSecurityLog --
Microsoft Entra ID
SigninLogs --
Azure Activity
AzureActivity --
Amazon Web Services
AWSCloudTrail --
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.
Create rule

Activity 3: Create a rule logic for *Log4j vulnerability exploit aka Log4Shell IP IOC* and configure settings.	1. On the **Analytics** page, on the **Log4j vulnerability exploit aka Log4Shell IP IOC** wizard that appears on the right, select **Create rule**. 
	2. On the **Analytics rule wizard – Create a new Scheduled rule** page, on the **General** tab, leave the settings as default, and select **Next: Set rule logic**.



3. On the **Set rule logic** tab, review the query as it appears under the **Rule query** section.



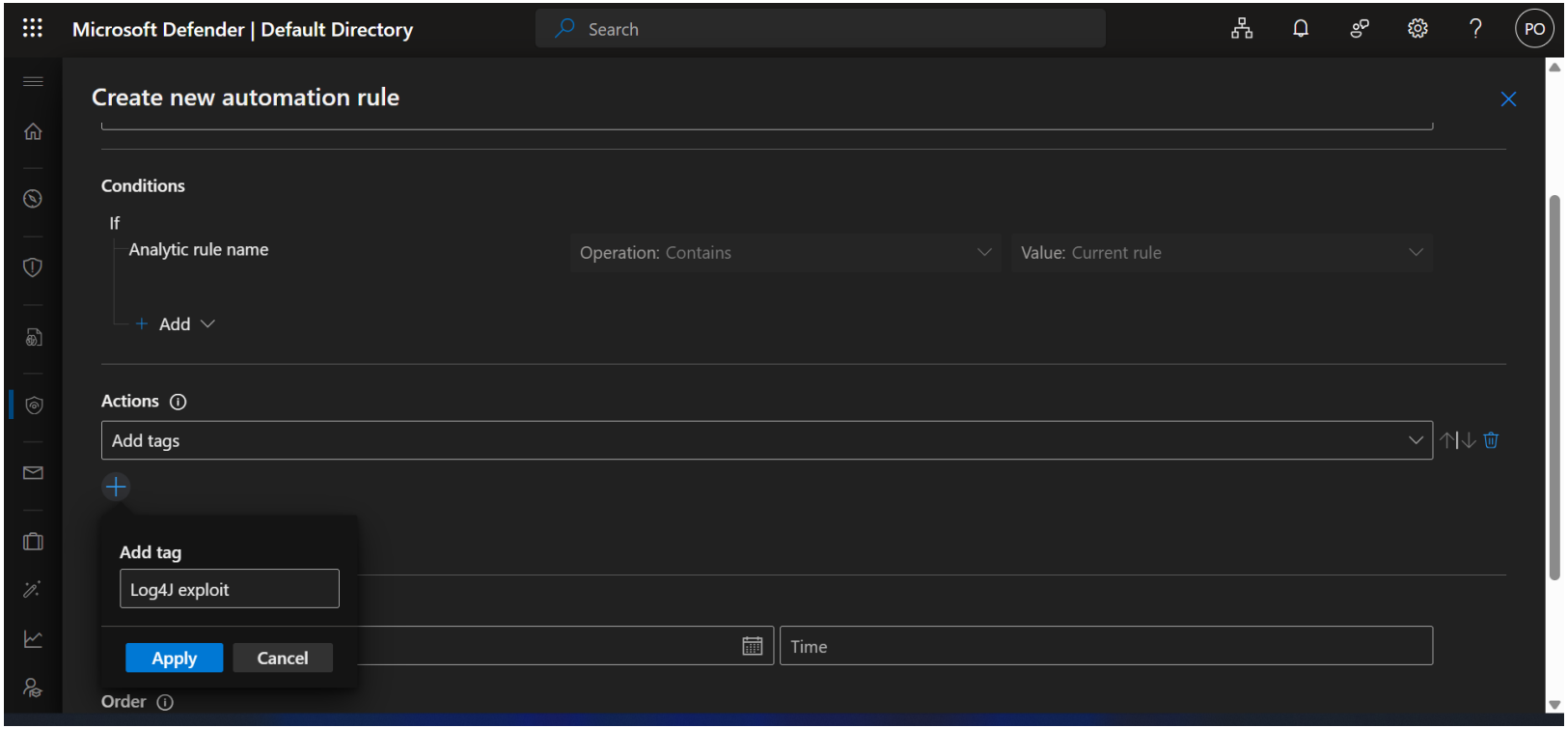
4. Then, in the **Custom details** section, in the **Key** field, enter **timestamp** to add the timestamp of each occurrence to the alert.
5. From the **Value** dropdown list, select **timestamp**.

6. In the **Alert details** section, in the **Alert Name Format** box, enter **Log4j vulnerability exploit aka Log4Shell IP IOC from {{timestamp}}.**
7. Leave the other settings as default and select **Next: Incident settings**.

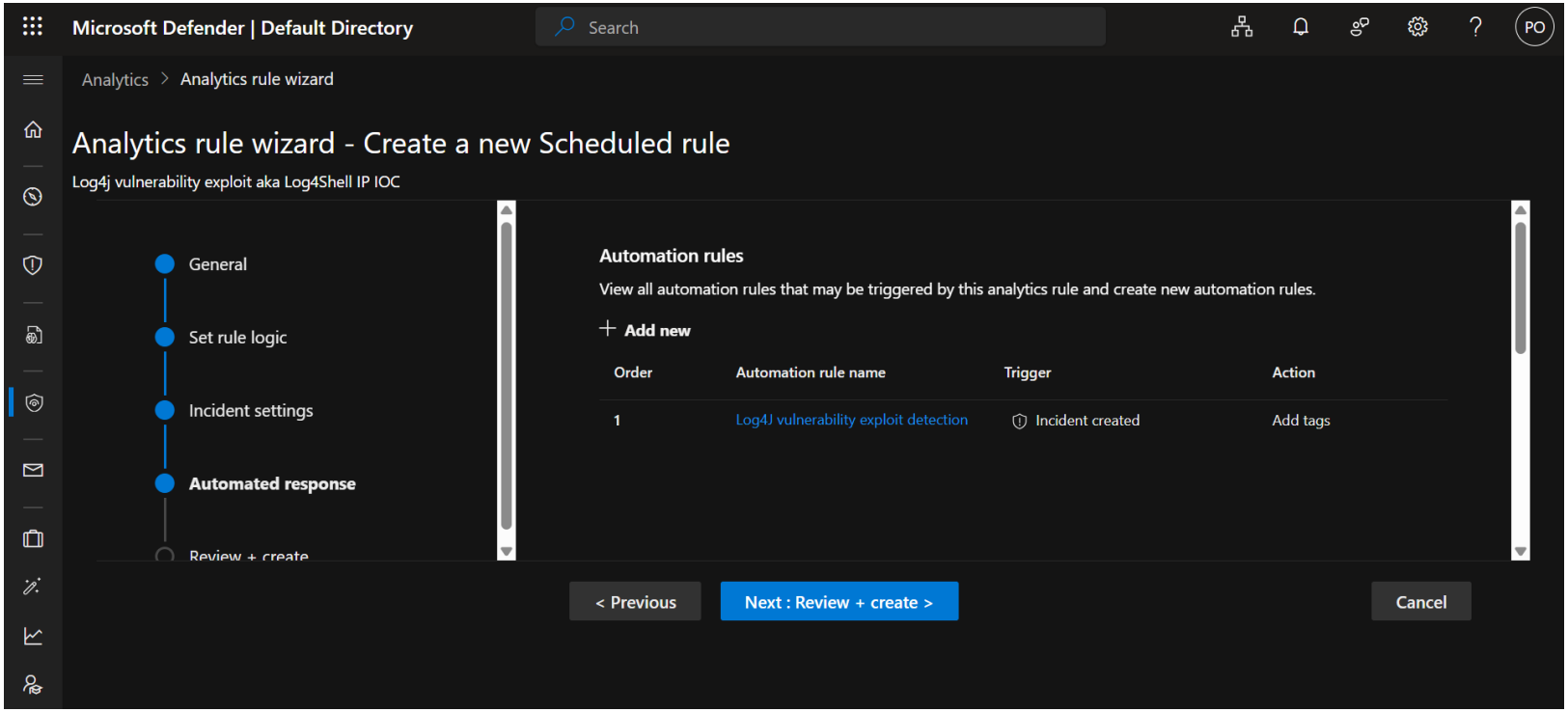
8. Review the remaining settings on the **Incident settings** tab, leave it as default, and select **Next: Automated response**.

9. On the **Automated response** tab, in the **Automation rules** section, select **Add new** to create a new automation rule for this analytics rule.

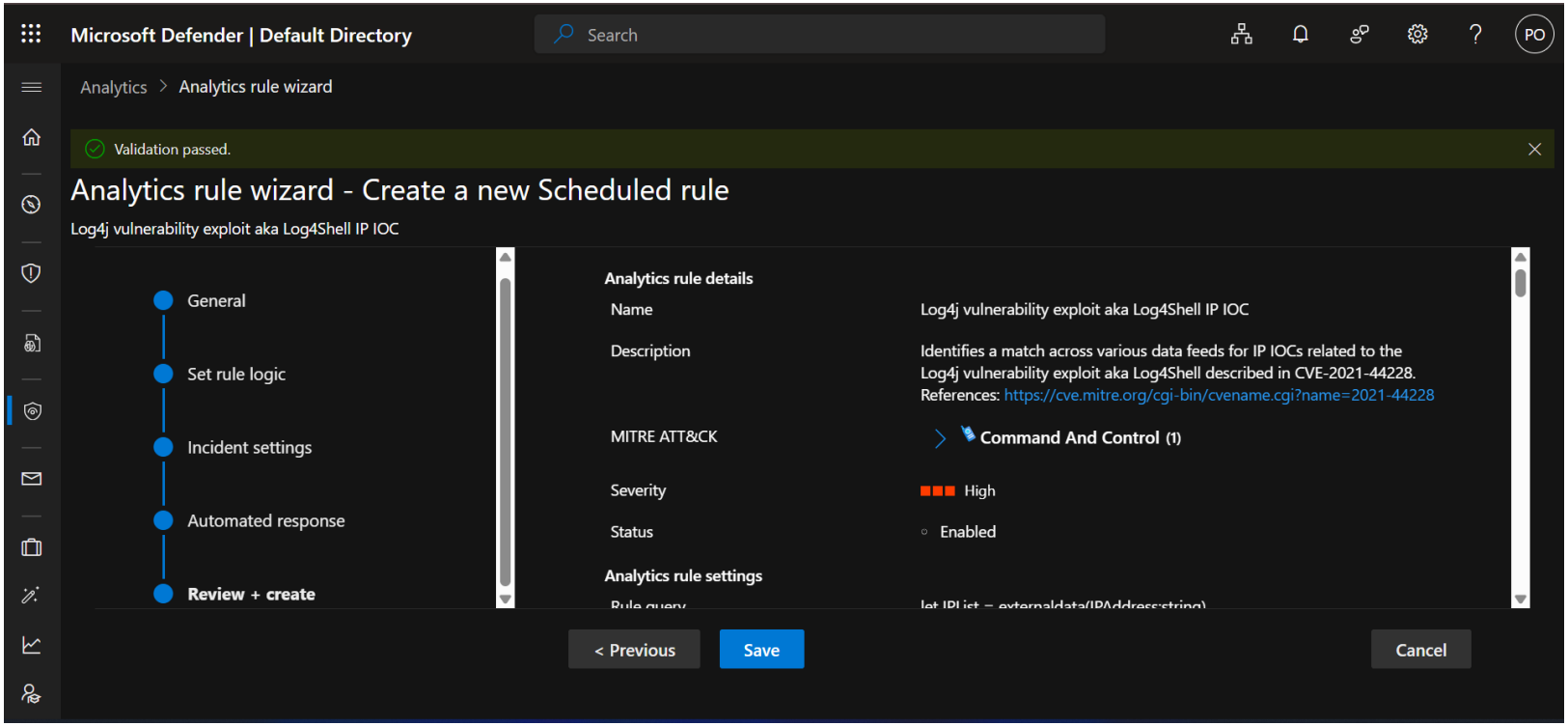
10. On the **Create new automation rule** wizard that appears, in the **Automation rule name** box, enter **Log4J vulnerability exploit detection**.
11. Then, from the **Actions** dropdown list, select **Add tags**.

