AZ-500 Course 3 – Manage Security Operations – updated 2-6-22

COURSE

Microsoft Azure Security Technologies (AZ-500) Cert Prep: 3 Manage Security Operations

LinkedIn Learning · By: Pete Zerger · 2 months ago

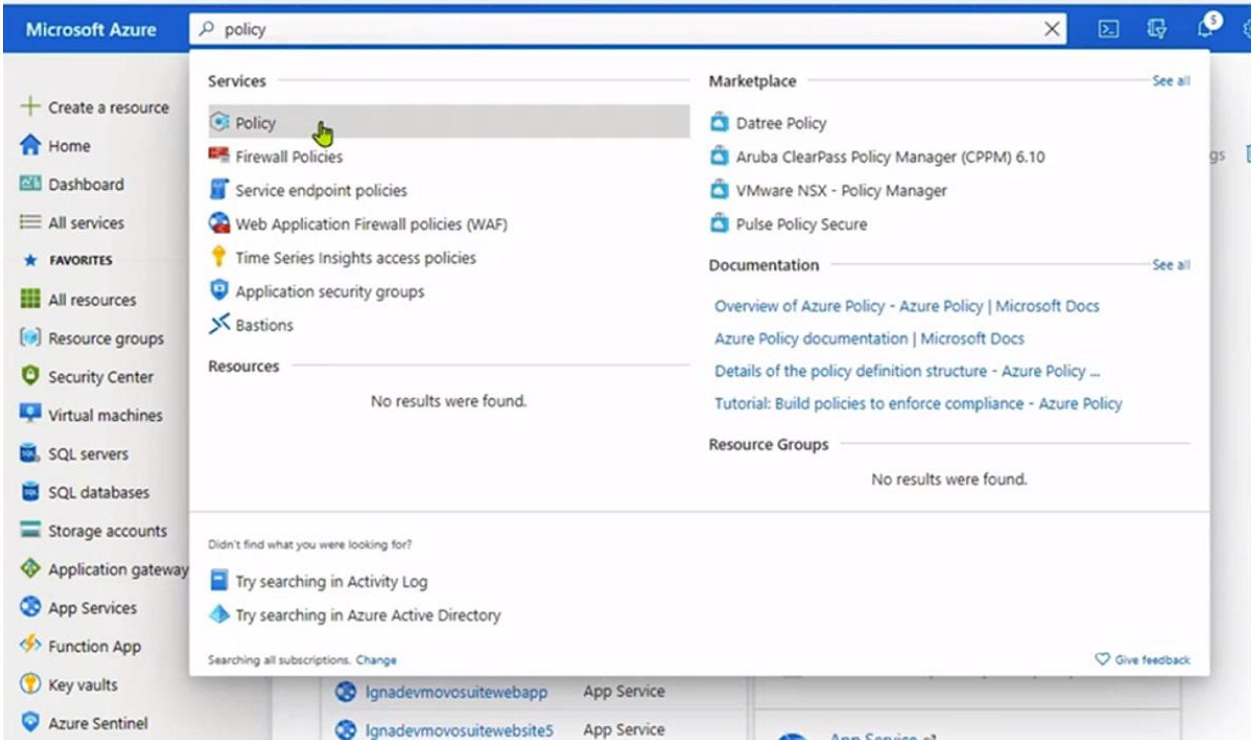
Start your preparations for the "Manage security operations" domain of the AZ-500 exam.

[Become an Azure Security Engineer (linkedin.com)](https://www.linkedin.com)

Table of Contents

1. Configure Centralized Policy Management

1.1 Configure a custom security policy



Microsoft Azure

policy

Services

- Policy
- Firewall Policies
- Service endpoint policies
- Web Application Firewall policies (WAF)
- Time Series Insights access policies
- Application security groups
- Bastions

Resources

No results were found.

Marketplace — See all

- Datree Policy
- Aruba ClearPass Policy Manager (CPPM) 6.10
- VMware NSX - Policy Manager
- Pulse Policy Secure

Documentation — See all

- Overview of Azure Policy - Azure Policy | Microsoft Docs
- Azure Policy documentation | Microsoft Docs
- Details of the policy definition structure - Azure Policy ...
- Tutorial: Build policies to enforce compliance - Azure Policy

Resource Groups

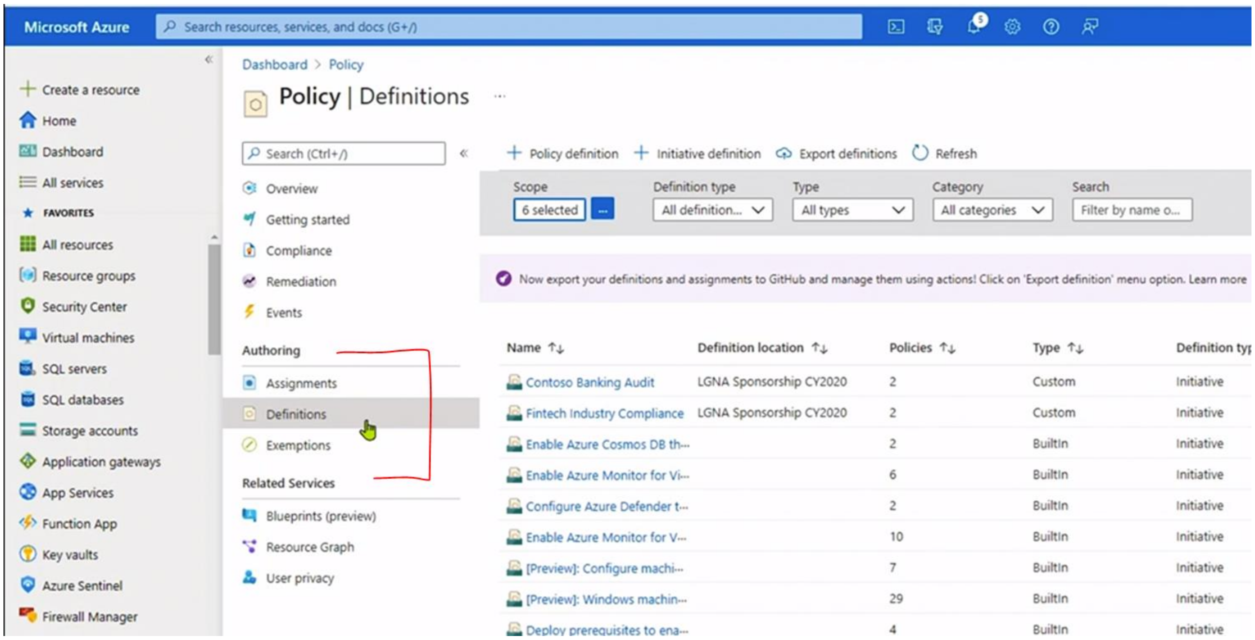
No results were found.

Didn't find what you were looking for?

- Try searching in Activity Log
- Try searching in Azure Active Directory

Searching all subscriptions. Change

Give feedback



Microsoft Azure

Search resources, services, and docs (G+/)

Dashboard > Policy

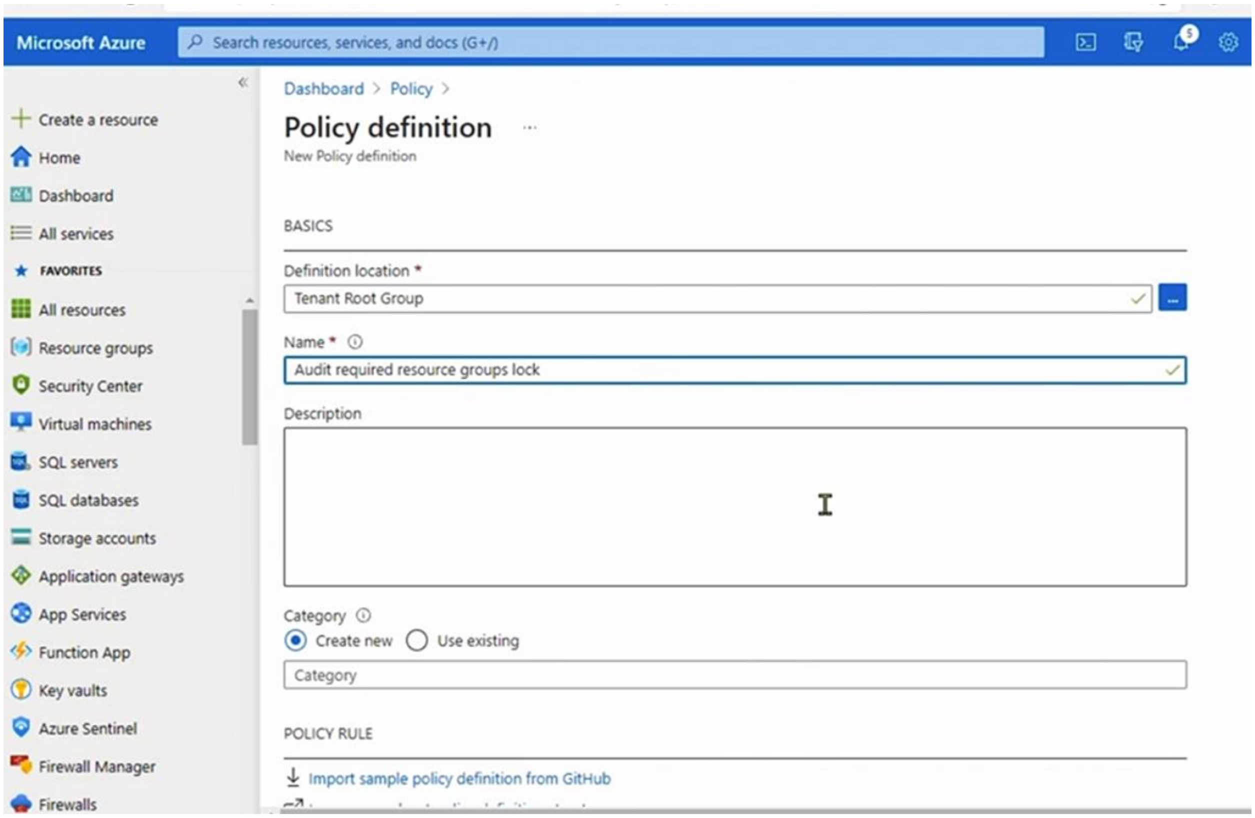
Policy | Definitions

+ Policy definition | + Initiative definition | Export definitions | Refresh

Scope: 6 selected | Definition type: All definition... | Type: All types | Category: All categories | Search: Filter by name o...

Now export your definitions and assignments to GitHub and manage them using actions! Click on 'Export definition' menu option. Learn more

Name ↑↓	Definition location ↑↓	Policies ↑↓	Type ↑↓	Definition typ
Contoso Banking Audit	LGNA Sponsorship CY2020	2	Custom	Initiative
Fintech Industry Compliance	LGNA Sponsorship CY2020	2	Custom	Initiative
Enable Azure Cosmos DB th...		2	BuiltIn	Initiative
Enable Azure Monitor for Vi...		6	BuiltIn	Initiative
Configure Azure Defender t...		2	BuiltIn	Initiative
Enable Azure Monitor for V...		10	BuiltIn	Initiative
[Preview]: Configure machi...		7	BuiltIn	Initiative
[Preview]: Windows machin...		29	BuiltIn	Initiative
Deploy prerequisites to ena...		4	BuiltIn	Initiative



Policy definition

New Policy definition

BASICS

Definition location *: Tenant Root Group

Name *: Audit required resource groups lock

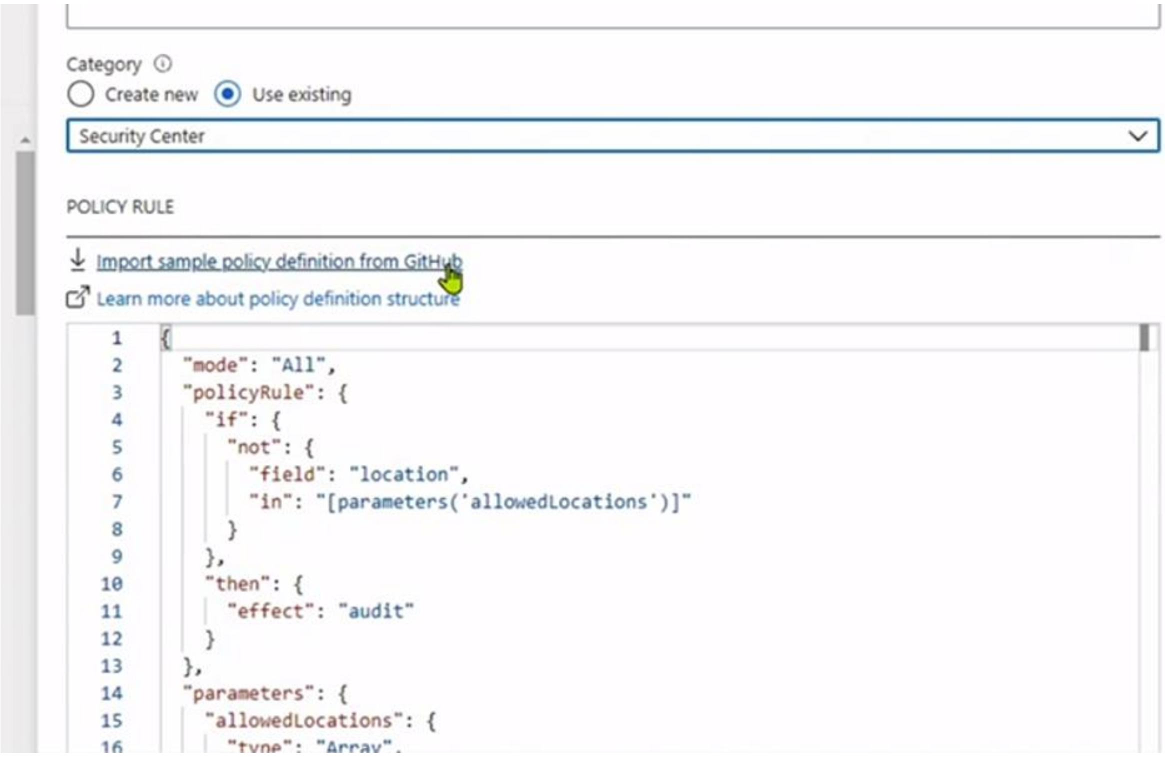
Description

Category: ● Create new ○ Use existing

Category

POLICY RULE

Import sample policy definition from GitHub



Category: ○ Create new ● Use existing

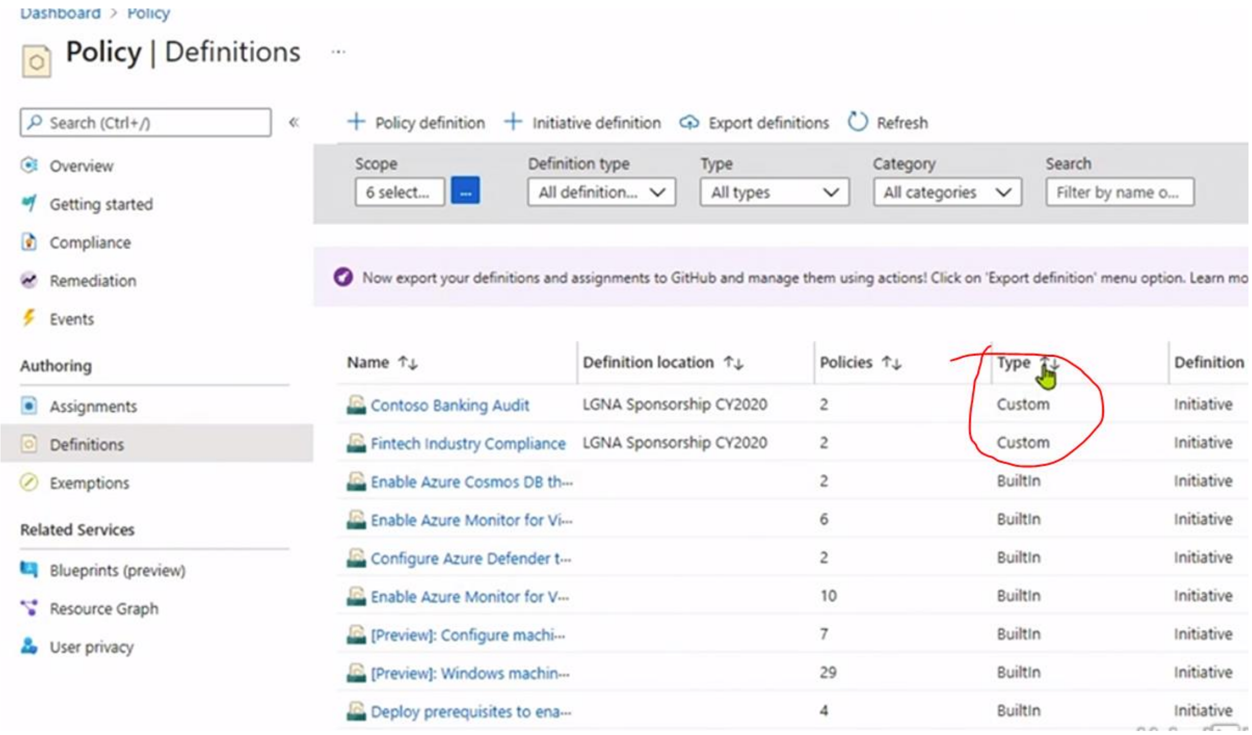
Security Center

POLICY RULE

Import sample policy definition from GitHub

Learn more about policy definition structure

```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "not": {
        "field": "location",
        "in": "[parameters('allowedLocations')]"
      }
    },
    "then": {
      "effect": "audit"
    }
  },
  "parameters": {
    "allowedLocations": {
      "type": "Array",
```



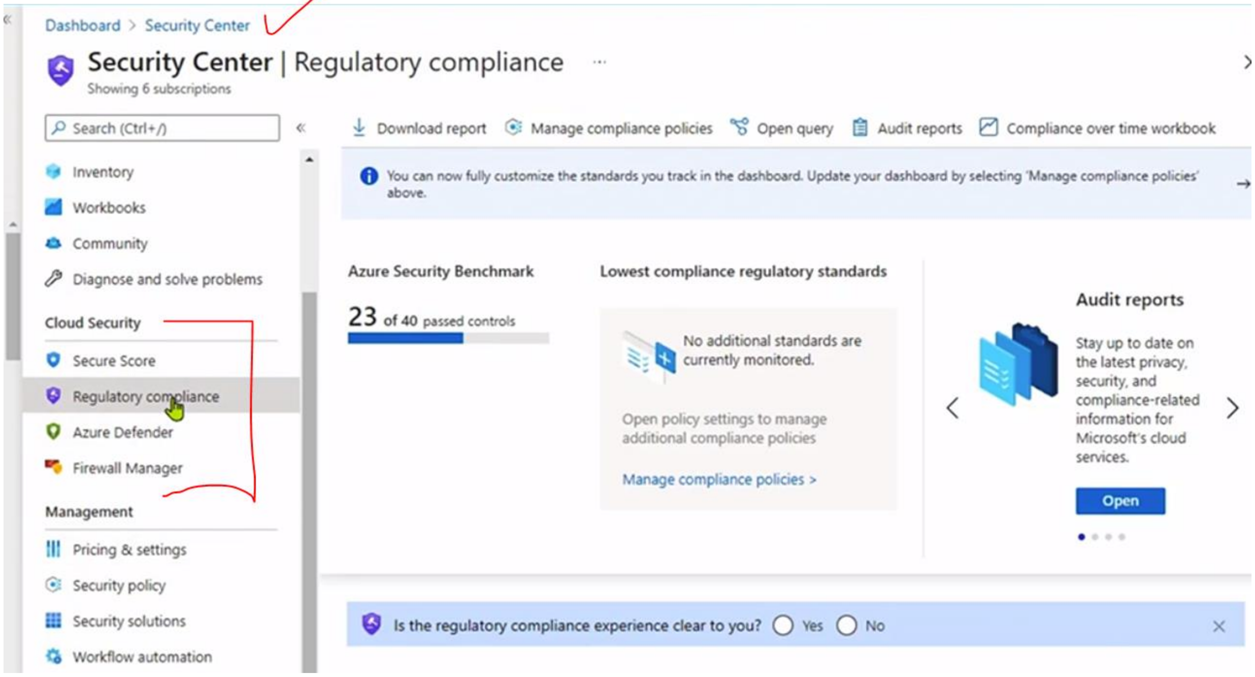
Dashboard > Policy

Policy | Definitions

Scope: 6 select... | Definition type: All definition... | Type: All types | Category: All categories | Search: Filter by name o...

Now export your definitions and assignments to GitHub and manage them using actions! Click on 'Export definition' menu option. Learn mo

Name ↑↓	Definition location ↑↓	Policies ↑↓	Type ↑↓	Definition
Contoso Banking Audit	LGNA Sponsorship CY2020	2	Custom	Initiative
Fintech Industry Compliance	LGNA Sponsorship CY2020	2	Custom	Initiative
Enable Azure Cosmos DB th...		2	BuiltIn	Initiative
Enable Azure Monitor for Vi...		6	BuiltIn	Initiative
Configure Azure Defender t...		2	BuiltIn	Initiative
Enable Azure Monitor for V...		10	BuiltIn	Initiative
[Preview]: Configure machi...		7	BuiltIn	Initiative
[Preview]: Windows machin...		29	BuiltIn	Initiative
Deploy prerequisites to ena...		4	BuiltIn	Initiative



Dashboard > Security Center

Security Center | Regulatory compliance

Showing 6 subscriptions

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.

Azure Security Benchmark

23 of 40 passed controls

Lowest compliance regulatory standards

No additional standards are currently monitored.

Open policy settings to manage additional compliance policies

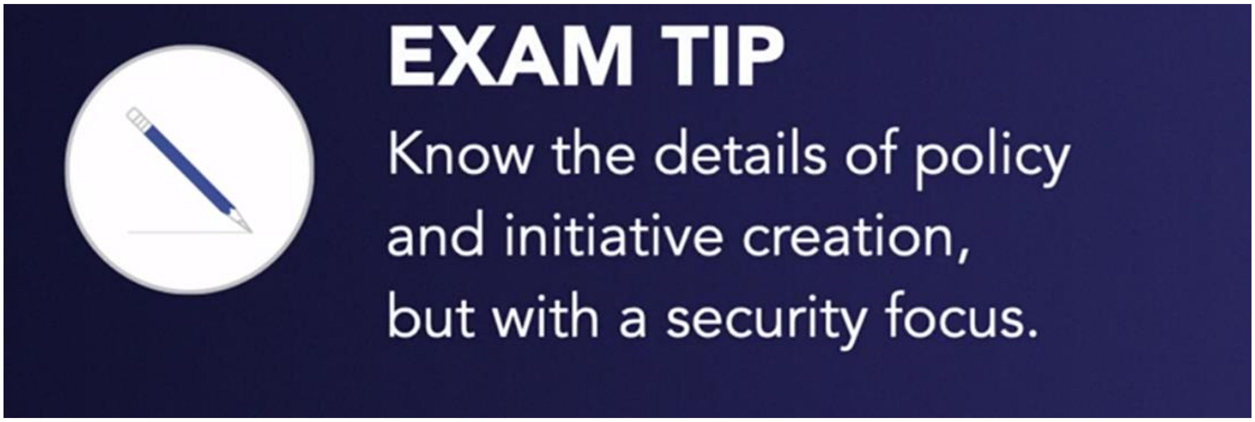
Manage compliance policies >

Audit reports

Stay up to date on the latest privacy, security, and compliance-related information for Microsoft's cloud services.

Open

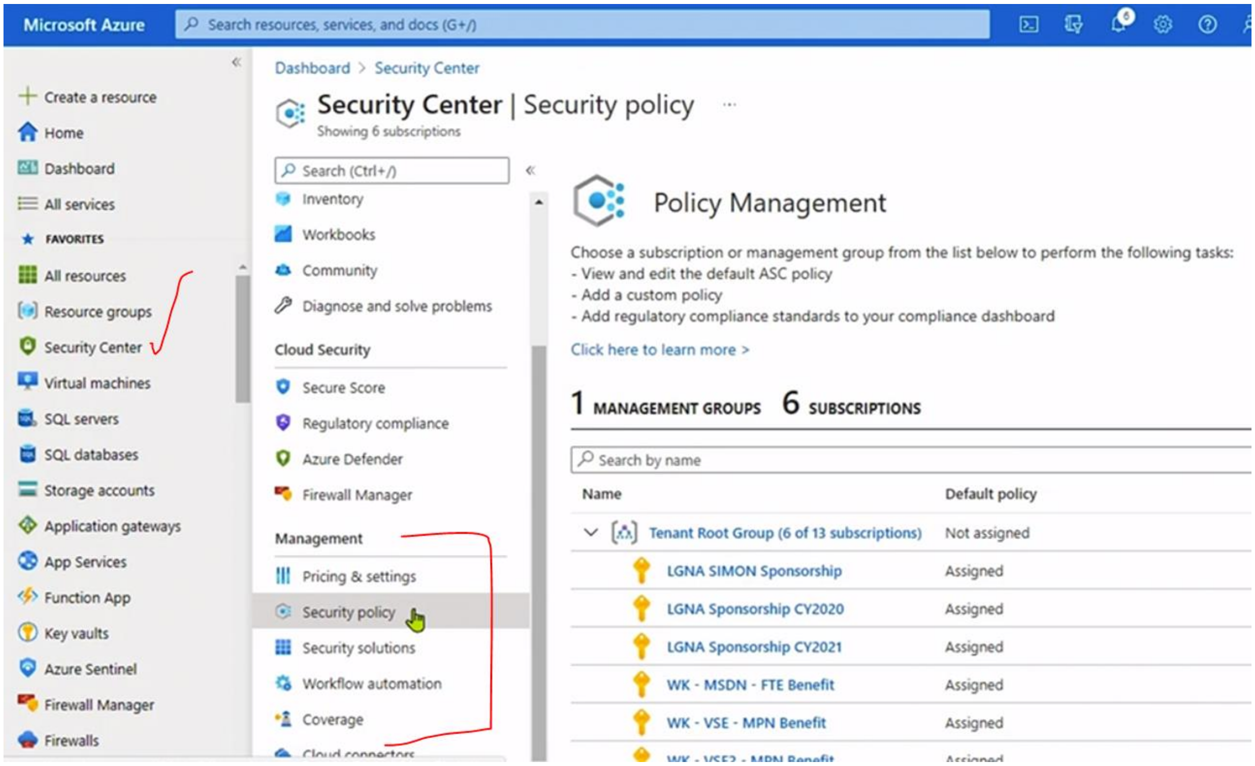
Is the regulatory compliance experience clear to you? ○ Yes ○ No



EXAM TIP

Know the details of policy and initiative creation, but with a security focus.

1.2 Create a policy initiative



Policy Management

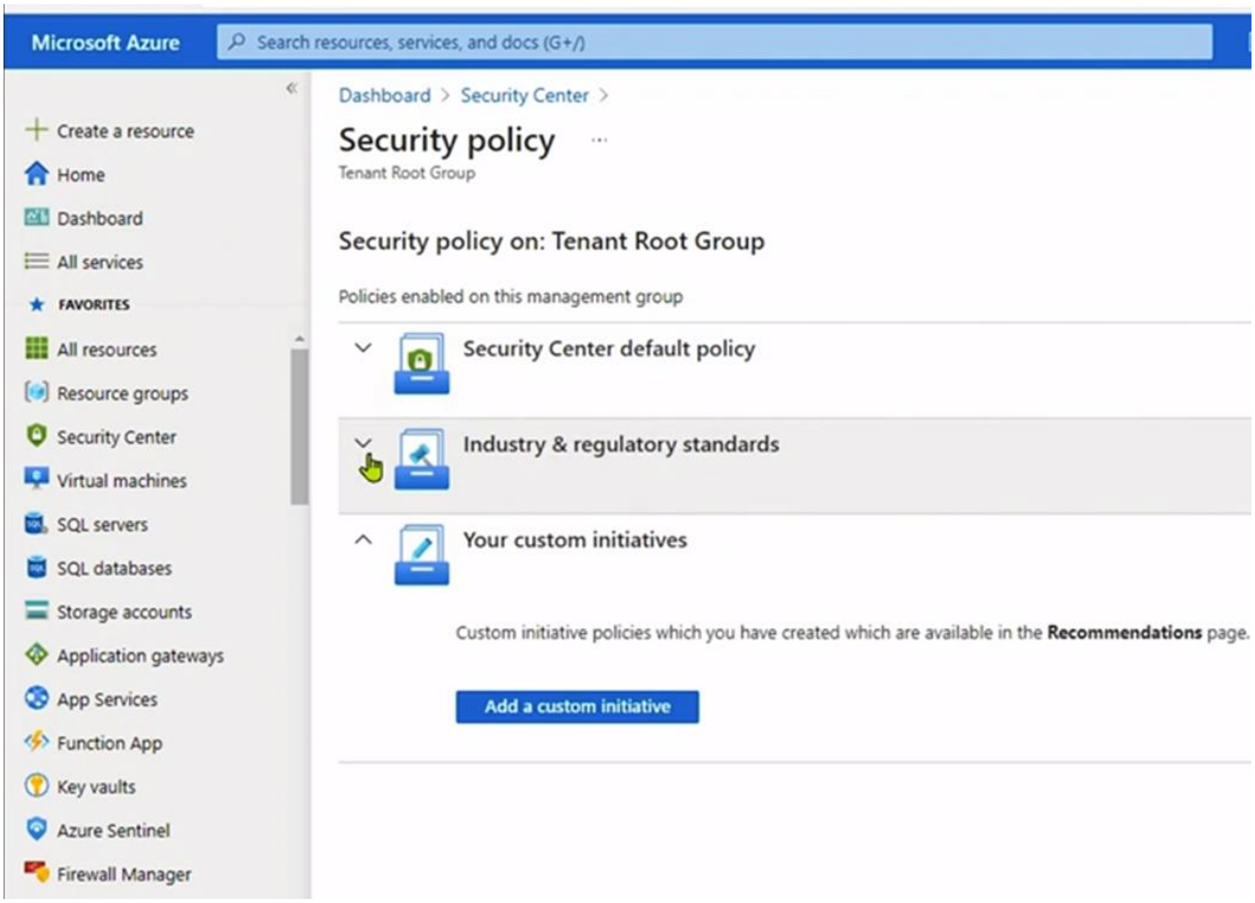
Choose a subscription or management group from the list below to perform the following tasks:
- View and edit the default ASC policy
- Add a custom policy
- Add regulatory compliance standards to your compliance dashboard

Click here to learn more >

1 MANAGEMENT GROUPS 6 SUBSCRIPTIONS

Search by name

Name	Default policy
Tenant Root Group (6 of 13 subscriptions)	Not assigned
LGNA SIMON Sponsorship	Assigned
LGNA Sponsorship CY2020	Assigned
LGNA Sponsorship CY2021	Assigned
WK - MSDN - FTE Benefit	Assigned
WK - VSE - MPN Benefit	Assigned
WK - VSE2 - MPN Benefit	Assigned



Security policy ...

Tenant Root Group

Security policy on: Tenant Root Group

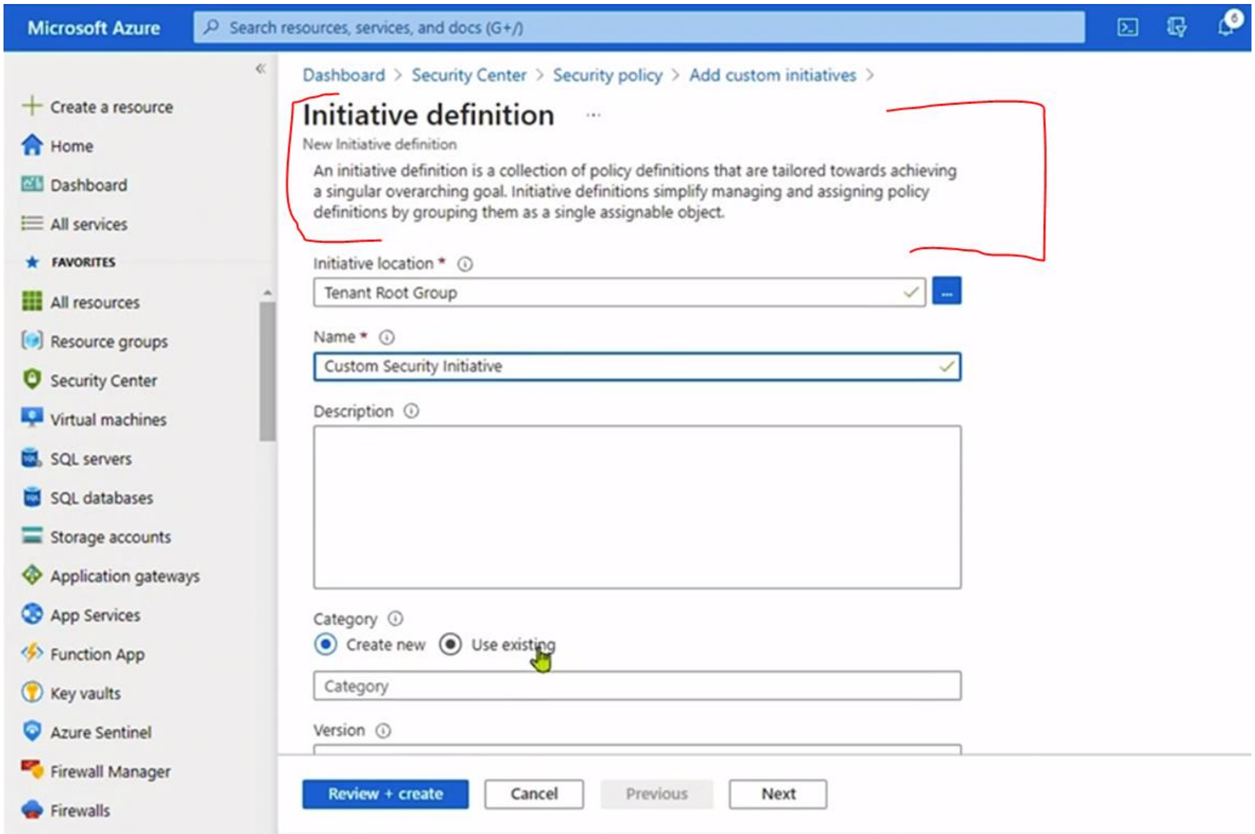
Policies enabled on this management group

Security Center default policy

Industry & regulatory standards

Your custom initiatives

Custom initiative policies which you have created which are available in the **Recommendations** page.



Dashboard > Security Center > Security policy > Add custom initiatives >

Initiative definition ...

New Initiative definition

An initiative definition is a collection of policy definitions that are tailored towards achieving a singular overarching goal. Initiative definitions simplify managing and assigning policy definitions by grouping them as a single assignable object.