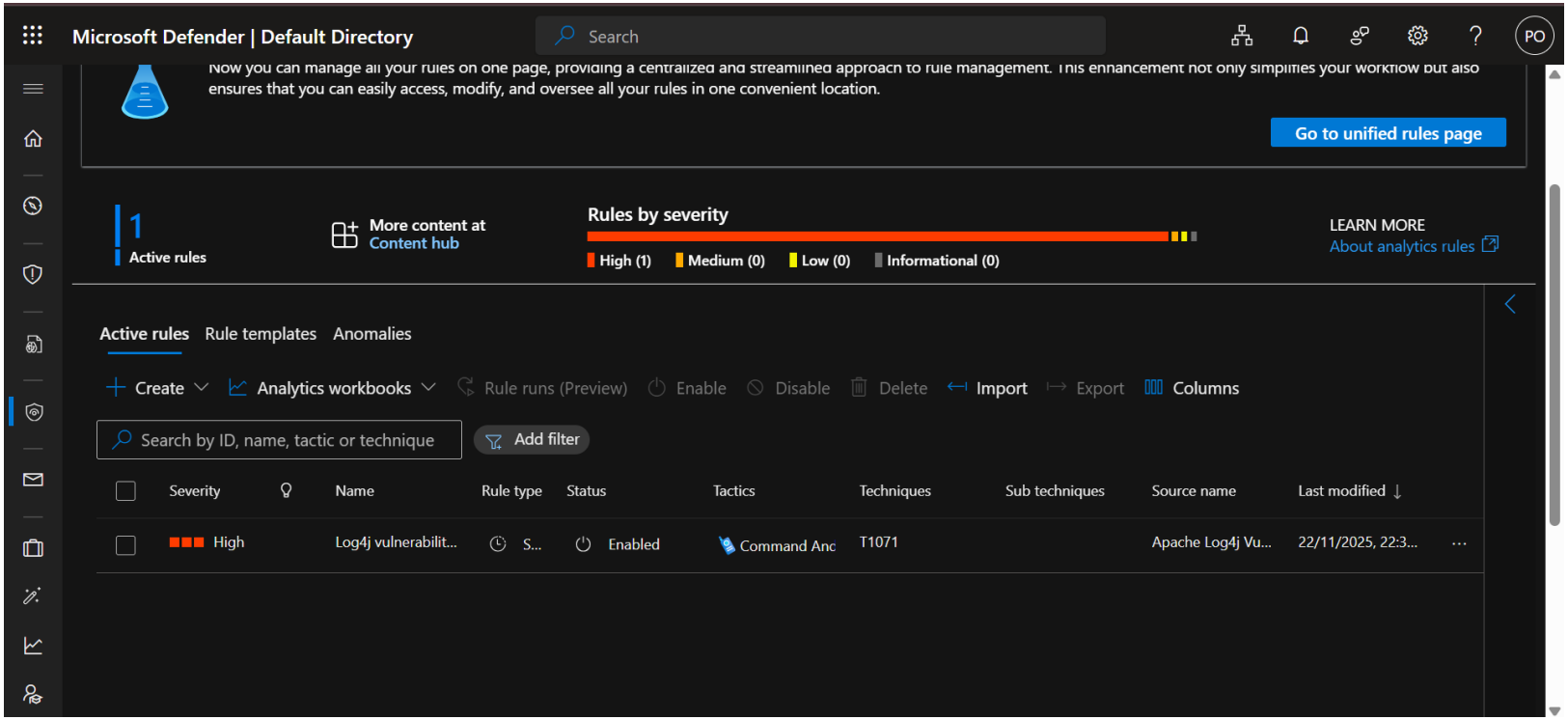


12. Select **Add tag**.
13. Enter **Log4J exploit** in the text box and select **OK.**
14. Next, select **Apply.**
15. Then, select **Next: Review and create**.



16. Review all the settings for your new analytics rule on the **Review and create** tab and select **Save.**


Microsoft Defender | Default Directory
Search
PO
Analytics
Analytics rule wizard
Validation passed.
Analytics rule wizard - Create a new Scheduled rule
Log4j vulnerability exploit aka Log4Shell IP IOC
General
Set rule logic
Incident settings
Automated response
Review + create
Analytics rule details
Name
Log4j vulnerability exploit aka Log4Shell IP IOC
Description
Identifies a match across various data feeds for IP IOCs related to the Log4j vulnerability exploit aka Log4Shell described in CVE-2021-44228.
References: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228
MITRE ATT&CK
Command And Control (1)
Severity
High
Status
Enabled
Analytics rule settings
< Previous
Save
Cancel



Outcome

The analytics rule now provides continuous detection of known malicious Log4Shell-related IP interactions. Automated tagging enhances SOC workflow efficiency, improves triage speed, and aligns incidents under a standardized taxonomy.

Part 2 — Azure VM Availability Monitoring

Objective

Enable near real-time alerting for virtual machine downtime by leveraging Azure Monitor's VM Availability metric and Action Groups for escalation notifications.

Tools & Technologies

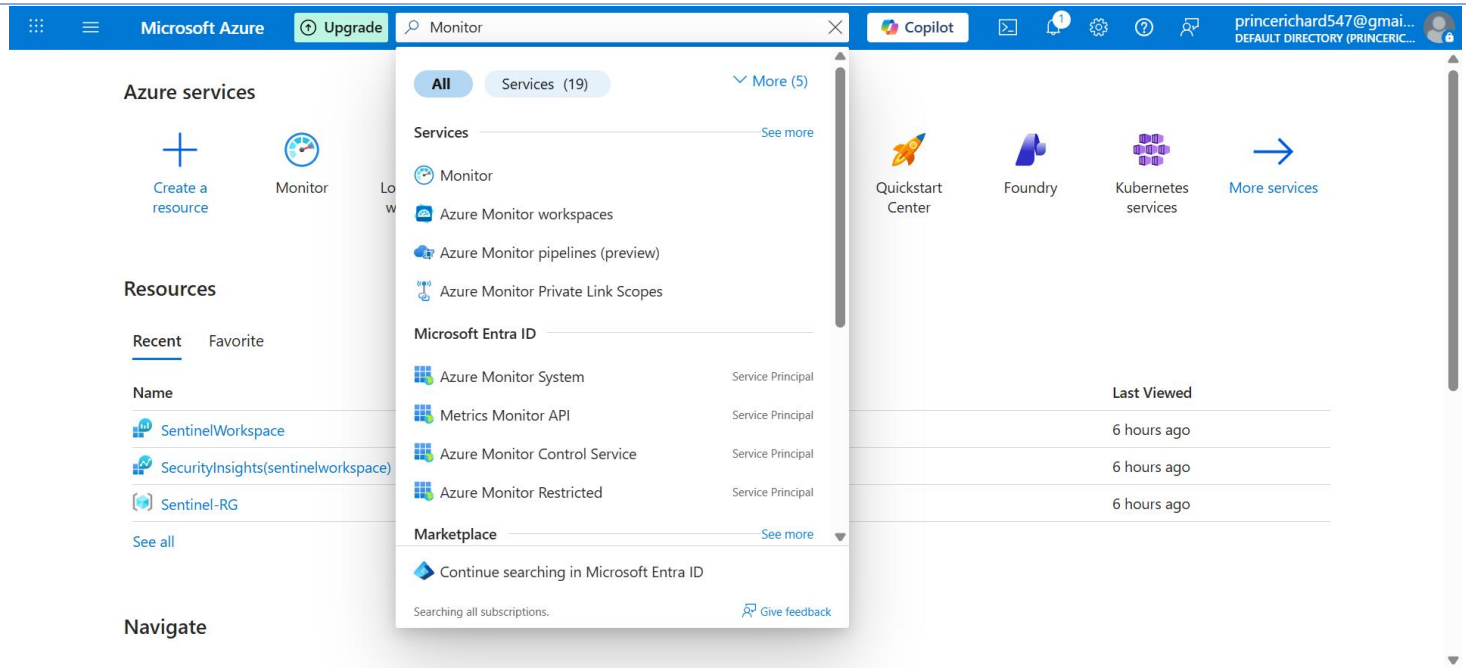
- Azure Monitor
- VM Availability Metric (Preview)
- Azure Metrics Explorer
- Action Groups (SMS/Email)
- Azure Alerting Engine

Implementation Summary

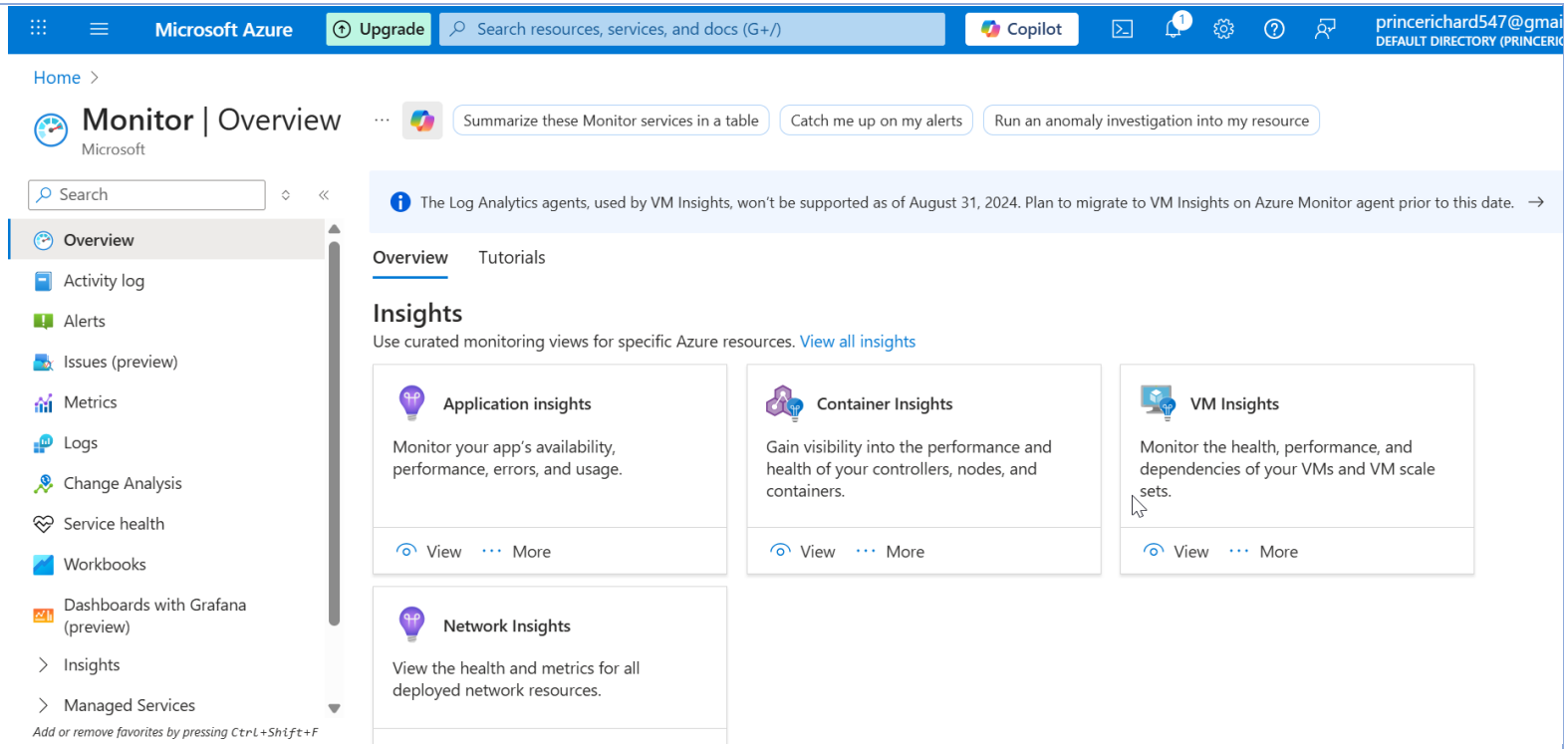
1. Configured Azure Monitor metrics scope for VM IPO-VM.
2. Selected the 'VM Availability Metric (Preview)' to monitor uptime (1 = available, 0 = unavailable).
3. Created an alert rule that fires when availability falls below 1 within a 1-minute evaluation window.
4. Configured an Action Group with SMS/email notifications for immediate response.