Initiative location * : Tenant Root Group

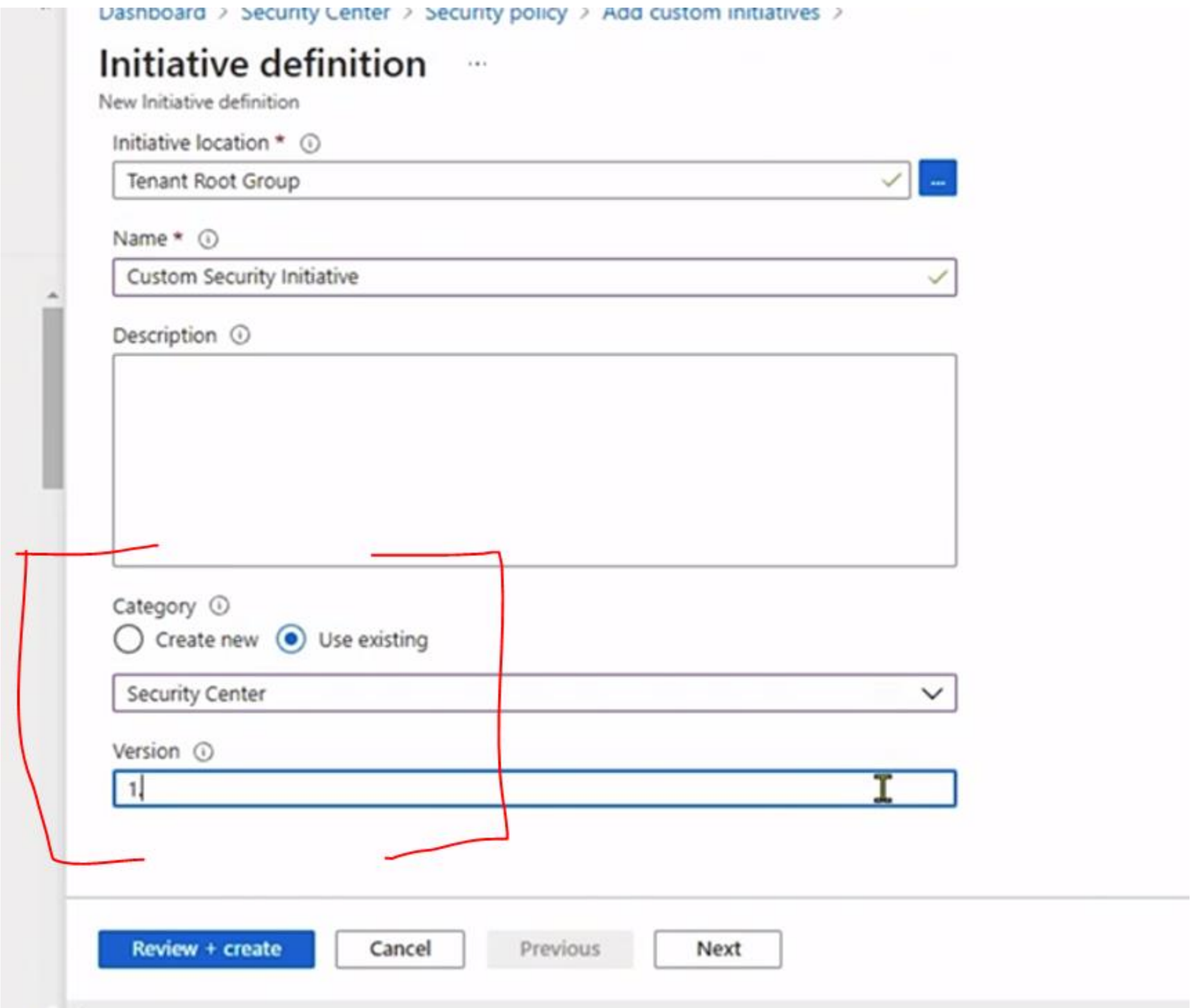
Name * : Custom Security Initiative

Description

Category
● Create new ○ Use existing

Category

Version



Dashboard > Security Center > Security policy > Add custom initiatives >

Initiative definition

New Initiative definition

Initiative location * : Tenant Root Group

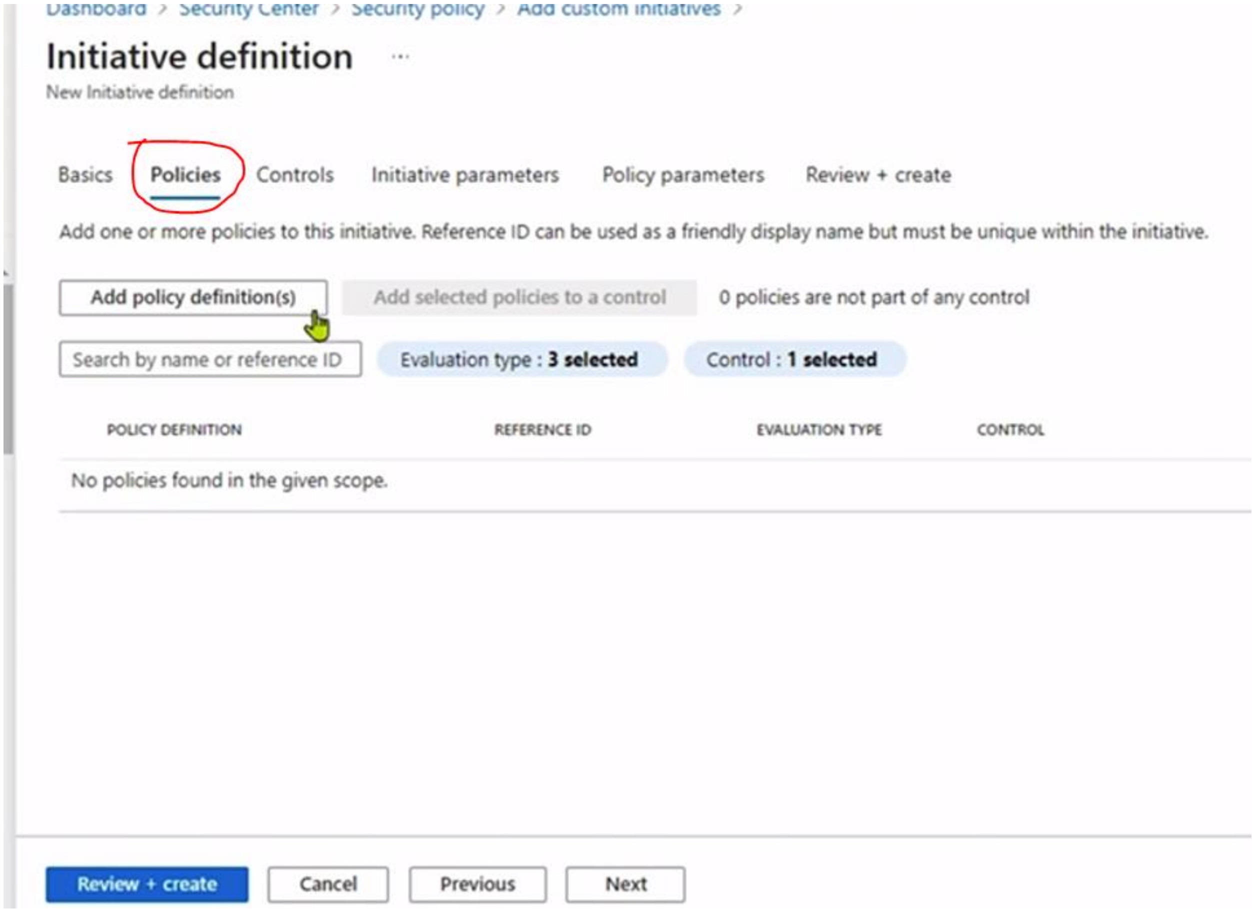
Name * : Custom Security Initiative

Description :

Category
○ Create new ● Use existing

Security Center

Version : 1



Dashboard > Security Center > Security policy > Add custom initiatives >

Initiative definition

New Initiative definition

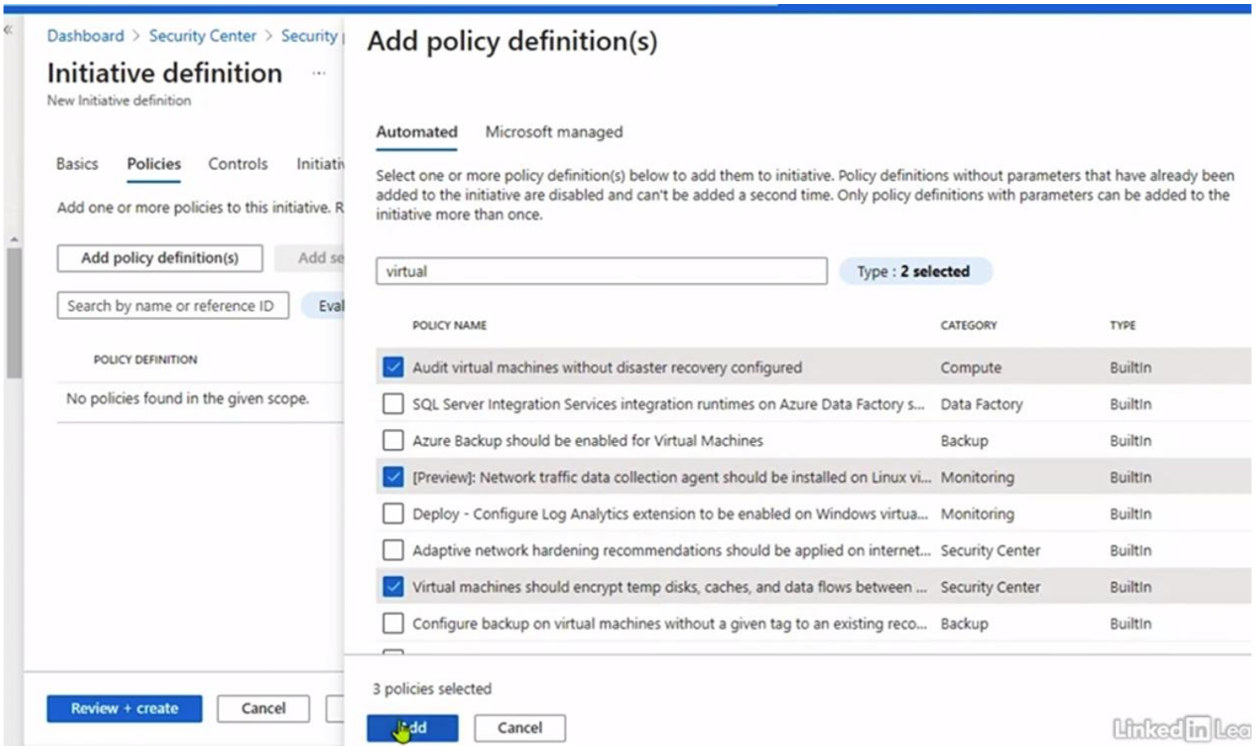
Add one or more policies to this initiative. Reference ID can be used as a friendly display name but must be unique within the initiative.

0 policies are not part of any control

Evaluation type : **3 selected**

Control : **1 selected**

POLICY DEFINITION	REFERENCE ID	EVALUATION TYPE	CONTROL
No policies found in the given scope.			



Dashboard > Security Center > Security

Initiative definition

New Initiative definition

Add one or more policies to this initiative. R

POLICY DEFINITION
No policies found in the given scope.

Add policy definition(s)

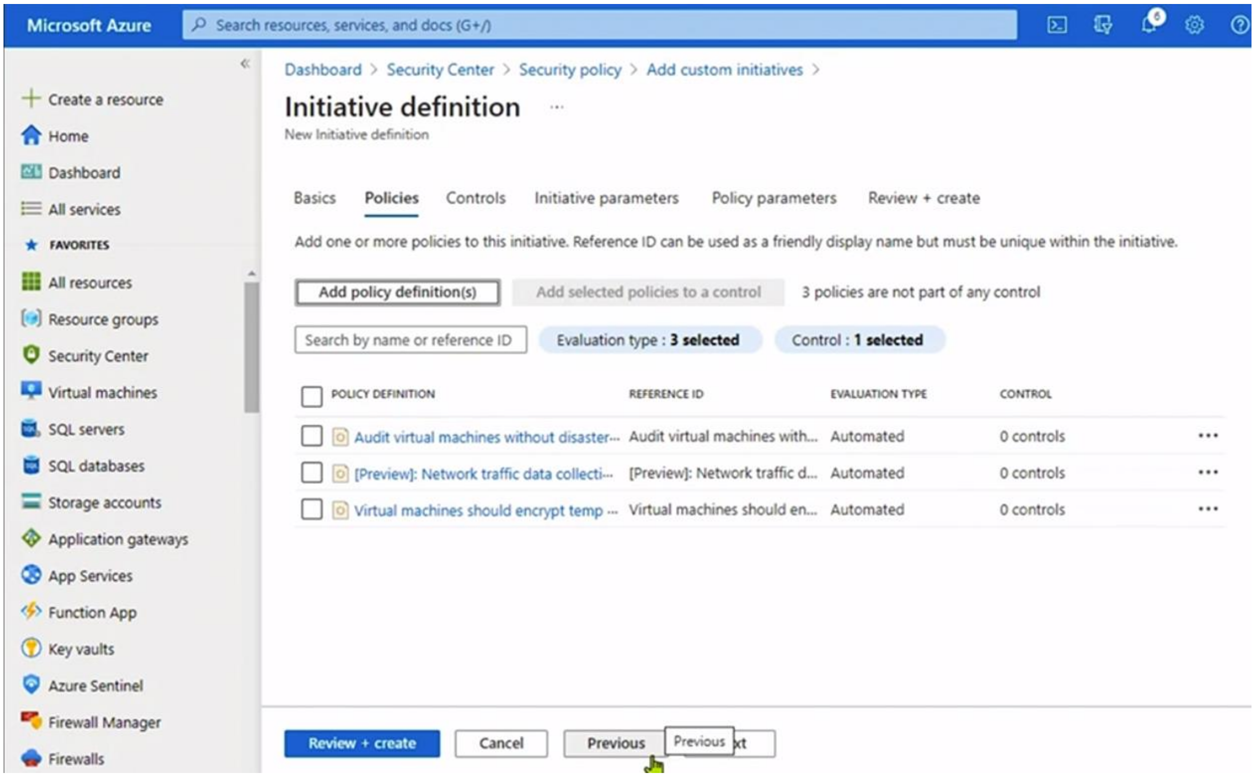
Select one or more policy definition(s) below to add them to initiative. Policy definitions without parameters that have already been added to the initiative are disabled and can't be added a second time. Only policy definitions with parameters can be added to the initiative more than once.

Search: virtual

Type : **2 selected**

	POLICY NAME	CATEGORY	TYPE
☑	Audit virtual machines without disaster recovery configured	Compute	BuiltIn
□	SQL Server Integration Services integration runtimes on Azure Data Factory s...	Data Factory	BuiltIn
□	Azure Backup should be enabled for Virtual Machines	Backup	BuiltIn
☑	[Preview]: Network traffic data collection agent should be installed on Linux vi...	Monitoring	BuiltIn
□	Deploy - Configure Log Analytics extension to be enabled on Windows virtua...	Monitoring	BuiltIn
□	Adaptive network hardening recommendations should be applied on internet...	Security Center	BuiltIn
☑	Virtual machines should encrypt temp disks, caches, and data flows between ...	Security Center	BuiltIn
□	Configure backup on virtual machines without a given tag to an existing reco...	Backup	BuiltIn

3 policies selected



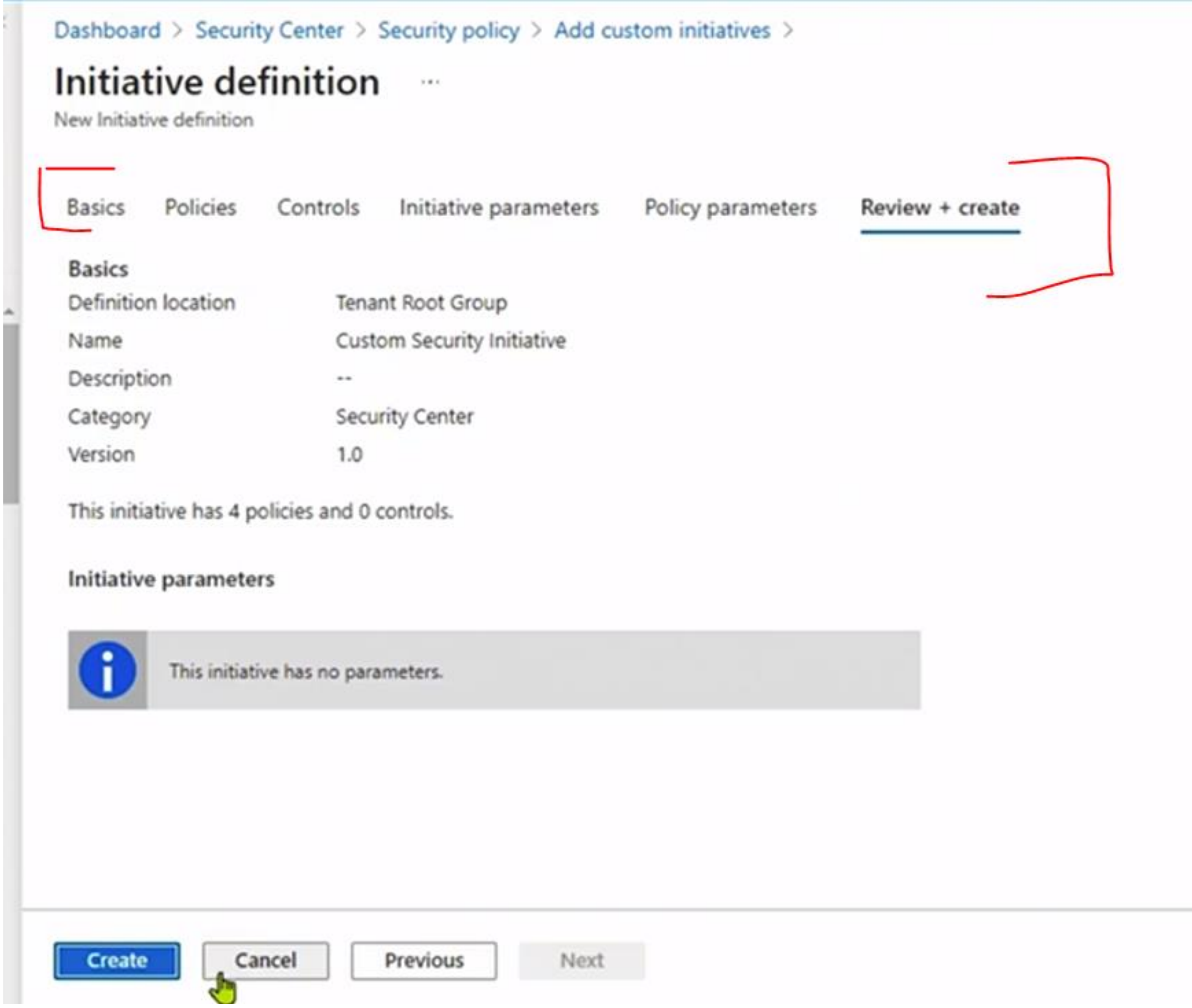
Initiative definition

New Initiative definition

Add one or more policies to this initiative. Reference ID can be used as a friendly display name but must be unique within the initiative.

3 policies are not part of any control

	POLICY DEFINITION	REFERENCE ID	EVALUATION TYPE	CONTROL
□	Audit virtual machines without disaster...	Audit virtual machines with...	Automated	0 controls
□	[Preview]: Network traffic data collecti...	[Preview]: Network traffic d...	Automated	0 controls
□	Virtual machines should encrypt temp ...	Virtual machines should en...	Automated	0 controls


Dashboard > Security Center > Security policy > Add custom initiatives >

Initiative definition

New Initiative definition

Basics

Definition location	Tenant Root Group
Name	Custom Security Initiative
Description	--
Category	Security Center
Version	1.0

This initiative has 4 policies and 0 controls.

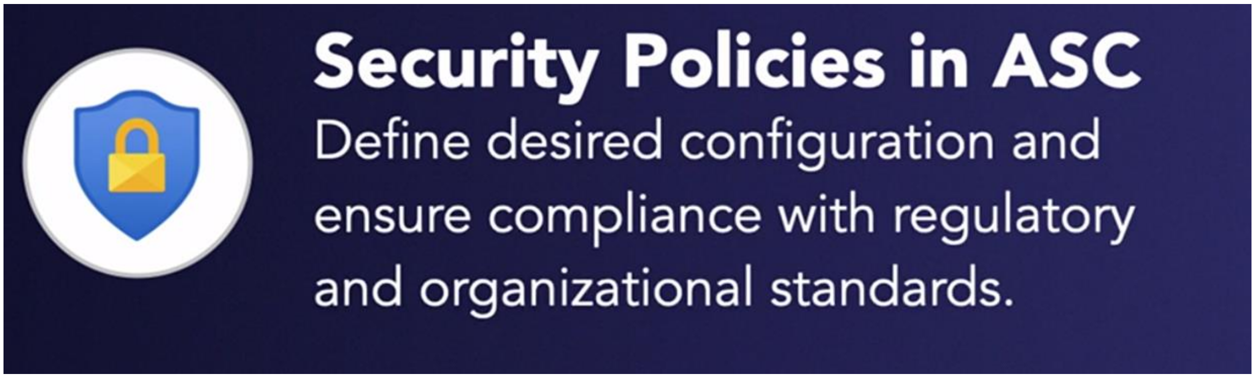
Initiative parameters

This initiative has no parameters.

EXAM TIP

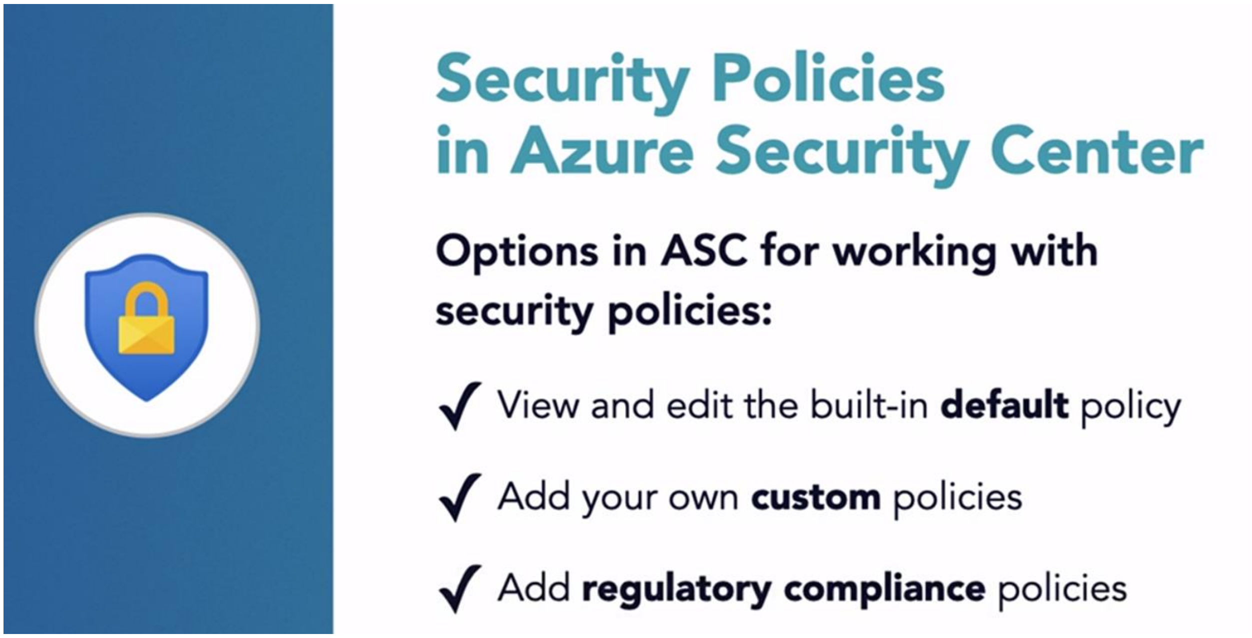
Know the details of policy and initiative creation, but with a security focus.

1.3 Configure security settings and auditing using Azure Policy



Security Policies in ASC

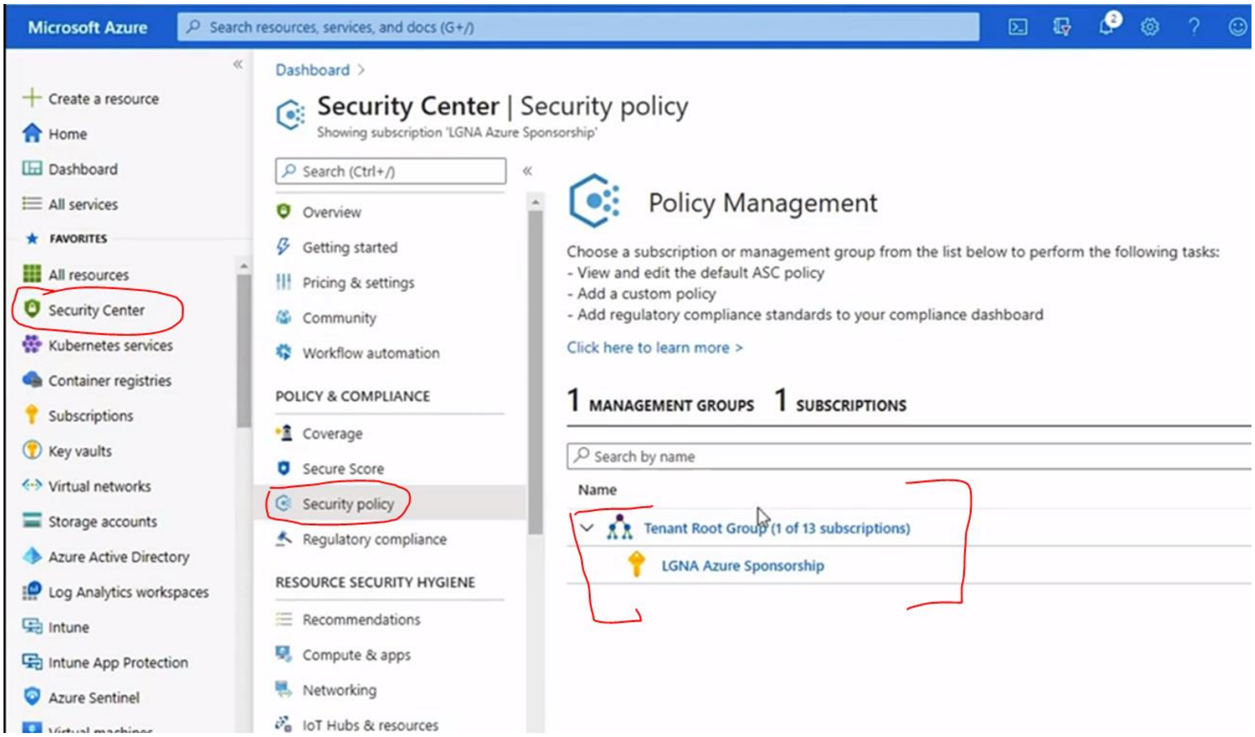
Define desired configuration and ensure compliance with regulatory and organizational standards.



Security Policies in Azure Security Center

Options in ASC for working with security policies:

- ✓ View and edit the built-in **default** policy
- ✓ Add your own **custom** policies
- ✓ Add **regulatory compliance** policies



Security Center | Security policy

Showing subscription 'LGNA Azure Sponsorship'

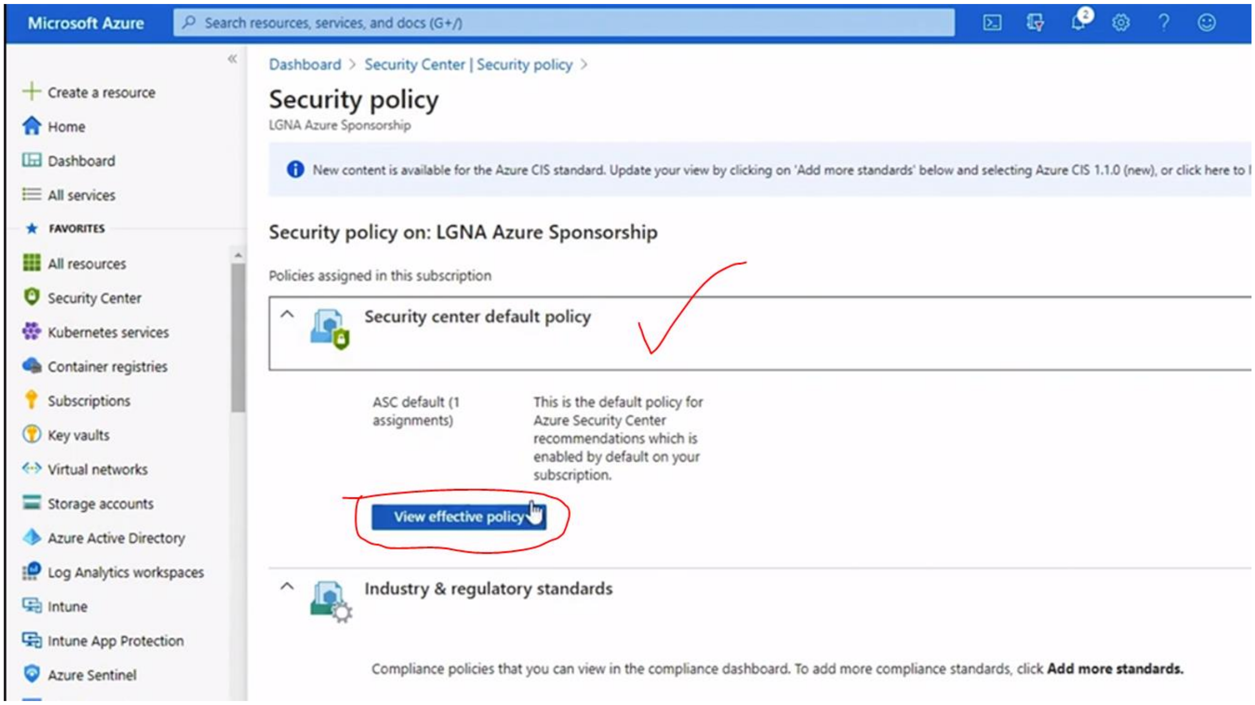
Policy Management

Choose a subscription or management group from the list below to perform the following tasks:
- View and edit the default ASC policy
- Add a custom policy
- Add regulatory compliance standards to your compliance dashboard

Click here to learn more >

1 MANAGEMENT GROUPS 1 SUBSCRIPTIONS

Name
Tenant Root Group (1 of 13 subscriptions)
LGNA Azure Sponsorship



Security policy

LGNA Azure Sponsorship

New content is available for the Azure CIS standard. Update your view by clicking on 'Add more standards' below and selecting Azure CIS 1.1.0 (new), or click here to l

Security policy on: LGNA Azure Sponsorship

Policies assigned in this subscription

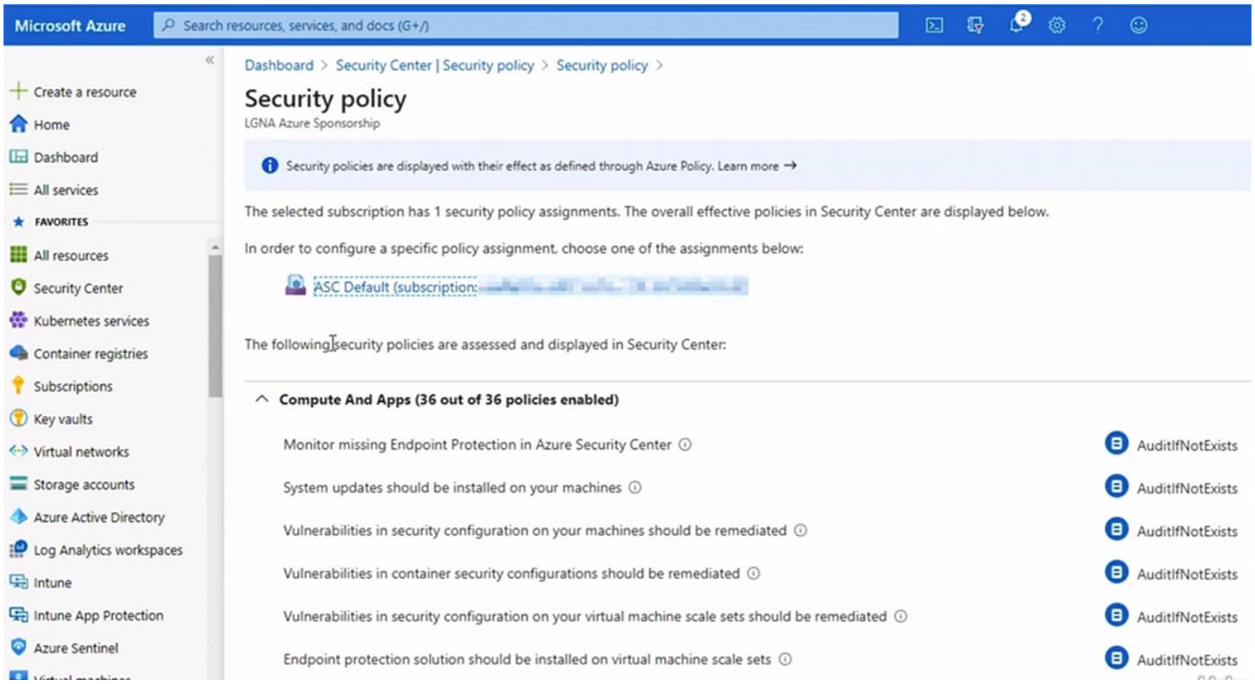
Security center default policy

ASC default (1 assignments)

This is the default policy for Azure Security Center recommendations which is enabled by default on your subscription.

Industry & regulatory standards

Compliance policies that you can view in the compliance dashboard. To add more compliance standards, click **Add more standards.**



Security policy

LGNA Azure Sponsorship

Security policies are displayed with their effect as defined through Azure Policy. Learn more →

The selected subscription has 1 security policy assignments. The overall effective policies in Security Center are displayed below.

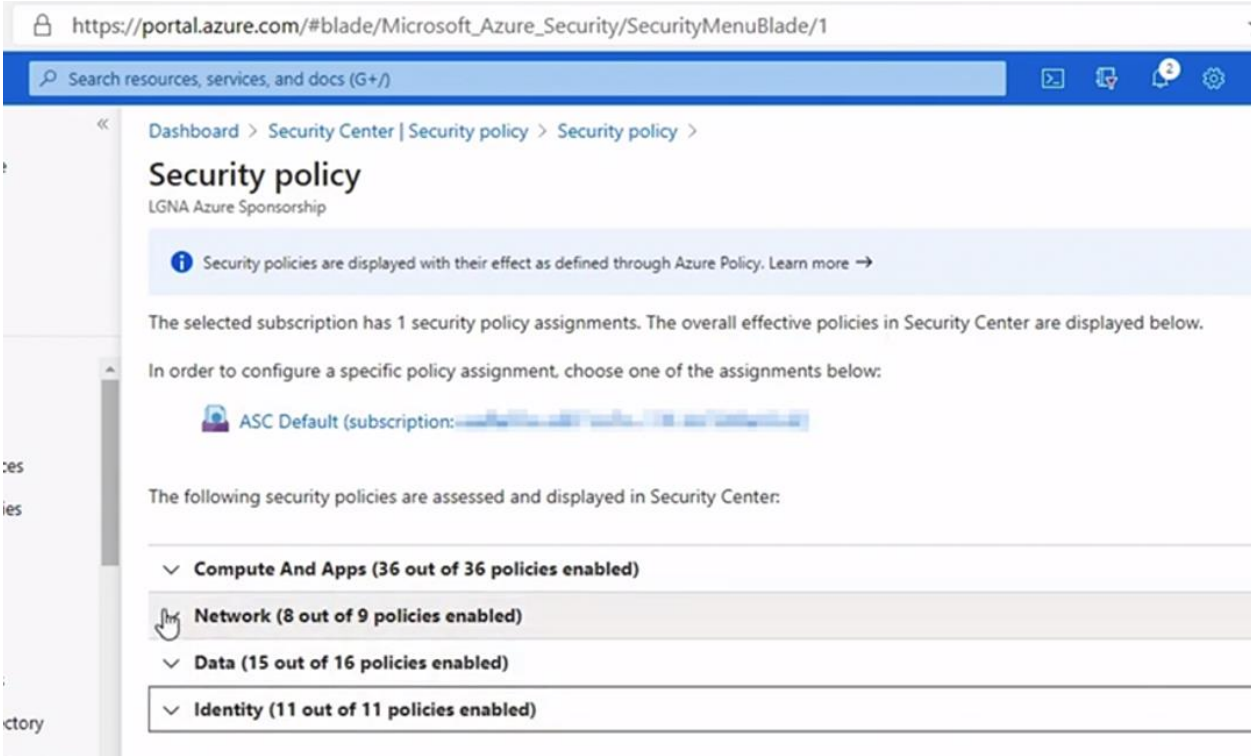
In order to configure a specific policy assignment, choose one of the assignments below:

ASC Default (subscription: [redacted]

The following security policies are assessed and displayed in Security Center:

Compute And Apps (36 out of 36 policies enabled)

Monitor missing Endpoint Protection in Azure Security Center	AuditIfNotExists
System updates should be installed on your machines	AuditIfNotExists
Vulnerabilities in security configuration on your machines should be remediated	AuditIfNotExists
Vulnerabilities in container security configurations should be remediated	AuditIfNotExists
Vulnerabilities in security configuration on your virtual machine scale sets should be remediated	AuditIfNotExists
Endpoint protection solution should be installed on virtual machine scale sets	AuditIfNotExists


https://portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/1
Search resources, services, and docs (G+/)
Dashboard > Security Center | Security policy > Security policy >

Security policy

LGNA Azure Sponsorship

Security policies are displayed with their effect as defined through Azure Policy. Learn more →

The selected subscription has 1 security policy assignments. The overall effective policies in Security Center are displayed below.

In order to configure a specific policy assignment, choose one of the assignments below:

ASC Default (subscription: [redacted]

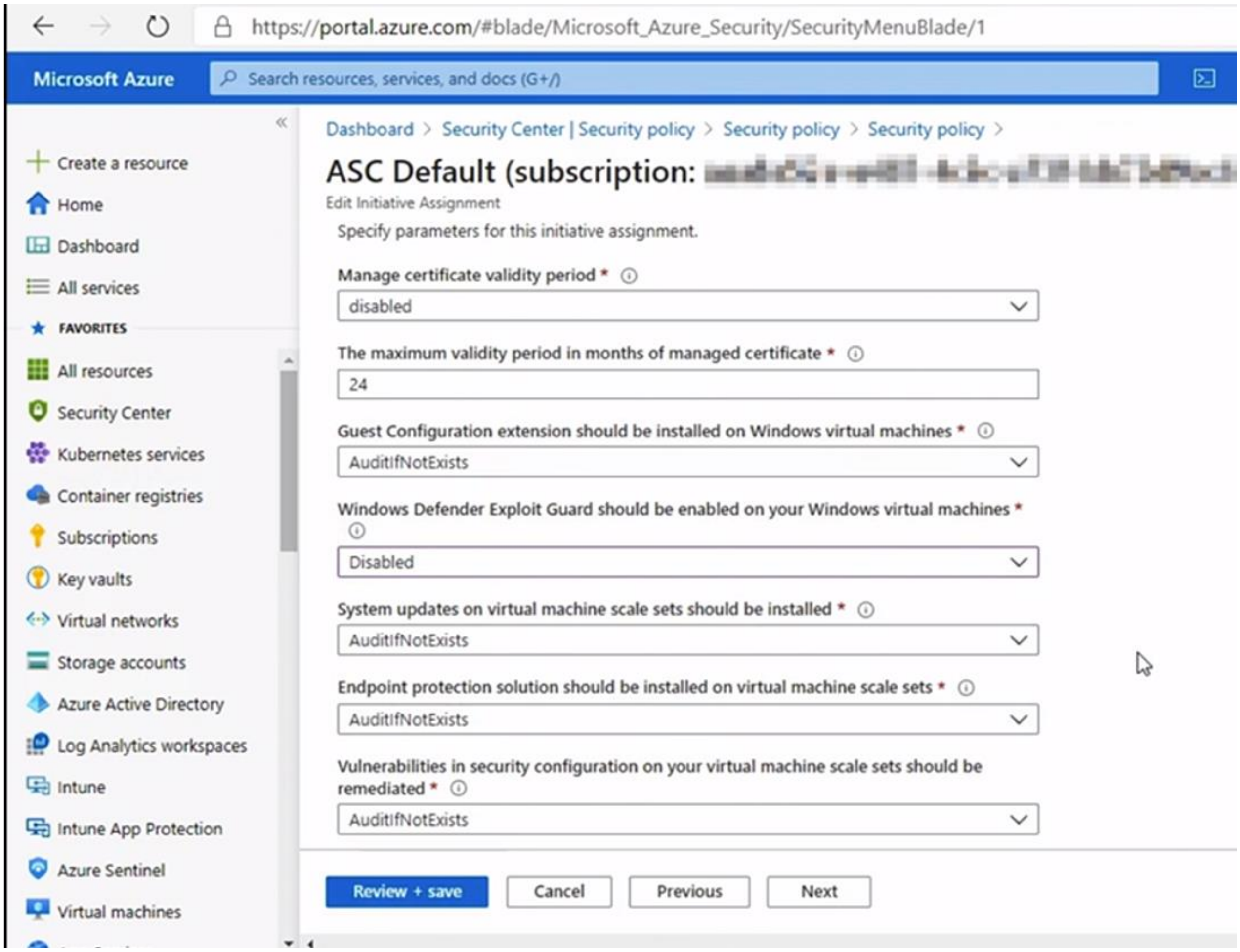
The following security policies are assessed and displayed in Security Center:

Compute And Apps (36 out of 36 policies enabled)

Network (8 out of 9 policies enabled)

Data (15 out of 16 policies enabled)

Identity (11 out of 11 policies enabled)



ASC Default (subscription: [redacted]

Edit Initiative Assignment

Specify parameters for this initiative assignment.