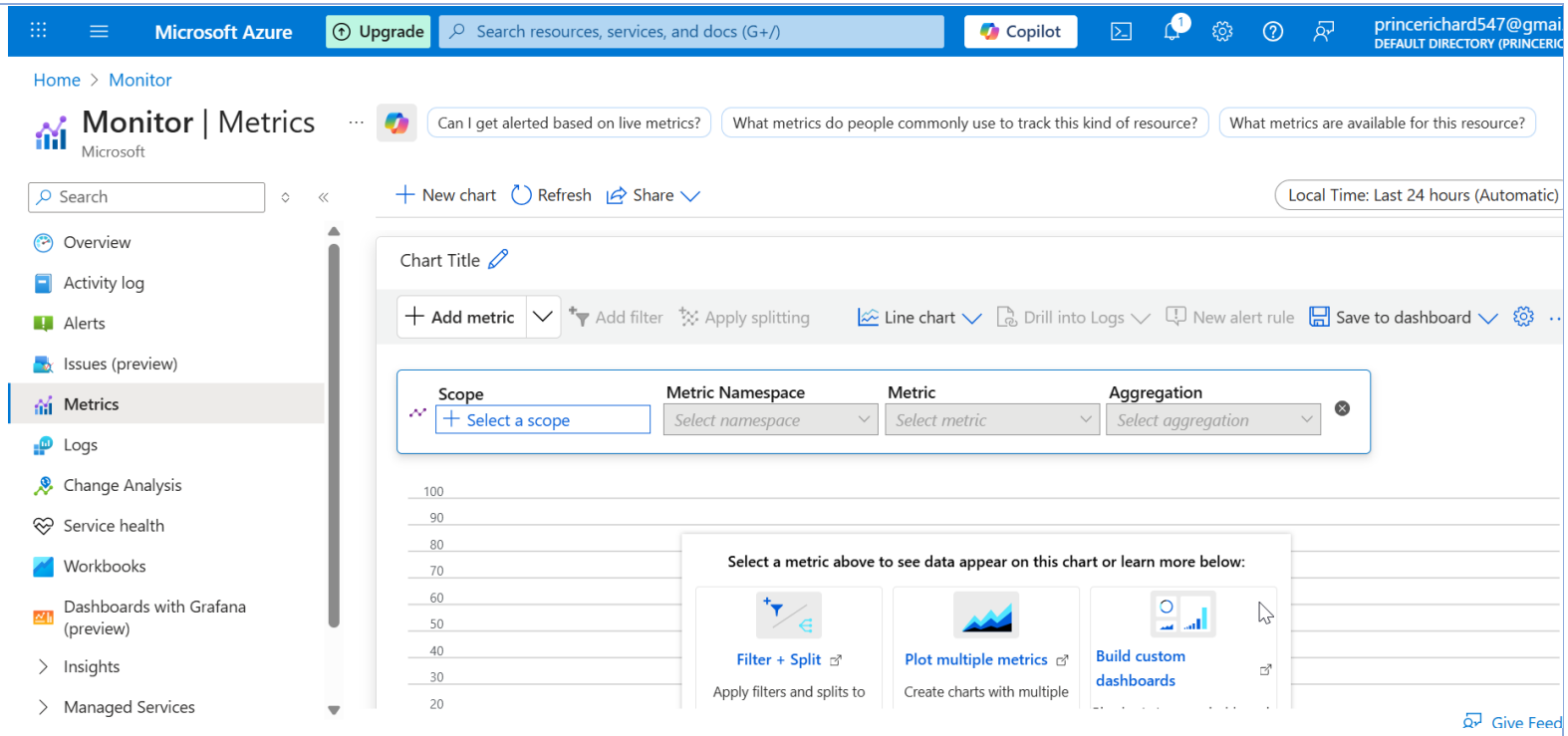
Implementation Steps:

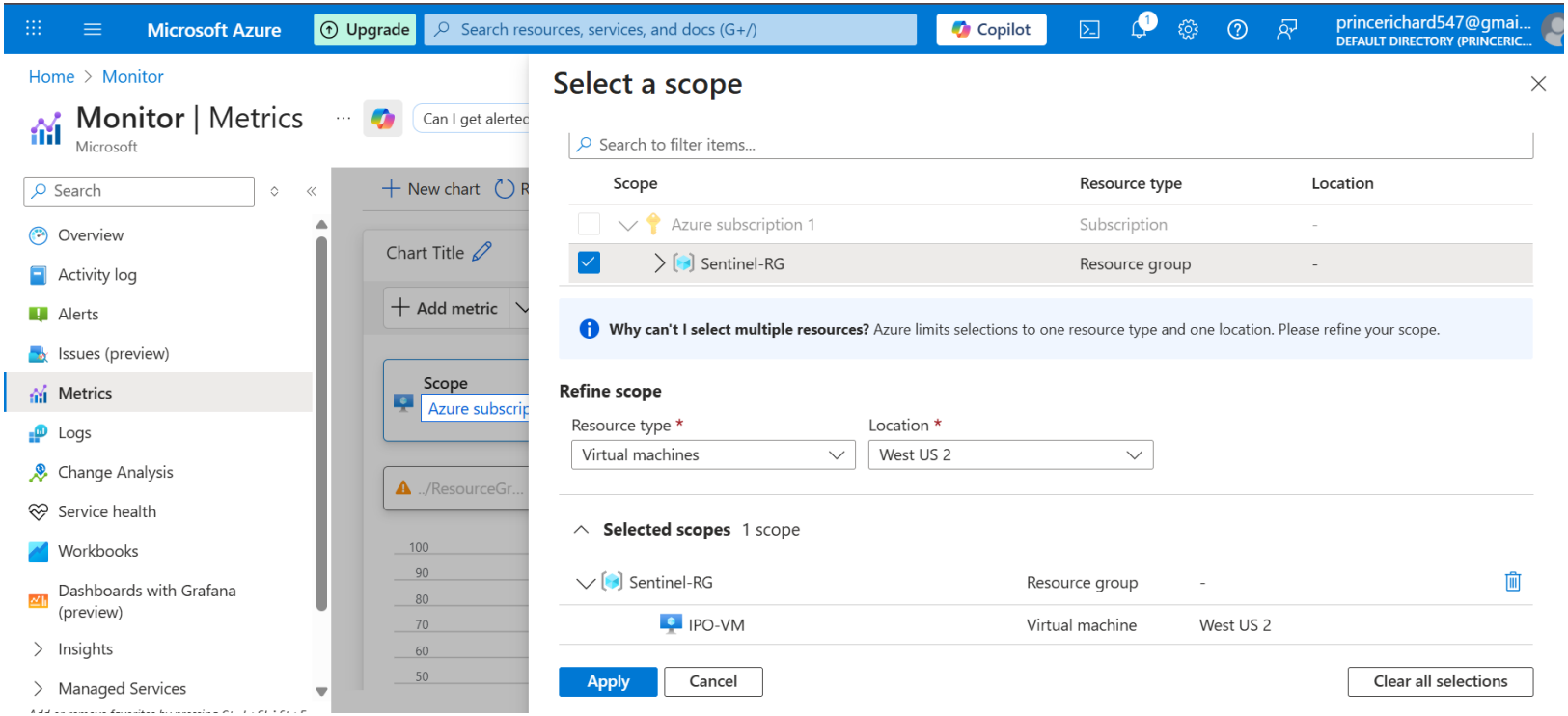
Activity #	Steps
Activity 1: Set the scope in metrics explorer for a subscription or resource group with the VM to monitor.	1. Sign in to the Azure portal with your login credentials. 2. In the global search box, search for and select **Monitor**.

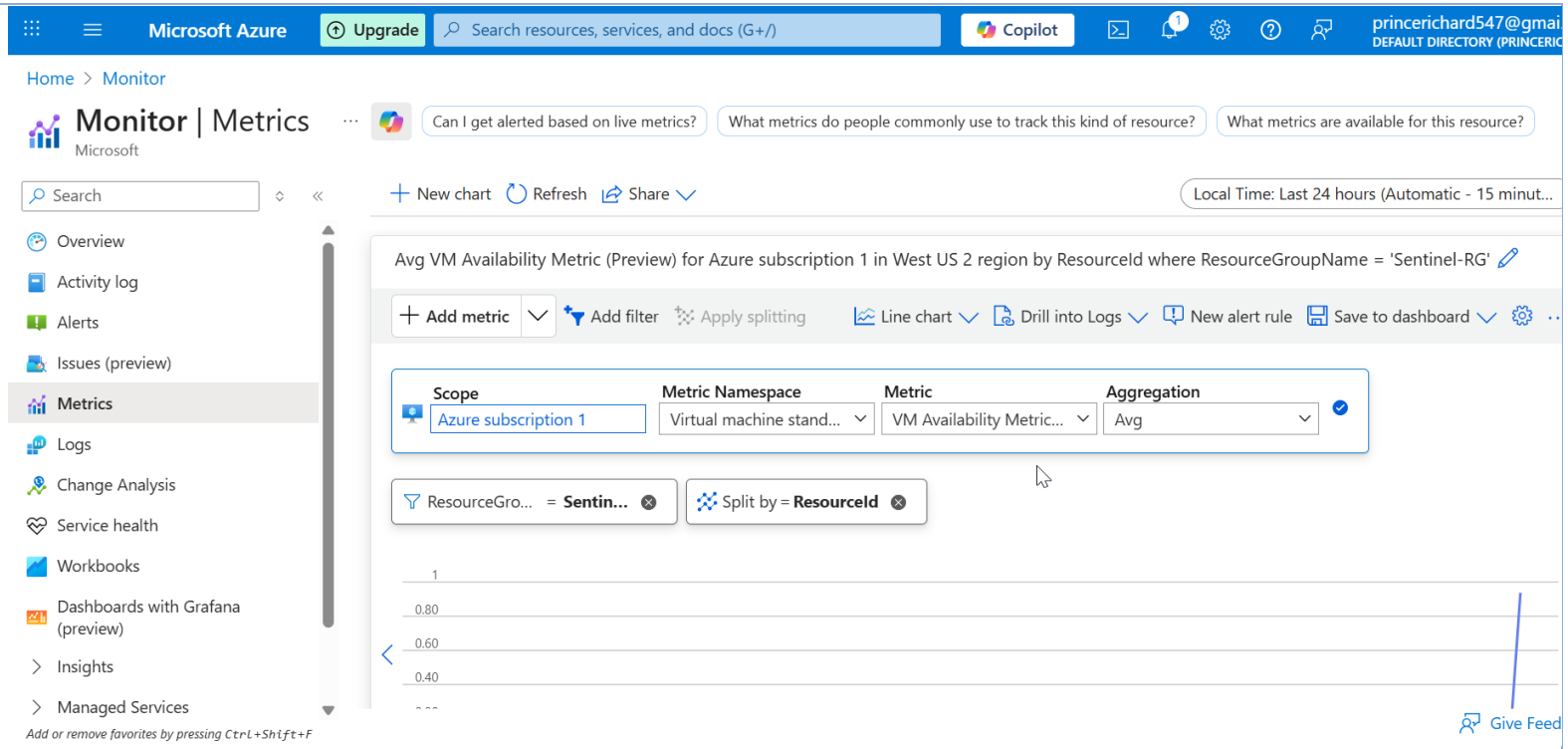


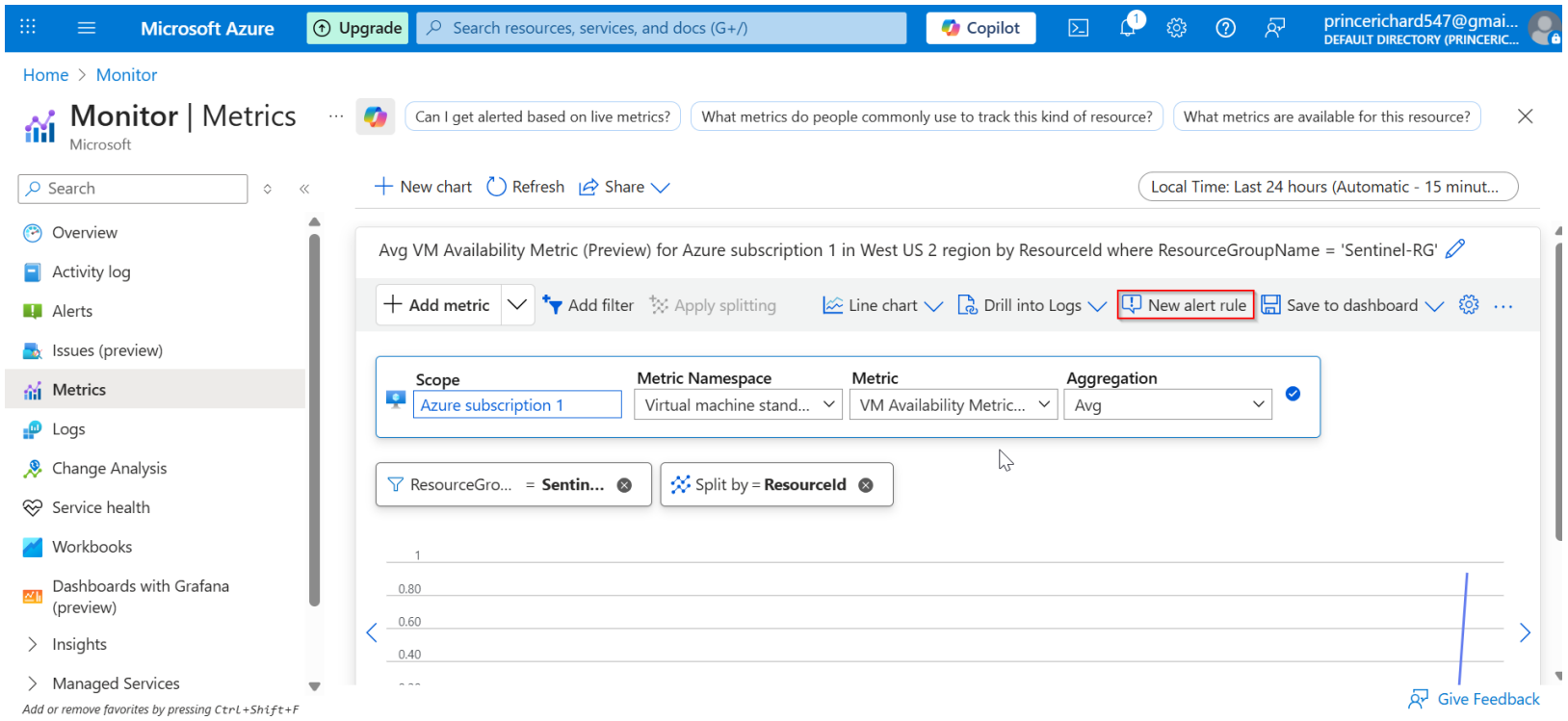
3. Select **Metrics** from the **Monitor** menu.
4. On the **Metrics** page, choose **Select a scope**.
5. In the **Select a scope wizard that appears**, select a subscription or resource group with the VM to monitor.
6. In the **Refine scope section**, from the **Resource type dropdown list**, select **Virtual machines**.
7. Then, select the desired **Location**.
8. Select **Apply** to set the scope in metrics explorer.


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
princerichard547@gmai
DEFAULT DIRECTORY (PRINCERI
Home
Monitor | Overview
Microsoft
Summarize these Monitor services in a table
Catch me up on my alerts
Run an anomaly investigation into my resource
Search
Overview
Activity log
Alerts
Issues (preview)
Metrics
Logs
Change Analysis
Service health
Workbooks
Dashboards with Grafana (preview)
Insights
Managed Services
Add or remove favorites by pressing Ctrl+Shift+F
The Log Analytics agents, used by VM Insights, won't be supported as of August 31, 2024. Plan to migrate to VM Insights on Azure Monitor agent prior to this date.
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 performance and health of your controllers, nodes, and containers.
View
More
VM Insights
Monitor the health, performance, and dependencies of your VMs and VM scale sets.
View
More
Network Insights
View the health and metrics for all deployed network resources.


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
princerichard547@gmai
DEFAULT DIRECTORY (PRINCERIC
Home > Monitor
Monitor | Metrics
Microsoft
Can I get alerted based on live metrics?
What metrics do people commonly use to track this kind of resource?
What metrics are available for this resource?
Search
Overview
Activity log
Alerts
Issues (preview)
Metrics
Logs
Change Analysis
Service health
Workbooks
Dashboards with Grafana (preview)
Insights
Managed Services
New chart
Refresh
Share
Local Time: Last 24 hours (Automatic)
Chart Title
Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Save to dashboard
Scope
Select a scope
Metric Namespace
Select namespace
Metric
Select metric
Aggregation
Select aggregation
100
90
80
70
60
50
40
30
20
Select a metric above to see data appear on this chart or learn more below:
Filter + Split
Apply filters and splits to
Plot multiple metrics
Create charts with multiple
Build custom dashboards
Give Feed


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
princerichard547@gmai...
DEFAULT DIRECTORY (PRINCERIC...
Home > Monitor
Monitor | Metrics
Microsoft
Search
Overview
Activity log
Alerts
Issues (preview)
Metrics
Logs
Change Analysis
Service health
Workbooks
Dashboards with Grafana (preview)
Insights
Managed Services
New chart
Chart Title
Add metric
Scope
Azure subscrip
../ResourceGr...
100
90
80
70
60
50
Select a scope
Search to filter items...
Scope
Resource type
Location
Azure subscription 1
Subscription
Sentinel-RG
Resource group
Why can't I select multiple resources? Azure limits selections to one resource type and one location. Please refine your scope.
Refine scope
Resource type *
Virtual machines
Location *
West US 2
Selected scopes 1 scope
Sentinel-RG
Resource group
IPO-VM
Virtual machine
West US 2
Apply
Cancel
Clear all selections

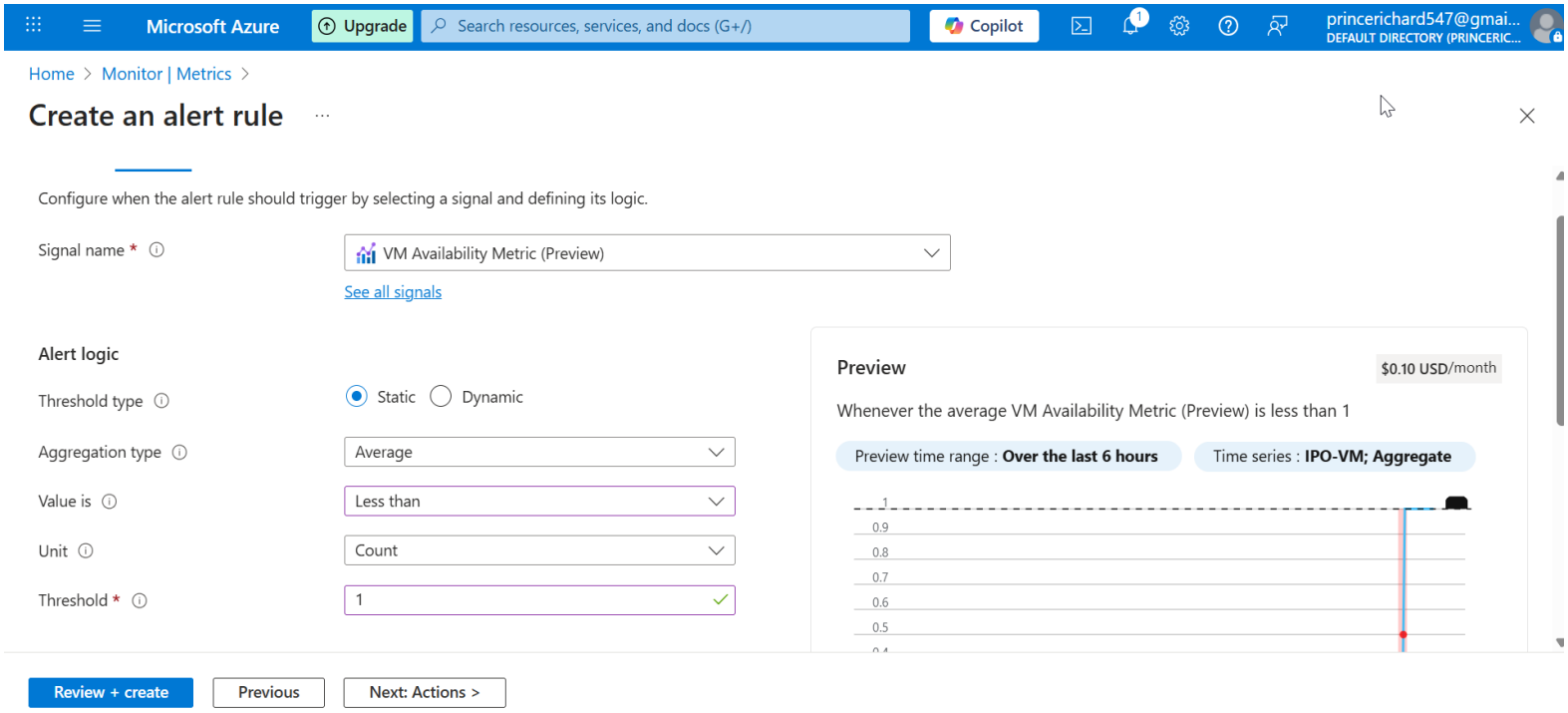
	
Activity 2: Create an alert rule and action group.	1. On the **Metrics** page, from the **Metric** dropdown list, select ***VM Availability Metric (Preview)***. 2. Then, select **New alert rule** to create an alert rule.



3. On the **Create an alert rule** page, select the **Condition** tab.
4. In the **Alert logic** section, set the following values:

Setting	**Value**
Threshold	Static
Aggregation type	Average
Operator	Greater than
Unit	Count
Threshold value	1

Note: The alert logic specifies that an alert should fire whenever the average value of the availability metric falls below 1, indicating that the VM in the selected scope isn't functional.

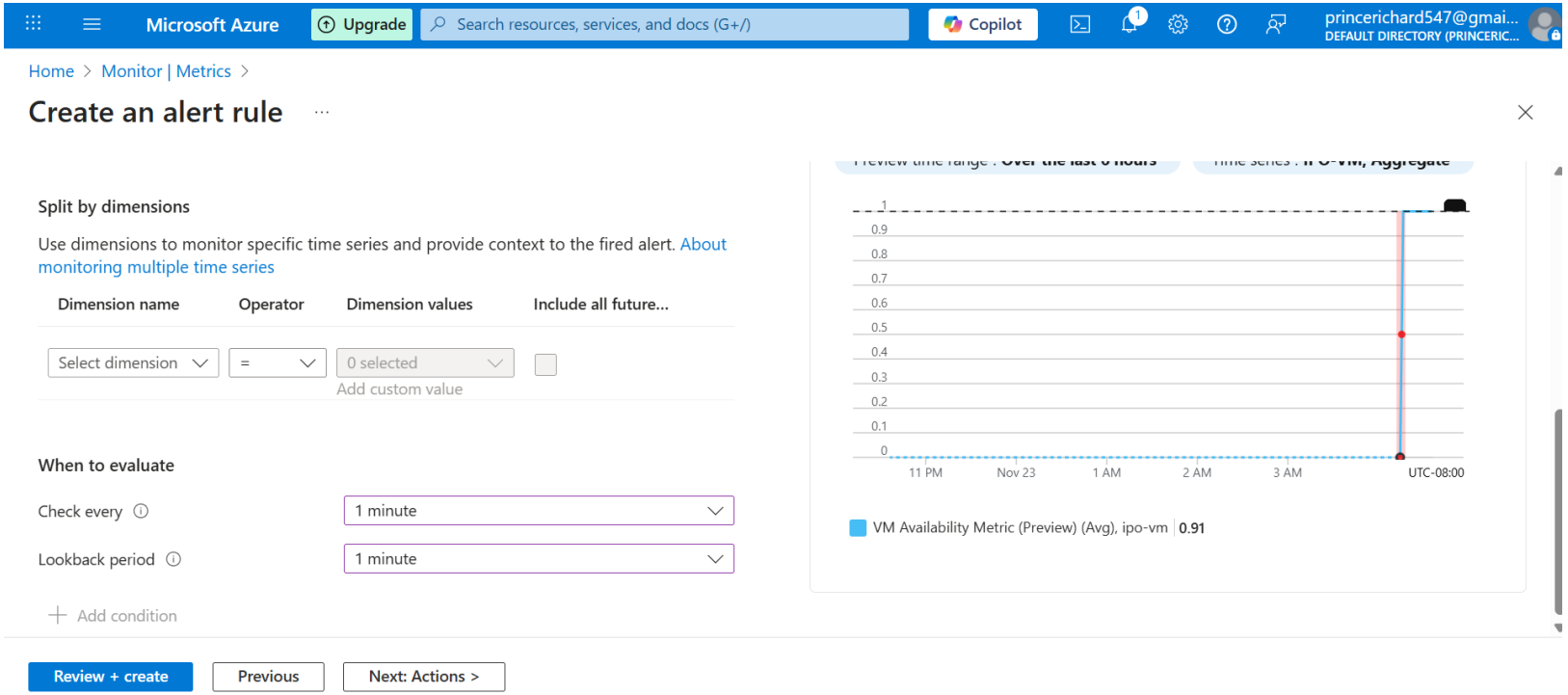


5. In the **When to evaluate section,** set the following values:

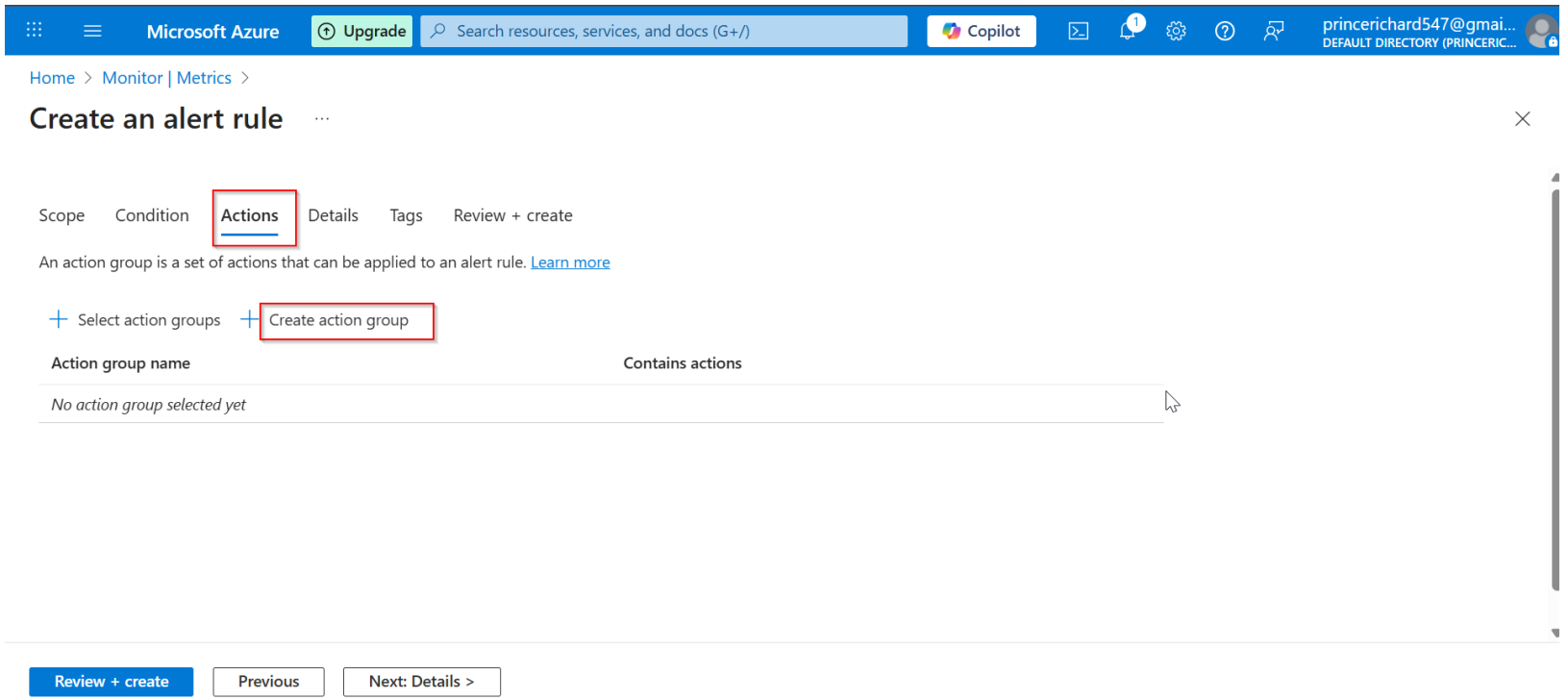
Setting	Value
Check every	1 minute
Loopback period	1 minute

Note: These values specify that the alert rule will check the log data every minute to identify issues with the specified VM.