Manage certificate validity period * : disabled

The maximum validity period in months of managed certificate * : 24

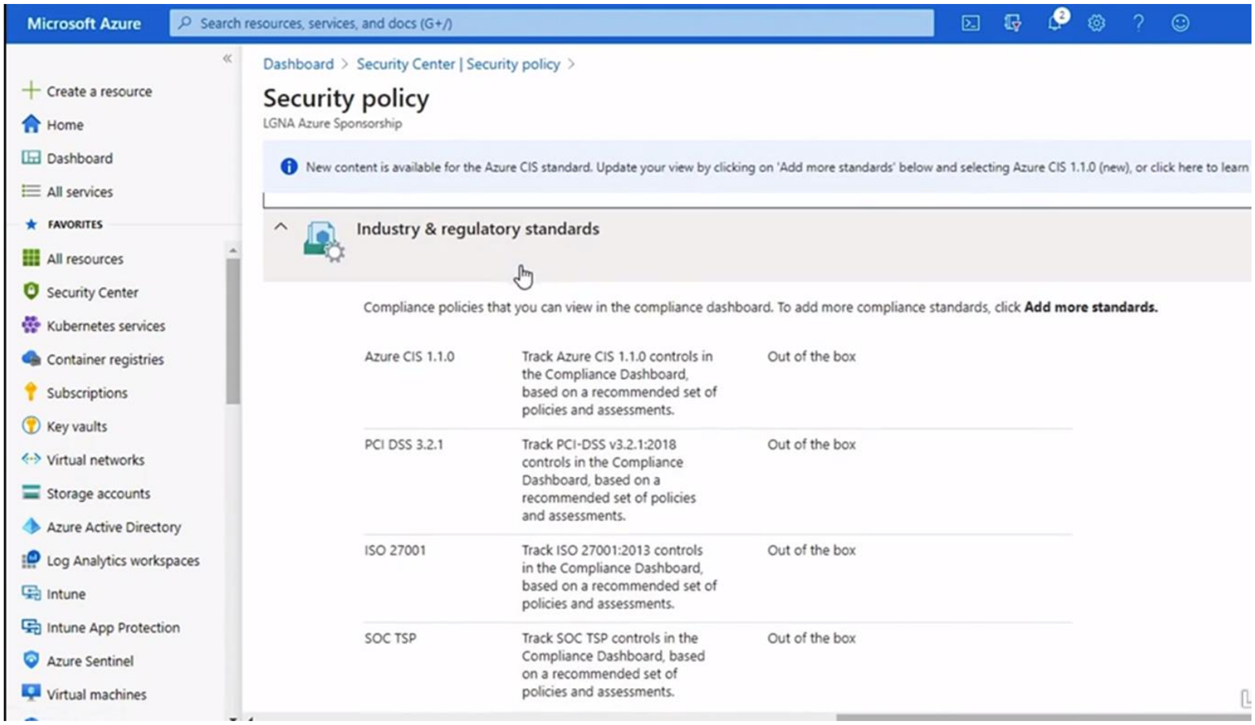
Guest Configuration extension should be installed on Windows virtual machines * : AuditIfNotExists

Windows Defender Exploit Guard should be enabled on your Windows virtual machines * : Disabled

System updates on virtual machine scale sets should be installed * : AuditIfNotExists

Endpoint protection solution should be installed on virtual machine scale sets * : AuditIfNotExists

Vulnerabilities in security configuration on your virtual machine scale sets should be remediated * : AuditIfNotExists



Security policy

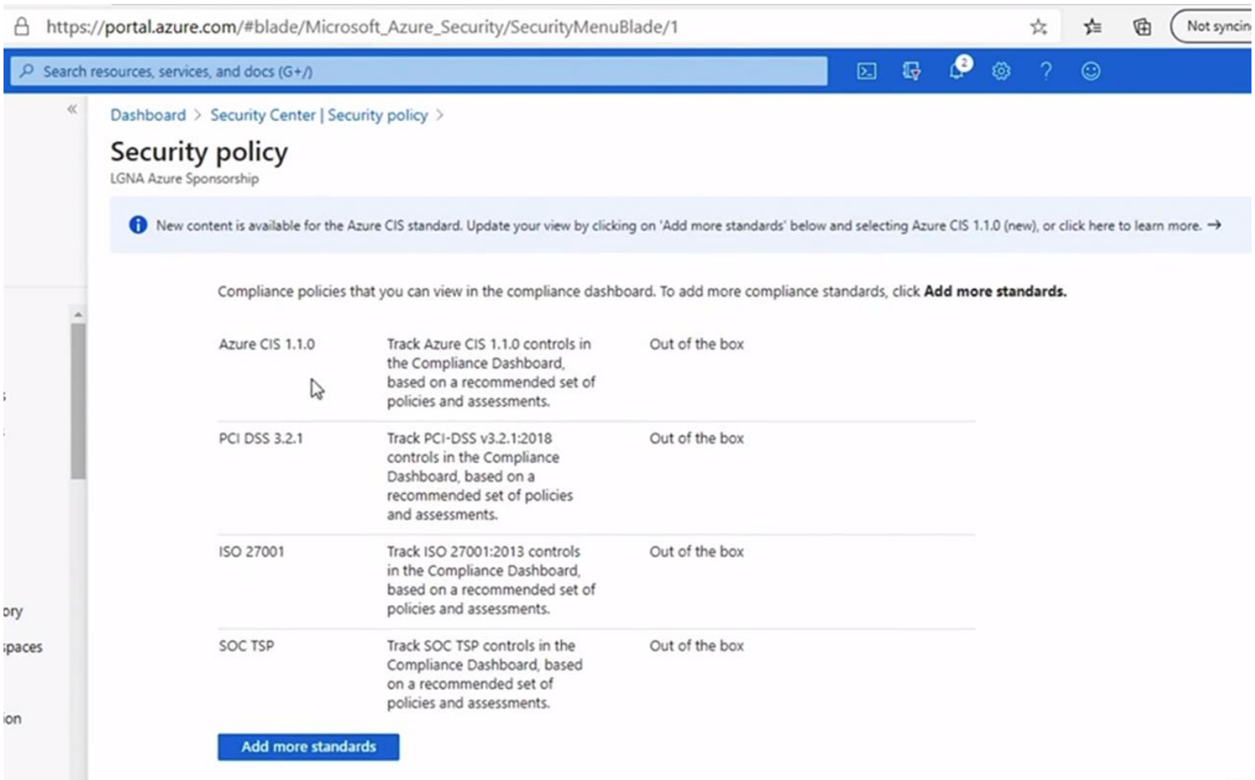
LGNA Azure Sponsorship

New content is available for the Azure CIS standard. Update your view by clicking on 'Add more standards' below and selecting Azure CIS 1.1.0 (new), or click here to learn

Industry & regulatory standards

Compliance policies that you can view in the compliance dashboard. To add more compliance standards, click **Add more standards.**

Azure CIS 1.1.0	Track Azure CIS 1.1.0 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box
PCI DSS 3.2.1	Track PCI-DSS v3.2.1:2018 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box
ISO 27001	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box
SOC TSP	Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box


https://portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/1
Not syncin
Search resources, services, and docs (G+/)

Dashboard > Security Center | Security policy >

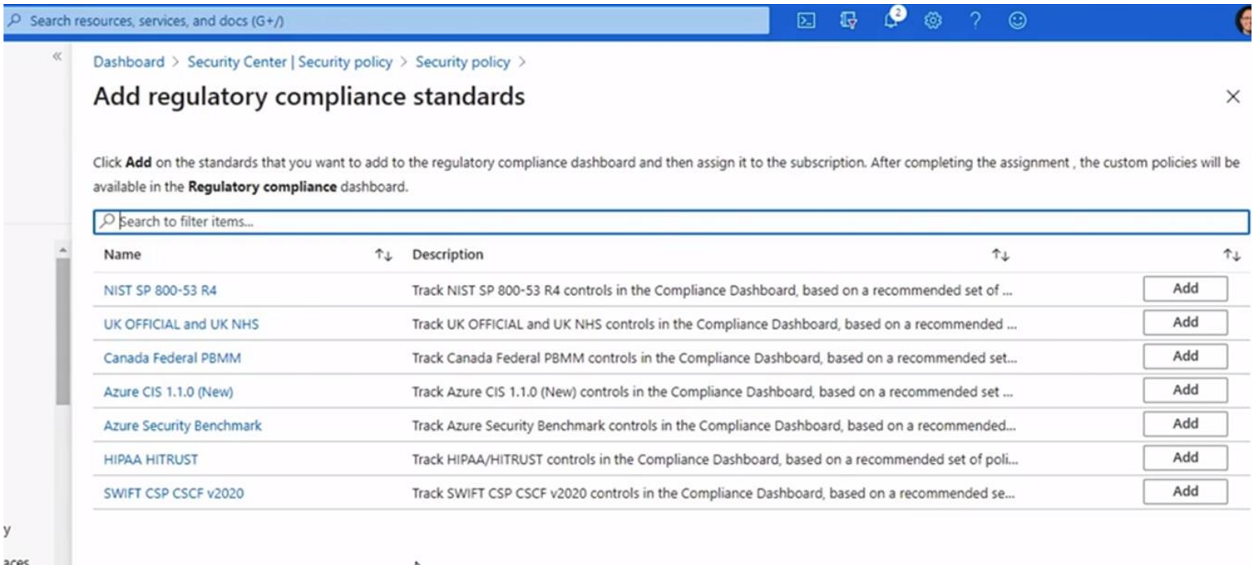
Security policy

LGNA Azure Sponsorship

New content is available for the Azure CIS standard. Update your view by clicking on 'Add more standards' below and selecting Azure CIS 1.1.0 (new), or click here to learn more. →

Compliance policies that you can view in the compliance dashboard. To add more compliance standards, click **Add more standards.**

Azure CIS 1.1.0	Track Azure CIS 1.1.0 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box
PCI DSS 3.2.1	Track PCI-DSS v3.2.1:2018 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box
ISO 27001	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box
SOC TSP	Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box


Search resources, services, and docs (G+/)

Dashboard > Security Center | Security policy > Security policy >

Add regulatory compliance standards

Click **Add** on the standards that you want to add to the regulatory compliance dashboard and then assign it to the subscription. After completing the assignment , the custom policies will be available in the **Regulatory compliance** dashboard.

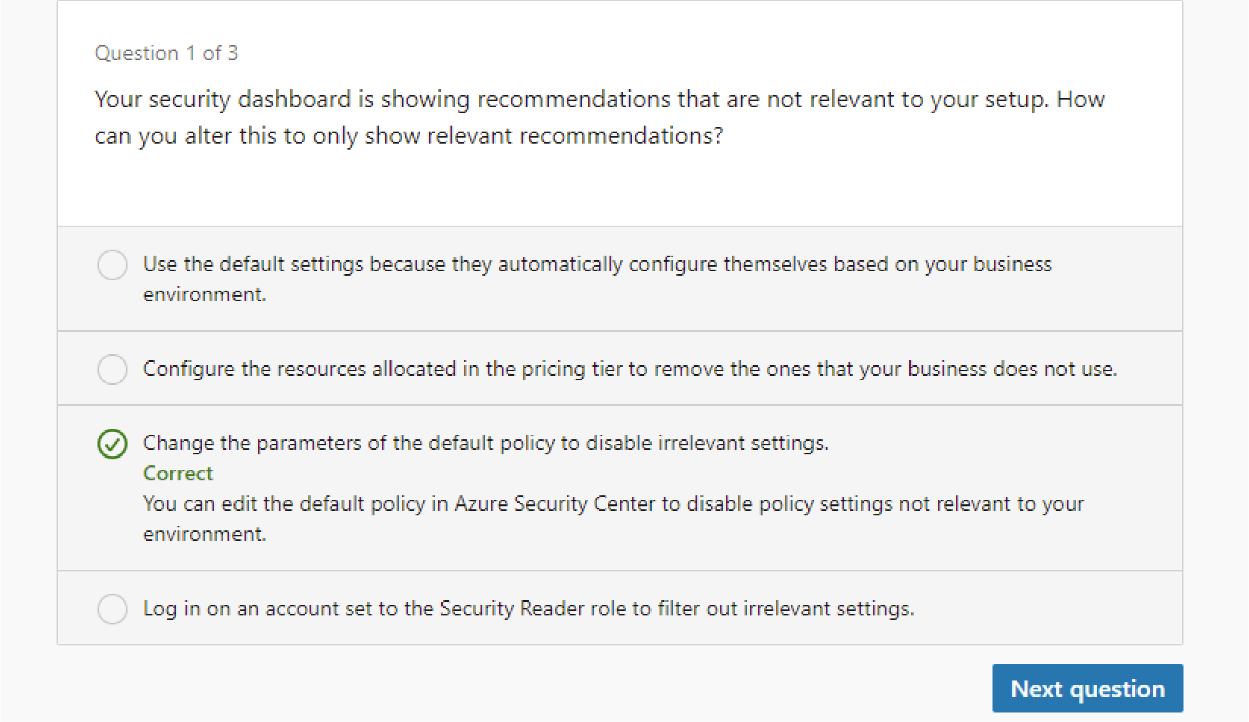
Search to filter items...

Name	Description	
NIST SP 800-53 R4	Track NIST SP 800-53 R4 controls in the Compliance Dashboard, based on a recommended set of ...	Add
UK OFFICIAL and UK NHS	Track UK OFFICIAL and UK NHS controls in the Compliance Dashboard, based on a recommended ...	Add
Canada Federal PBMM	Track Canada Federal PBMM controls in the Compliance Dashboard, based on a recommended set...	Add
Azure CIS 1.1.0 (New)	Track Azure CIS 1.1.0 (New) controls in the Compliance Dashboard, based on a recommended set ...	Add
Azure Security Benchmark	Track Azure Security Benchmark controls in the Compliance Dashboard, based on a recommended...	Add
HIPAA HITRUST	Track HIPAA/HITRUST controls in the Compliance Dashboard, based on a recommended set of poli...	Add
SWIFT CSP CSCF v2020	Track SWIFT CSP CSCF v2020 controls in the Compliance Dashboard, based on a recommended se...	Add

Exam Tip

Know your security policy options in ASC and how to configure them.

1.4 Quiz



Question 1 of 3

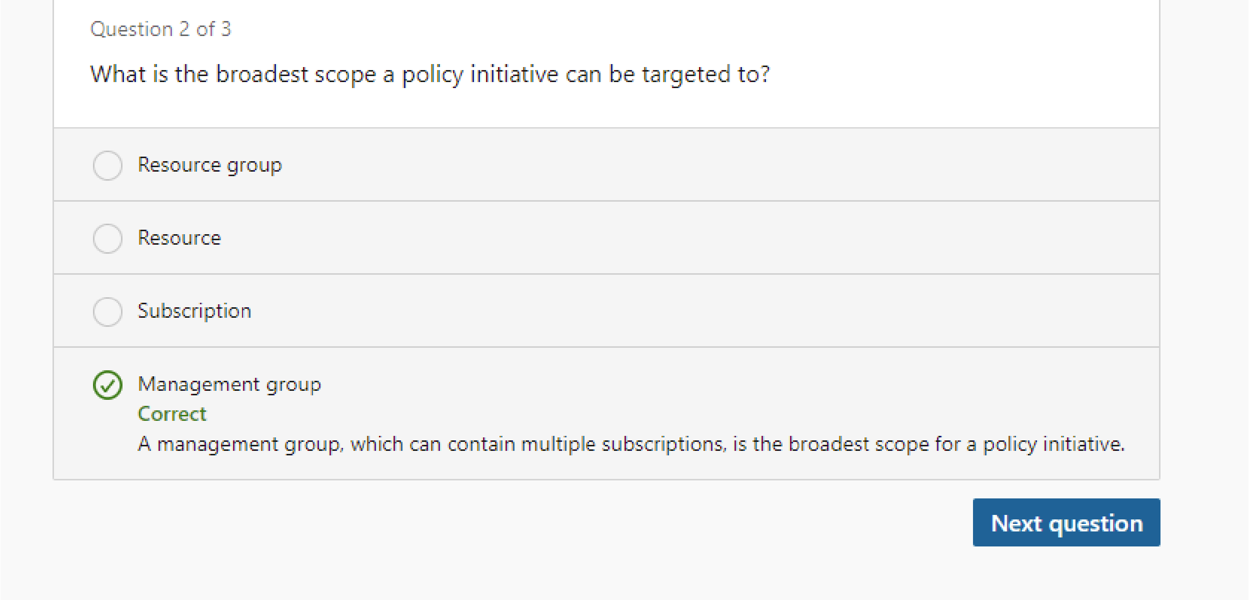
Your security dashboard is showing recommendations that are not relevant to your setup. How can you alter this to only show relevant recommendations?

○ Use the default settings because they automatically configure themselves based on your business environment.

○ Configure the resources allocated in the pricing tier to remove the ones that your business does not use.

✓ Change the parameters of the default policy to disable irrelevant settings.
Correct
You can edit the default policy in Azure Security Center to disable policy settings not relevant to your environment.

○ Log in on an account set to the Security Reader role to filter out irrelevant settings.



Question 2 of 3

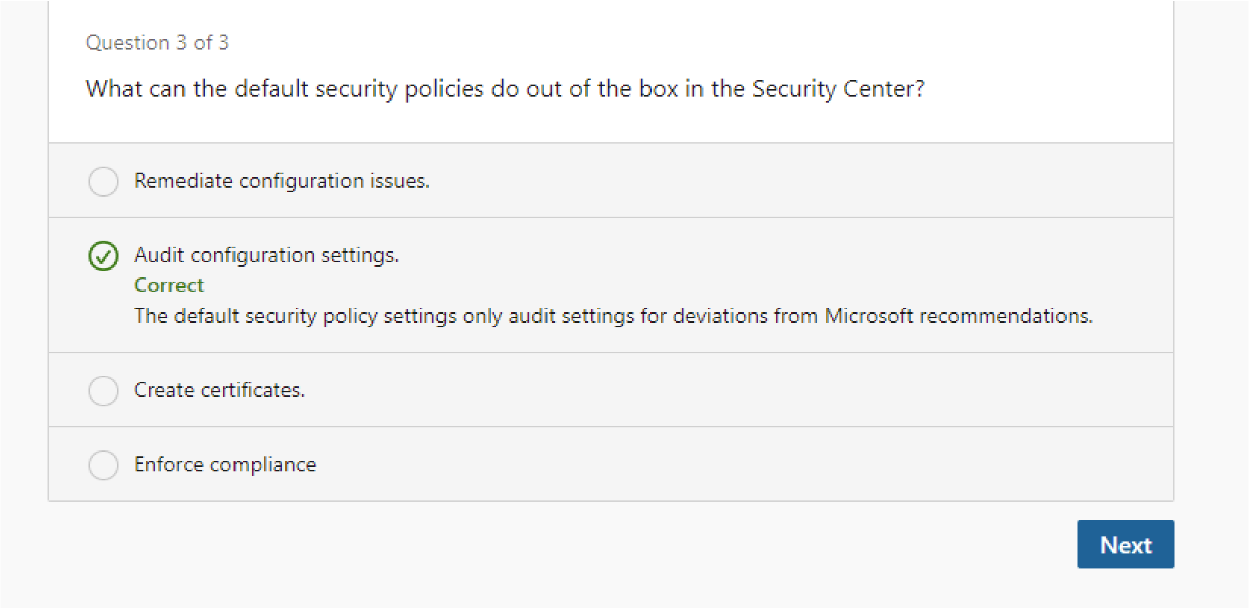
What is the broadest scope a policy initiative can be targeted to?

○ Resource group

○ Resource

○ Subscription

✓ Management group
Correct
A management group, which can contain multiple subscriptions, is the broadest scope for a policy initiative.



Question 3 of 3

What can the default security policies do out of the box in the Security Center?

○ Remediate configuration issues.

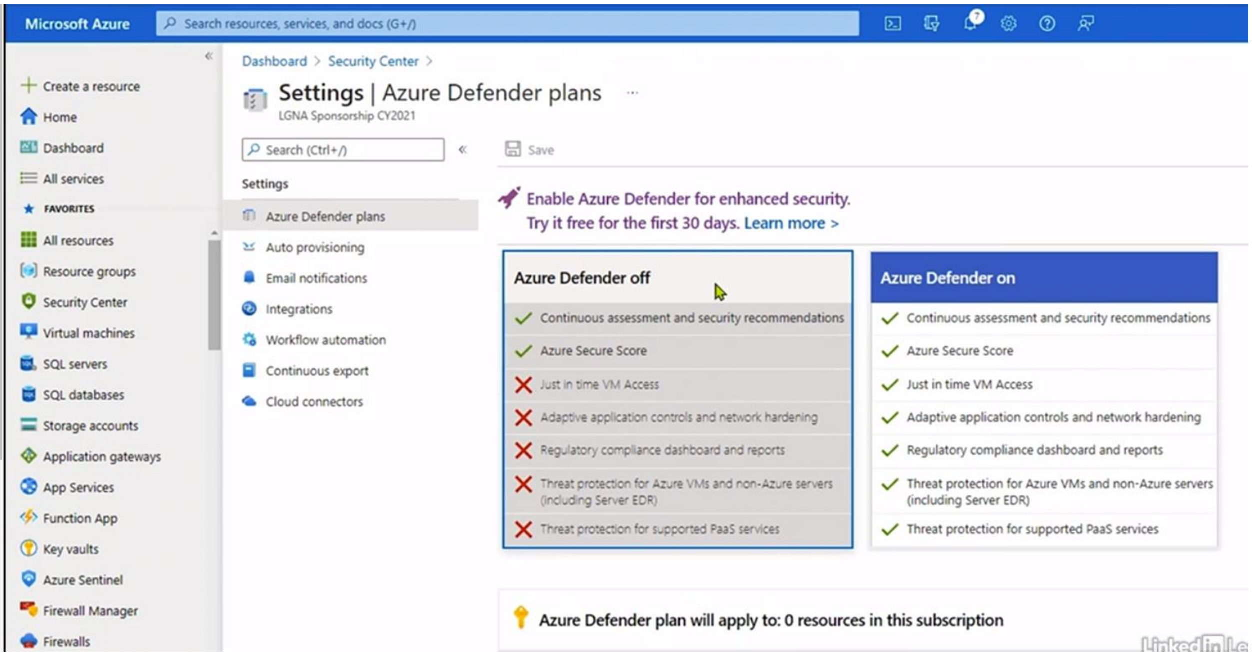
✓ Audit configuration settings.
Correct
The default security policy settings only audit settings for deviations from Microsoft recommendations.

○ Create certificates.

○ Enforce compliance

2. Configure and Manage Threat Protection

2.1 Configure Azure Defender for Servers



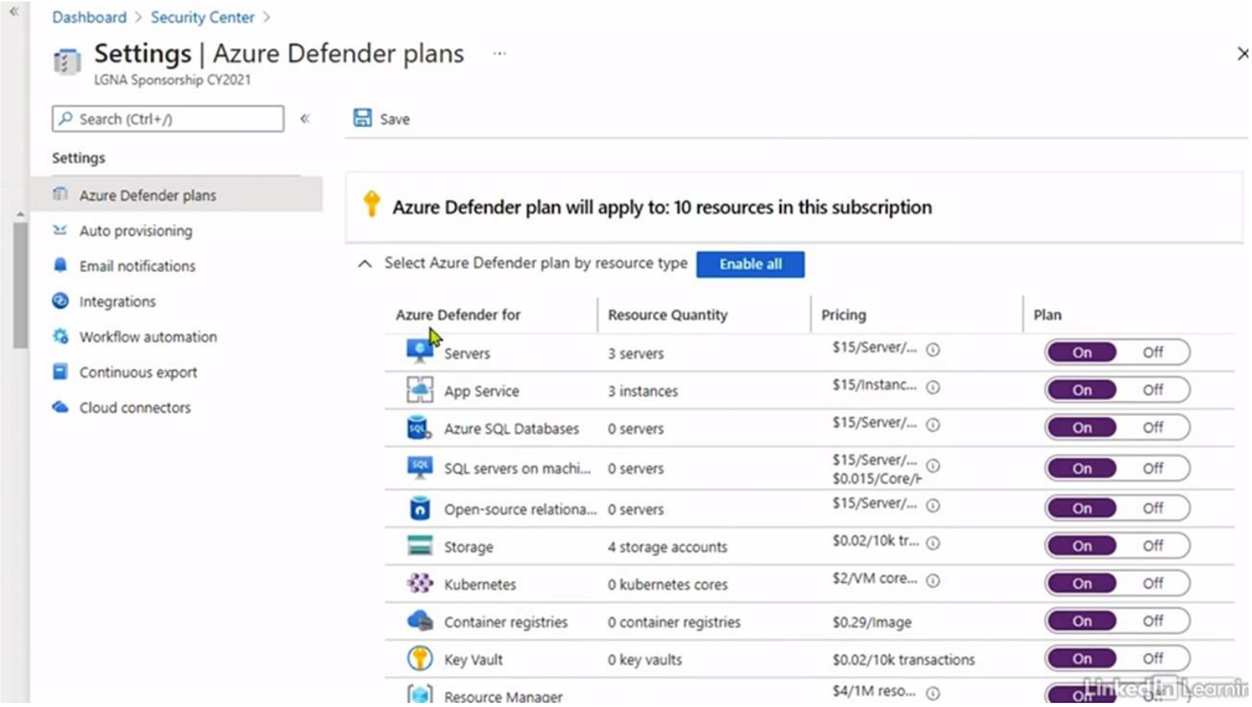
Settings | Azure Defender plans

LGNA Sponsorship CY2021

Enable Azure Defender for enhanced security.
Try it free for the first 30 days. Learn more >

Azure Defender off	Azure Defender on
✓ Continuous assessment and security recommendations	✓ Continuous assessment and security recommendations
✓ Azure Secure Score	✓ Azure Secure Score
✗ Just in time VM Access	✓ Just in time VM Access
✗ Adaptive application controls and network hardening	✓ Adaptive application controls and network hardening
✗ Regulatory compliance dashboard and reports	✓ Regulatory compliance dashboard and reports
✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)	✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
✗ Threat protection for supported PaaS services	✓ Threat protection for supported PaaS services

Azure Defender plan will apply to: 0 resources in this subscription



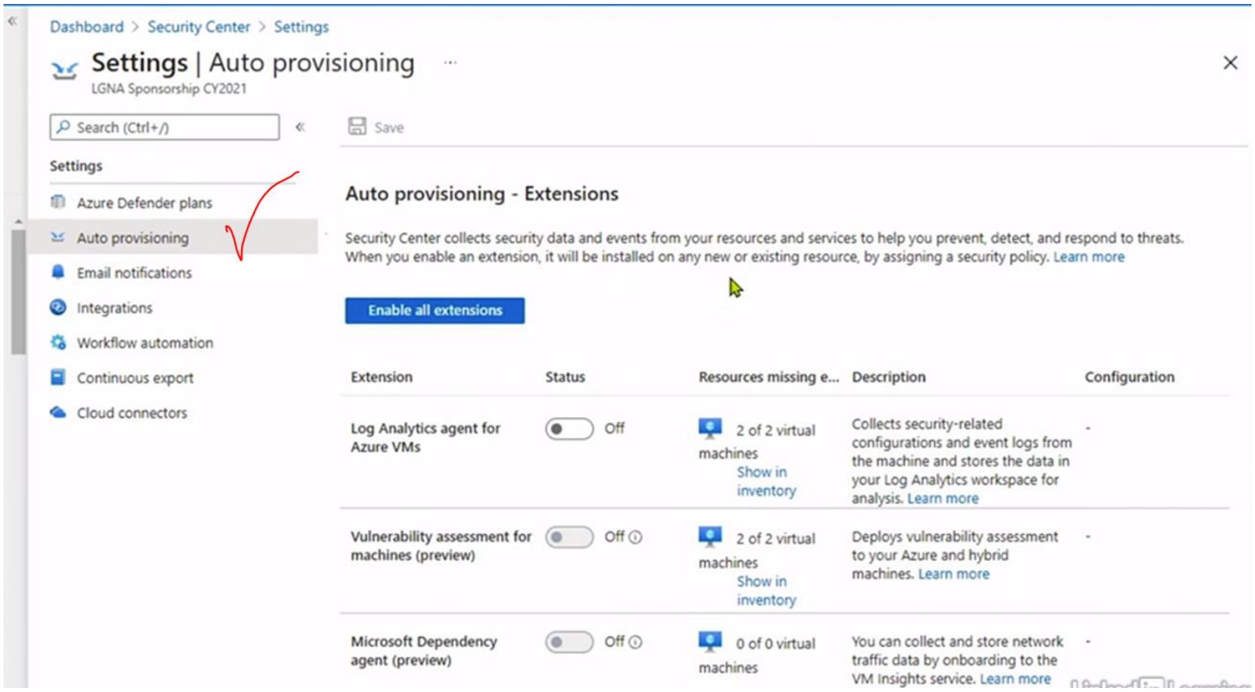
Settings | Azure Defender plans

LGNA Sponsorship CY2021

Azure Defender plan will apply to: 10 resources in this subscription

Select Azure Defender plan by resource type

Azure Defender for	Resource Quantity	Pricing	Plan
Servers	3 servers	$15/Server/...	On Off
App Service	3 instances	$15/Instanc...	On Off
Azure SQL Databases	0 servers	$15/Server/...	On Off
SQL servers on machi...	0 servers	$15/Server/... $0.015/Core/H	On Off
Open-source relationa...	0 servers	$15/Server/...	On Off
Storage	4 storage accounts	$0.02/10k tr...	On Off
Kubernetes	0 kubernetes cores	$2/VM core...	On Off
Container registries	0 container registries	$0.29/Image	On Off
Key Vault	0 key vaults	$0.02/10k transactions	On Off
Resource Manager		$4/1M reso...	On



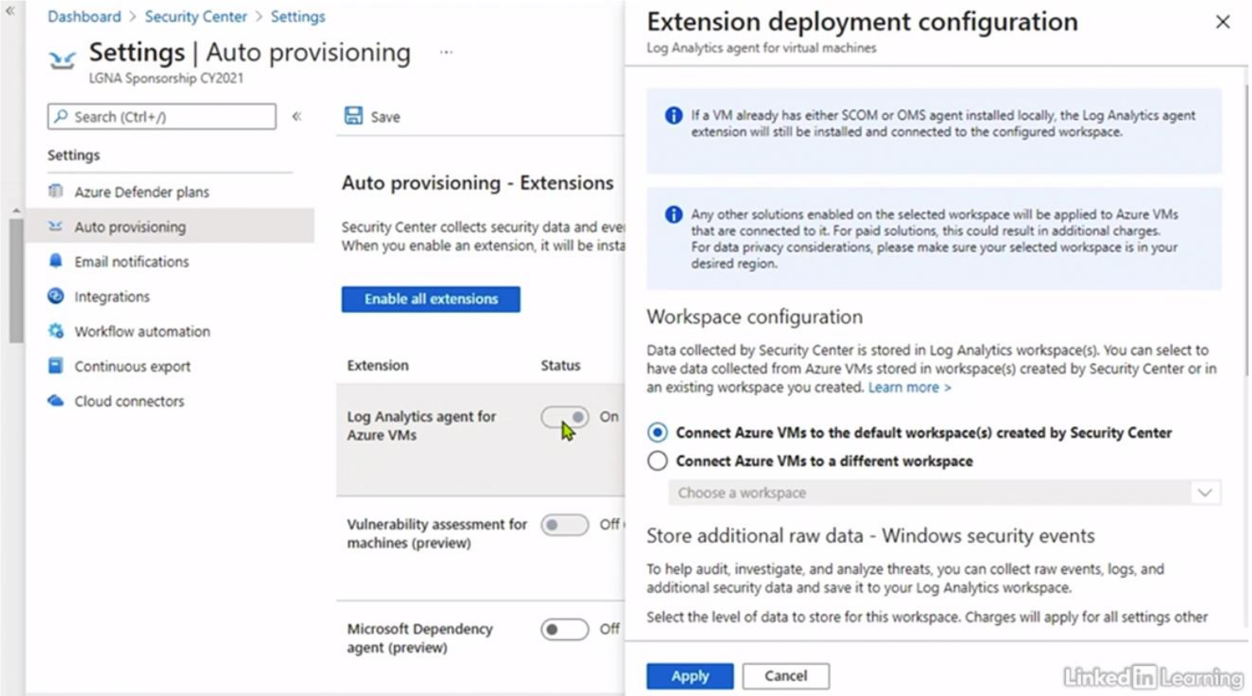
Settings | Auto provisioning

LGNA Sponsorship CY2021

Auto provisioning - Extensions

Security Center collects security data and events from your resources and services to help you prevent, detect, and respond to threats. When you enable an extension, it will be installed on any new or existing resource, by assigning a security policy. Learn more

Extension	Status	Resources missing e...	Description	Configuration
Log Analytics agent for Azure VMs	Off	2 of 2 virtual machines Show in inventory	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. Learn more	-
Vulnerability assessment for machines (preview)	Off ⓘ	2 of 2 virtual machines Show in inventory	Deploys vulnerability assessment to your Azure and hybrid machines. Learn more	-
Microsoft Dependency agent (preview)	Off ⓘ	0 of 0 virtual machines	You can collect and store network traffic data by onboarding to the VM Insights service. Learn more	-



Settings | Auto provisioning

LGNA Sponsorship CY2021

Auto provisioning - Extensions

Security Center collects security data and eve
When you enable an extension, it will be insta

Extension	Status
Log Analytics agent for Azure VMs	On
Vulnerability assessment for machines (preview)	Off
Microsoft Dependency agent (preview)	Off

Extension deployment configuration

Log Analytics agent for virtual machines

ⓘ If a VM already has either SCOM or OMS agent installed locally, the Log Analytics agent extension will still be installed and connected to the configured workspace.

ⓘ Any other solutions enabled on the selected workspace will be applied to Azure VMs that are connected to it. For paid solutions, this could result in additional charges. For data privacy considerations, please make sure your selected workspace is in your desired region.

Workspace configuration

Data collected by Security Center is stored in Log Analytics workspace(s). You can select to have data collected from Azure VMs stored in workspace(s) created by Security Center or in an existing workspace you created. Learn more >

● **Connect Azure VMs to the default workspace(s) created by Security Center**

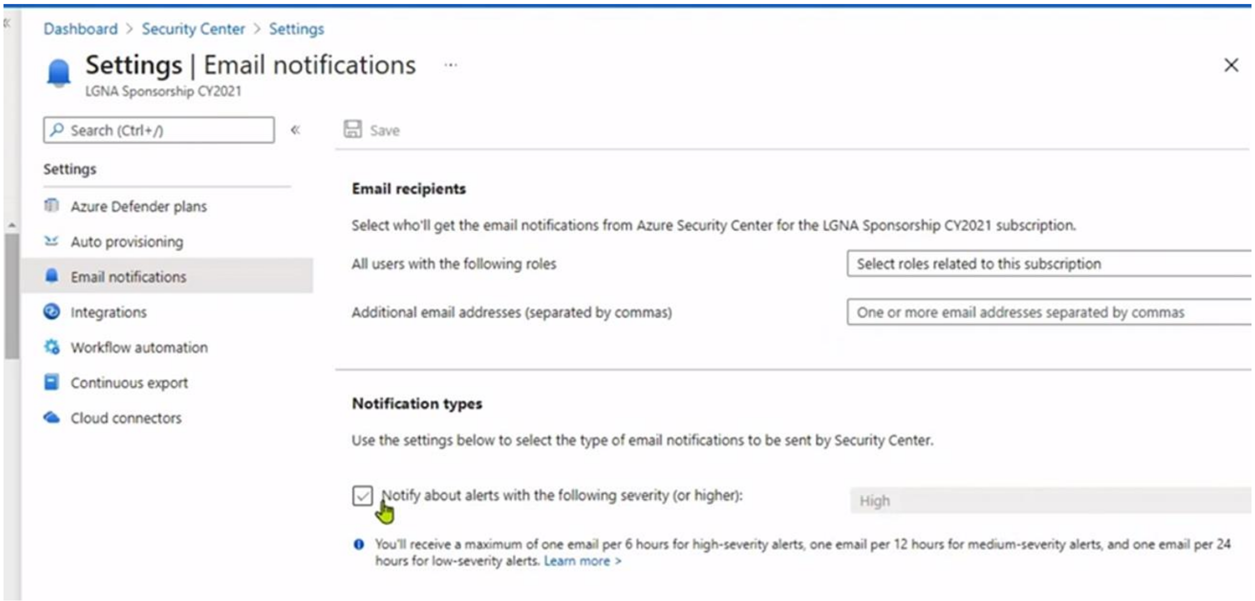
○ **Connect Azure VMs to a different workspace**

Choose a workspace

Store additional raw data - Windows security events

To help audit, investigate, and analyze threats, you can collect raw events, logs, and additional security data and save it to your Log Analytics workspace.

Select the level of data to store for this workspace. Charges will apply for all settings other



Dashboard > Security Center > Settings

Settings | Email notifications ...

LGNA Sponsorship CY2021

Email recipients

Select who'll get the email notifications from Azure Security Center for the LGNA Sponsorship CY2021 subscription.

All users with the following roles: Select roles related to this subscription

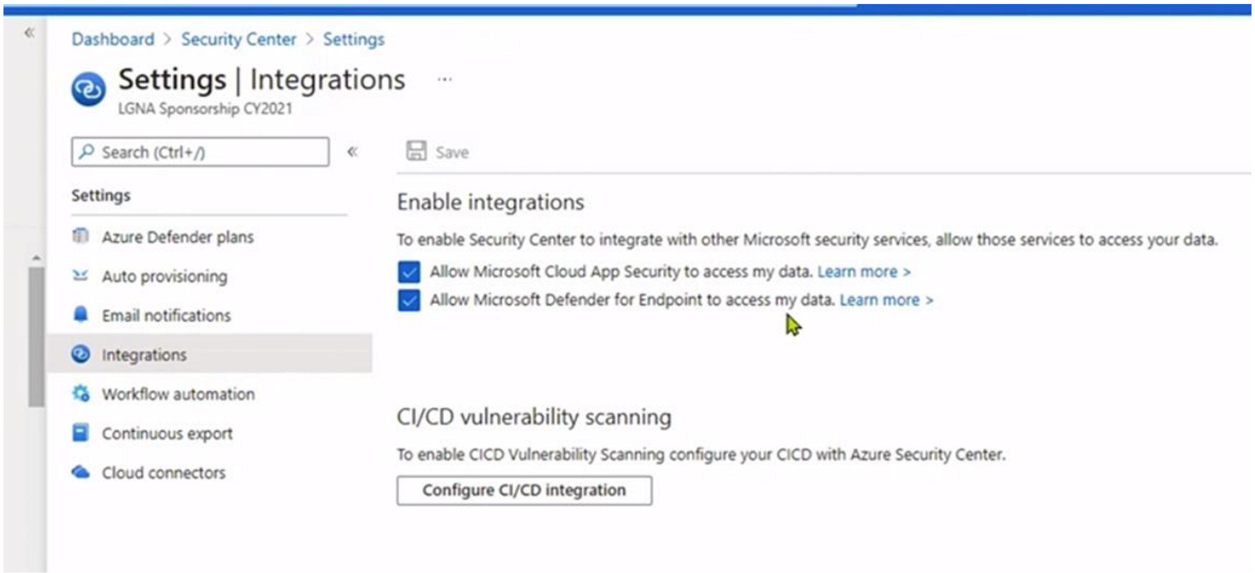
Additional email addresses (separated by commas): One or more email addresses separated by commas

Notification types

Use the settings below to select the type of email notifications to be sent by Security Center.

☑ Notify about alerts with the following severity (or higher): High

You'll receive a maximum of one email per 6 hours for high-severity alerts, one email per 12 hours for medium-severity alerts, and one email per 24 hours for low-severity alerts. Learn more >



Dashboard > Security Center > Settings

Settings | Integrations ...

LGNA Sponsorship CY2021

Enable integrations

To enable Security Center to integrate with other Microsoft security services, allow those services to access your data.

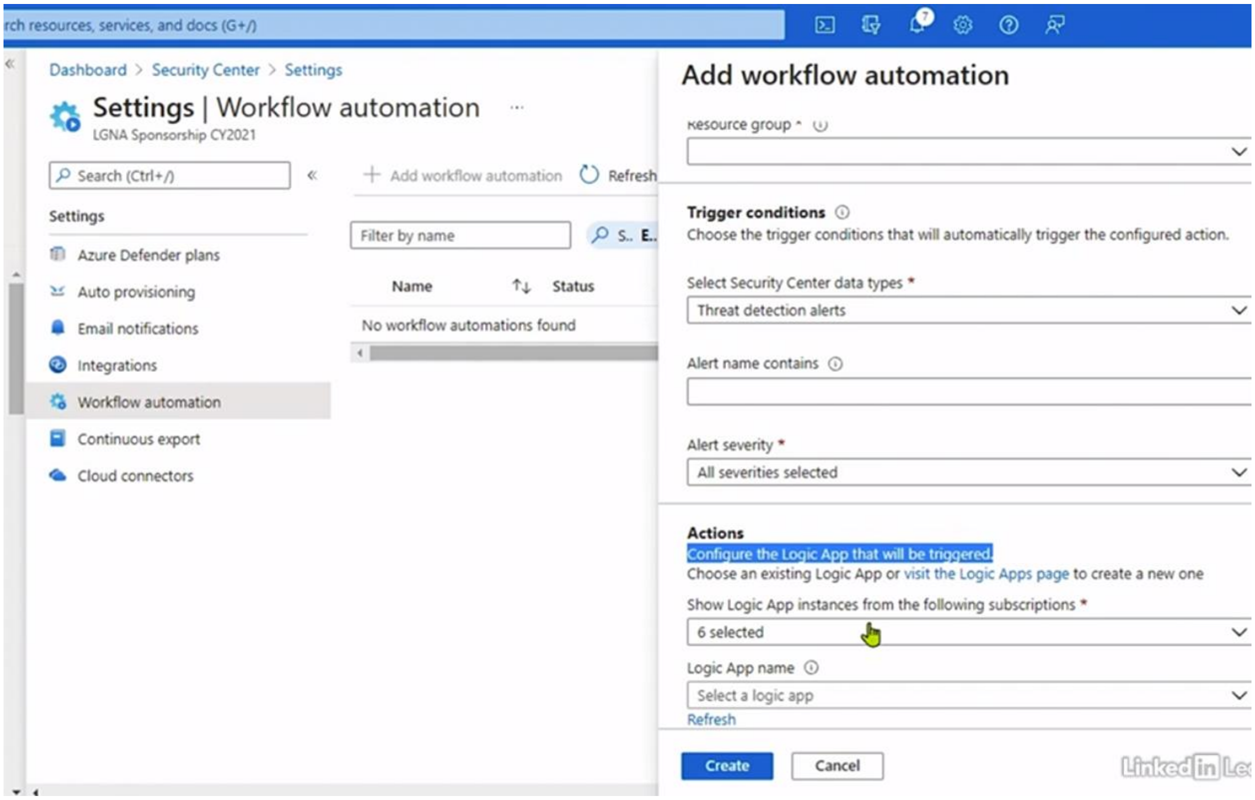
☑ Allow Microsoft Cloud App Security to access my data. Learn more >

☑ Allow Microsoft Defender for Endpoint to access my data. Learn more >

CI/CD vulnerability scanning

To enable CICD Vulnerability Scanning configure your CICD with Azure Security Center.

Configure CI/CD integration



Settings | Workflow automation

LGNA Sponsorship CY2021

No workflow automations found

Add workflow automation

Resource group *

Trigger conditions

Choose the trigger conditions that will automatically trigger the configured action.

Select Security Center data types *: Threat detection alerts

Alert name contains

Alert severity *: All severities selected

Actions

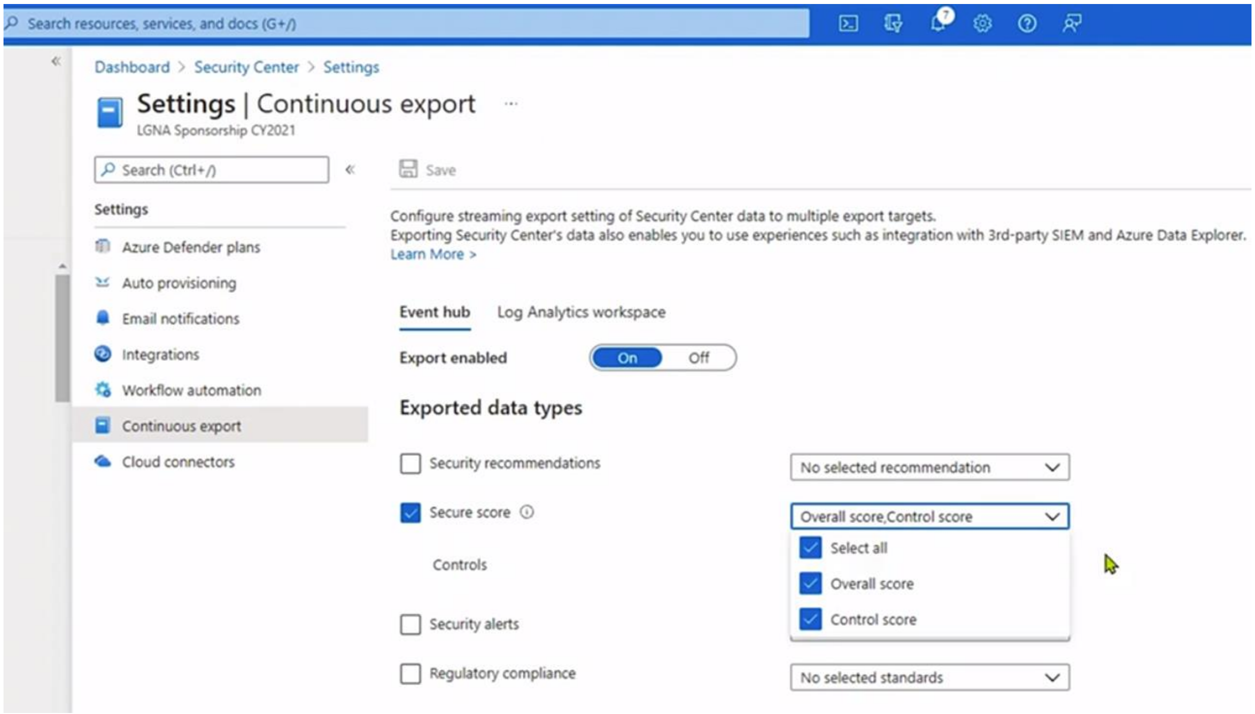
Configure the Logic App that will be triggered.

Choose an existing Logic App or visit the Logic Apps page to create a new one

Show Logic App instances from the following subscriptions *: 6 selected

Logic App name: Select a logic app

Refresh



Settings | Continuous export

LGNA Sponsorship CY2021

Configure streaming export setting of Security Center data to multiple export targets.
Exporting Security Center's data also enables you to use experiences such as integration with 3rd-party SIEM and Azure Data Explorer.
Learn More >

Event hub | Log Analytics workspace

Export enabled: ● On ○ Off

Exported data types

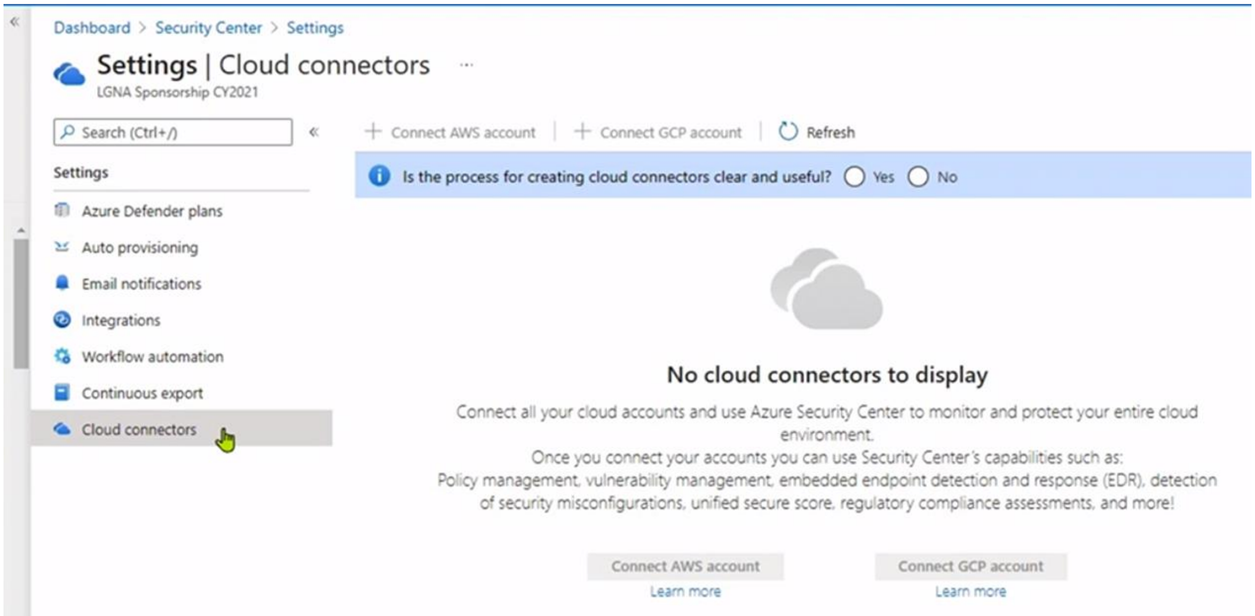
□ Security recommendations — No selected recommendation

☑ Secure score — Overall score,Control score
- ☑ Select all
- ☑ Overall score
- ☑ Control score

Controls

□ Security alerts

□ Regulatory compliance — No selected standards



Dashboard > Security Center > Settings

Settings | Cloud connectors ···

LGNA Sponsorship CY2021

Search (Ctrl+/) «

Settings

- Azure Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export
- Cloud connectors

+ Connect AWS account | + Connect GCP account | Refresh

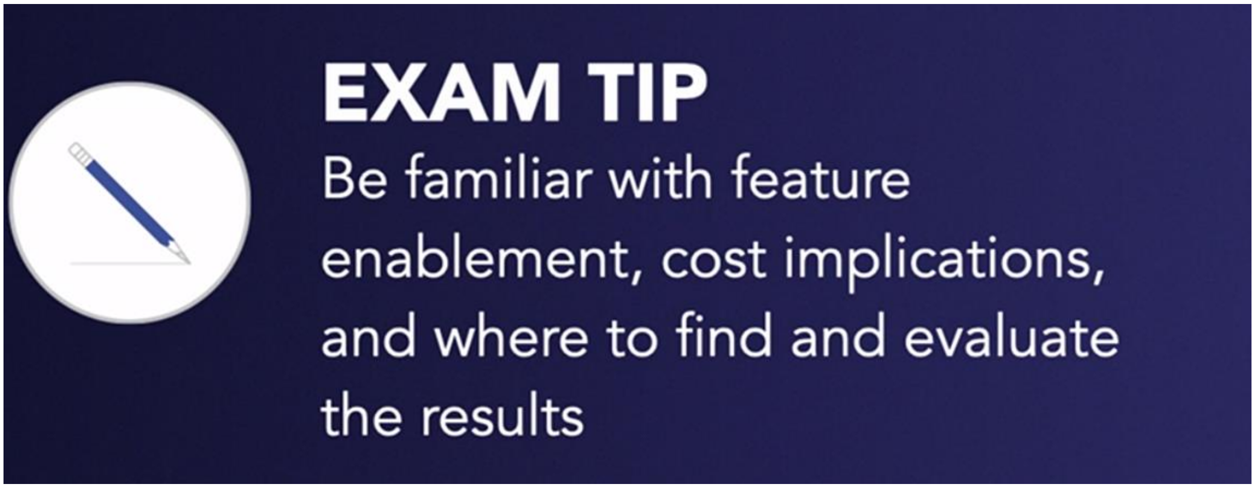
Is the process for creating cloud connectors clear and useful? ○ Yes ○ No

No cloud connectors to display

Connect all your cloud accounts and use Azure Security Center to monitor and protect your entire cloud environment.
Once you connect your accounts you can use Security Center's capabilities such as:
Policy management, vulnerability management, embedded endpoint detection and response (EDR), detection of security misconfigurations, unified secure score, regulatory compliance assessments, and more!

Connect AWS account
Learn more

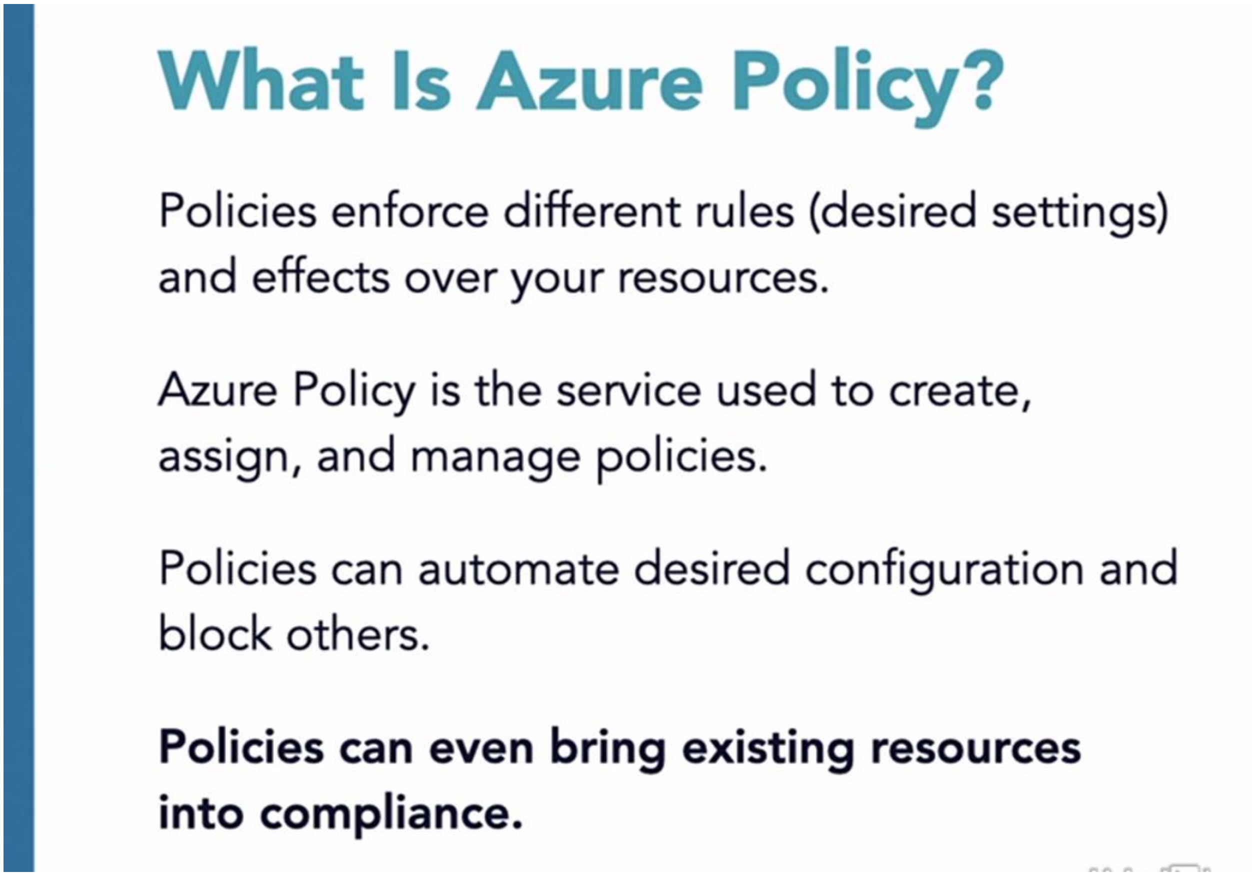
Connect GCP account
Learn more



EXAM TIP

Be familiar with feature enablement, cost implications, and where to find and evaluate the results

2.2 Evaluate vulnerability scans from Azure Defender



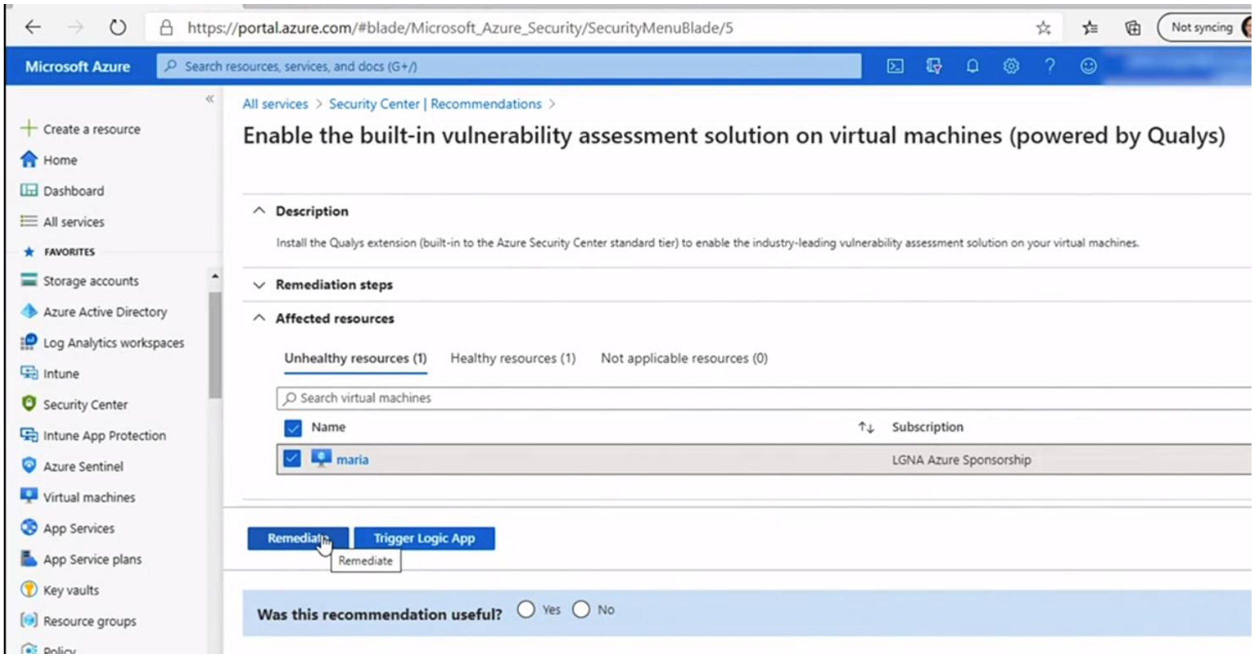
What Is Azure Policy?

Policies enforce different rules (desired settings) and effects over your resources.

Azure Policy is the service used to create, assign, and manage policies.

Policies can automate desired configuration and block others.

Policies can even bring existing resources into compliance.



Enable the built-in vulnerability assessment solution on virtual machines (powered by Qualys)

Description

Install the Qualys extension (built-in to the Azure Security Center standard tier) to enable the industry-leading vulnerability assessment solution on your virtual machines.

Remediation steps

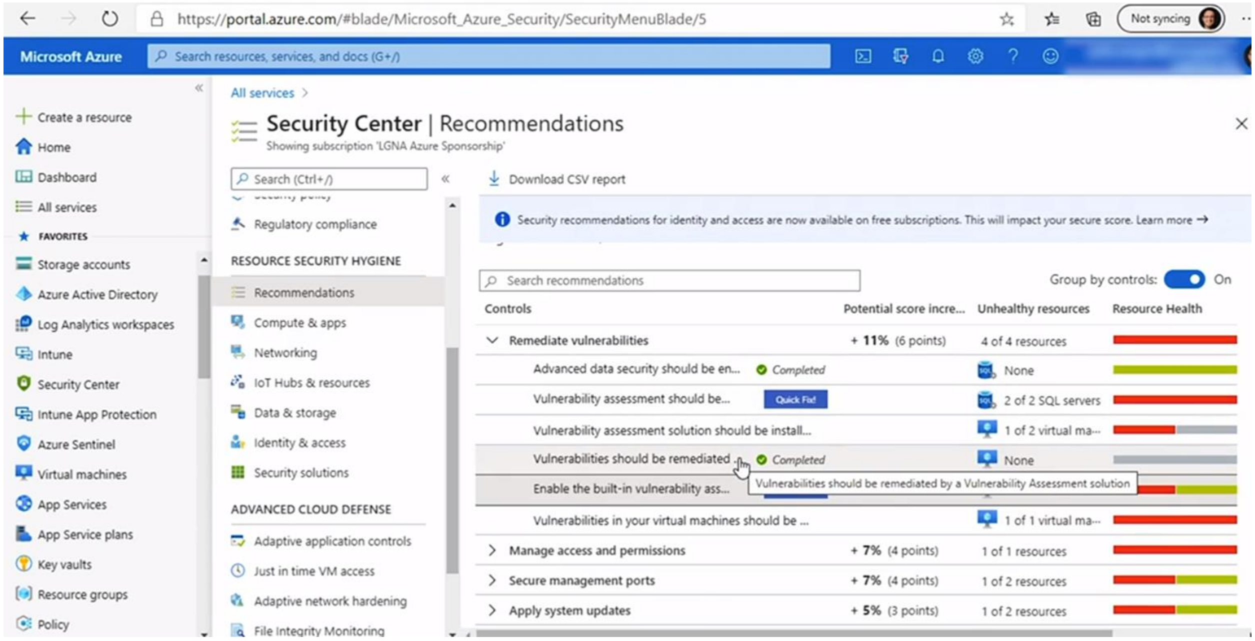
Affected resources

Unhealthy resources (1) | Healthy resources (1) | Not applicable resources (0)

Search virtual machines

☑ Name	Subscription
☑ maria	LGNA Azure Sponsorship

Was this recommendation useful? ○ Yes ○ No



Security Center | Recommendations

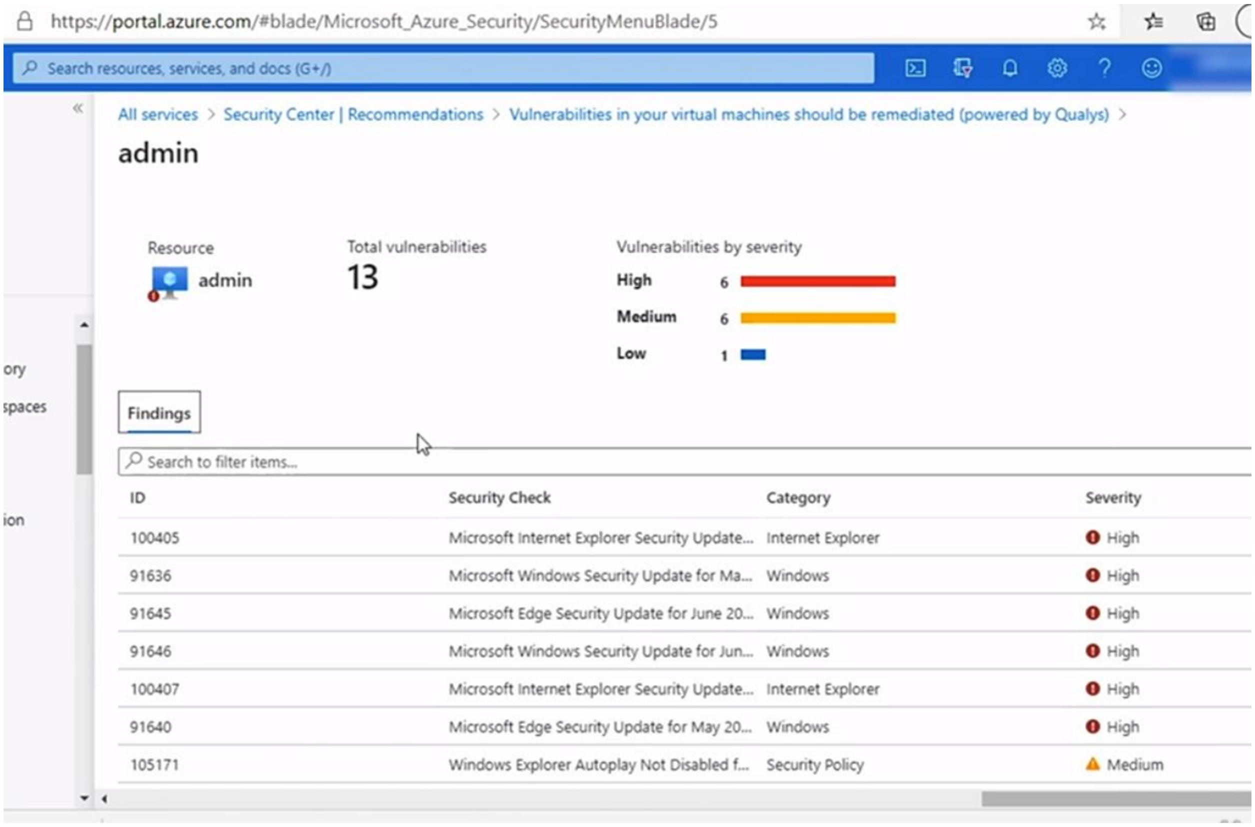
Showing subscription 'LGNA Azure Sponsorship'

Security recommendations for identity and access are now available on free subscriptions. This will impact your secure score. Learn more →

Group by controls: On

Controls		Potential score incre...	Unhealthy resources	Resource Health
Remediate vulnerabilities		+ 11% (6 points)	4 of 4 resources	
Advanced data security should be en...	Completed		None	
Vulnerability assessment should be...	Quick Fix!		2 of 2 SQL servers	
Vulnerability assessment solution should be install...			1 of 2 virtual ma...	
Vulnerabilities should be remediated ...	Completed		None	
Enable the built-in vulnerability ass...				
Vulnerabilities in your virtual machines should be ...			1 of 1 virtual ma...	
Manage access and permissions		+ 7% (4 points)	1 of 1 resources	
Secure management ports		+ 7% (4 points)	1 of 2 resources	
Apply system updates		+ 5% (3 points)	1 of 2 resources	

Vulnerabilities should be remediated by a Vulnerability Assessment solution


https://portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/5
Search resources, services, and docs (G+/)
ory
spaces
ion
Findings
Search to filter items...

All services > Security Center | Recommendations > Vulnerabilities in your virtual machines should be remediated (powered by Qualys) >

admin

Resource: admin

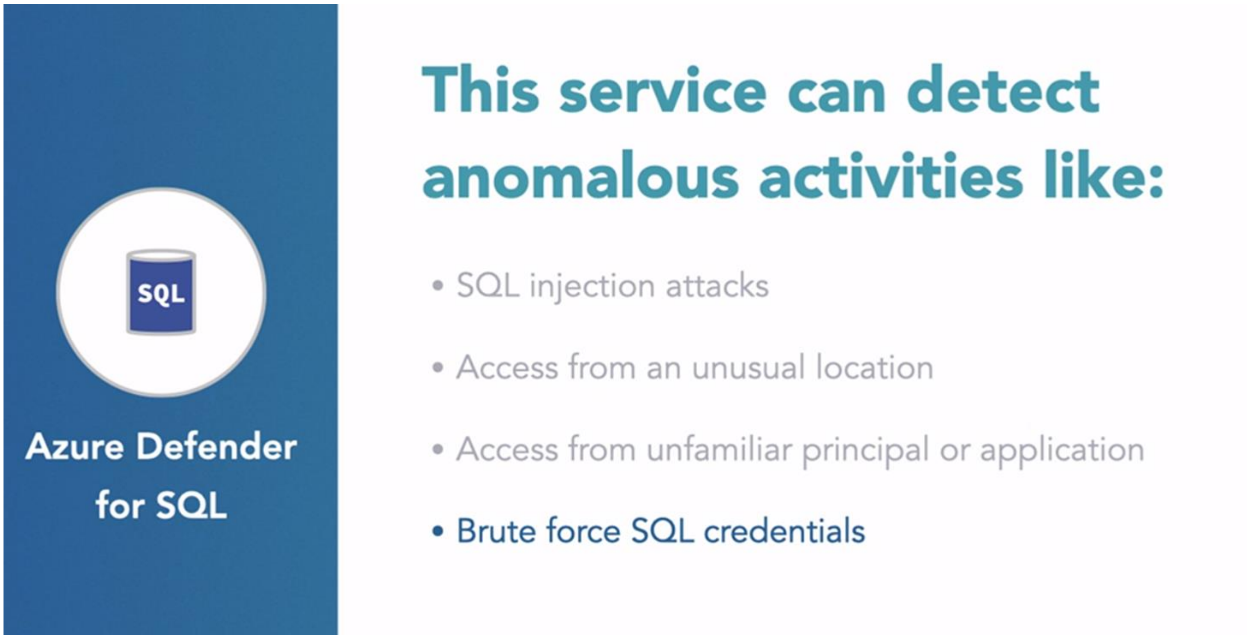
Total vulnerabilities: 13

Vulnerabilities by severity

High	6
Medium	6
Low	1

ID	Security Check	Category	Severity
100405	Microsoft Internet Explorer Security Update...	Internet Explorer	High
91636	Microsoft Windows Security Update for Ma...	Windows	High
91645	Microsoft Edge Security Update for June 20...	Windows	High
91646	Microsoft Windows Security Update for Jun...	Windows	High
100407	Microsoft Internet Explorer Security Update...	Internet Explorer	High
91640	Microsoft Edge Security Update for May 20...	Windows	High
105171	Windows Explorer Autoplay Not Disabled f...	Security Policy	Medium

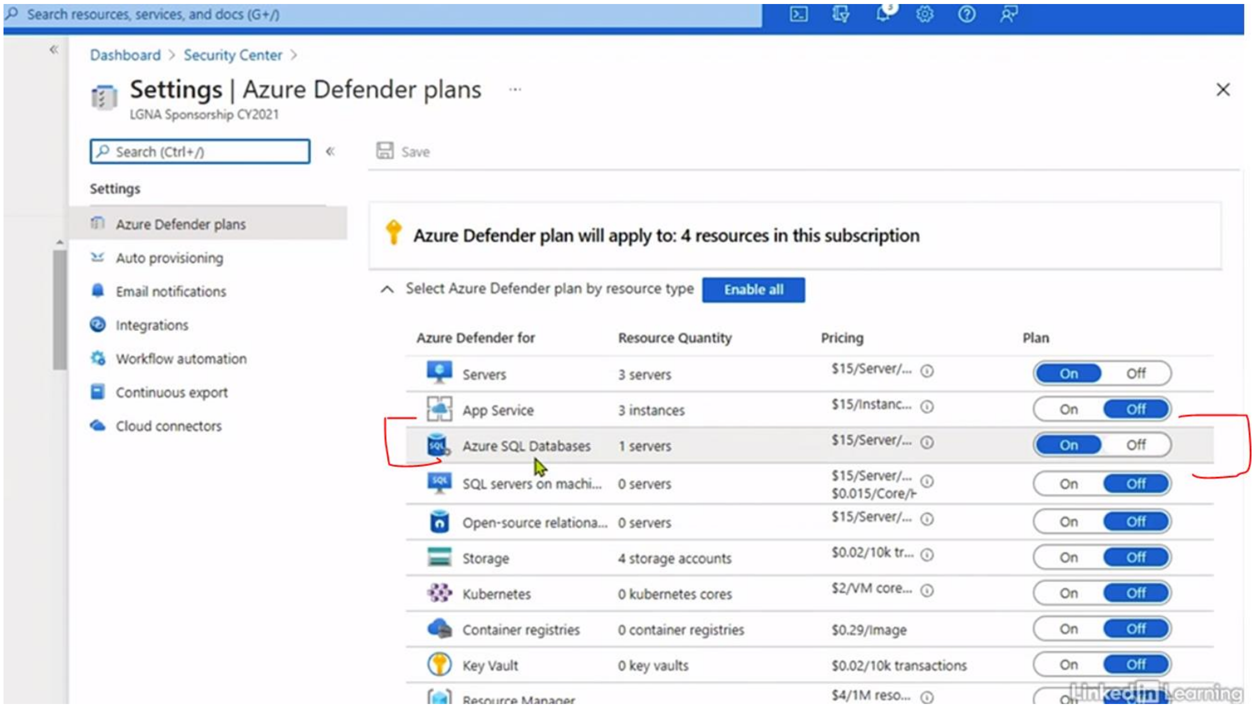
2.3 Configure Azure Defender for SQL



Azure Defender for SQL

This service can detect anomalous activities like:

- SQL injection attacks
- Access from an unusual location
- Access from unfamiliar principal or application
- Brute force SQL credentials



Dashboard > Security Center >

Settings | Azure Defender plans ···

LGNA Sponsorship CY2021

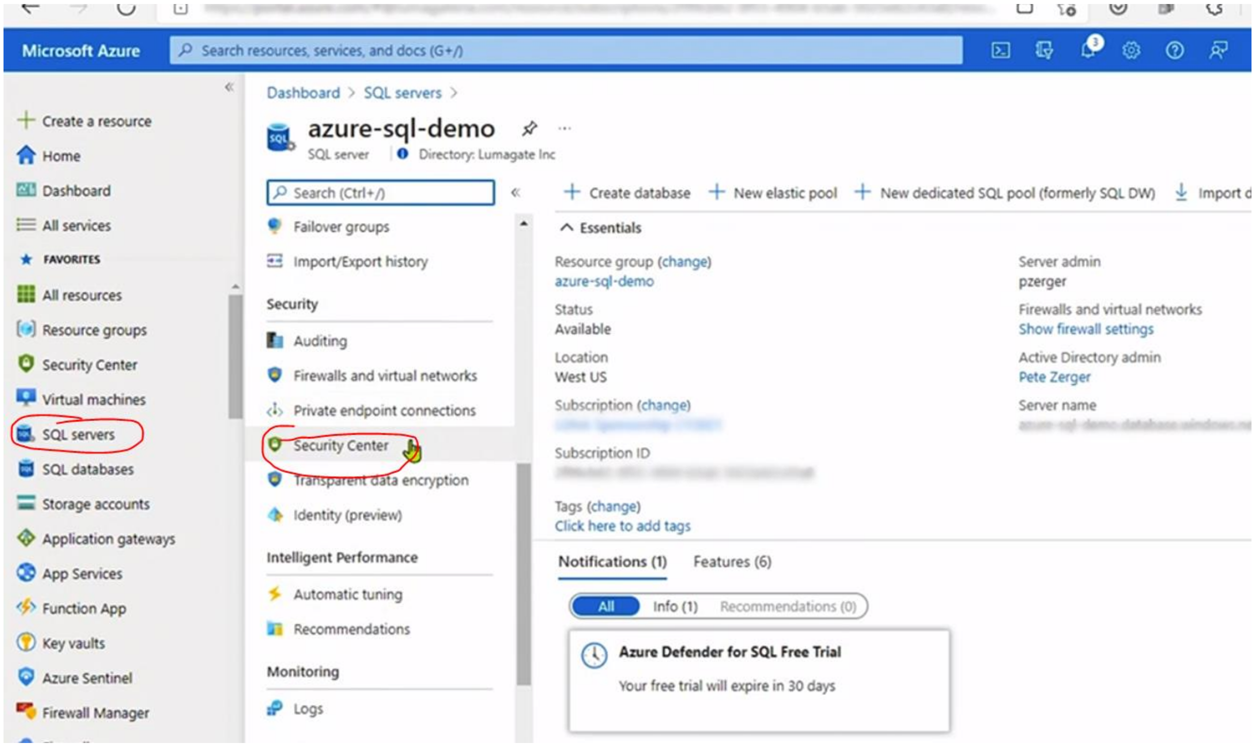
Settings

- Azure Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export
- Cloud connectors

Azure Defender plan will apply to: 4 resources in this subscription

Select Azure Defender plan by resource type **Enable all**

Azure Defender for	Resource Quantity	Pricing	Plan
Servers	3 servers	$15/Server/...	[✓ On] Off
App Service	3 instances	$15/Instanc...	On [✓ Off]
Azure SQL Databases	1 servers	$15/Server/...	[✓ On] Off
SQL servers on machi...	0 servers	$15/Server/... $0.015/Core/ŀ	On [✓ Off]
Open-source relationa...	0 servers	$15/Server/...	On [✓ Off]
Storage	4 storage accounts	$0.02/10k tr...	On [✓ Off]
Kubernetes	0 kubernetes cores	$2/VM core...	On [✓ Off]
Container registries	0 container registries	$0.29/Image	On [✓ Off]
Key Vault	0 key vaults	$0.02/10k transactions	On [✓ Off]
Resource Manager		$4/1M reso...	