6. Select **Next: Actions** to move to the **Actions** tab.
Note: The **Actions** tab allows you to add one or more action groups to the alert rule. Action groups define a set of actions to take when an alert is fired, such as sending an email or an SMS.

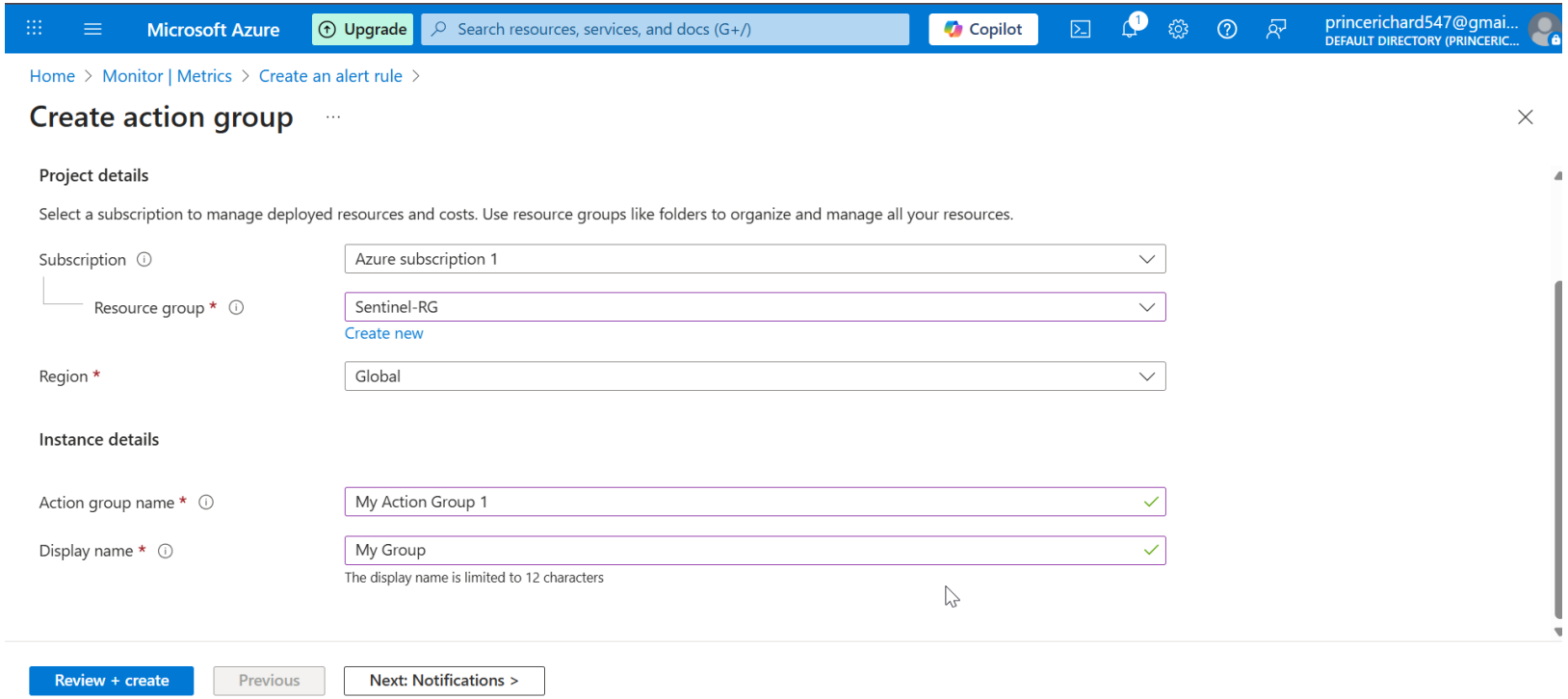


7. On the **Actions** tab, select **Create action group**.

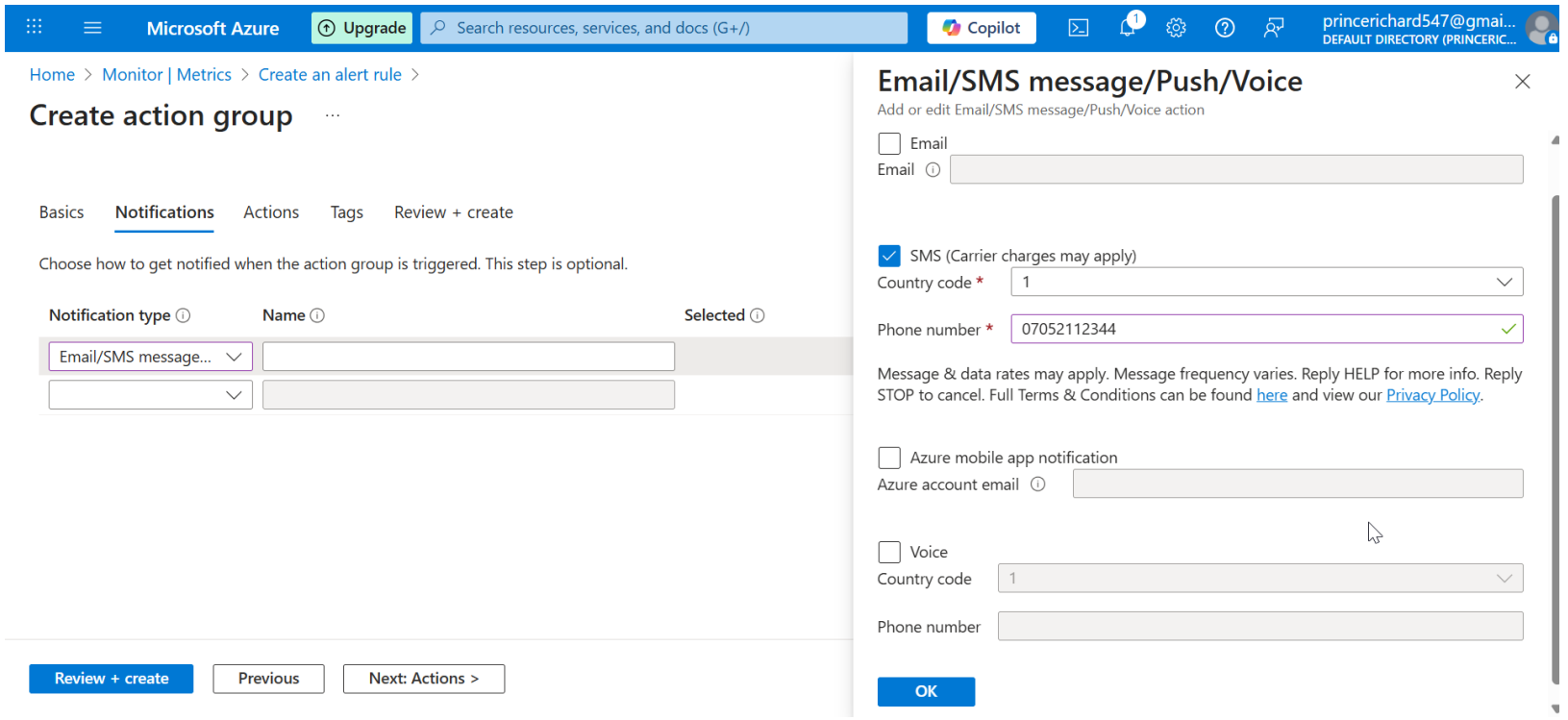


Note: If you already have an action group, choose **Select action groups** to add an existing group to the alert rule instead of creating a new one.

8. On the **Create action group** page, on the **Basics** tab, in the **Project details** sections, select a **Subscription** and **Resource group** for the action group.
9. Next, select the region.
10. Then, in the **Instance details** section, enter the **Action group name and the Display name.**
    Note: The action group name will appear on the Azure portal, and the **Display name** will appear in email and SMS notifications.
11. Select **Next: Notifications**.

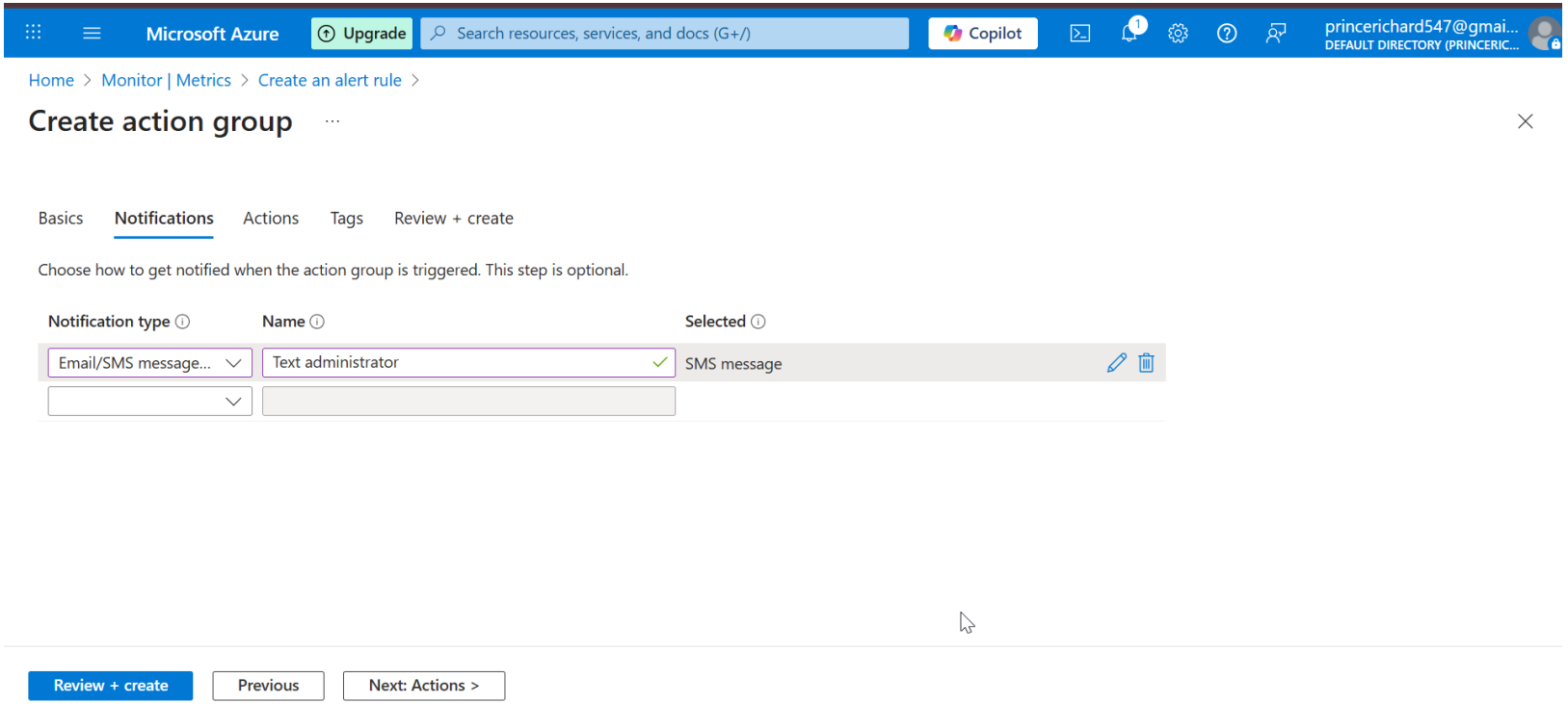


12. On the **Notifications** tab, from the **Notification type** dropdown list, select **Email/SMS message/Push/Voice**.
13. In the **Email/SMS message/Push/Voice** wizard that appears, select **SMS**, enter the mandatory details, and then select **OK**.