[redacted]

azure-sql-demo

SQL server | Directory: Lumagate Inc

Resource group (change)
azure-sql-demo

Status
Available

Location
West US

Subscription (change)
[redacted]

Subscription ID
[redacted]

Tags (change)
Click here to add tags

Server admin
pzerger

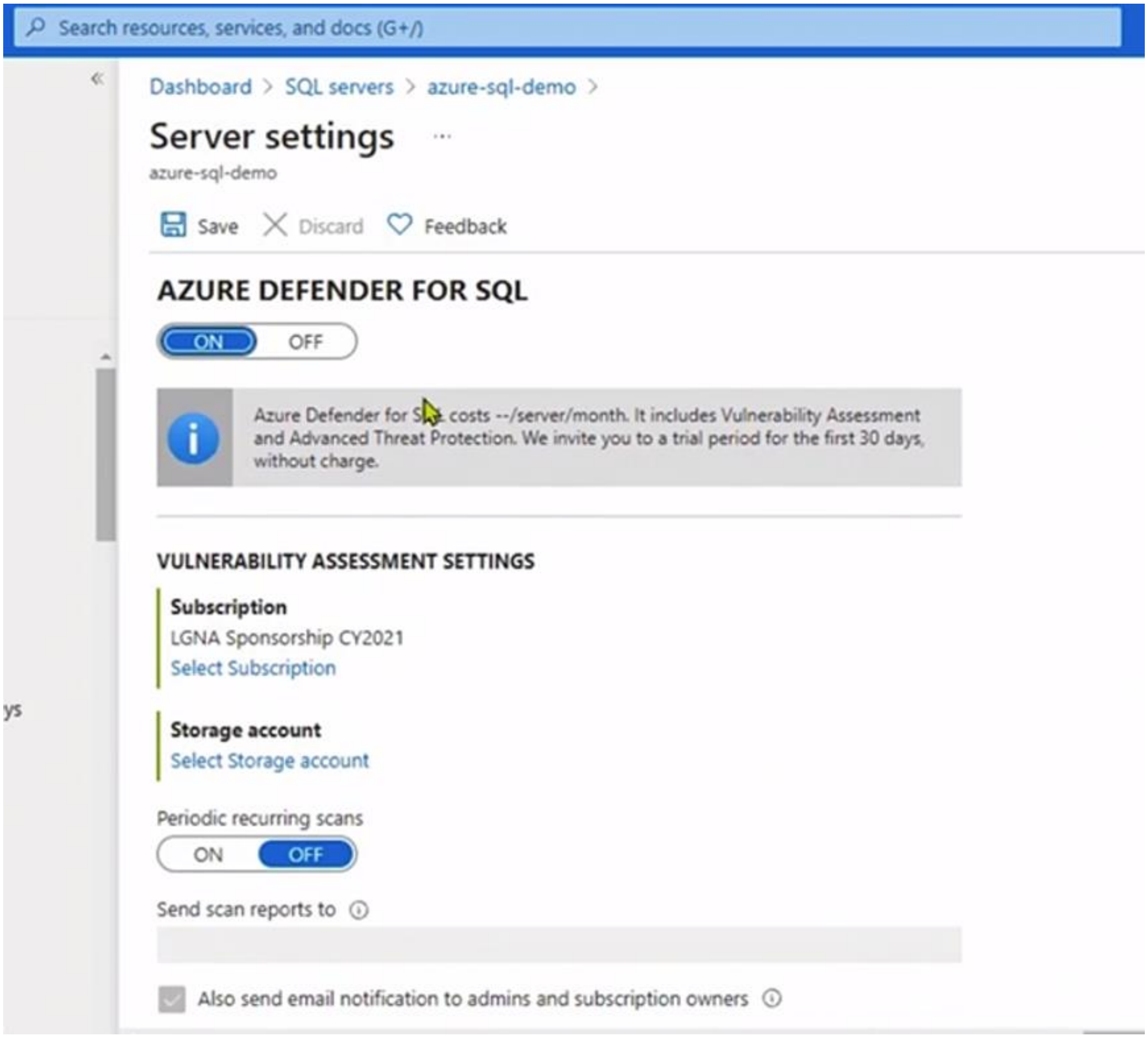
Firewalls and virtual networks
Show firewall settings

Active Directory admin
Pete Zerger

Server name
[redacted]

Azure Defender for SQL Free Trial

Your free trial will expire in 30 days



Search resources, services, and docs (G+/)
Dashboard > SQL servers > azure-sql-demo >
ys

Server settings ...

azure-sql-demo

Save Discard Feedback

AZURE DEFENDER FOR SQL

ON OFF

Azure Defender for SQL costs --/server/month. It includes Vulnerability Assessment and Advanced Threat Protection. We invite you to a trial period for the first 30 days, without charge.

VULNERABILITY ASSESSMENT SETTINGS

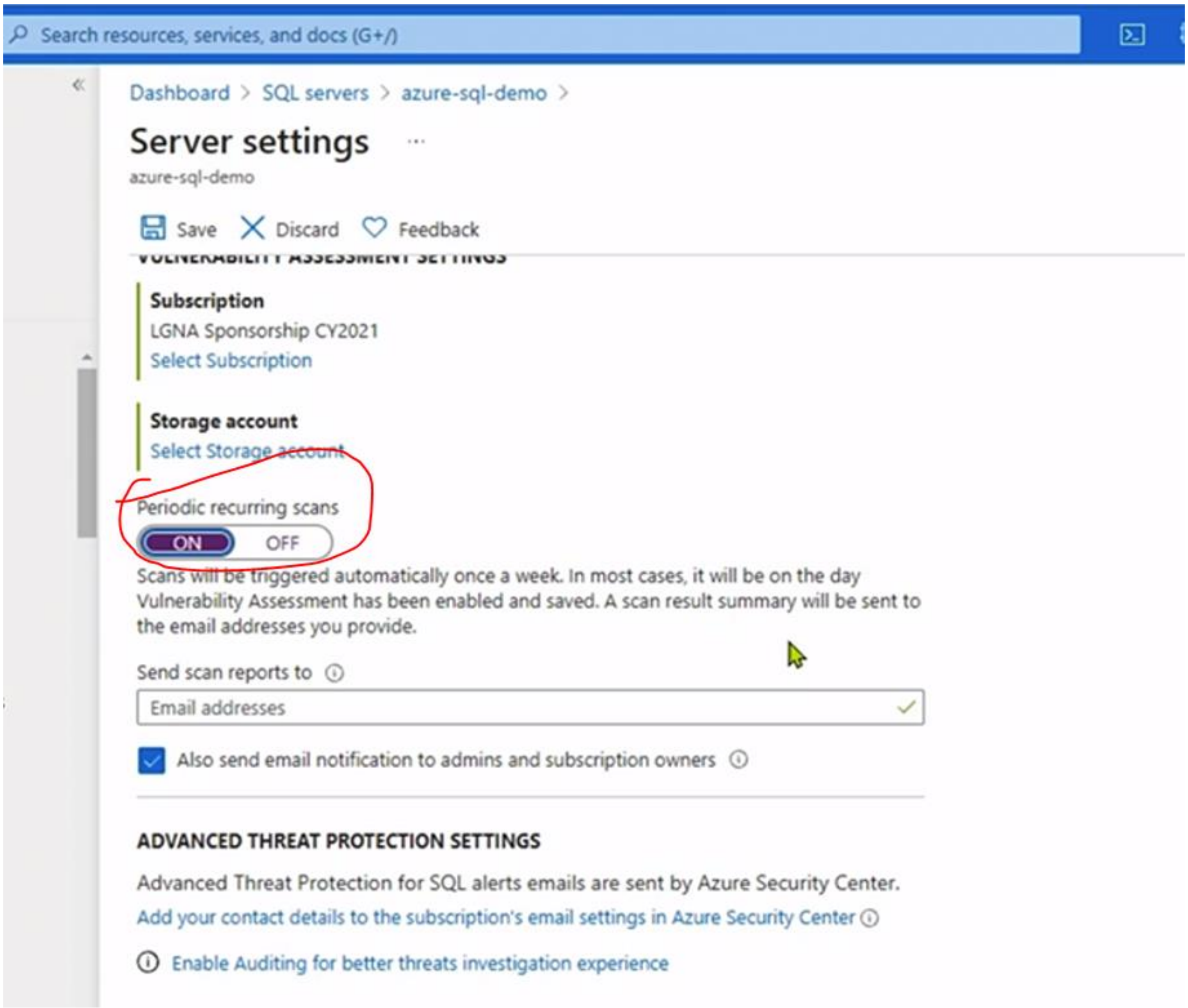
Subscription
LGNA Sponsorship CY2021
Select Subscription

Storage account
Select Storage account

Periodic recurring scans
ON OFF

Send scan reports to ⓘ

☑ Also send email notification to admins and subscription owners ⓘ


Search resources, services, and docs (G+/)
Dashboard > SQL servers > azure-sql-demo >
Save
Discard
Feedback

Server settings ...

azure-sql-demo

VULNERABILITY ASSESSMENT SETTINGS

Subscription

LGNA Sponsorship CY2021

Select Subscription

Storage account

Select Storage account

Periodic recurring scans

ON OFF

Scans will be triggered automatically once a week. In most cases, it will be on the day Vulnerability Assessment has been enabled and saved. A scan result summary will be sent to the email addresses you provide.

Send scan reports to ⓘ

Email addresses

☑ Also send email notification to admins and subscription owners ⓘ

ADVANCED THREAT PROTECTION SETTINGS

Advanced Threat Protection for SQL alerts emails are sent by Azure Security Center.

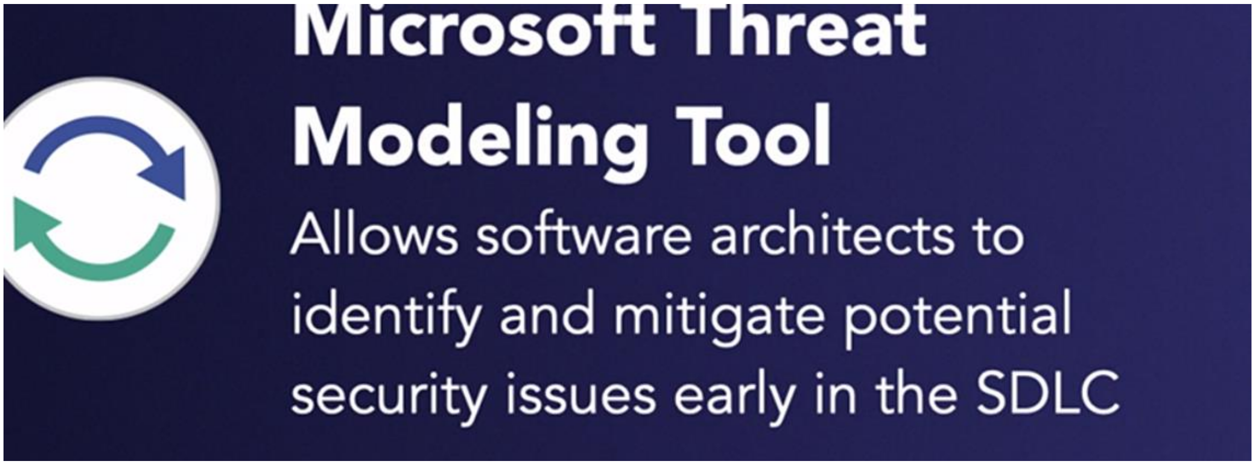
Add your contact details to the subscription's email settings in Azure Security Center ⓘ

ⓘ Enable Auditing for better threats investigation experience

EXAM TIP

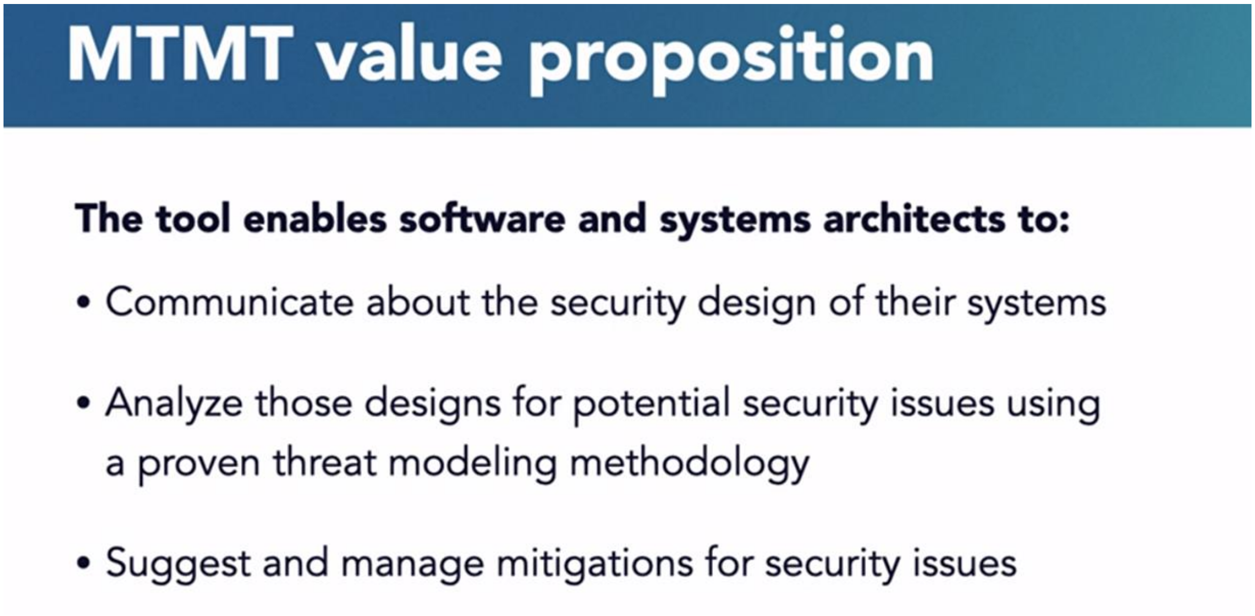
Know how to configure Azure Defender for SQL and the protections it offers.

2.4 Use the Microsoft Threat Modeling Tool



Microsoft Threat Modeling Tool

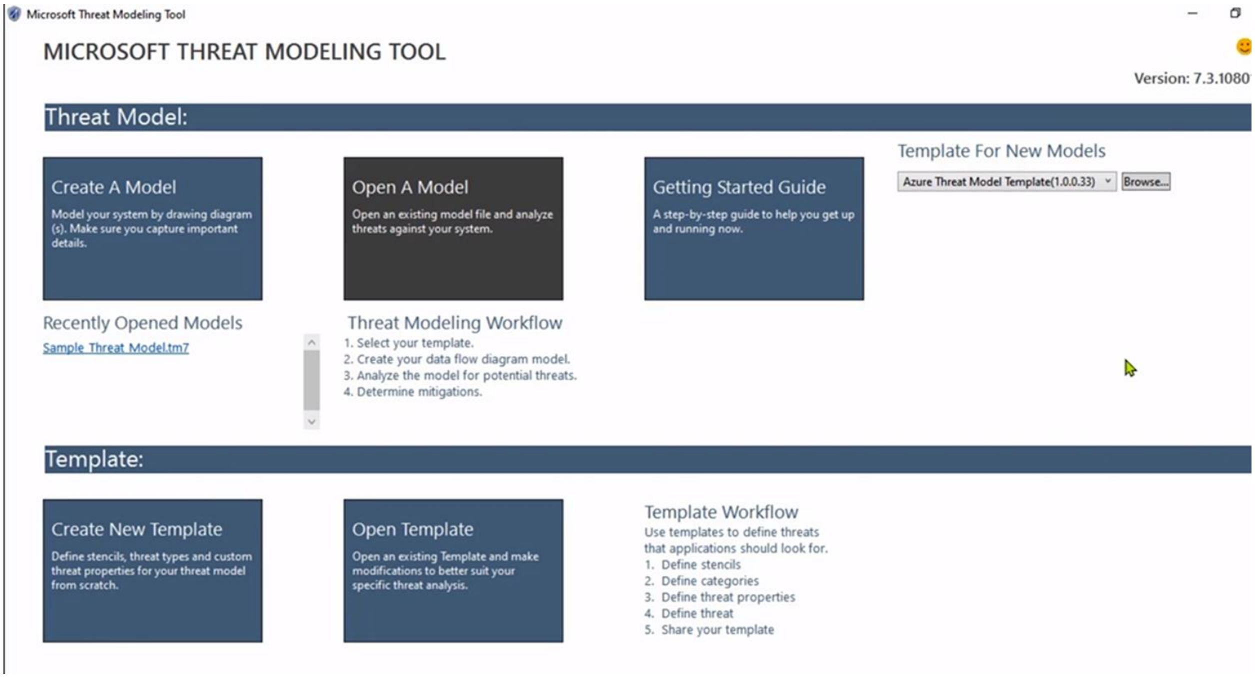
Allows software architects to identify and mitigate potential security issues early in the SDLC



MTMT value proposition

The tool enables software and systems architects to:

- Communicate about the security design of their systems
- Analyze those designs for potential security issues using a proven threat modeling methodology
- Suggest and manage mitigations for security issues



MICROSOFT THREAT MODELING TOOL

Version: 7.3.1080

Threat Model:

Create A Model
Model your system by drawing diagram (s). Make sure you capture important details.

Open A Model
Open an existing model file and analyze threats against your system.

Getting Started Guide
A step-by-step guide to help you get up and running now.

Template For New Models
Azure Threat Model Template(1.0.0.33)

Recently Opened Models
Sample Threat Model.tm7

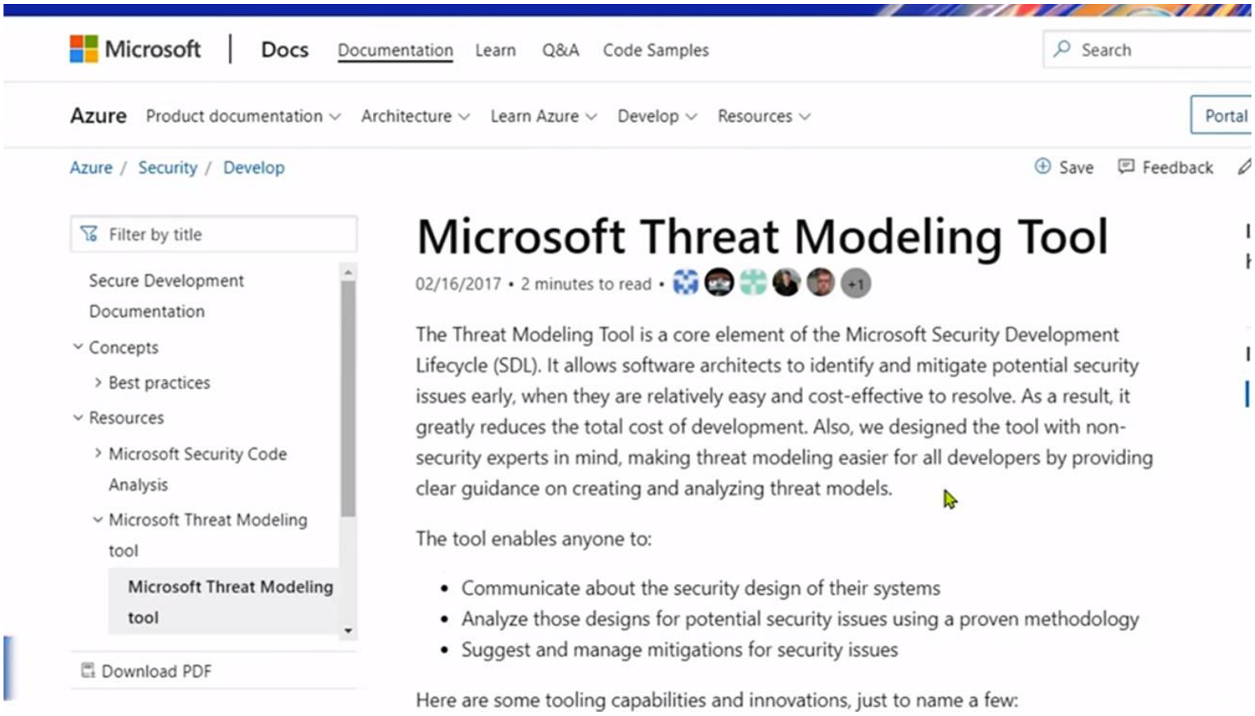
Threat Modeling Workflow
1. Select your template.
2. Create your data flow diagram model.
3. Analyze the model for potential threats.
4. Determine mitigations.

Template:

Create New Template
Define stencils, threat types and custom threat properties for your threat model from scratch.

Open Template
Open an existing Template and make modifications to better suit your specific threat analysis.

Template Workflow
Use templates to define threats that applications should look for.
1. Define stencils
2. Define categories
3. Define threat properties
4. Define threat
5. Share your template



Microsoft Threat Modeling Tool

02/16/2017 • 2 minutes to read • +1

The Threat Modeling Tool is a core element of the Microsoft Security Development Lifecycle (SDL). It allows software architects to identify and mitigate potential security issues early, when they are relatively easy and cost-effective to resolve. As a result, it greatly reduces the total cost of development. Also, we designed the tool with non-security experts in mind, making threat modeling easier for all developers by providing clear guidance on creating and analyzing threat models.

The tool enables anyone to:

- Communicate about the security design of their systems
- Analyze those designs for potential security issues using a proven methodology
- Suggest and manage mitigations for security issues

Here are some tooling capabilities and innovations, just to name a few:

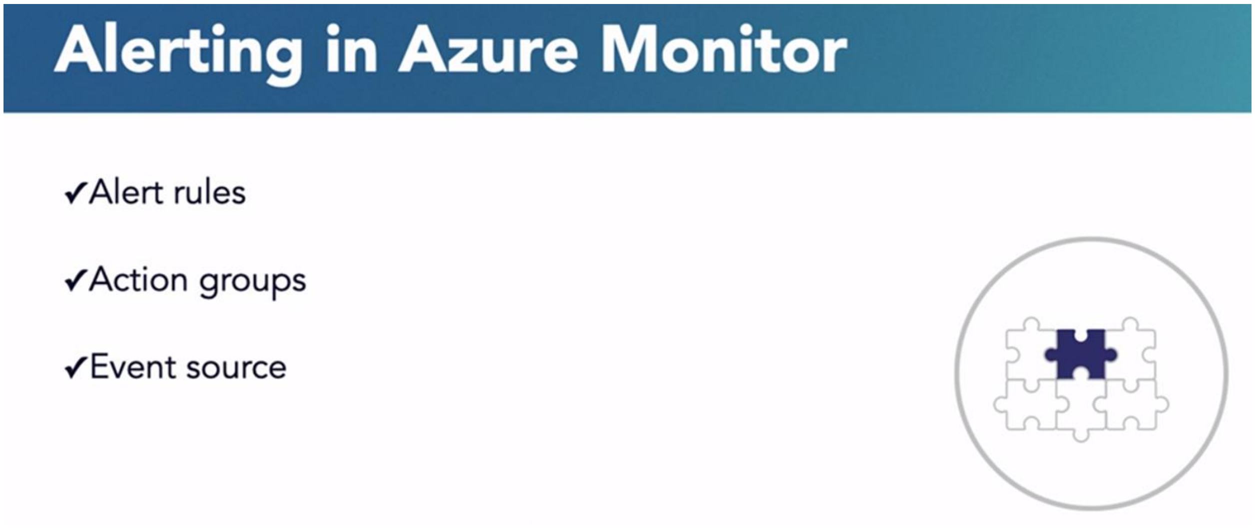
EXAM TIP

Know the purpose and process behind the Microsoft Threat Modeling Tool, and how to use it.

2.5 Quiz

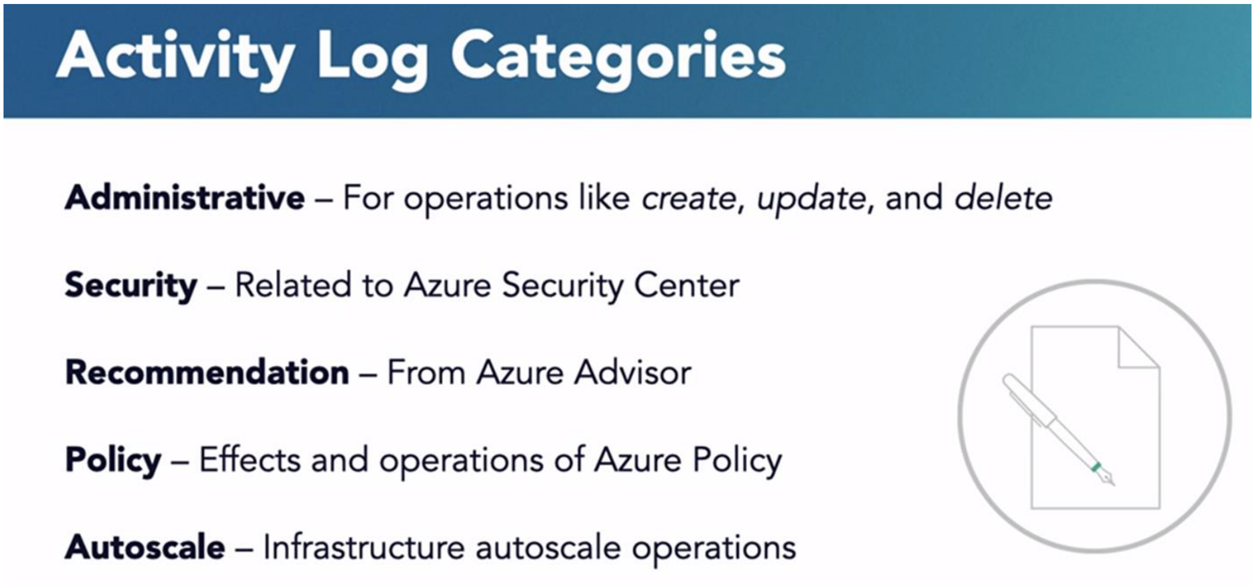
3. Configure and Manage Security Monitoring

3.1 Create and customize alert rules using Azure Monitor



Alerting in Azure Monitor

- ✓Alert rules
- ✓Action groups
- ✓Event source



Activity Log Categories

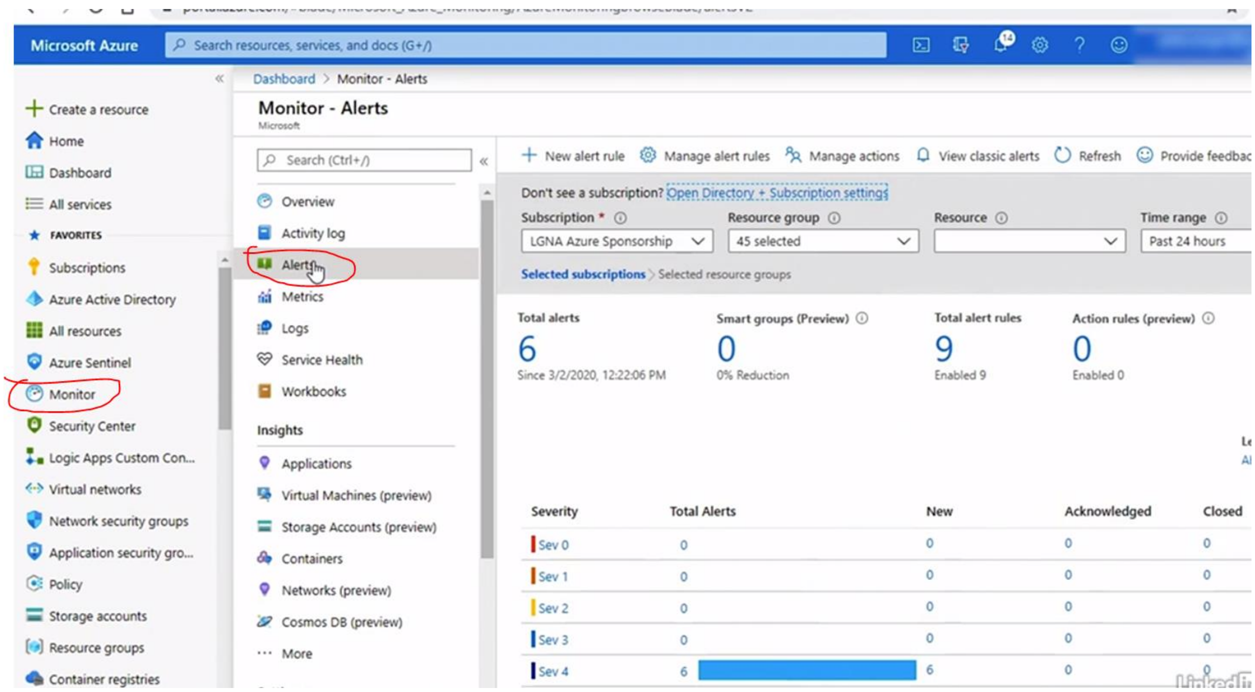
Administrative – For operations like *create*, *update*, and *delete*

Security – Related to Azure Security Center

Recommendation – From Azure Advisor

Policy – Effects and operations of Azure Policy

Autoscale – Infrastructure autoscale operations



Monitor - Alerts

Microsoft

Don't see a subscription? Open Directory + Subscription settings

Subscription * : LGNA Azure Sponsorship

Resource group: 45 selected

Resource:

Time range: Past 24 hours

Selected subscriptions > Selected resource groups

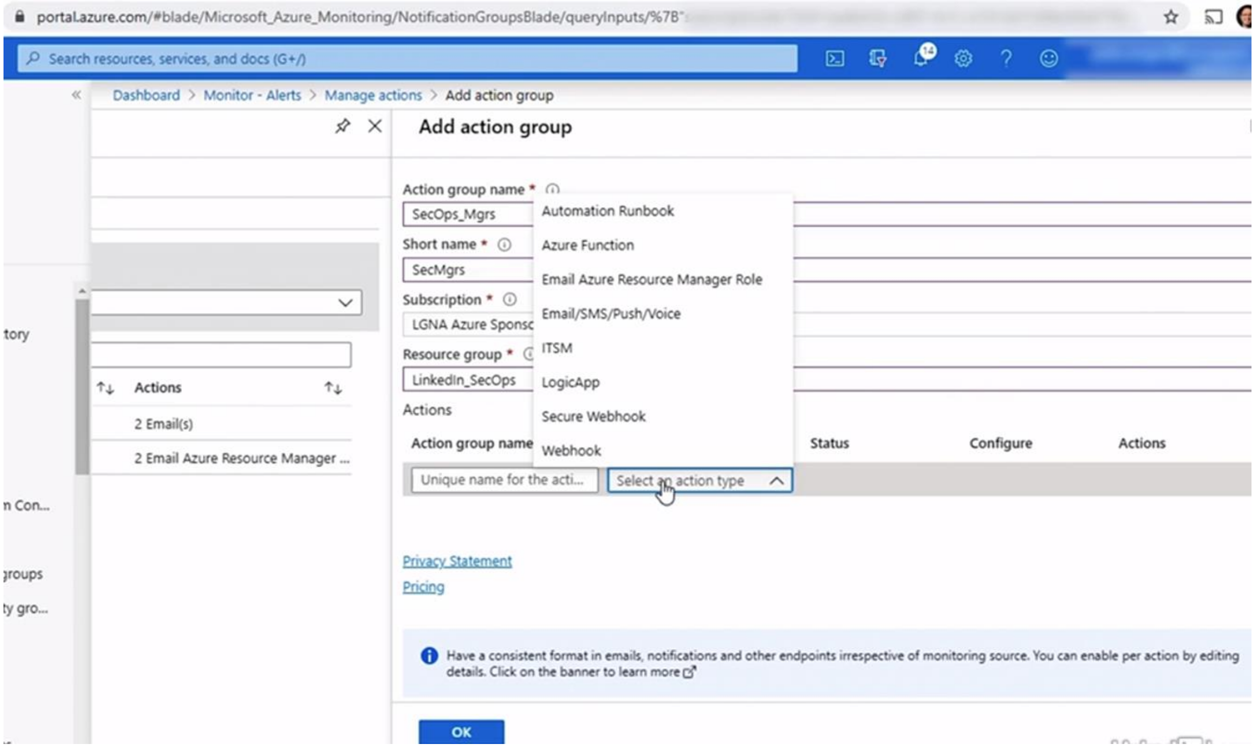
Total alerts: 6 — Since 3/2/2020, 12:22:06 PM

Smart groups (Preview): 0 — 0% Reduction

Total alert rules: 9 — Enabled 9

Action rules (preview): 0 — Enabled 0

Severity	Total Alerts	New	Acknowledged	Closed
Sev 0	0	0	0	0
Sev 1	0	0	0	0
Sev 2	0	0	0	0
Sev 3	0	0	0	0
Sev 4	6	6	0	0



portal.azure.com/#blade/Microsoft_Azure_Monitoring/NotificationGroupsBlade/queryInputs/%7B"

Dashboard > Monitor - Alerts > Manage actions > Add action group

Add action group

Action group name *: SecOps_Mgrs

Short name *: SecMgrs

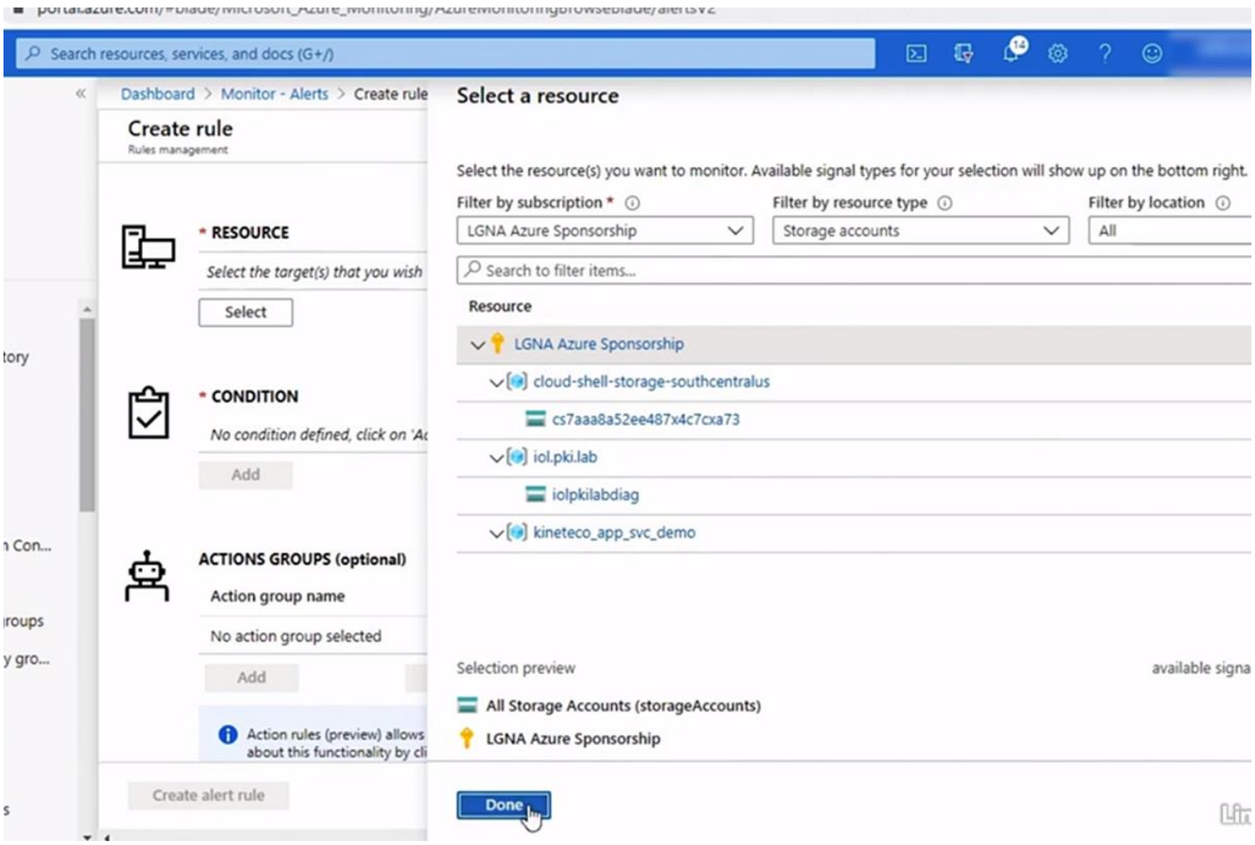
Subscription *: LGNA Azure Sponsc

Resource group *: LinkedIn_SecOps

Actions

Action group name	Action type	Status	Configure	Actions
Unique name for the acti...	Select an action type			

Have a consistent format in emails, notifications and other endpoints irrespective of monitoring source. You can enable per action by editing details. Click on the banner to learn more



portal.azure.com/#blade/Microsoft_Azure_Monitoring/AzureMonitoringBrowseBlade/alertsV2

Dashboard > Monitor - Alerts > Create rule

Create rule
Rules management

* RESOURCE
Select the target(s) that you wish

* CONDITION
No condition defined, click on 'Ac

ACTIONS GROUPS (optional)

Action group name
No action group selected

Action rules (preview) allows about this functionality by cli

Select a resource

Select the resource(s) you want to monitor. Available signal types for your selection will show up on the bottom right.

Filter by subscription *: LGNA Azure Sponsorship

Filter by resource type: Storage accounts

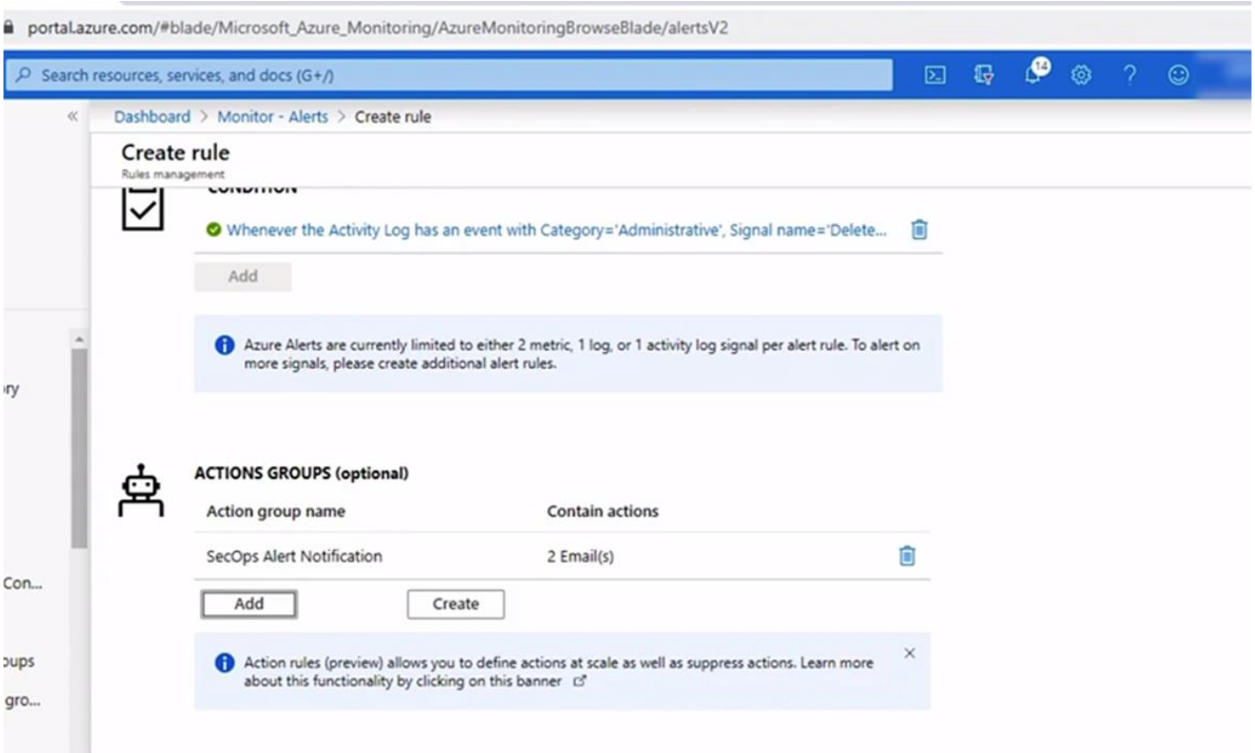
Filter by location: All

Resource
- LGNA Azure Sponsorship
  - cloud-shell-storage-southcentralus
    - cs7aaa8a52ee487x4c7cxa73
  - iol.pki.lab
    - iolpkilabdiag
  - kineteco_app_svc_demo

Selection preview
- All Storage Accounts (storageAccounts)
- LGNA Azure Sponsorship

available signa

Search resources, services, and docs (G+/)
tory
n Con...
roups
y gro...
s
Select
Add
Add
Create alert rule
Search to filter items...
Done



portal.azure.com/#blade/Microsoft_Azure_Monitoring/AzureMonitoringBrowseBlade/alertsV2

Dashboard > Monitor - Alerts > Create rule

Create rule
Rules management

CONDITION

Whenever the Activity Log has an event with Category='Administrative', Signal name='Delete...

Add

Azure Alerts are currently limited to either 2 metric, 1 log, or 1 activity log signal per alert rule. To alert on more signals, please create additional alert rules.

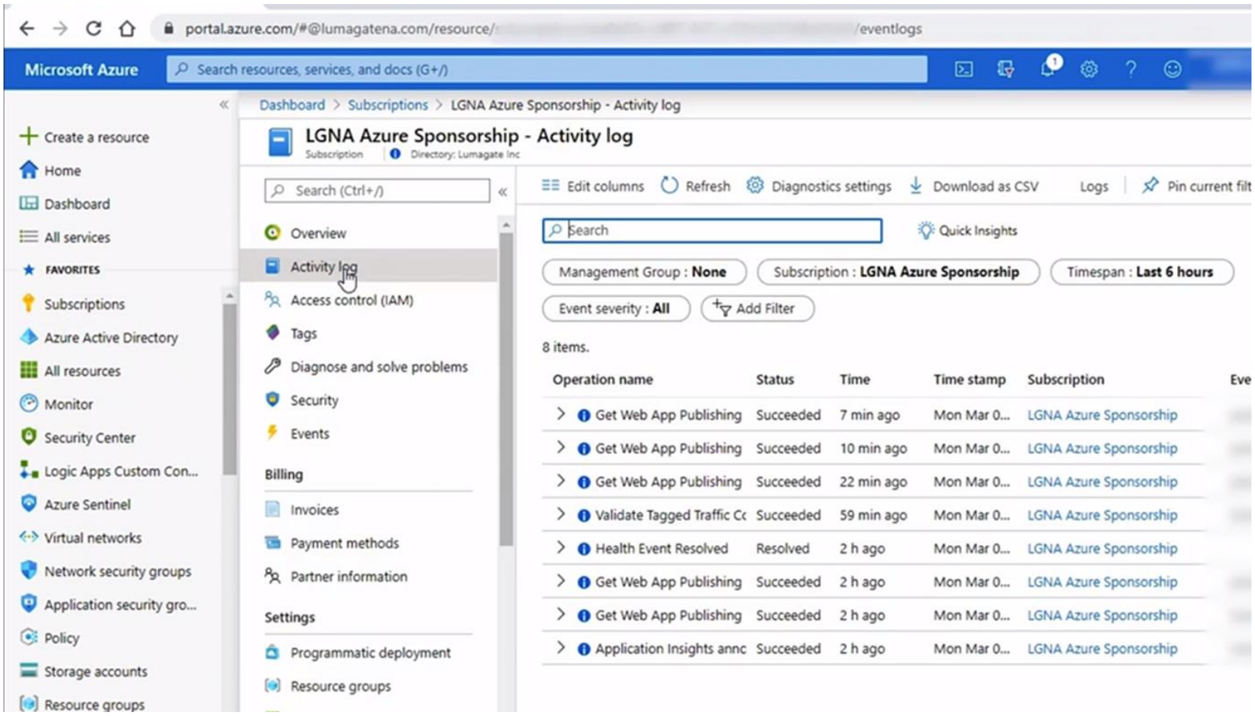
ACTIONS GROUPS (optional)

Action group name	Contain actions
SecOps Alert Notification	2 Email(s)

Add Create

Action rules (preview) allows you to define actions at scale as well as suppress actions. Learn more about this functionality by clicking on this banner

3.2 Diagnostic logging and log retention using Azure Monitor



portal.azure.com/#@lumagatena.com/resource/ /eventlogs

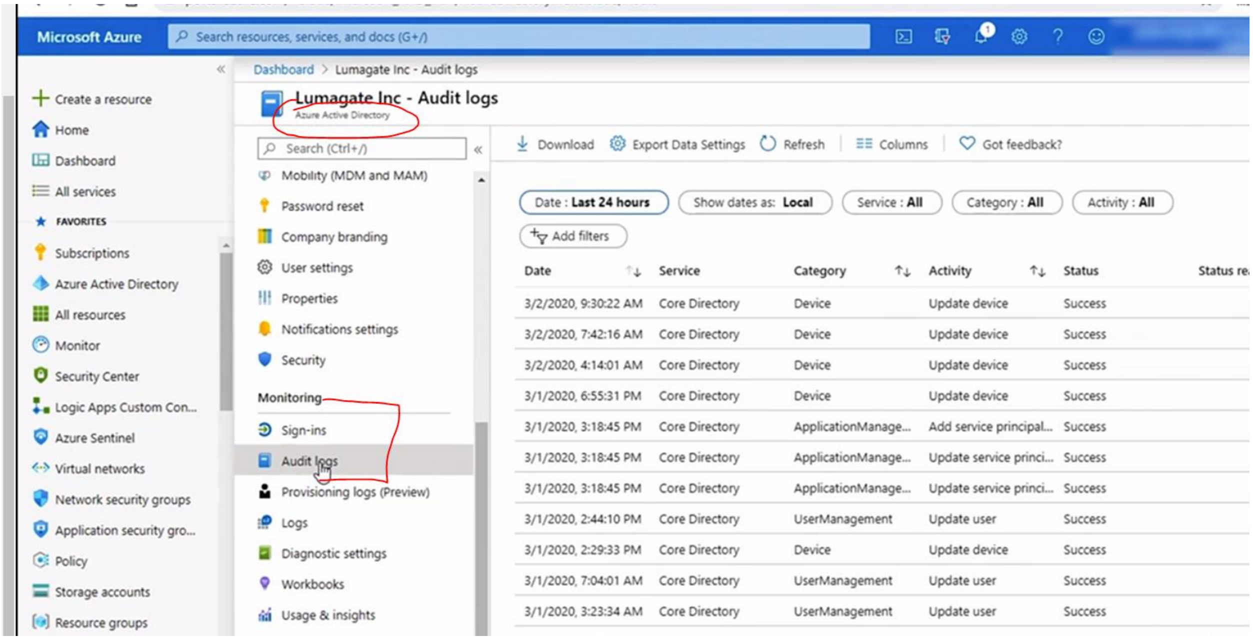
Dashboard > Subscriptions > LGNA Azure Sponsorship - Activity log

LGNA Azure Sponsorship - Activity log
Subscription Directory: Lumagate Inc

Management Group : None Subscription : LGNA Azure Sponsorship Timespan : Last 6 hours
Event severity : All Add Filter

8 items.

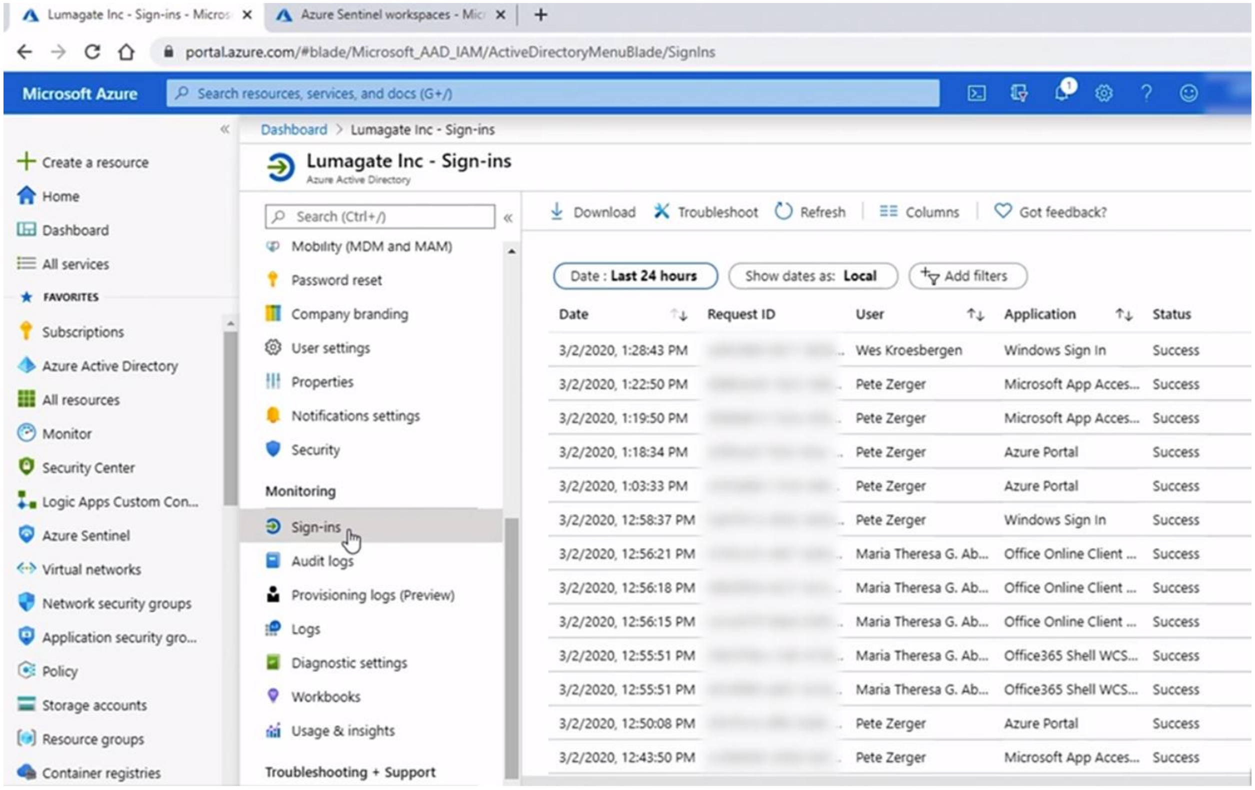
Operation name	Status	Time	Time stamp	Subscription
Get Web App Publishing	Succeeded	7 min ago	Mon Mar 0...	LGNA Azure Sponsorship
Get Web App Publishing	Succeeded	10 min ago	Mon Mar 0...	LGNA Azure Sponsorship
Get Web App Publishing	Succeeded	22 min ago	Mon Mar 0...	LGNA Azure Sponsorship
Validate Tagged Traffic Cc	Succeeded	59 min ago	Mon Mar 0...	LGNA Azure Sponsorship
Health Event Resolved	Resolved	2 h ago	Mon Mar 0...	LGNA Azure Sponsorship
Get Web App Publishing	Succeeded	2 h ago	Mon Mar 0...	LGNA Azure Sponsorship
Get Web App Publishing	Succeeded	2 h ago	Mon Mar 0...	LGNA Azure Sponsorship
Application Insights annc	Succeeded	2 h ago	Mon Mar 0...	LGNA Azure Sponsorship



Lumagate Inc - Audit logs
Azure Active Directory

Date : **Last 24 hours** | Show dates as: **Local** | Service : **All** | Category : **All** | Activity : **All**

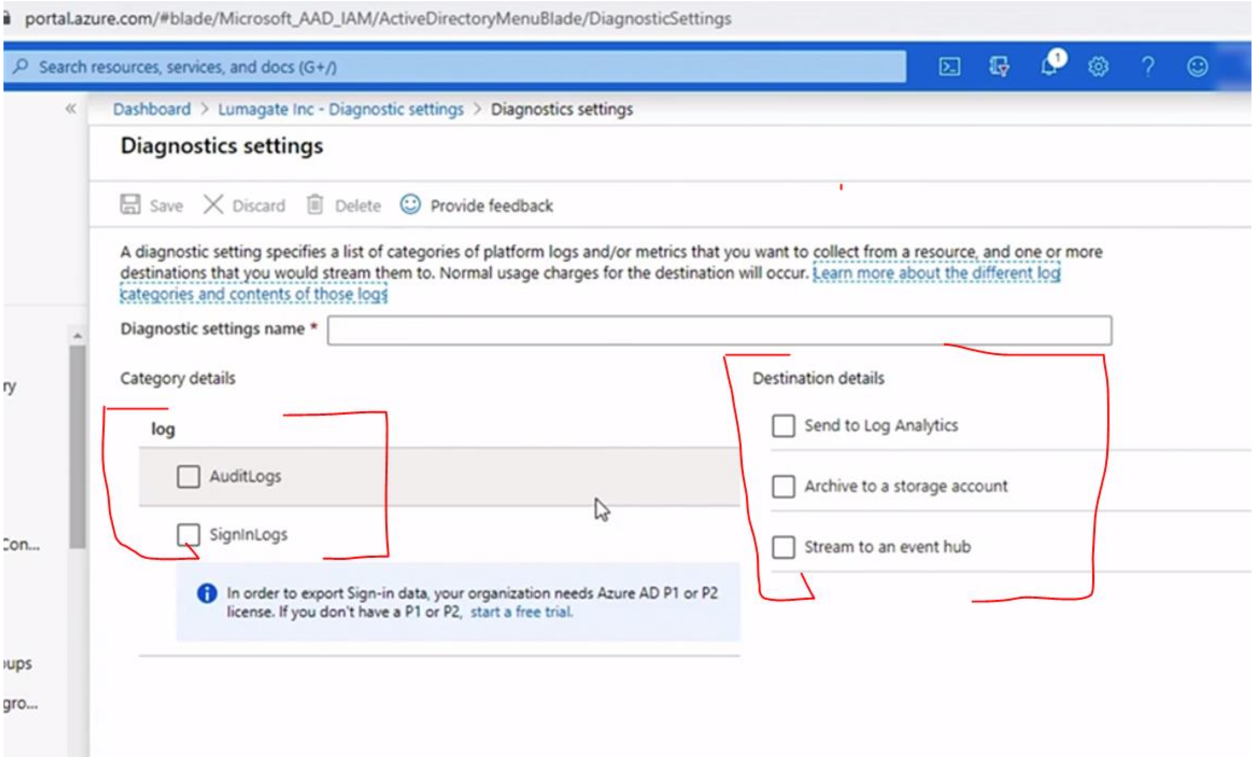
Date	Service	Category	Activity	Status	Status re
3/2/2020, 9:30:22 AM	Core Directory	Device	Update device	Success	
3/2/2020, 7:42:16 AM	Core Directory	Device	Update device	Success	
3/2/2020, 4:14:01 AM	Core Directory	Device	Update device	Success	
3/1/2020, 6:55:31 PM	Core Directory	Device	Update device	Success	
3/1/2020, 3:18:45 PM	Core Directory	ApplicationManage...	Add service principal...	Success	
3/1/2020, 3:18:45 PM	Core Directory	ApplicationManage...	Update service princi...	Success	
3/1/2020, 3:18:45 PM	Core Directory	ApplicationManage...	Update service princi...	Success	
3/1/2020, 2:44:10 PM	Core Directory	UserManagement	Update user	Success	
3/1/2020, 2:29:33 PM	Core Directory	Device	Update device	Success	
3/1/2020, 7:04:01 AM	Core Directory	UserManagement	Update user	Success	
3/1/2020, 3:23:34 AM	Core Directory	UserManagement	Update user	Success	



Lumagate Inc - Sign-ins
Azure Active Directory

Date : **Last 24 hours** | Show dates as: **Local**

Date	Request ID	User	Application	Status
3/2/2020, 1:28:43 PM	[redacted]	Wes Kroesbergen	Windows Sign In	Success
3/2/2020, 1:22:50 PM	[redacted]	Pete Zerger	Microsoft App Acces...	Success
3/2/2020, 1:19:50 PM	[redacted]	Pete Zerger	Microsoft App Acces...	Success
3/2/2020, 1:18:34 PM	[redacted]	Pete Zerger	Azure Portal	Success
3/2/2020, 1:03:33 PM	[redacted]	Pete Zerger	Azure Portal	Success
3/2/2020, 12:58:37 PM	[redacted]	Pete Zerger	Windows Sign In	Success
3/2/2020, 12:56:21 PM	[redacted]	Maria Theresa G. Ab...	Office Online Client ...	Success
3/2/2020, 12:56:18 PM	[redacted]	Maria Theresa G. Ab...	Office Online Client ...	Success
3/2/2020, 12:56:15 PM	[redacted]	Maria Theresa G. Ab...	Office Online Client ...	Success
3/2/2020, 12:55:51 PM	[redacted]	Maria Theresa G. Ab...	Office365 Shell WCS...	Success
3/2/2020, 12:55:51 PM	[redacted]	Maria Theresa G. Ab...	Office365 Shell WCS...	Success
3/2/2020, 12:50:08 PM	[redacted]	Pete Zerger	Azure Portal	Success
3/2/2020, 12:43:50 PM	[redacted]	Pete Zerger	Microsoft App Acces...	Success



portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/DiagnosticSettings
Search resources, services, and docs (G+/)
Dashboard > Lumagate Inc - Diagnostic settings > Diagnostics settings
Save
Discard
Delete
Provide feedback

Diagnostics settings

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic settings name *

Category details

log

□ AuditLogs

□ SignInLogs

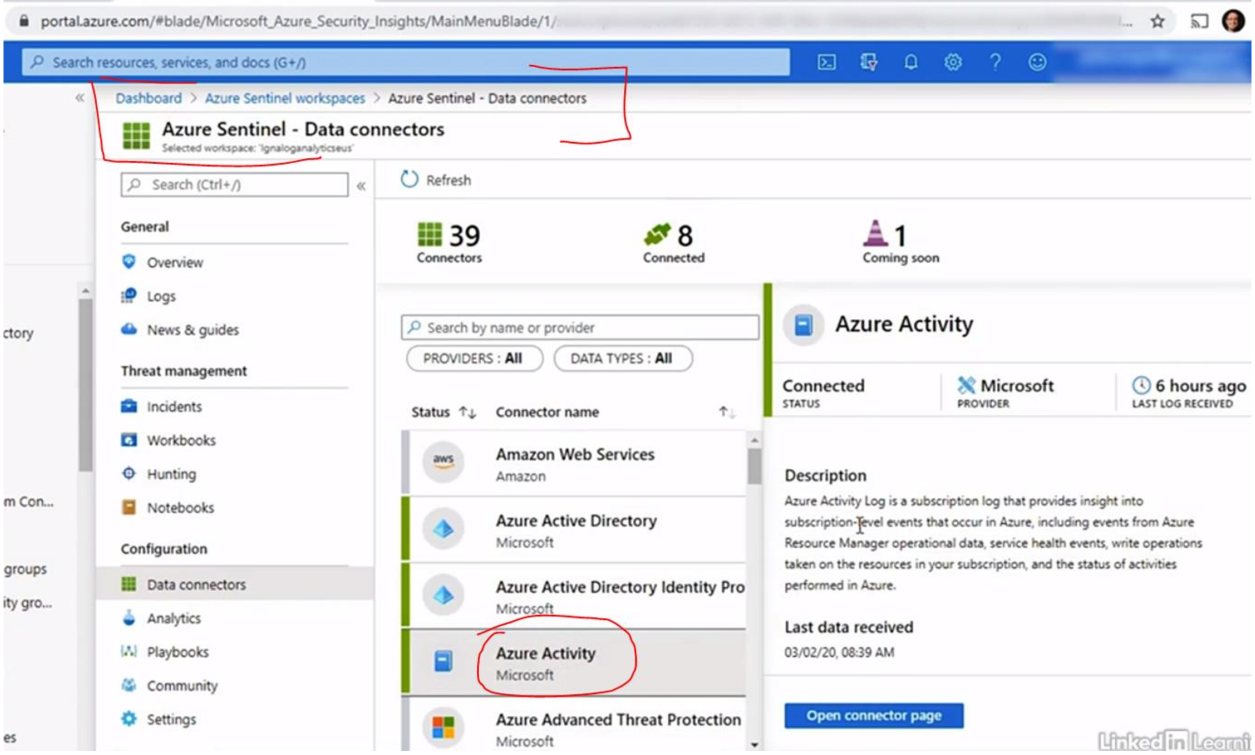
In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, start a free trial.

Destination details

□ Send to Log Analytics

□ Archive to a storage account

□ Stream to an event hub



Azure Sentinel - Data connectors

Selected workspace: 'lgnaloganalyticseus'

39 Connectors | 8 Connected | 1 Coming soon

Status	Connector name
	Amazon Web Services Amazon
	Azure Active Directory Microsoft
	Azure Active Directory Identity Pro Microsoft
	Azure Activity Microsoft
	Azure Advanced Threat Protection Microsoft

Azure Activity

Connected STATUS | Microsoft PROVIDER | 6 hours ago LAST LOG RECEIVED

Description

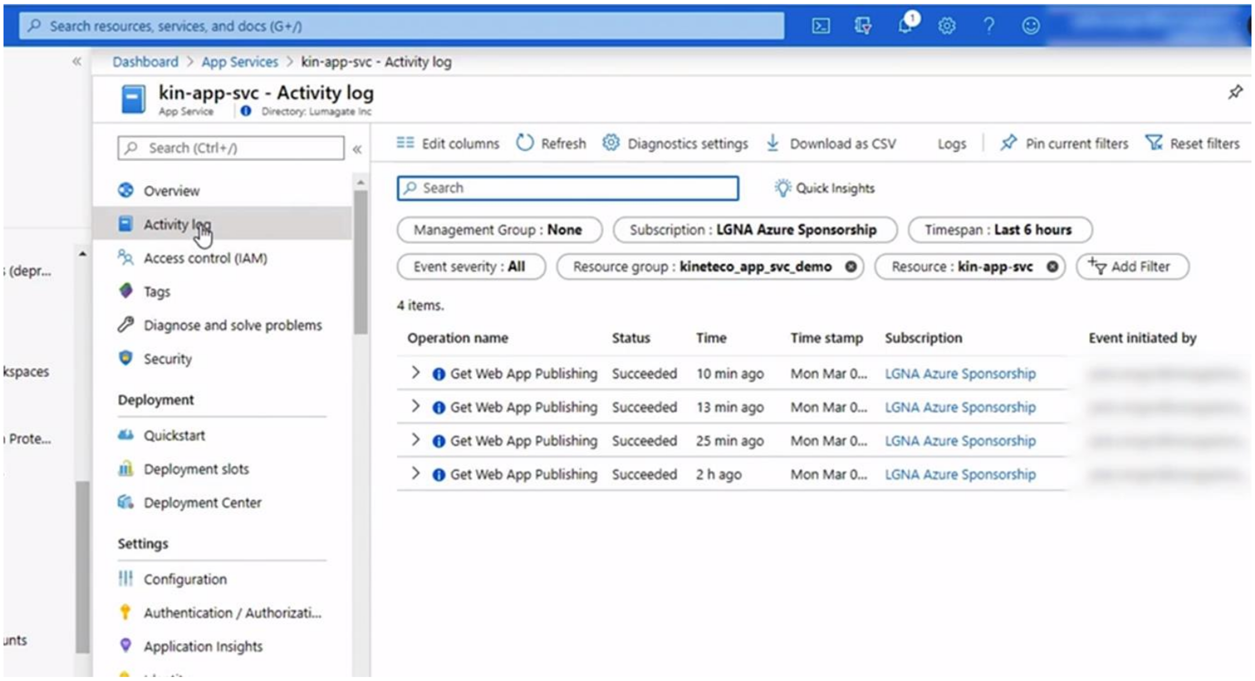
Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed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

Last data received

03/02/20, 08:39 AM

Sentinel Connectors are configured from the Sentinel Portal side, not from the Azure Portal Side.

Resource Logs



Search resources, services, and docs (G+/)

Dashboard > App Services > kin-app-svc - Activity log

kin-app-svc - Activity log

App Service | Directory: Lumagate Inc

Management Group : **None** | Subscription : **LGNA Azure Sponsorship** | Timespan : **Last 6 hours**

Event severity : **All** | Resource group : **kineteco_app_svc_demo** | Resource : **kin-app-svc**

4 items.

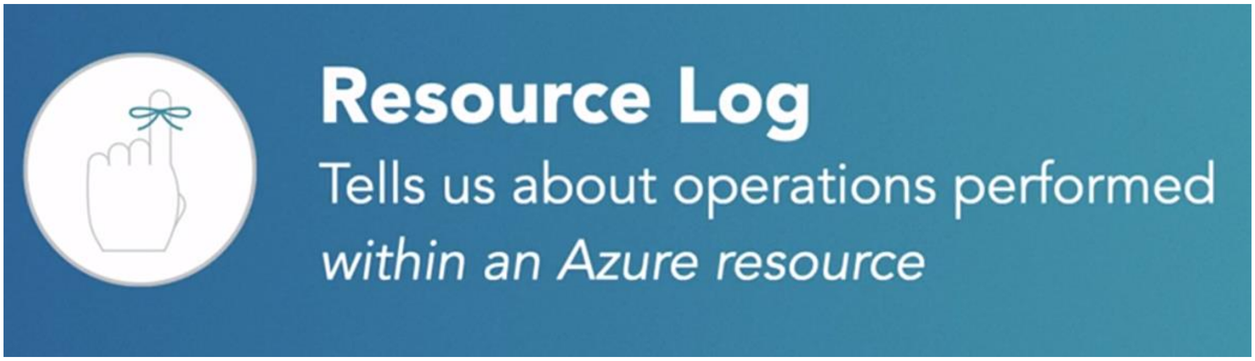
Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Get Web App Publishing	Succeeded	10 min ago	Mon Mar 0...	LGNA Azure Sponsorship	[redacted]
Get Web App Publishing	Succeeded	13 min ago	Mon Mar 0...	LGNA Azure Sponsorship	[redacted]
Get Web App Publishing	Succeeded	25 min ago	Mon Mar 0...	LGNA Azure Sponsorship	[redacted]
Get Web App Publishing	Succeeded	2 h ago	Mon Mar 0...	LGNA Azure Sponsorship	[redacted]

Activity Log

Tells us **who**, **what**, and **when** at the *subscription level*

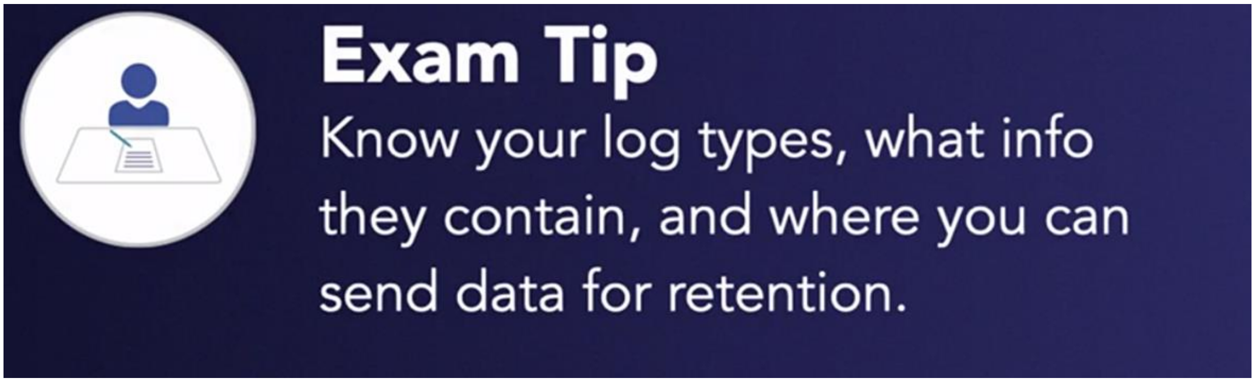
Azure Active Directory Logs

History of sign-in activity and audit trail of changes made *in an Azure AD tenant*



Resource Log

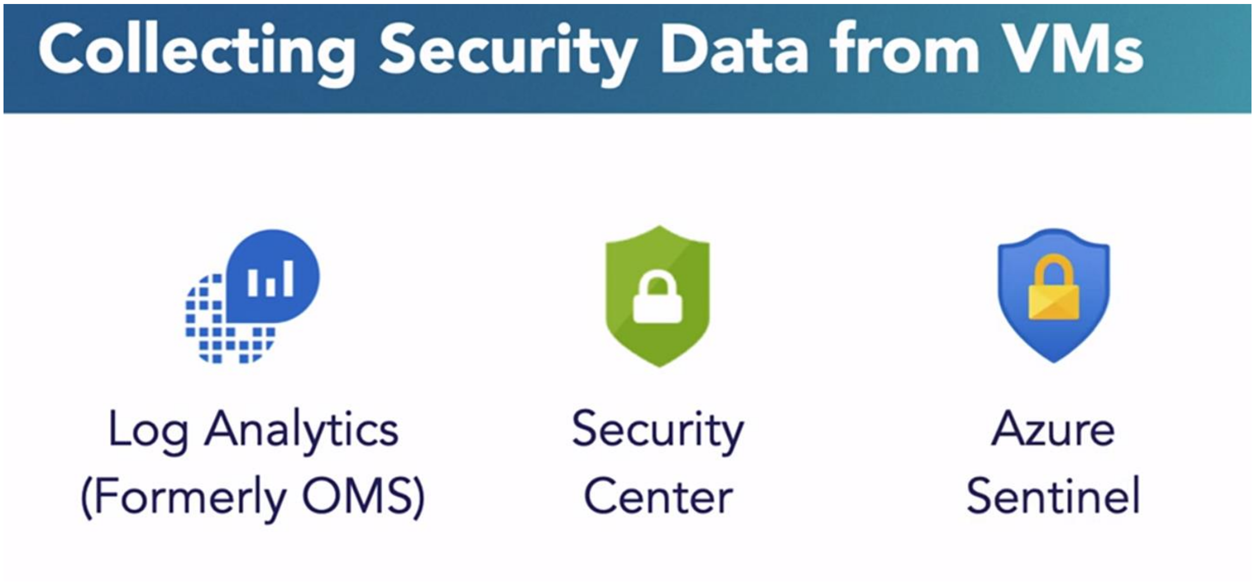
Tells us about operations performed *within an Azure resource*



Exam Tip

Know your log types, what info they contain, and where you can send data for retention.

3.3 Monitor security logs using Azure monitor

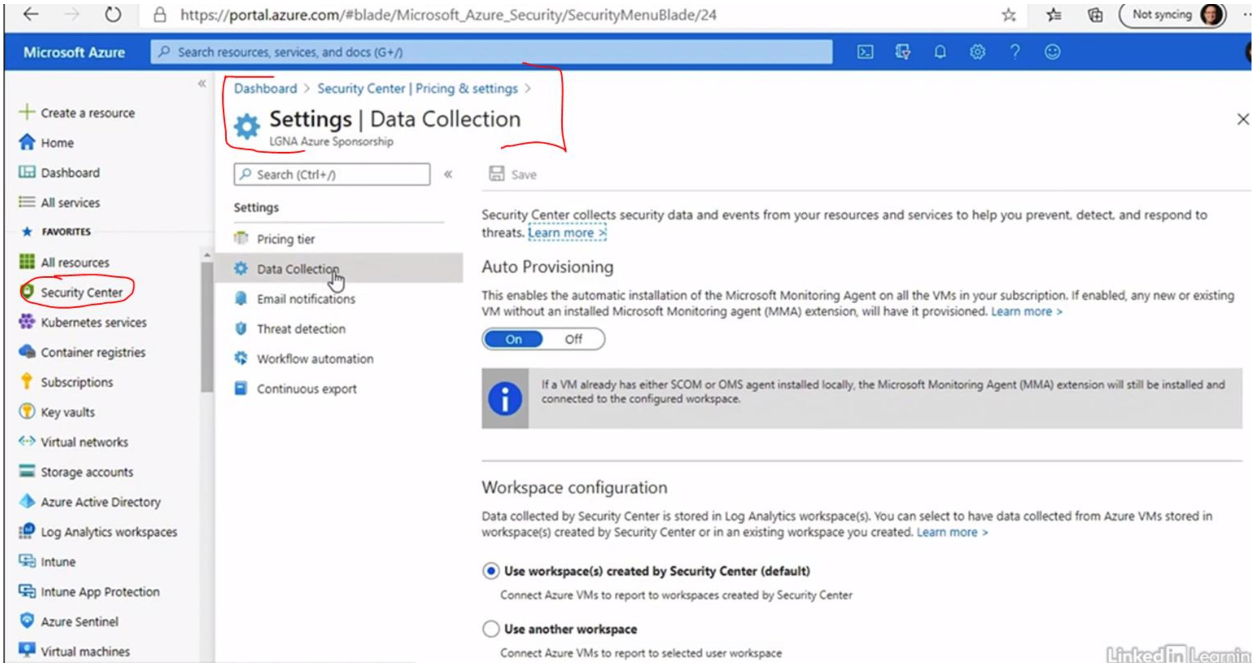


Collecting Security Data from VMs

Log Analytics (Formerly OMS)

Security Center

Azure Sentinel



Settings | Data Collection

LGNA Azure Sponsorship

Security Center collects security data and events from your resources and services to help you prevent, detect, and respond to threats. Learn more >

Auto Provisioning

This enables the automatic installation of the Microsoft Monitoring Agent on all the VMs in your subscription. If enabled, any new or existing VM without an installed Microsoft Monitoring agent (MMA) extension, will have it provisioned. Learn more >

[✓ On] Off

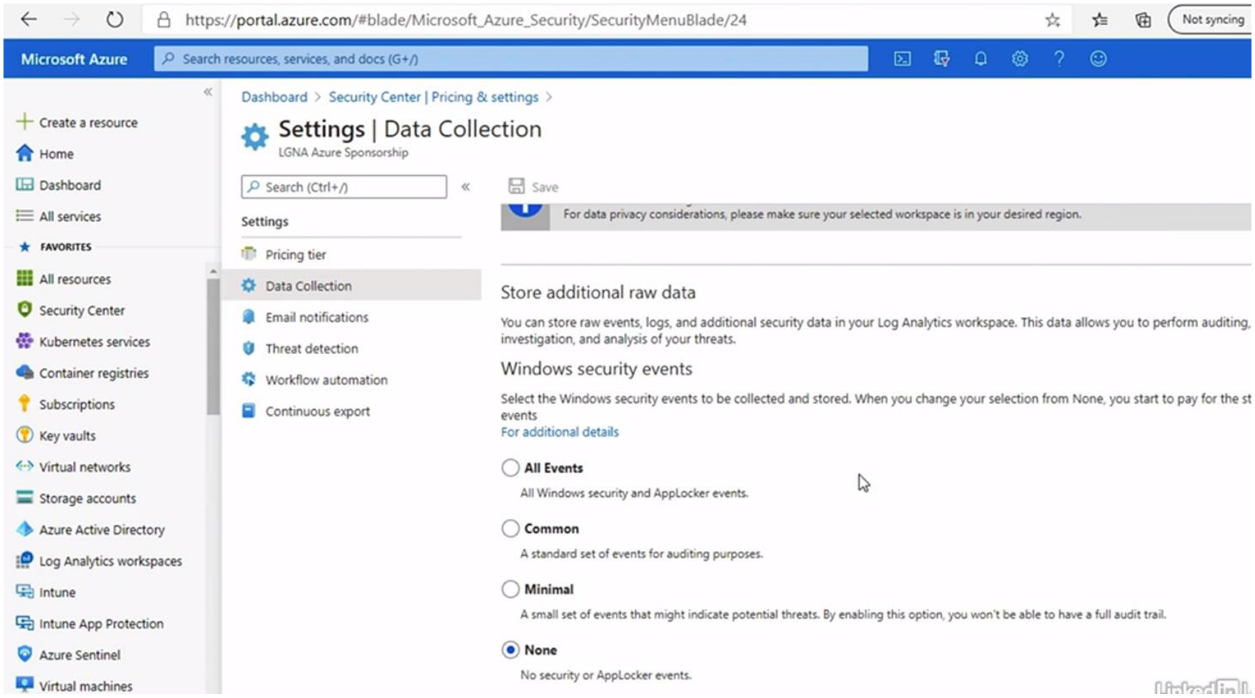
If a VM already has either SCOM or OMS agent installed locally, the Microsoft Monitoring Agent (MMA) extension will still be installed and connected to the configured workspace.

Workspace configuration

Data collected by Security Center is stored in Log Analytics workspace(s). You can select to have data collected from Azure VMs stored in workspace(s) created by Security Center or in an existing workspace you created. Learn more >

● **Use workspace(s) created by Security Center (default)**
Connect Azure VMs to report to workspaces created by Security Center

○ **Use another workspace**
Connect Azure VMs to report to selected user workspace



Settings | Data Collection

LGNA Azure Sponsorship

For data privacy considerations, please make sure your selected workspace is in your desired region.

Store additional raw data

You can store raw events, logs, and additional security data in your Log Analytics workspace. This data allows you to perform auditing, investigation, and analysis of your threats.

Windows security events

Select the Windows security events to be collected and stored. When you change your selection from None, you start to pay for the st events

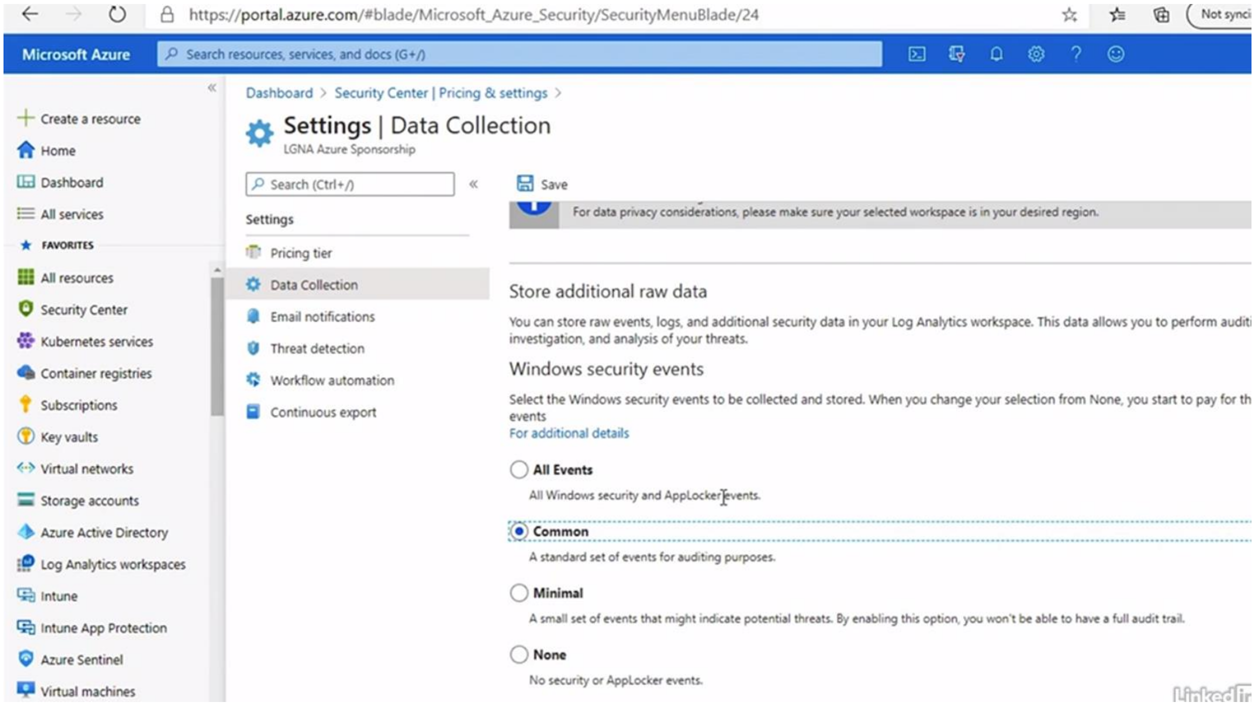
For additional details

○ **All Events**
All Windows security and AppLocker events.