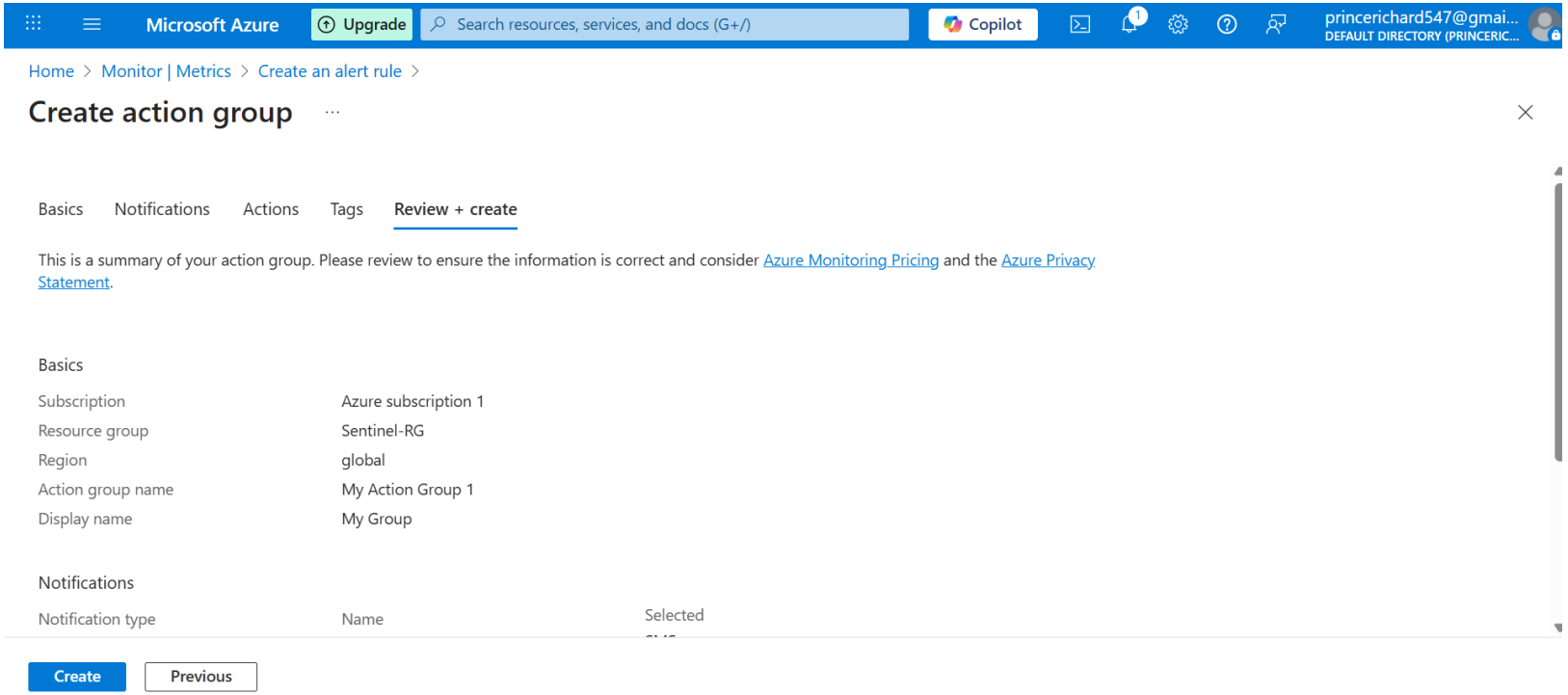


Note: The selected notification type is displayed in the **Selected** field.

14. Then, in the **Name** box, specify the people to be notified when the alert is fired.
15. Select **Review + create**.



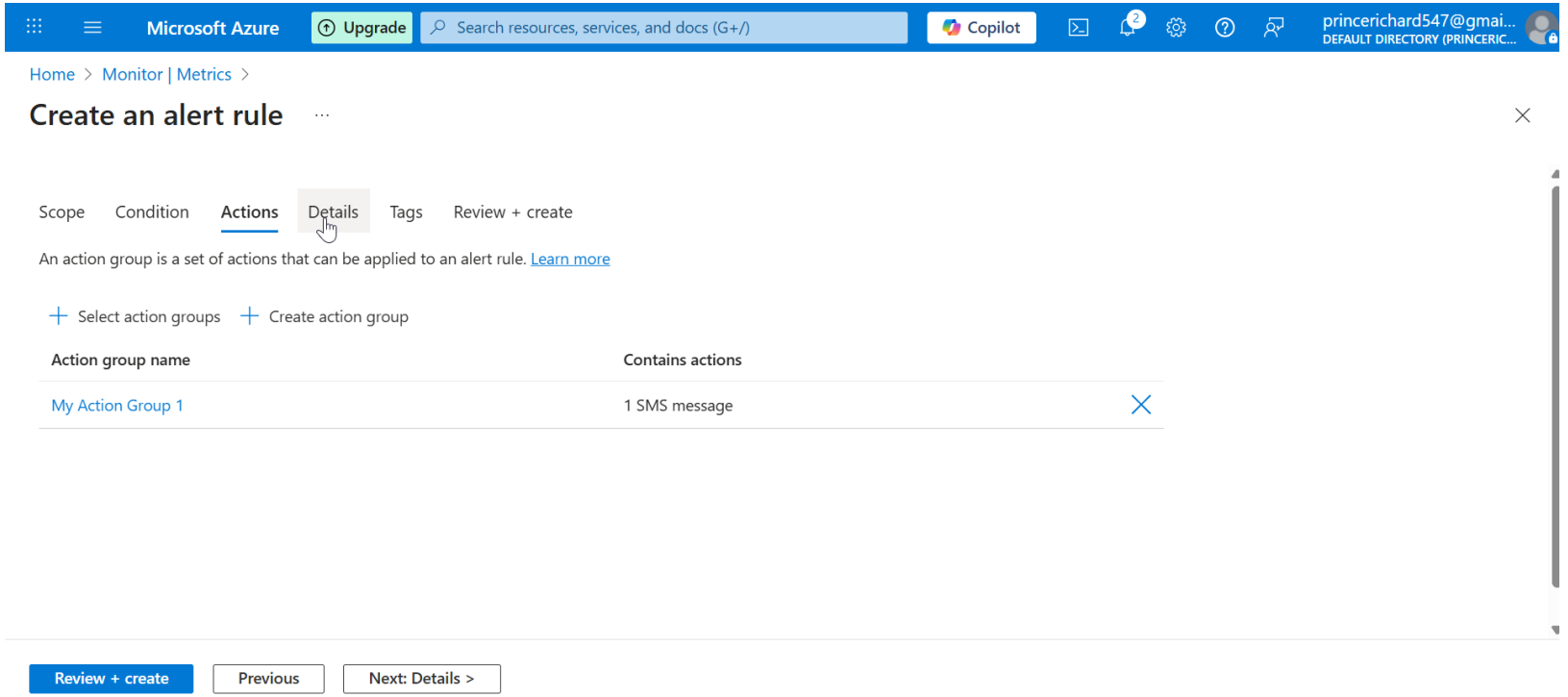
16. Review the details on the **Review + create** tab, and select **Create** to create the action group.

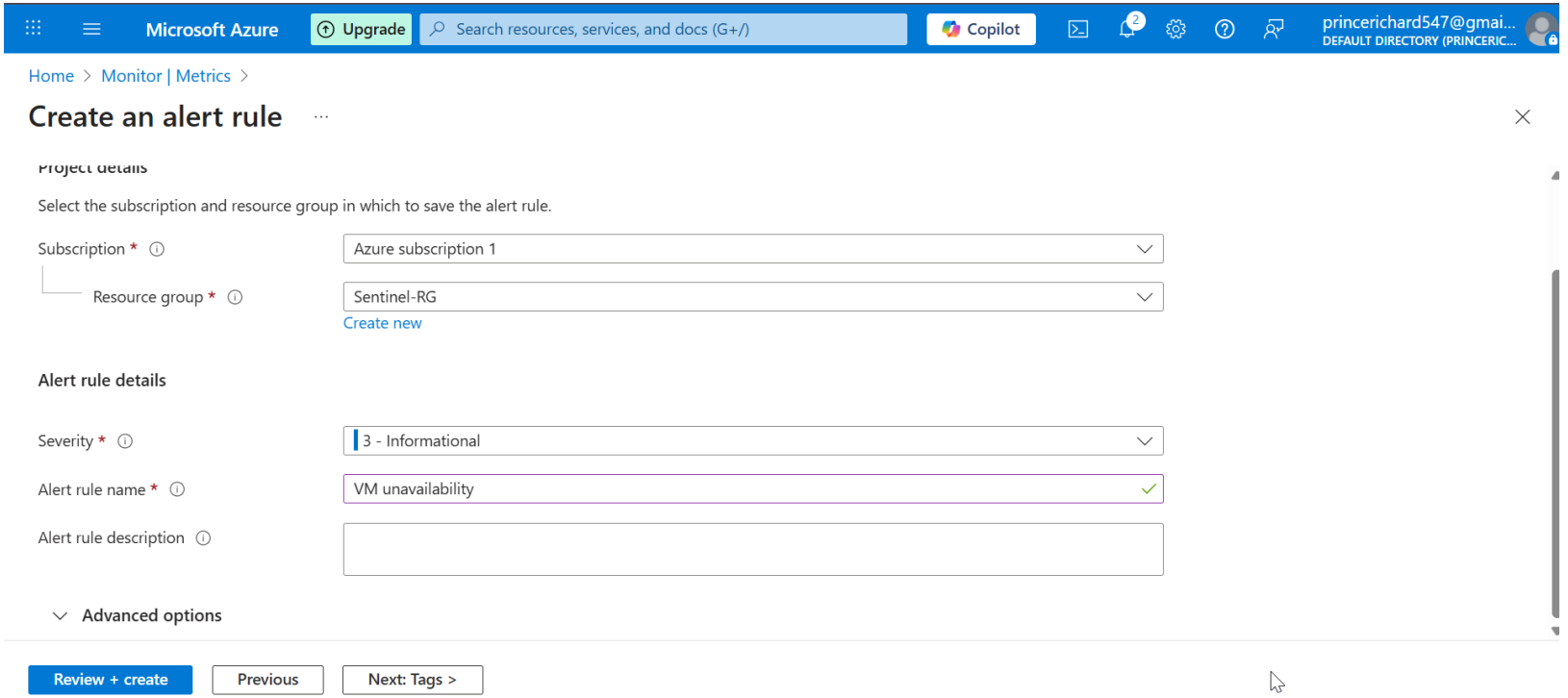


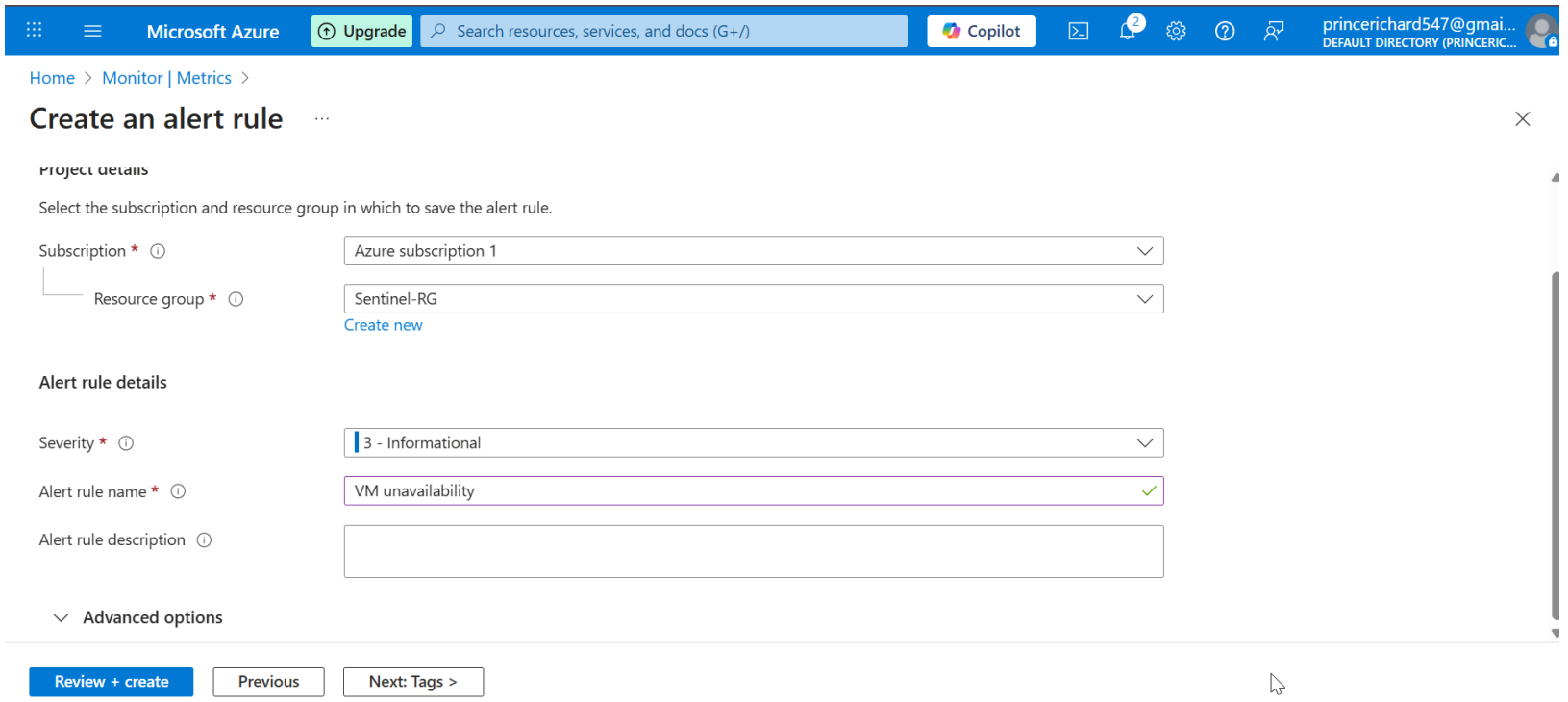
17. Then, navigate to the **Create an alert rule** page.
18. On the **Details** tab, configure the settings:

Setting	**Description**
Subscription	Select the desired subscription.
Resource group	Select the desired resource group.
Severity	Select a desired severity.
Alert rule name	VM unavailability
Alert rule description	Enter an optional description for the alert rule.