○ **Common**
A standard set of events for auditing purposes.

○ **Minimal**
A small set of events that might indicate potential threats. By enabling this option, you won't be able to have a full audit trail.

● **None**
No security or AppLocker events.



Settings | Data Collection

LGNA Azure Sponsorship

For data privacy considerations, please make sure your selected workspace is in your desired region.

Store additional raw data

You can store raw events, logs, and additional security data in your Log Analytics workspace. This data allows you to perform auditi investigation, and analysis of your threats.

Windows security events

Select the Windows security events to be collected and stored. When you change your selection from None, you start to pay for th events

For additional details

○ **All Events**

All Windows security and AppLocker events.

● **Common**

A standard set of events for auditing purposes.

○ **Minimal**

A small set of events that might indicate potential threats. By enabling this option, you won't be able to have a full audit trail.

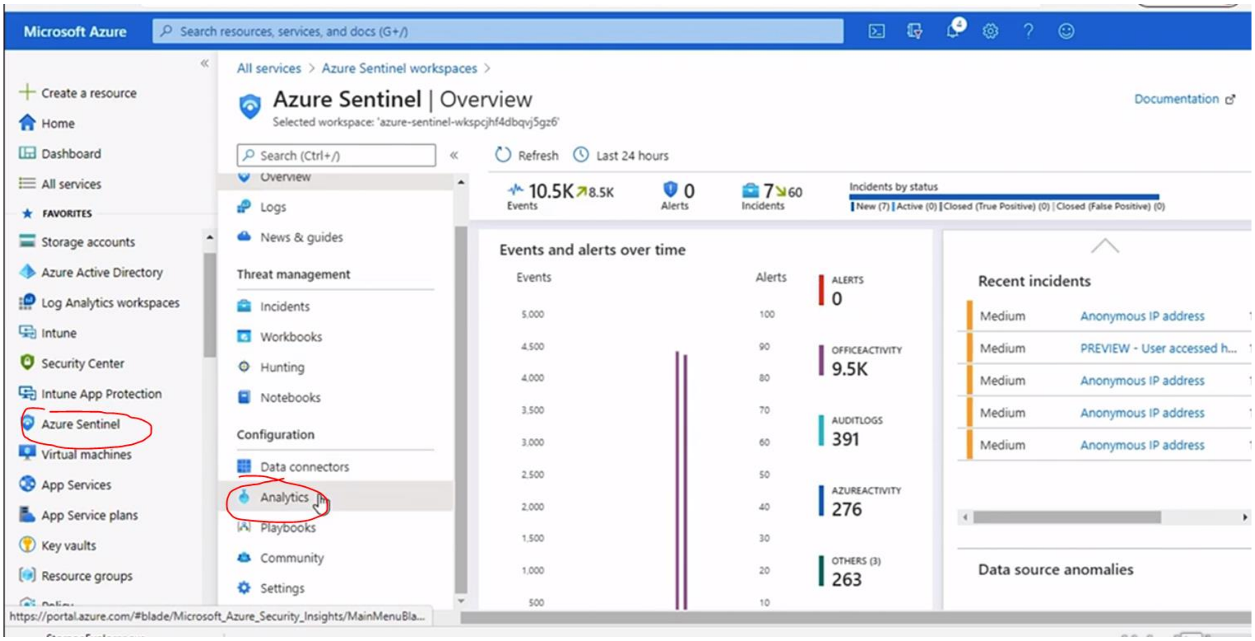
○ **None**

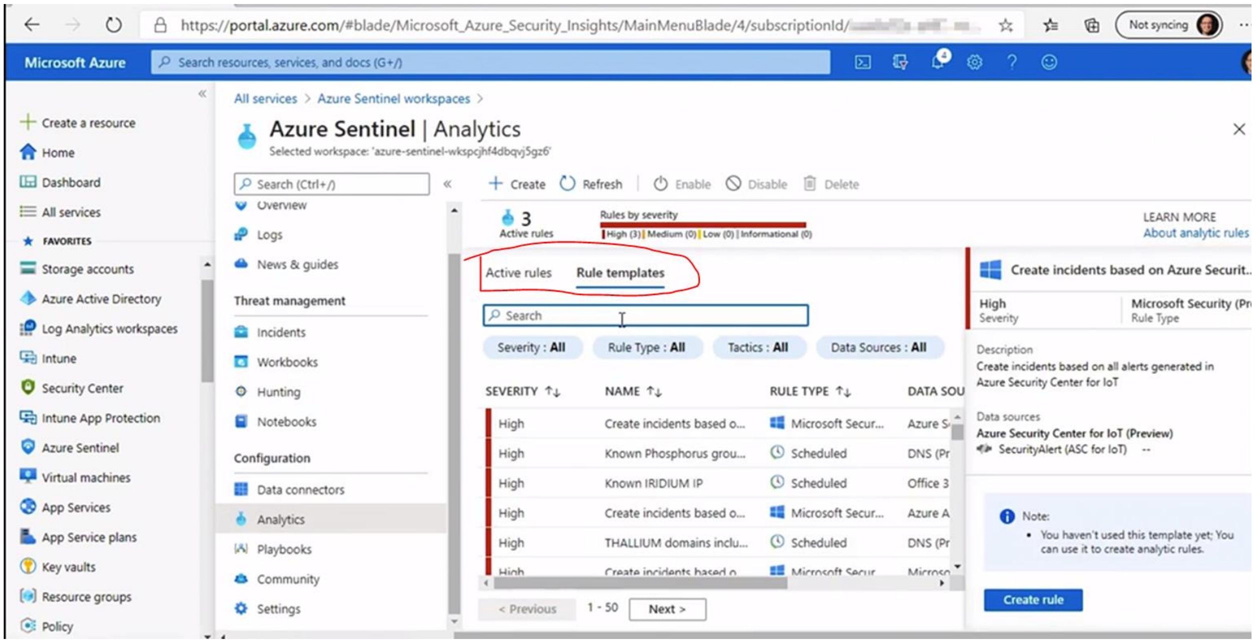
No security or AppLocker events.

Exam Tip

Know the Security Center and Azure Sentinel integration and config options.

3.4 Create and customize alert rules in Azure Sentinel



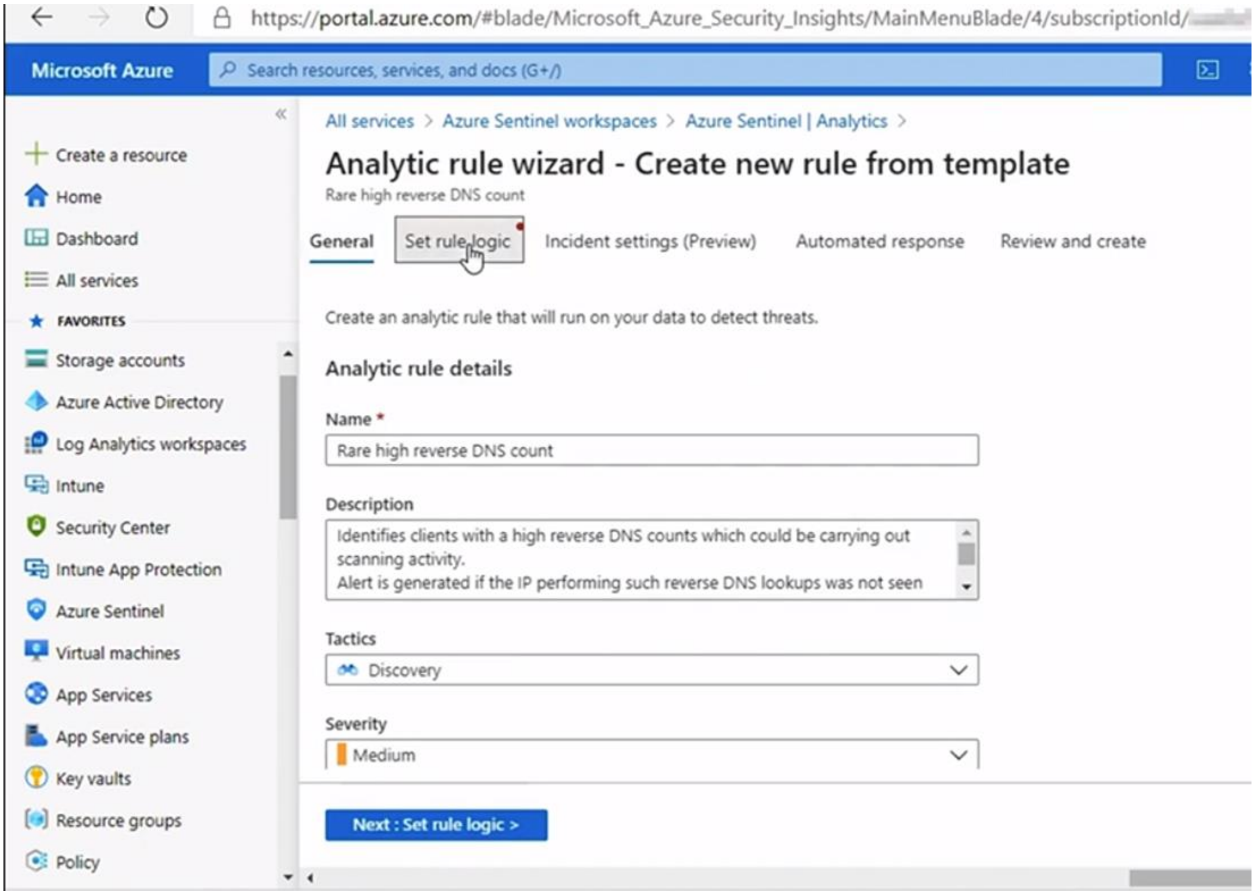


SEVERITY	NAME	RULE TYPE	DATA SOU
High	Create incidents based o...	Microsoft Secur...	Azure S
High	Known Phosphorus grou...	Scheduled	DNS (Pr
High	Known IRIDIUM IP	Scheduled	Office 3
High	Create incidents based o...	Microsoft Secur...	Azure A
High	THALLIUM domains inclu...	Scheduled	DNS (Pr
High	Create incidents based o...	Microsoft Secur...	Microso

Description
Create incidents based on all alerts generated in Azure Security Center for IoT

Data sources
Azure Security Center for IoT (Preview)
SecurityAlert (ASC for IoT) --

Note:
- You haven't used this template yet; You can use it to create analytic rules.



https://portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4/subscriptionId/[redacted]

Analytic rule wizard - Create new rule from template

Rare high reverse DNS count

Create an analytic rule that will run on your data to detect threats.

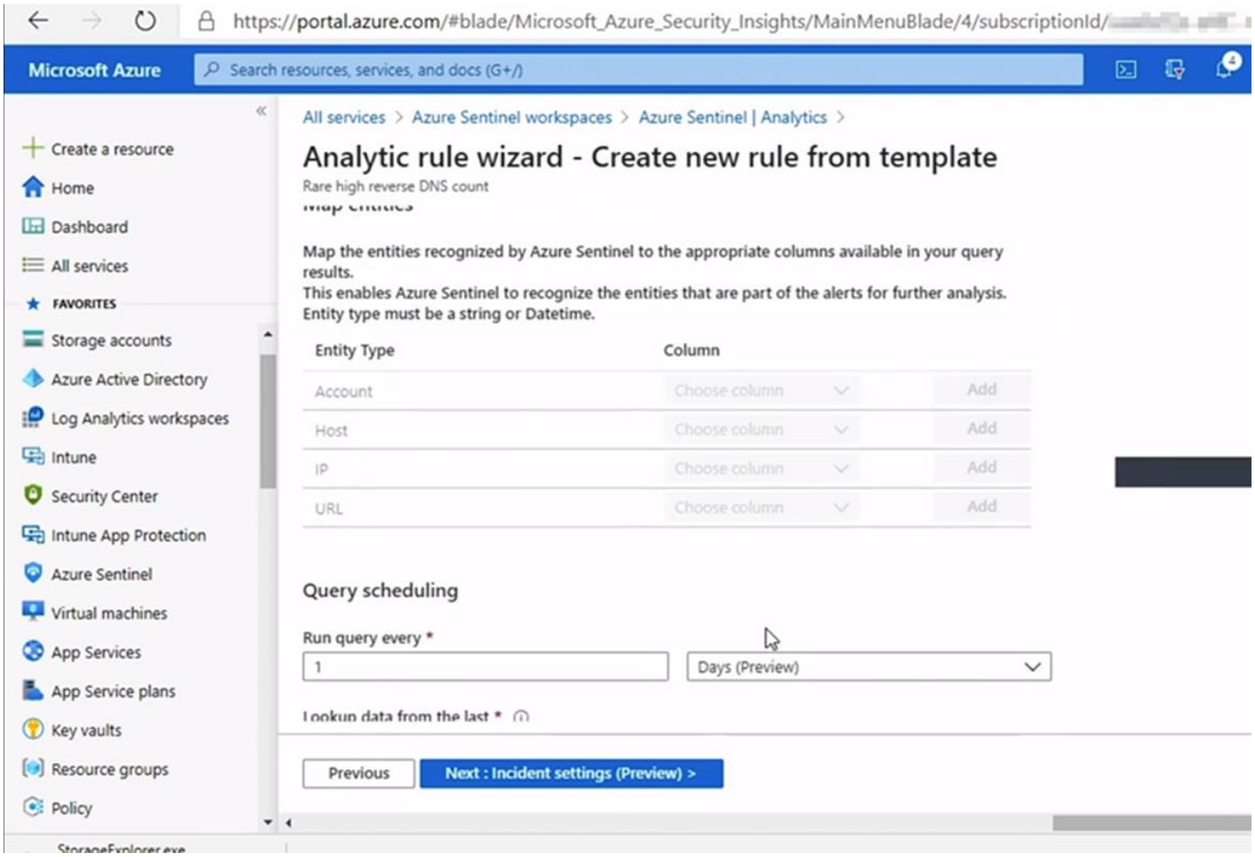
Analytic rule details

Name *
Rare high reverse DNS count

Description
Identifies clients with a high reverse DNS counts which could be carrying out scanning activity.
Alert is generated if the IP performing such reverse DNS lookups was not seen

Tactics
Discovery

Severity
Medium



Analytic rule wizard - Create new rule from template

Rare high reverse DNS count

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results.
This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis.
Entity type must be a string or Datetime.

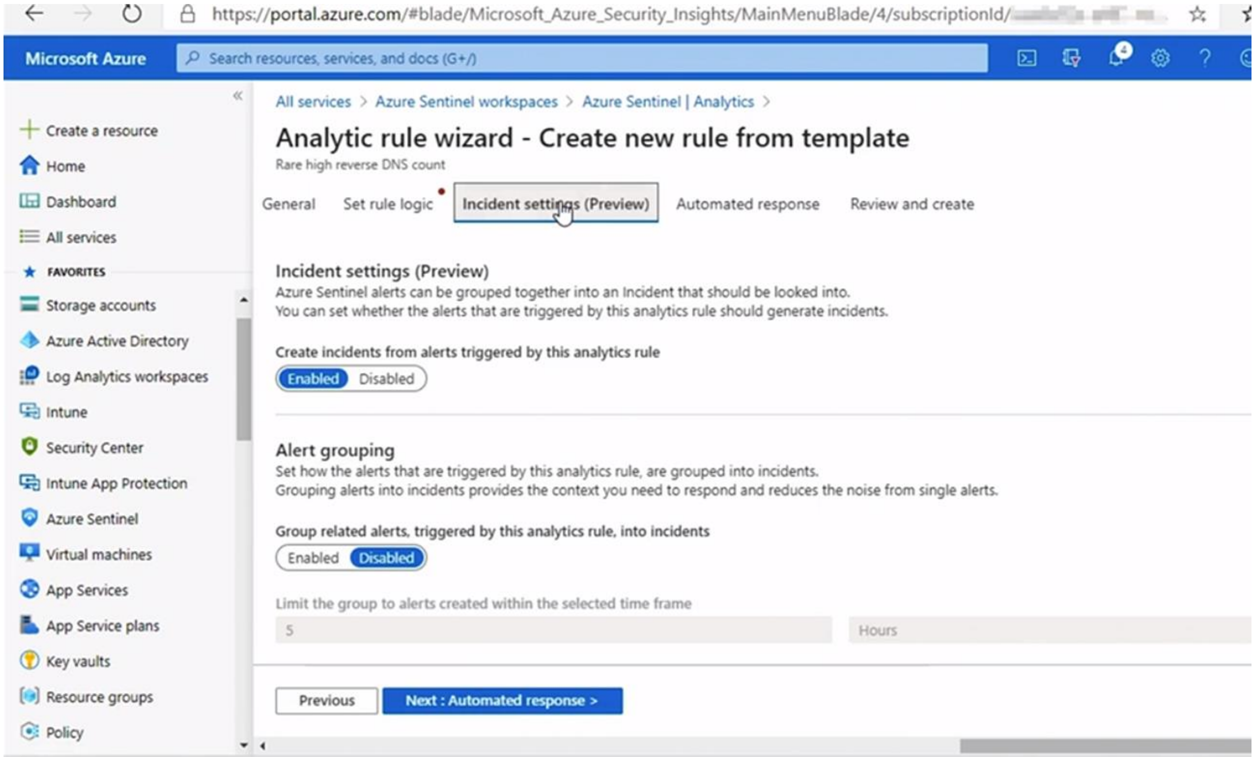
Entity Type	Column	
Account	Choose column	Add
Host	Choose column	Add
IP	Choose column	Add
URL	Choose column	Add

Query scheduling

Run query every *

1 | Days (Preview)

Lookup data from the last *



Analytic rule wizard - Create new rule from template

Rare high reverse DNS count

Incident settings (Preview)

Azure Sentinel alerts can be grouped together into an Incident that should be looked into.
You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule

[✓ Enabled] Disabled

Alert grouping

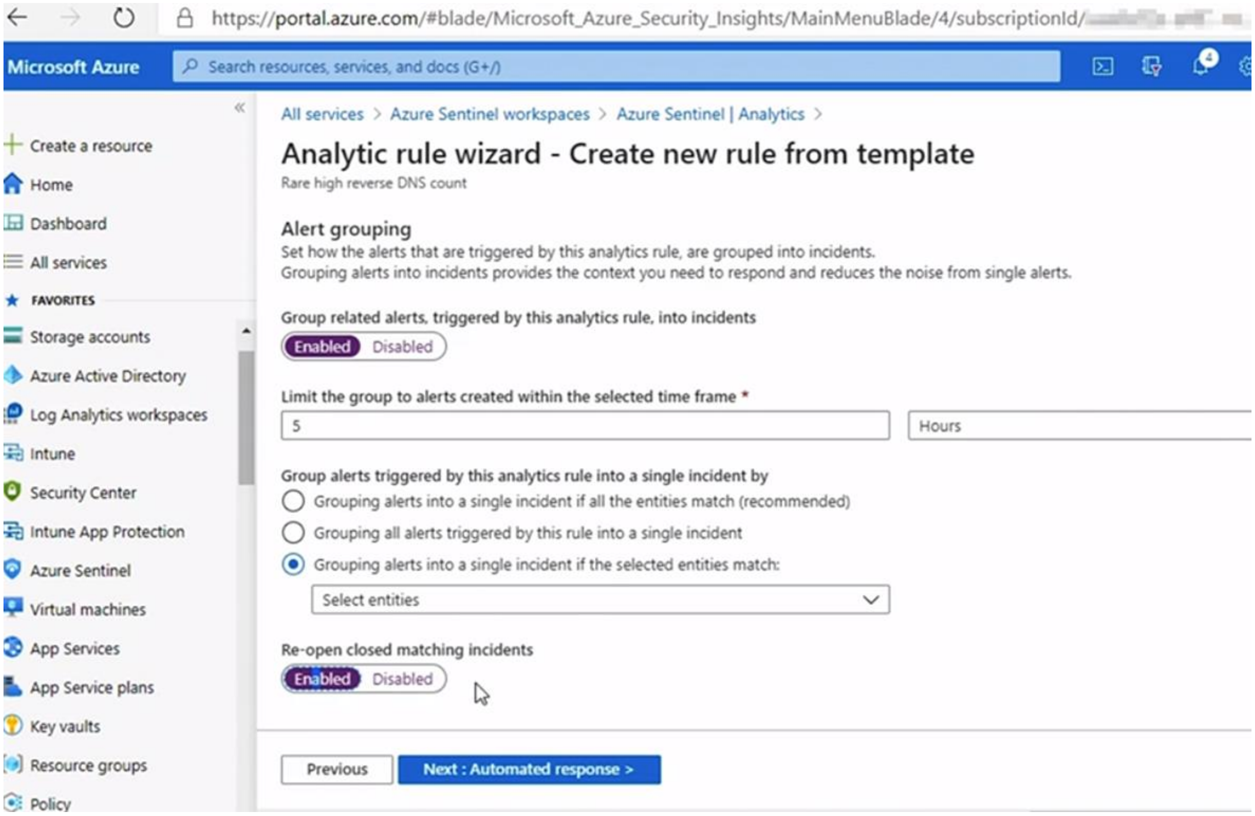
Set how the alerts that are triggered by this analytics rule, are grouped into incidents.
Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents

Enabled [✓ Disabled]

Limit the group to alerts created within the selected time frame

5 | Hours



Analytic rule wizard - Create new rule from template

Rare high reverse DNS count

Alert grouping

Set how the alerts that are triggered by this analytics rule, are grouped into incidents.
Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents

[✓ Enabled] Disabled

Limit the group to alerts created within the selected time frame *

5 Hours

Group alerts triggered by this analytics rule into a single incident by

○ Grouping alerts into a single incident if all the entities match (recommended)

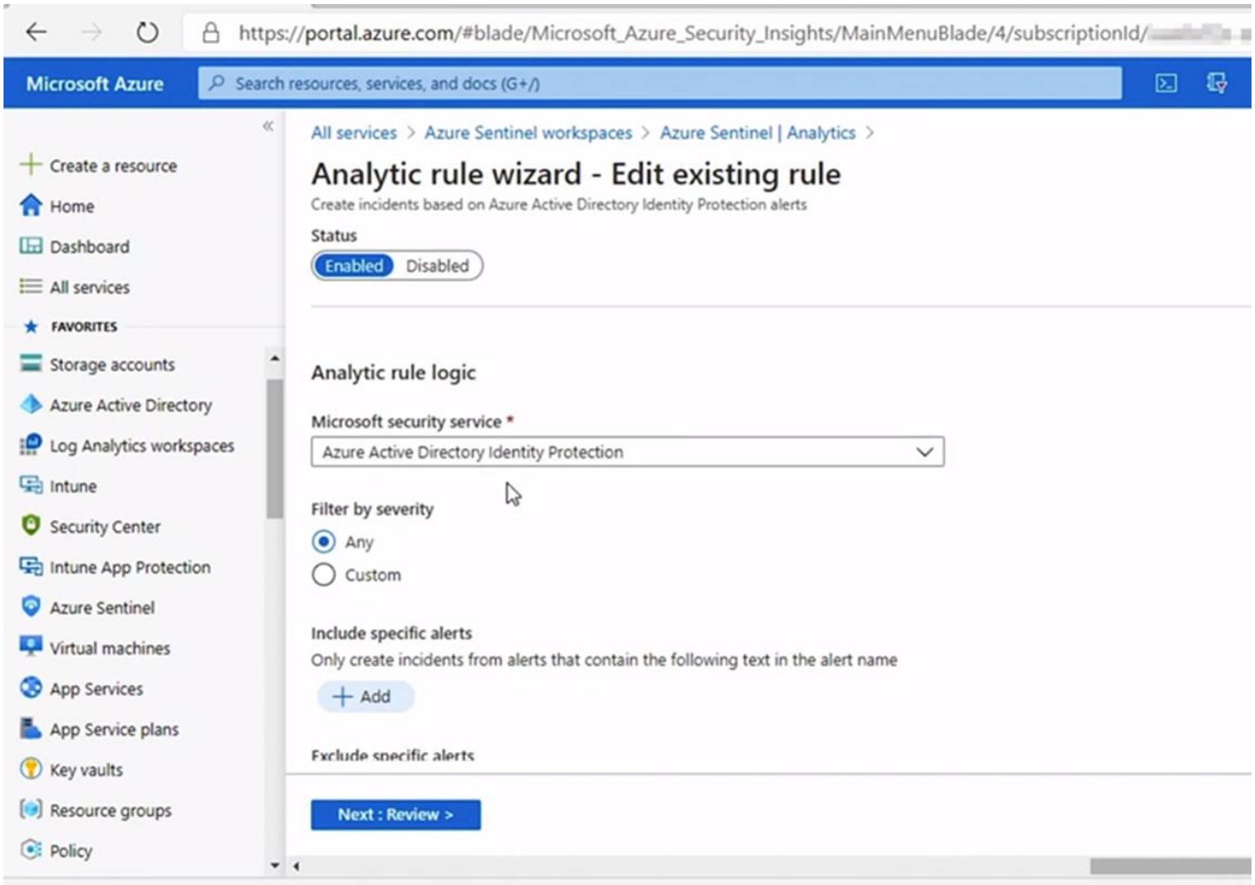
○ Grouping all alerts triggered by this rule into a single incident

● Grouping alerts into a single incident if the selected entities match:

Select entities

Re-open closed matching incidents

[✓ Enabled] Disabled



Analytic rule wizard - Edit existing rule

Create incidents based on Azure Active Directory Identity Protection alerts

Status

[✓ Enabled] Disabled

Analytic rule logic

Microsoft security service *

Azure Active Directory Identity Protection

Filter by severity

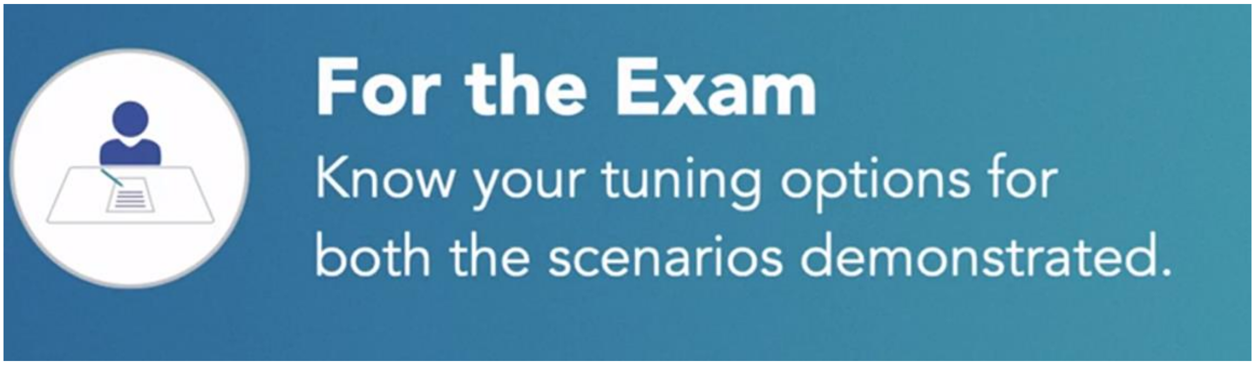
● Any

○ Custom

Include specific alerts

Only create incidents from alerts that contain the following text in the alert name

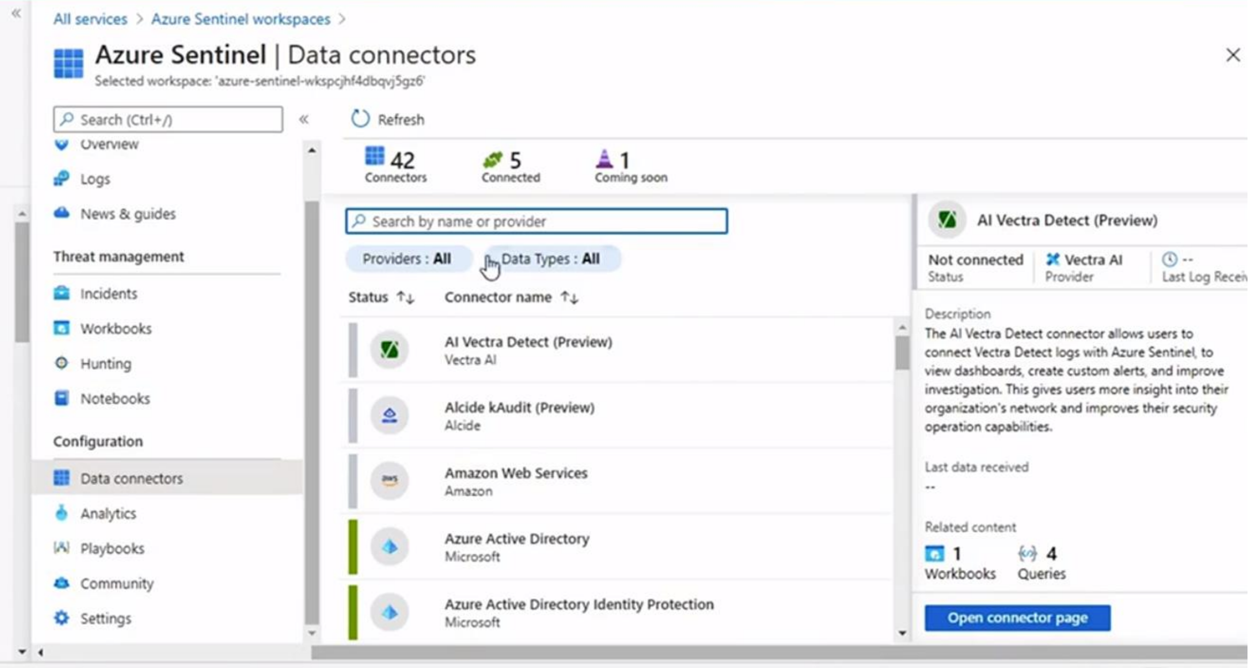
Exclude specific alerts



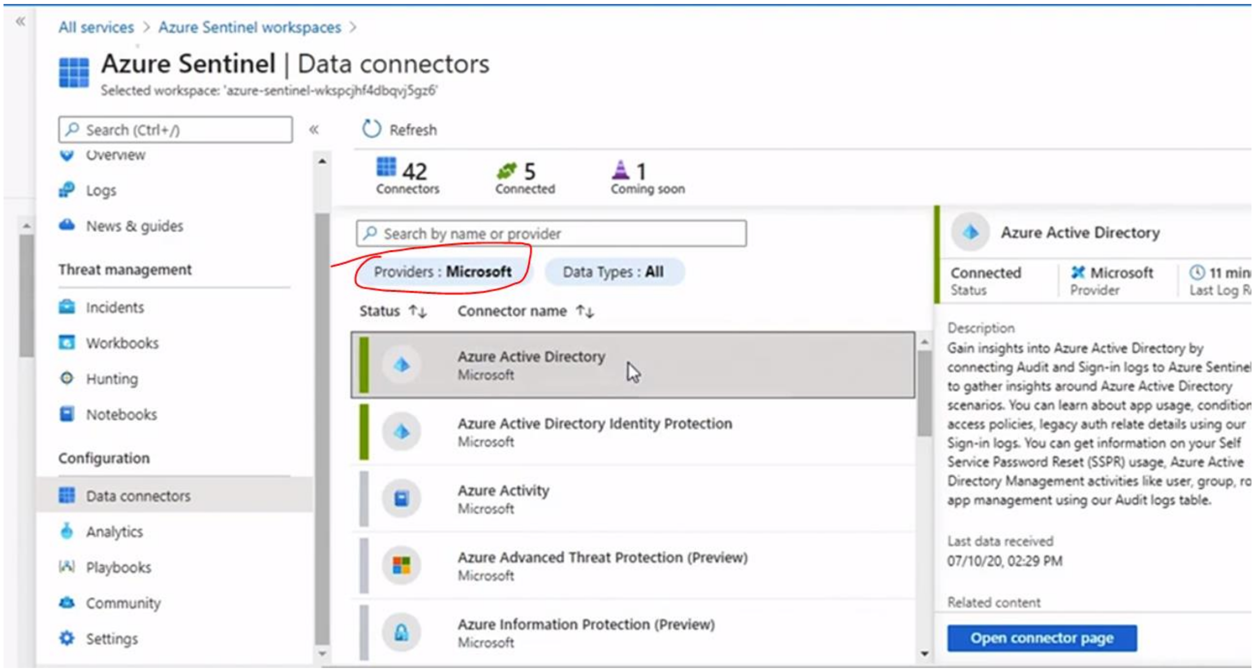
For the Exam

Know your tuning options for both the scenarios demonstrated.

3.5 Configure connectors in Azure Sentinel



The AI Vectra Detect connector allows users to connect Vectra Detect logs with Azure Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives users more insight into their organization's network and improves their security operation capabilities.



All services > Azure Sentinel workspaces >

Azure Sentinel | Data connectors

Selected workspace: 'azure-sentinel-wkspcjhf4dbqvj5gz6'

Search (Ctrl+/) «

Refresh

42 Connectors · 5 Connected · 1 Coming soon

Overview
Logs
News & guides

Threat management
Incidents
Workbooks
Hunting
Notebooks

Configuration
Data connectors
Analytics
Playbooks
Community
Settings

Search by name or provider

Providers : **Microsoft** · Data Types : **All**

Status ↑↓	Connector name ↑↓
	Azure Active Directory Microsoft
	Azure Active Directory Identity Protection Microsoft
	Azure Activity Microsoft
	Azure Advanced Threat Protection (Preview) Microsoft
	Azure Information Protection (Preview) Microsoft

Azure Active Directory

Connected · Microsoft · 11 min
Status · Provider · Last Log R

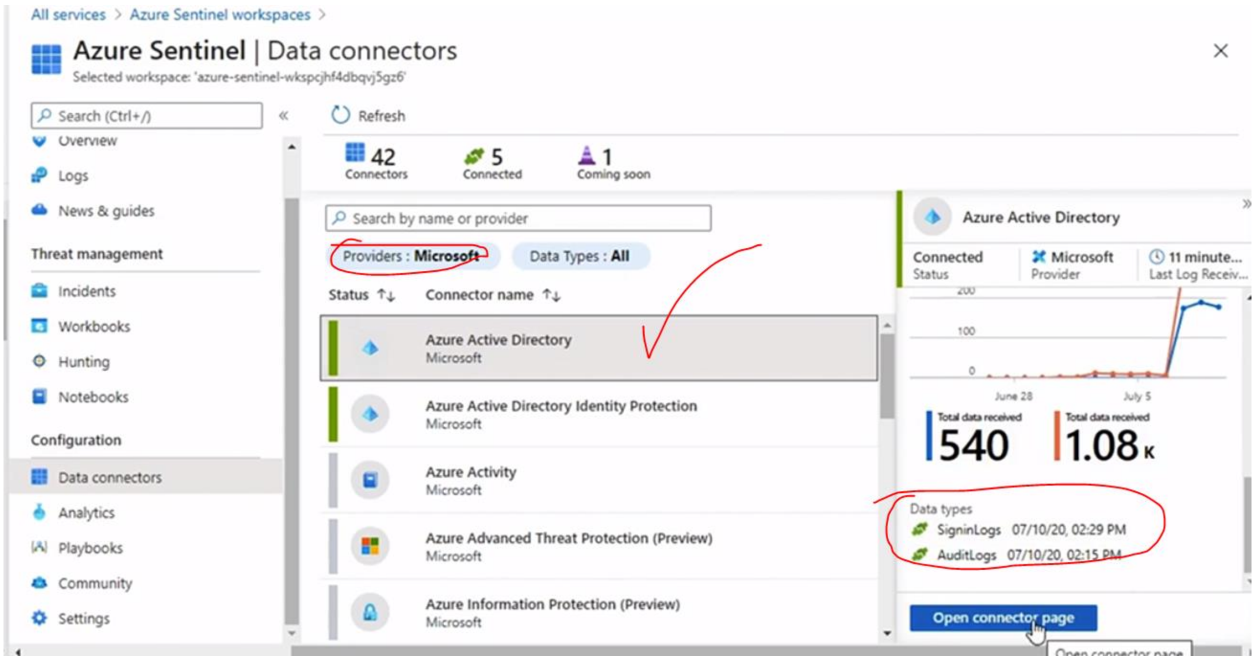
Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, condition access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, ro app management using our Audit logs table.

Last data received
07/10/20, 02:29 PM

Related content

Open connector page



All services > Azure Sentinel workspaces >

Azure Sentinel | Data connectors

Selected workspace: 'azure-sentinel-wkspcjhf4dbqvj5gz6'

Search (Ctrl+/) «

Refresh

42 Connectors · 5 Connected · 1 Coming soon

Overview
Logs
News & guides

Threat management
Incidents
Workbooks
Hunting
Notebooks

Configuration
Data connectors
Analytics
Playbooks
Community
Settings

Search by name or provider

Providers : **Microsoft** · Data Types : **All**

Status ↑↓	Connector name ↑↓
	Azure Active Directory Microsoft
	Azure Active Directory Identity Protection Microsoft
	Azure Activity Microsoft
	Azure Advanced Threat Protection (Preview) Microsoft
	Azure Information Protection (Preview) Microsoft

Azure Active Directory

Connected · Microsoft · 11 minute...
Status · Provider · Last Log Receiv...