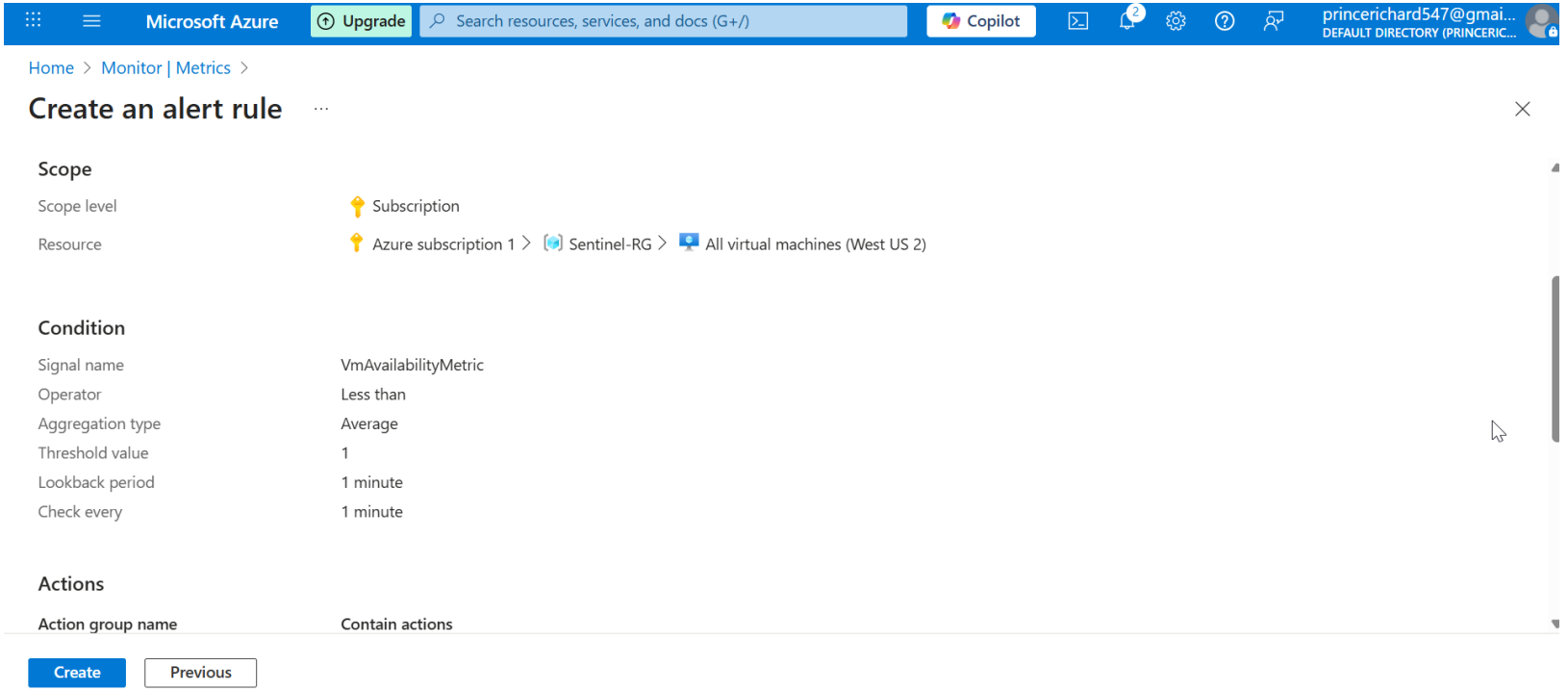
19. Then, select **Review + create**.

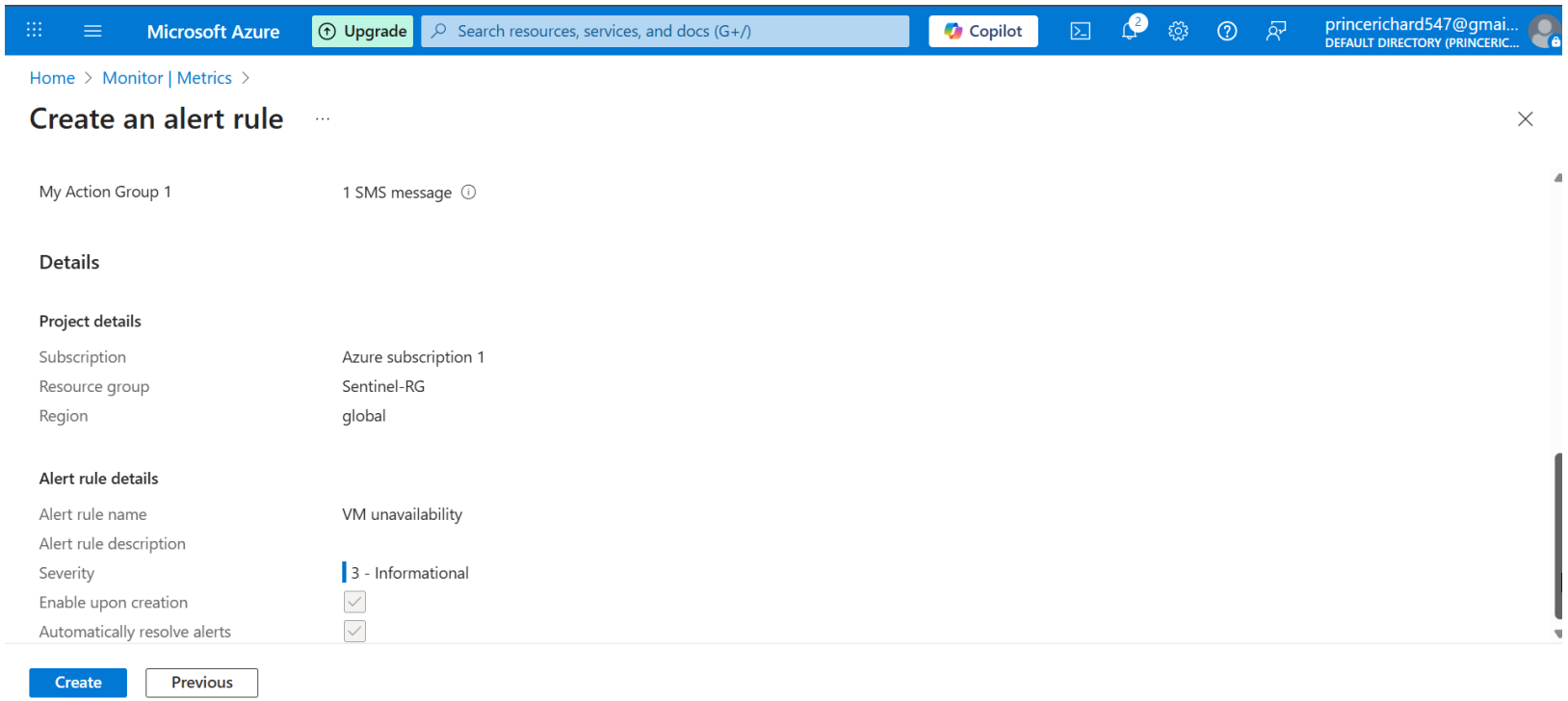

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
princerichard547@gmai...
DEFAULT DIRECTORY (PRINCERIC...
Home > Monitor | Metrics >
Create an alert rule
Scope
Condition
Actions
Details
Tags
Review + create
An action group is a set of actions that can be applied to an alert rule. Learn more
Select action groups
Create action group
Action group name
Contains actions
My Action Group 1
1 SMS message
Review + create
Previous
Next: Details >


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
princerichard547@gmai...
DEFAULT DIRECTORY (PRINCERIC...
Home > Monitor | Metrics >
Create an alert rule
Project details
Select the subscription and resource group in which to save the alert rule.
Subscription *
Azure subscription 1
Resource group *
Sentinel-RG
Create new
Alert rule details
Severity *
3 - Informational
Alert rule name *
VM unavailability
Alert rule description
Advanced options
Review + create
Previous
Next: Tags >

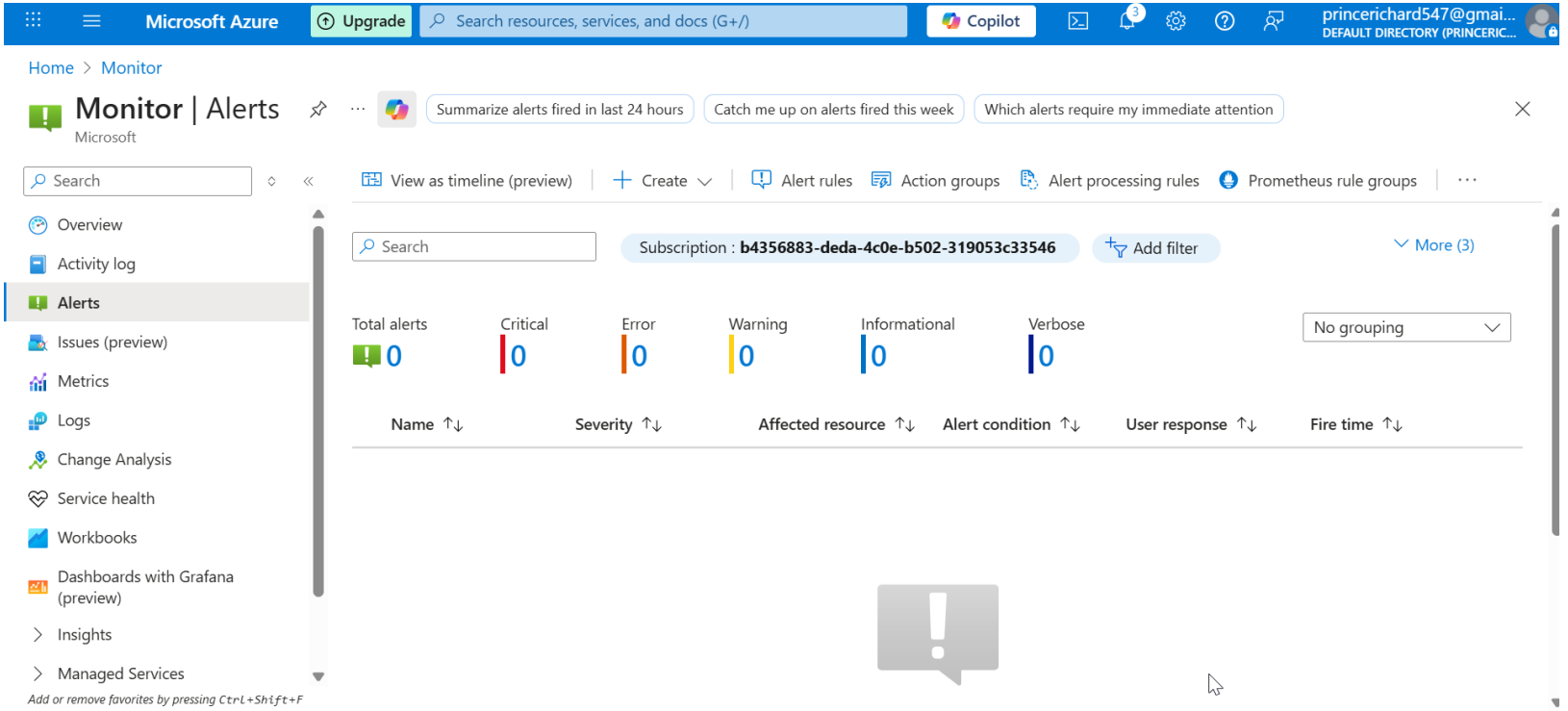


20. On the **Review + create** tab, select **Create** to create the alert rule.

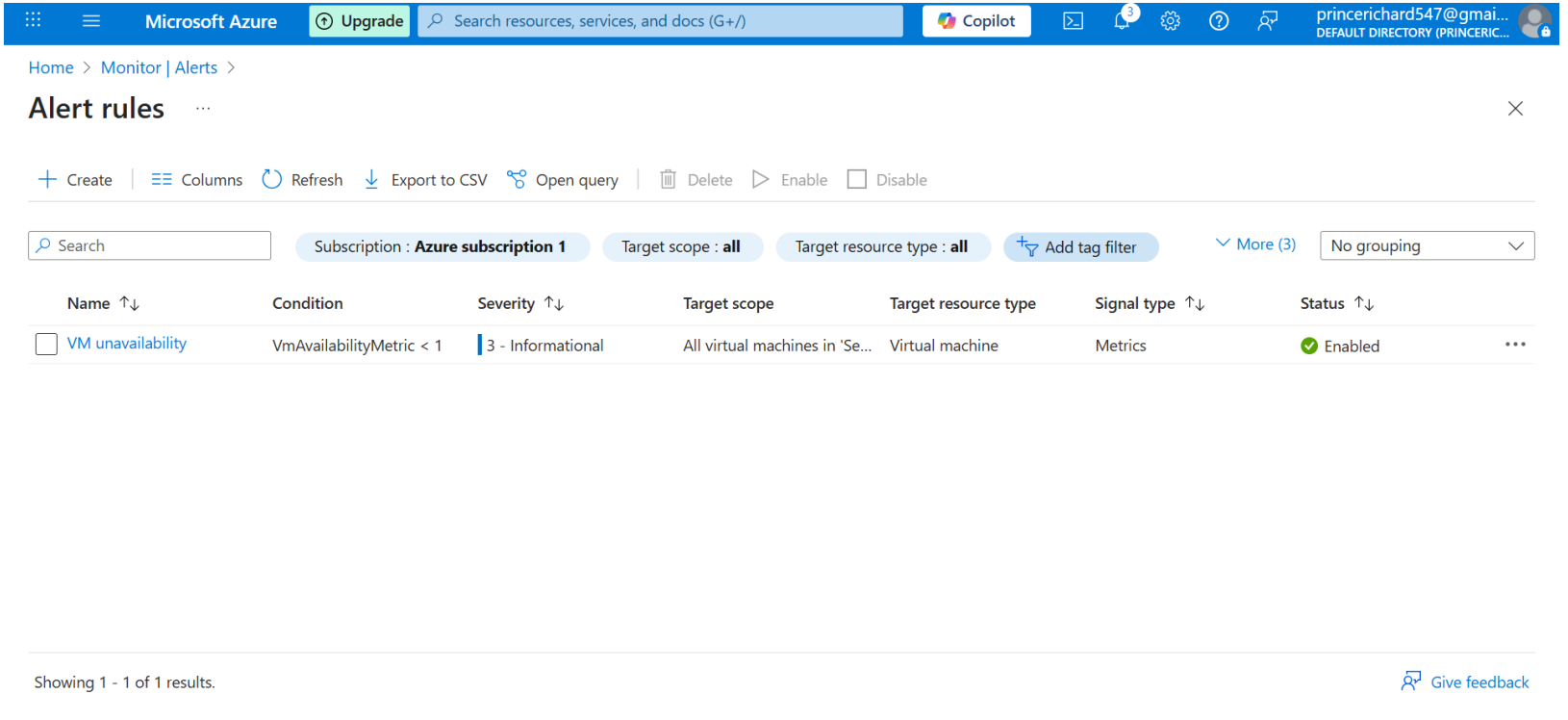

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
princerichard547@gmai...
DEFAULT DIRECTORY (PRINCERIC...
Home > Monitor | Metrics >
Create an alert rule
Scope
Scope level
Subscription
Resource
Azure subscription 1 > Sentinel-RG > All virtual machines (West US 2)
Condition
Signal name
VmAvailabilityMetric
Operator
Less than
Aggregation type
Average
Threshold value
1
Lookback period
1 minute
Check every
1 minute
Actions
Action group name
Contain actions
Create
Previous



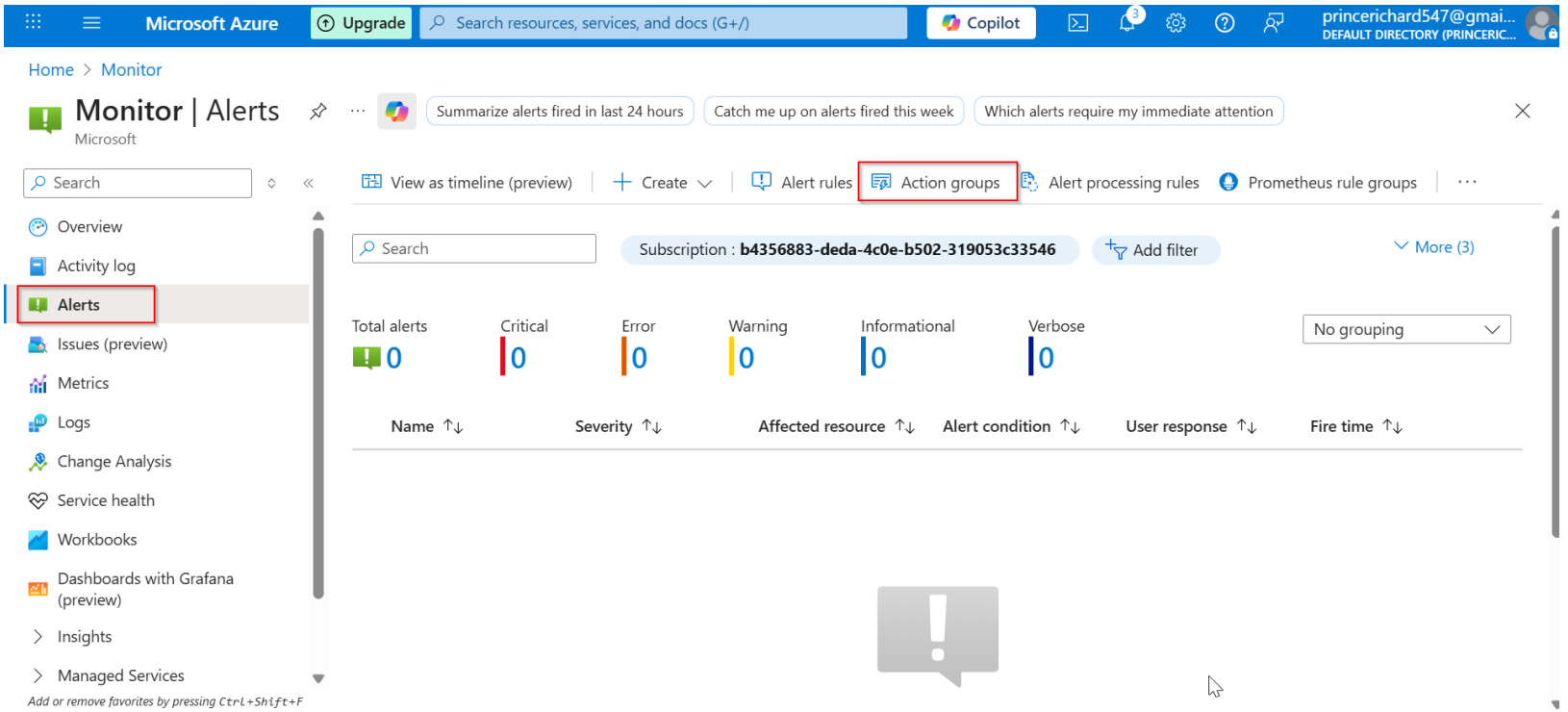
21. To view the alert rule, navigate to the **Monitor** homepage, and select **Alerts** from the menu.
22. Then, select **Alert rules**.



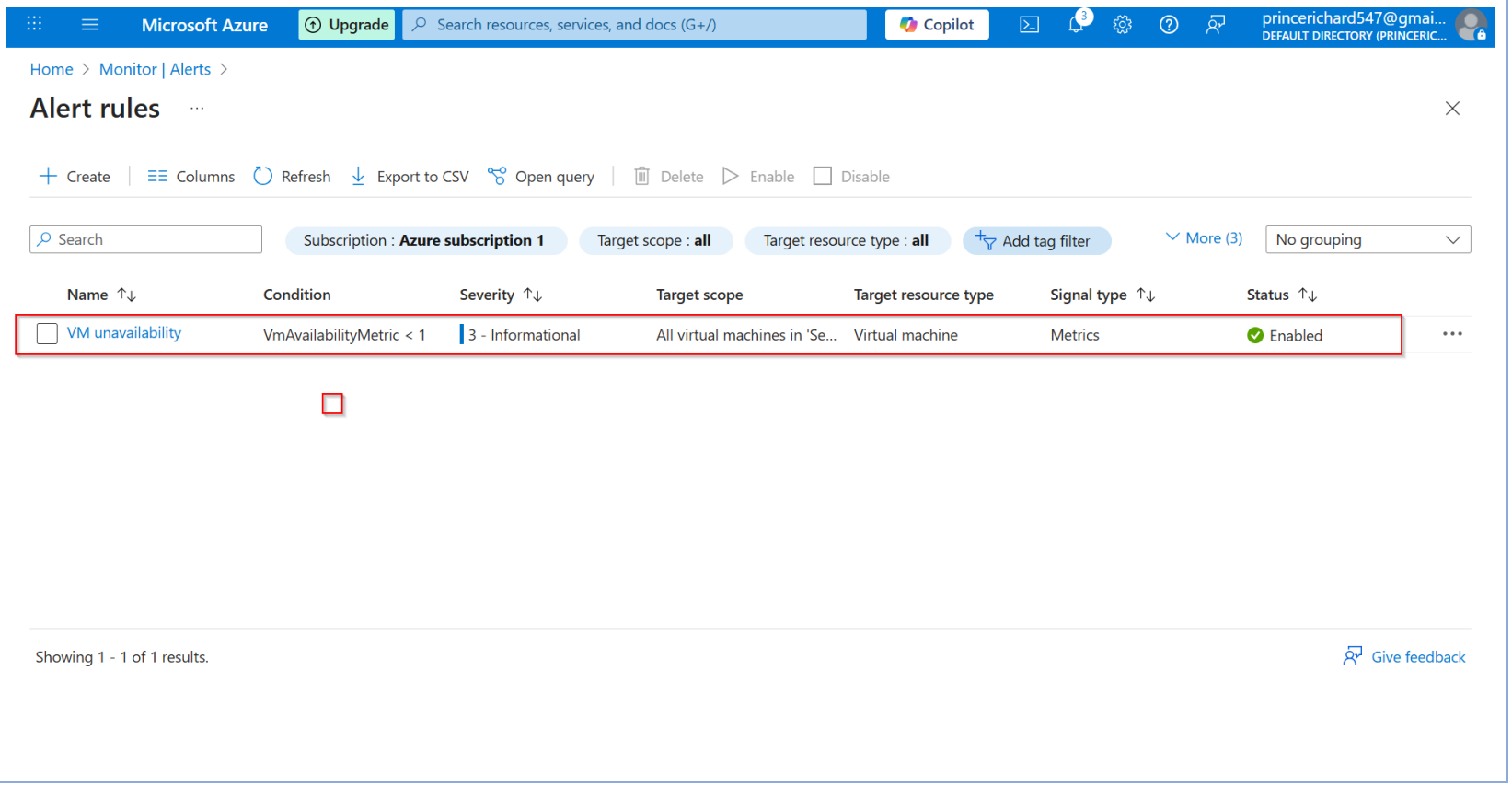
23. On the **Alert rules** page, view the alert rule created.



24. To view the action group, navigate to the **Monitor** homepage, and select **Alerts** from the menu.
25. Then, select **Action groups**.



26. On the **Action groups** page, view the action group created.



Outcome

The monitoring pipeline ensures rapid awareness of VM outages, improving service reliability, reducing response time, and enhancing operational resilience.

Skills Demonstrated

- SIEM Configuration & Operations
- Cloud Security Monitoring
- Threat Detection Engineering
- Scheduled Analytics Rule Development

- Threat Intelligence Integration
- KQL Reading & Interpretation
- Automation Workflow Configuration
- Cloud Reliability Engineering
- Alerting & Incident Response
- Technical Reporting & Documentation

Conclusion

This project successfully integrates threat detection, cloud observability, and automated response capabilities within Microsoft Azure. By combining Sentinel analytics with Azure Monitor alerting pipelines, it demonstrates practical SOC-ready expertise, the ability to engineer detections aligned with real-world threats, and the operational mindset required for security engineering and cloud monitoring roles.