Total data received 540

Total data received 1.08 K

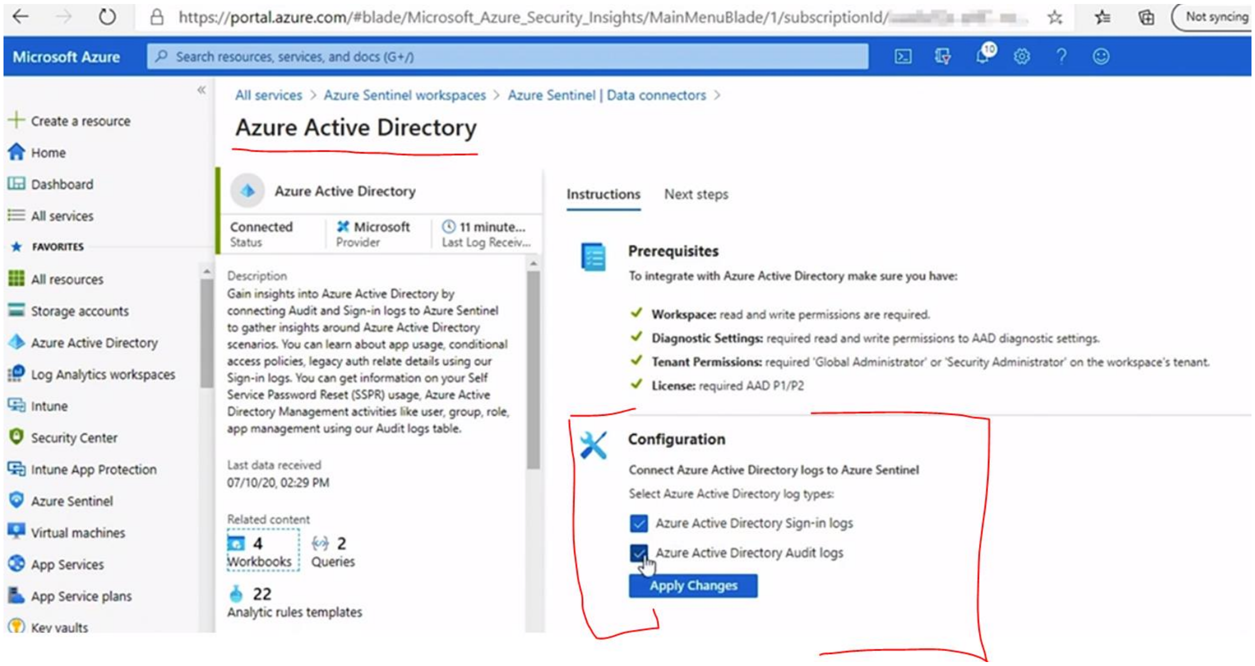
Data types

SigninLogs 07/10/20, 02:29 PM

AuditLogs 07/10/20, 02:15 PM

Open connector page

Open connector page



Azure Active Directory

Azure Active Directory

Connected	Microsoft	11 minute...
Status	Provider	Last Log Receiv...

Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

Last data received

07/10/20, 02:29 PM

Related content

4 Workbooks

2 Queries

22 Analytic rules templates

Prerequisites

To integrate with Azure Active Directory make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Diagnostic Settings:** required read and write permissions to AAD diagnostic settings.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- ✓ **License:** required AAD P1/P2

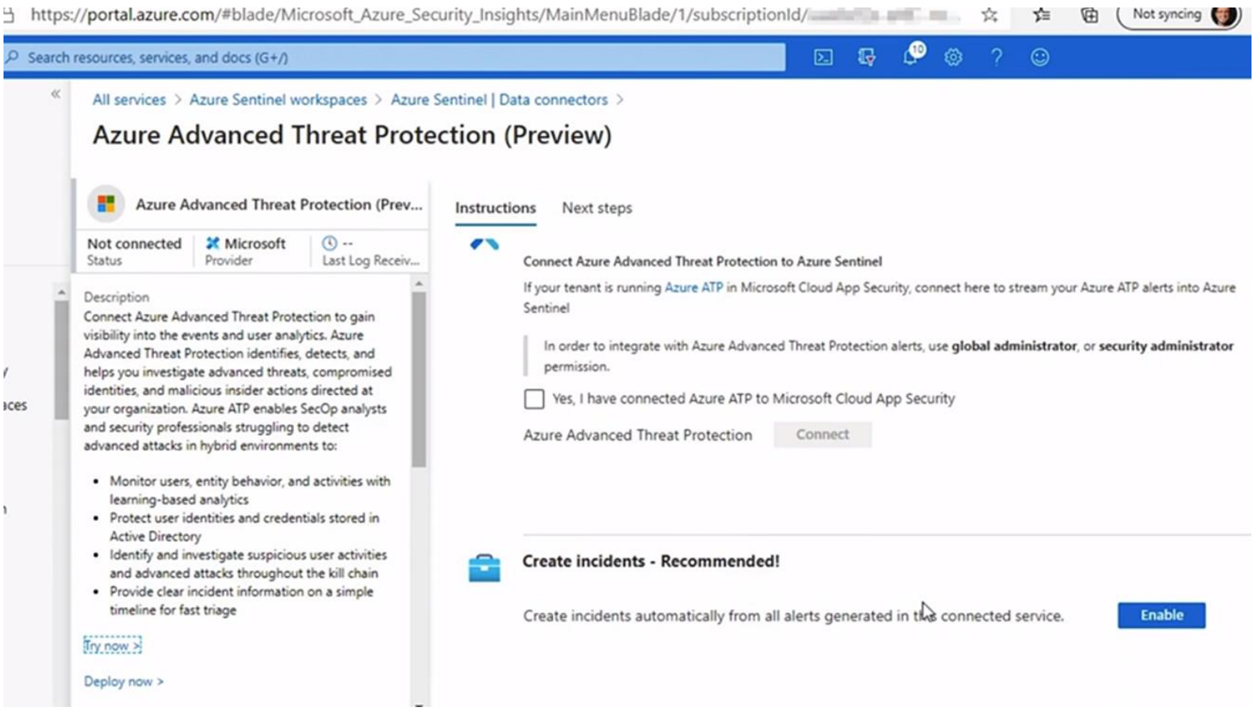
Configuration

Connect Azure Active Directory logs to Azure Sentinel

Select Azure Active Directory log types:

☑ Azure Active Directory Sign-in logs

☑ Azure Active Directory Audit logs


https://portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/1/subscriptionId/[redacted]
Not syncing
Search resources, services, and docs (G+/)
All services > Azure Sentinel workspaces > Azure Sentinel | Data connectors >

Azure Advanced Threat Protection (Preview)

Azure Advanced Threat Protection (Prev...

Not connected	Microsoft	--
Status	Provider	Last Log Receiv...

Description

Connect Azure Advanced Threat Protection to gain visibility into the events and user analytics. Azure Advanced Threat Protection identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Azure ATP enables SecOp analysts and security professionals struggling to detect advanced attacks in hybrid environments to:

- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

Try now >

Deploy now >

Connect Azure Advanced Threat Protection to Azure Sentinel

If your tenant is running Azure ATP in Microsoft Cloud App Security, connect here to stream your Azure ATP alerts into Azure Sentinel

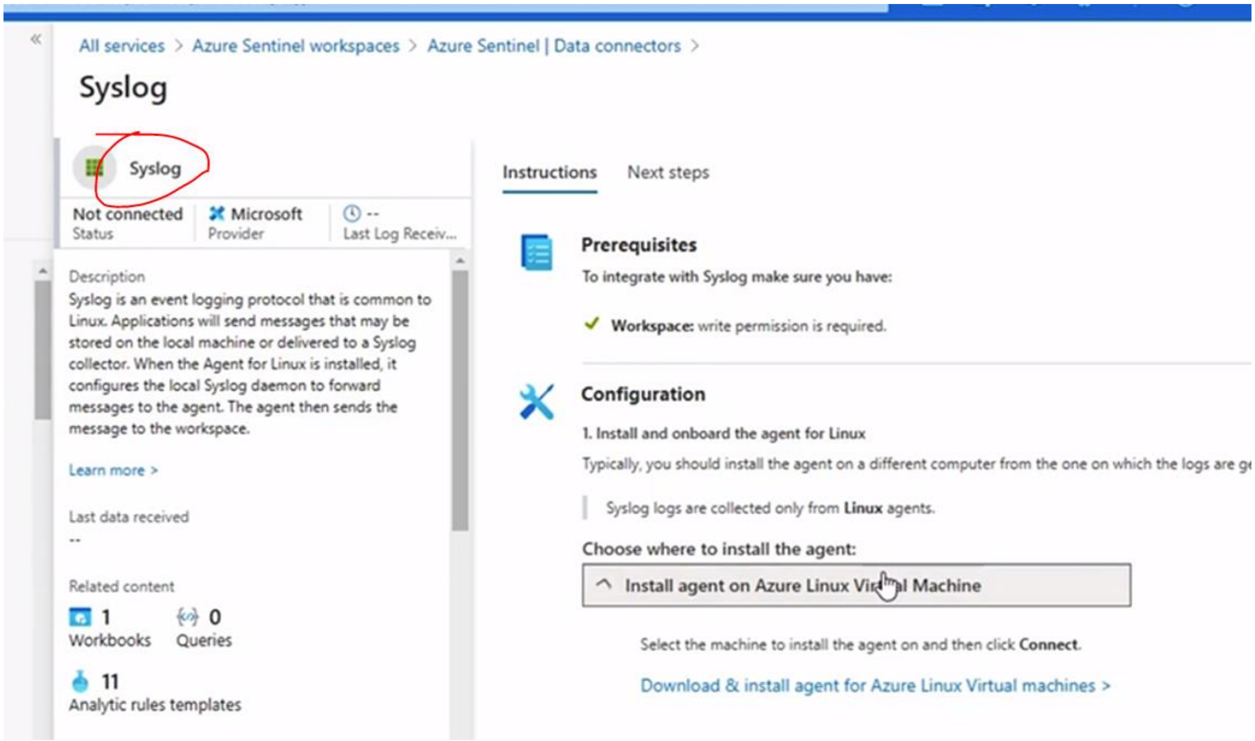
> In order to integrate with Azure Advanced Threat Protection alerts, use **global administrator**, or **security administrator** permission.

☐ Yes, I have connected Azure ATP to Microsoft Cloud App Security

Azure Advanced Threat Protection

Create incidents - Recommended!

Create incidents automatically from all alerts generated in this connected service.



All services > Azure Sentinel workspaces > Azure Sentinel | Data connectors >

Syslog

Syslog

Not connected Status | Microsoft Provider | -- Last Log Receiv...

Description

Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to a Syslog collector. When the Agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sends the message to the workspace.

Learn more >

Last data received

--

Related content

1 Workbooks | 0 Queries

11 Analytic rules templates

Instructions | Next steps

Prerequisites

To integrate with Syslog make sure you have:

✓ **Workspace:** write permission is required.

Configuration

1. Install and onboard the agent for Linux

Typically, you should install the agent on a different computer from the one on which the logs are ge

Syslog logs are collected only from **Linux** agents.

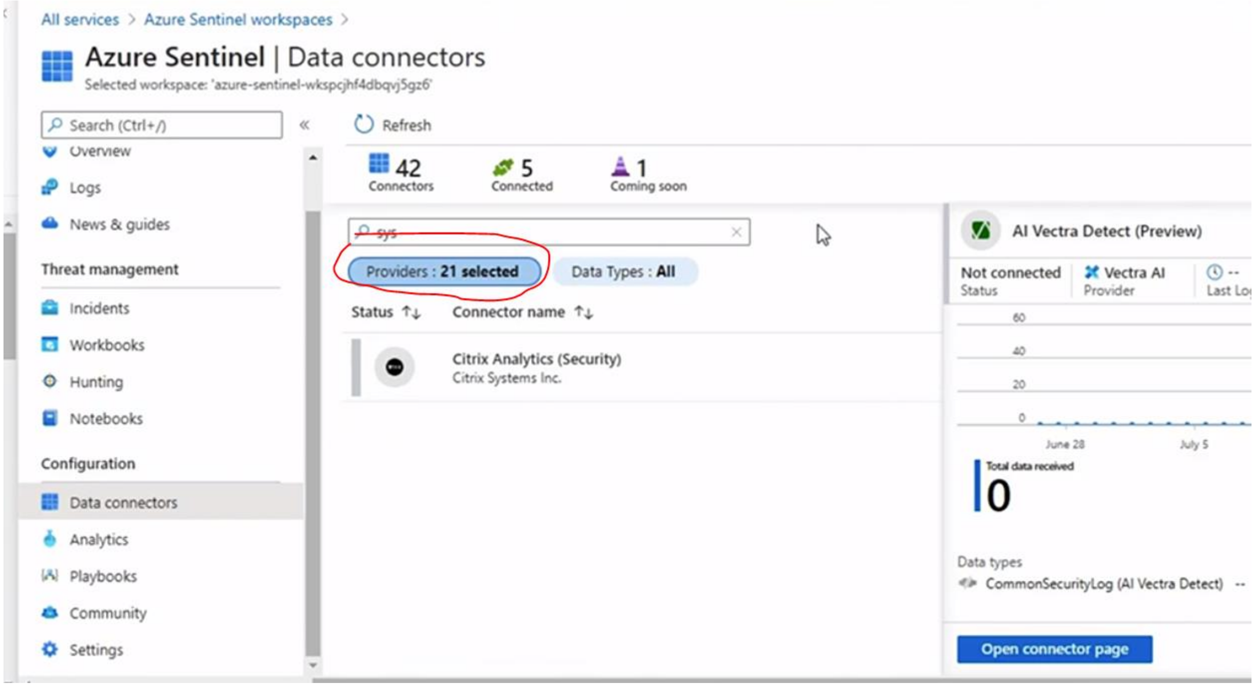
Choose where to install the agent:

Install agent on Azure Linux Virtual Machine

Select the machine to install the agent on and then click **Connect**.

Download & install agent for Azure Linux Virtual machines >

Non-Microsoft Providers



All services > Azure Sentinel workspaces >

Azure Sentinel | Data connectors

Selected workspace: 'azure-sentinel-wkspcjhf4dbqvj5gz6'

42 Connectors | 5 Connected | 1 Coming soon

~~sys~~

Providers : 21 selected | Data Types : All

Status	Connector name
	Citrix Analytics (Security) Citrix Systems Inc.

AI Vectra Detect (Preview)

Not connected Status | Vectra AI Provider | -- Last Lo

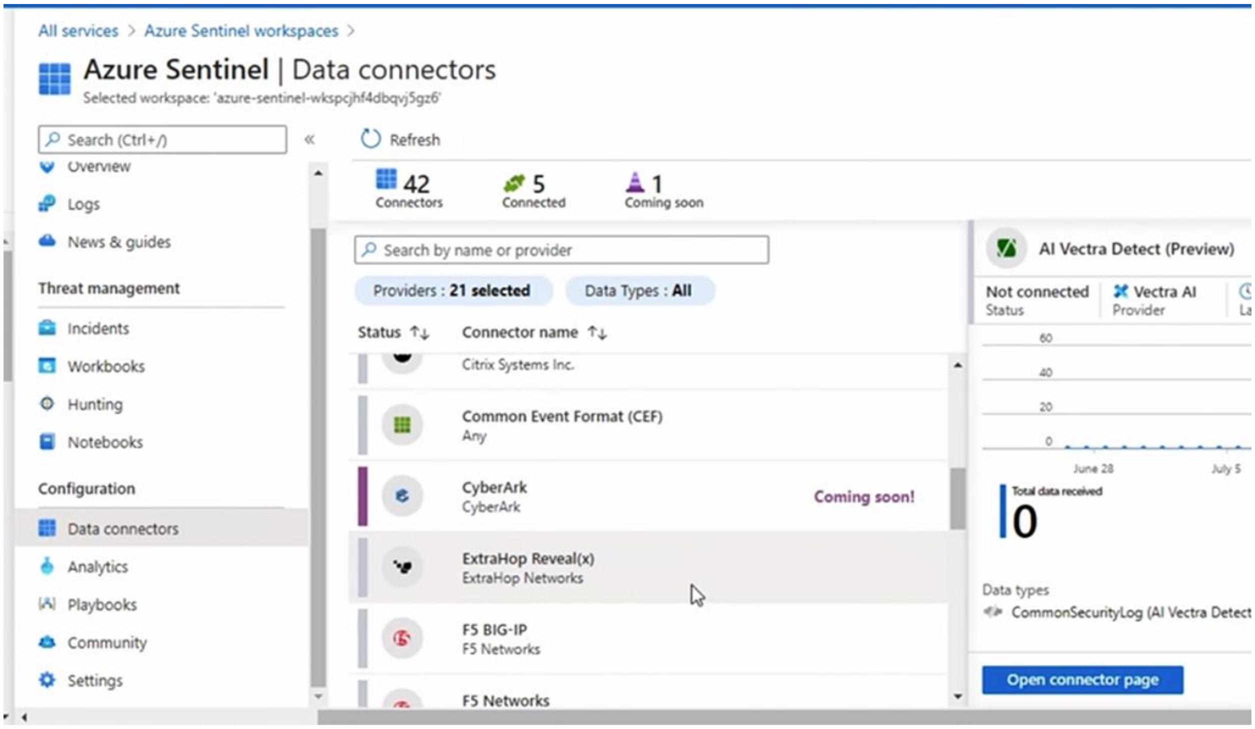
Total data received

0

Data types

CommonSecurityLog (AI Vectra Detect) --

Open connector page



All services > Azure Sentinel workspaces >

Azure Sentinel | Data connectors

Selected workspace: 'azure-sentinel-wkspcjhf4dbqvj5gz6'

42 Connectors | 5 Connected | 1 Coming soon

Search by name or provider

Providers : 21 selected | Data Types : All

Status	Connector name	
	Citrix Systems Inc.	
	Common Event Format (CEF) Any	
	CyberArk CyberArk	Coming soon!
	ExtraHop Reveal(x) ExtraHop Networks	
	F5 BIG-IP F5 Networks	
	F5 Networks	

AI Vectra Detect (Preview)

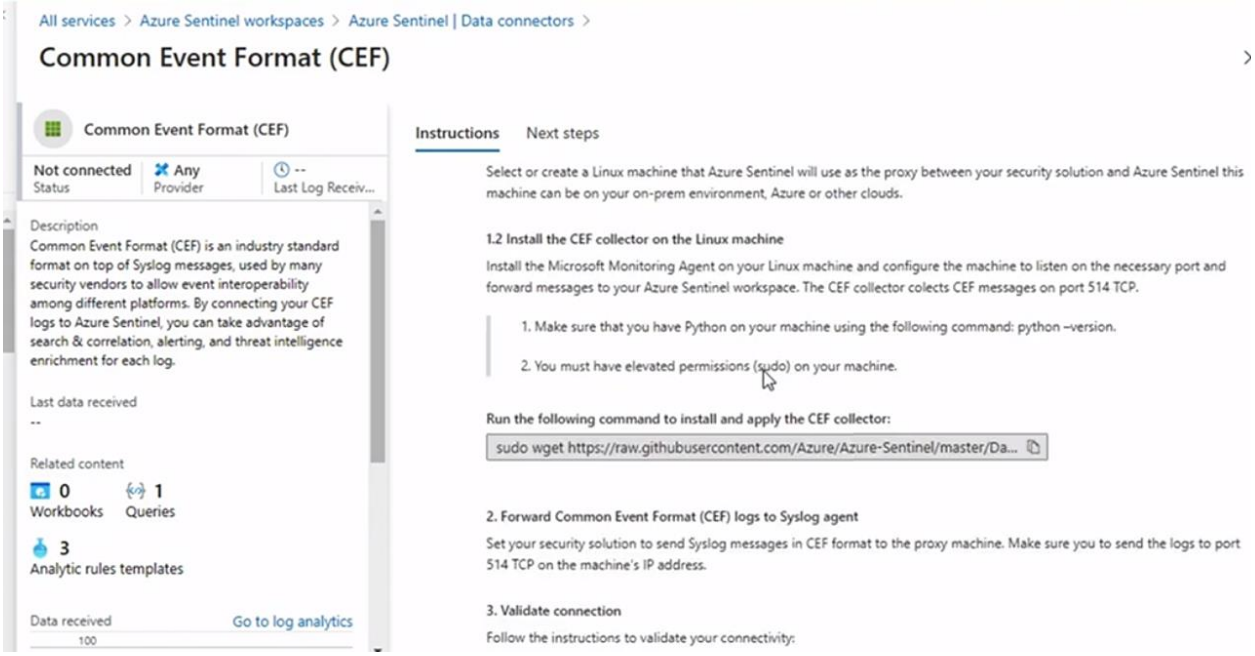
Not connected (Status) | Vectra AI (Provider)

Total data received: 0

Data types

CommonSecurityLog (AI Vectra Detect

Open connector page



All services > Azure Sentinel workspaces > Azure Sentinel | Data connectors >

Common Event Format (CEF)

Common Event Format (CEF)

Not connected (Status) | Any (Provider) | -- (Last Log Receiv...)

Description

Common Event Format (CEF) is an industry standard format on top of Syslog messages, used by many security vendors to allow event interoperability among different platforms. By connecting your CEF logs to Azure Sentinel, you can take advantage of search & correlation, alerting, and threat intelligence enrichment for each log.

Last data received

--

Related content

0 Workbooks | 1 Queries

3 Analytic rules templates

Data received | Go to log analytics

Instructions | Next steps

Select or create a Linux machine that Azure Sentinel will use as the proxy between your security solution and Azure Sentinel this machine can be on your on-prem environment, Azure or other clouds.

1.2 Install the CEF collector on the Linux machine

Install the Microsoft Monitoring Agent on your Linux machine and configure the machine to listen on the necessary port and forward messages to your Azure Sentinel workspace. The CEF collector colects CEF messages on port 514 TCP.

> 1. Make sure that you have Python on your machine using the following command: python –version.
>
> 2. You must have elevated permissions (sudo) on your machine.

Run the following command to install and apply the CEF collector:

```
sudo wget https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Da...
```

2. Forward Common Event Format (CEF) logs to Syslog agent

Set your security solution to send Syslog messages in CEF format to the proxy machine. Make sure you to send the logs to port 514 TCP on the machine's IP address.

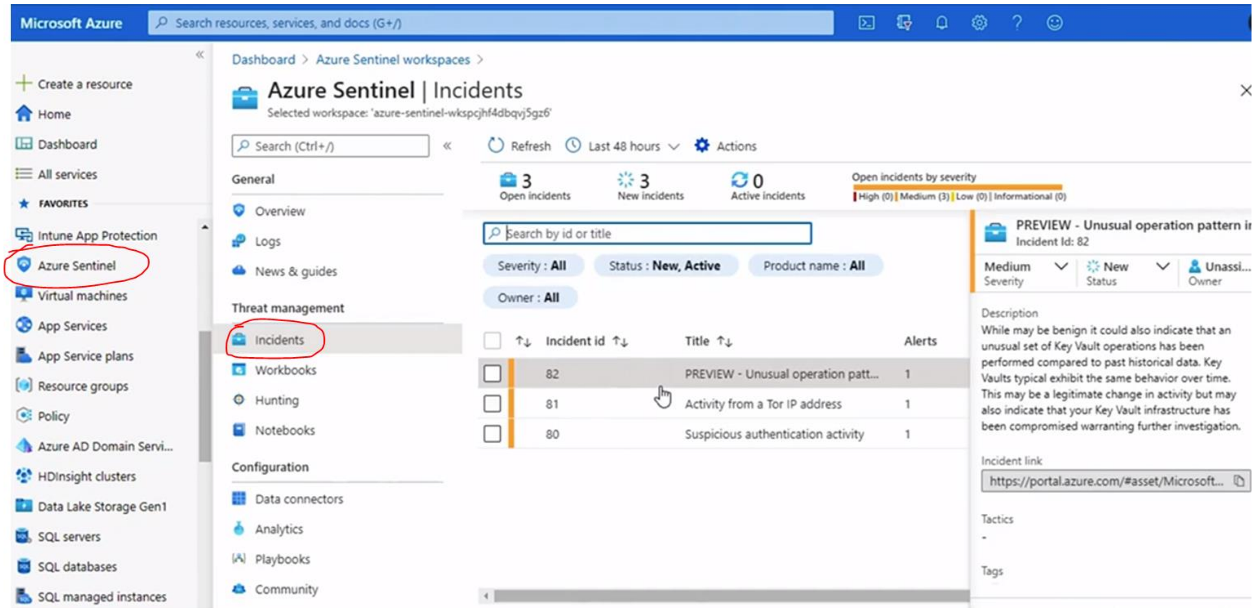
3. Validate connection

Follow the instructions to validate your connectivity:

For the Exam

Know your data sources and types, particularly Microsoft connectors and syslog.

3.6 Evaluate alerts and incidents in Azure Sentinel



Azure Sentinel | Incidents

Selected workspace: 'azure-sentinel-wkspcjhf4dbqvj5gz6'

3 Open incidents · 3 New incidents · 0 Active incidents

Open incidents by severity: High (0) | Medium (3) | Low (0) | Informational (0)

Severity : **All** · Status : **New, Active** · Product name : **All** · Owner : **All**

Incident id	Title	Alerts
82	PREVIEW - Unusual operation patt...	1
81	Activity from a Tor IP address	1
80	Suspicious authentication activity	1

PREVIEW - Unusual operation pattern i

Incident Id: 82

Severity: Medium · Status: New · Owner: Unassi...

Description

While may be benign it could also indicate that an unusual set of Key Vault operations has been performed compared to past historical data. Key Vaults typical exhibit the same behavior over time. This may be a legitimate change in activity but may also indicate that your Key Vault infrastructure has been compromised warranting further investigation.

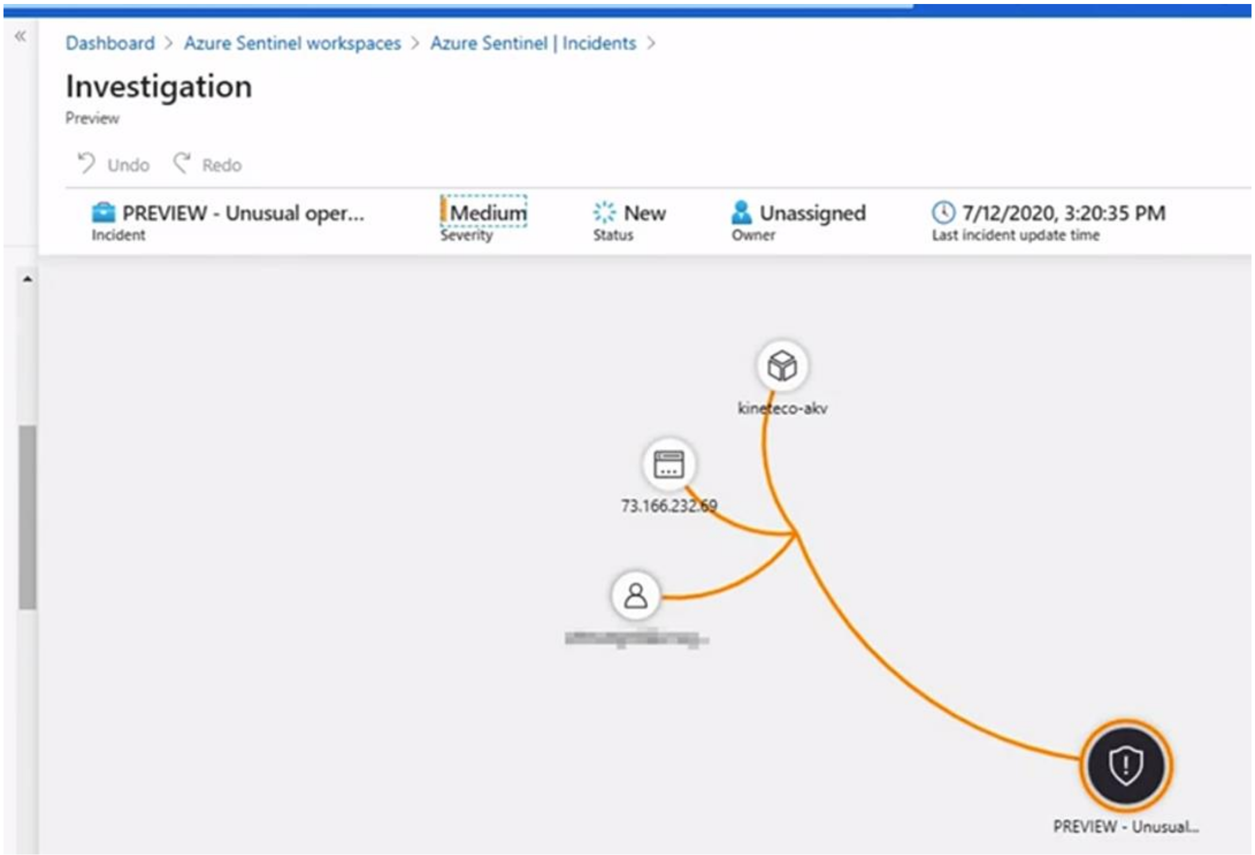
Incident link

https://portal.azure.com/#asset/Microsoft...

Tactics

-

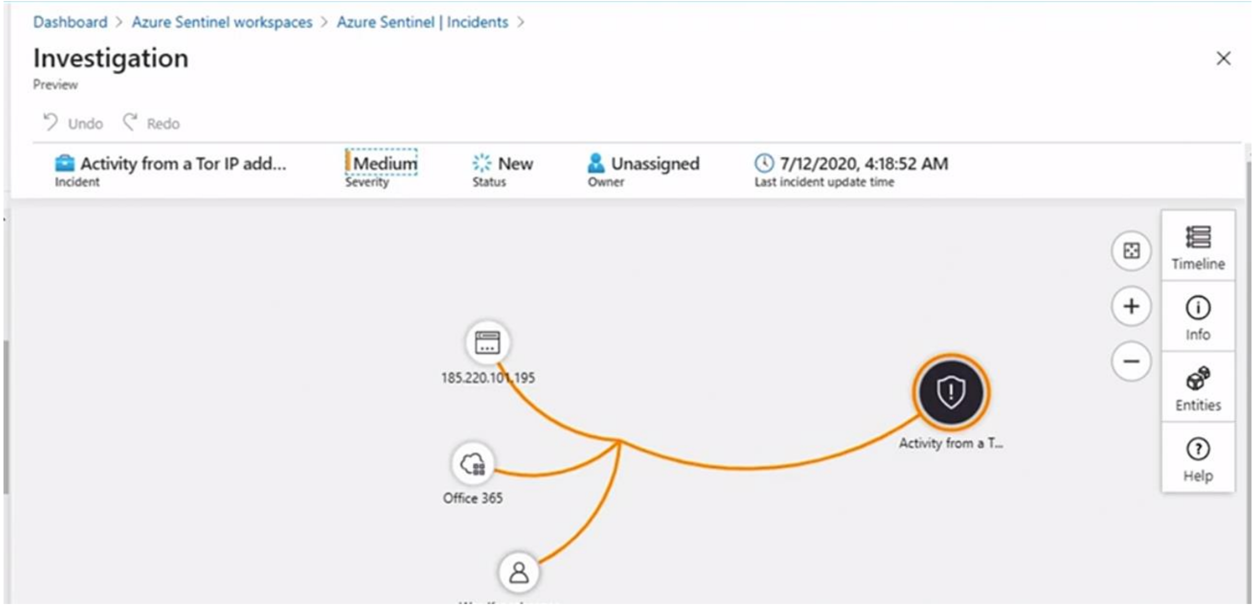
Tags


Dashboard > Azure Sentinel workspaces > Azure Sentinel | Incidents >
Undo
Redo
kineteco-akv
73.166.232.69
[redacted]
PREVIEW - Unusual...

Investigation

Preview

PREVIEW - Unusual oper...	Medium	New	Unassigned	7/12/2020, 3:20:35 PM
Incident	Severity	Status	Owner	Last incident update time



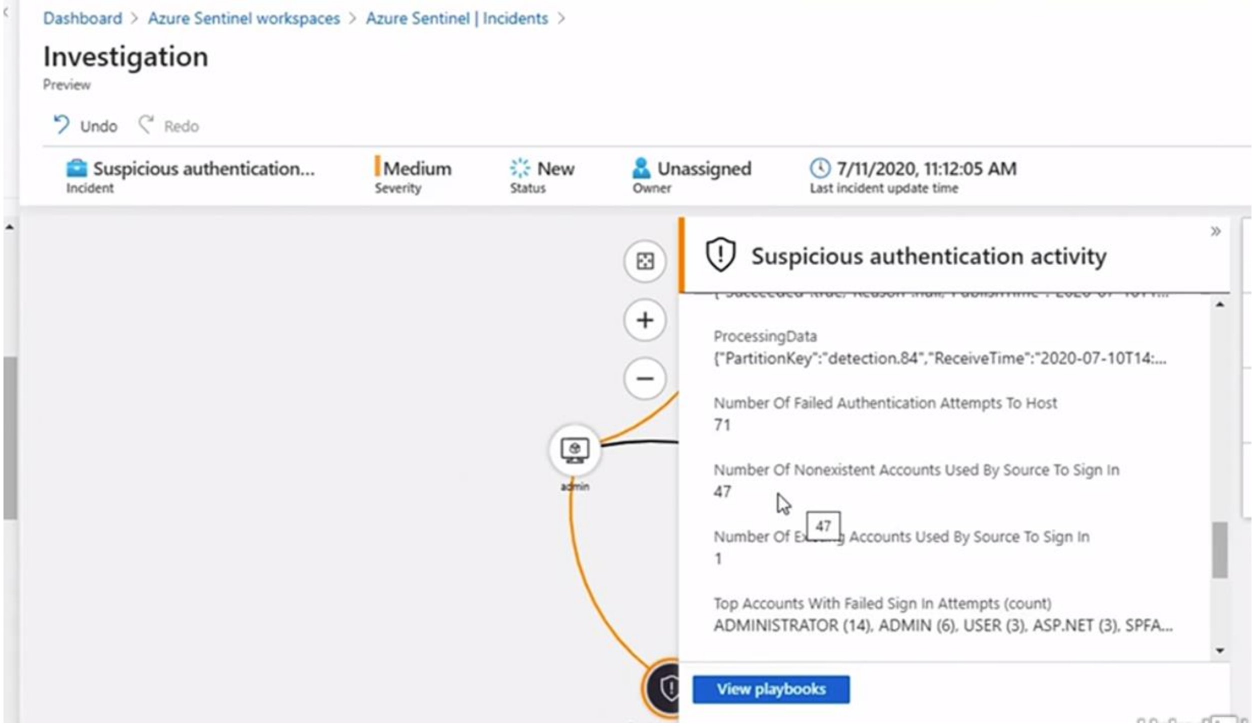
Dashboard > Azure Sentinel workspaces > Azure Sentinel | Incidents >

Investigation

Preview

Undo Redo

Incident	Severity	Status	Owner	Last incident update time
Activity from a Tor IP add...	Medium	New	Unassigned	7/12/2020, 4:18:52 AM



Dashboard > Azure Sentinel workspaces > Azure Sentinel | Incidents >

Investigation

Preview

Undo Redo

Incident	Severity	Status	Owner	Last incident update time
Suspicious authentication...	Medium	New	Unassigned	7/11/2020, 11:12:05 AM

Suspicious authentication activity

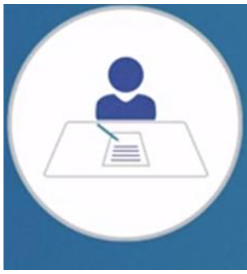
ProcessingData
{"PartitionKey":"detection.84","ReceiveTime":"2020-07-10T14:...

Number Of Failed Authentication Attempts To Host
71

Number Of Nonexistent Accounts Used By Source To Sign In
47

Number Of Existing Accounts Used By Source To Sign In
1

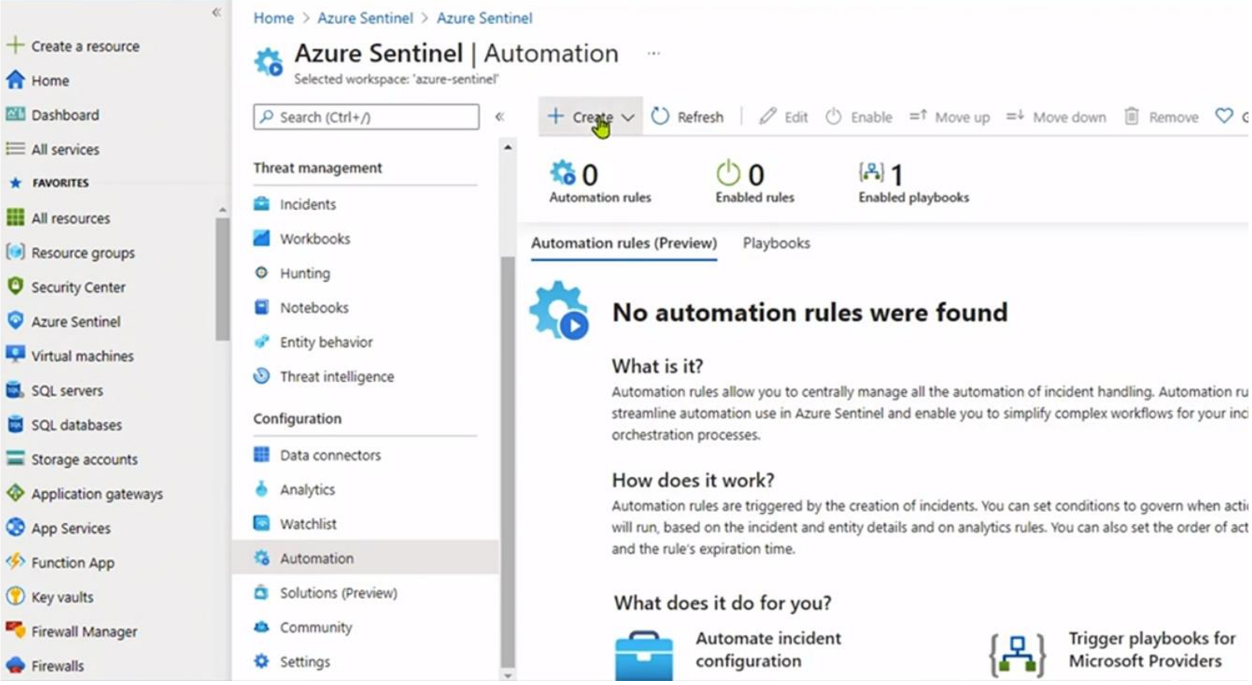
Top Accounts With Failed Sign In Attempts (count)
ADMINISTRATOR (14), ADMIN (6), USER (3), ASP.NET (3), SPFA...



For the Exam

Get familiar with the investigation and hunting interfaces.

3.7 Configure a playbook



Azure Sentinel | Automation

Selected workspace: 'azure-sentinel'

No automation rules were found

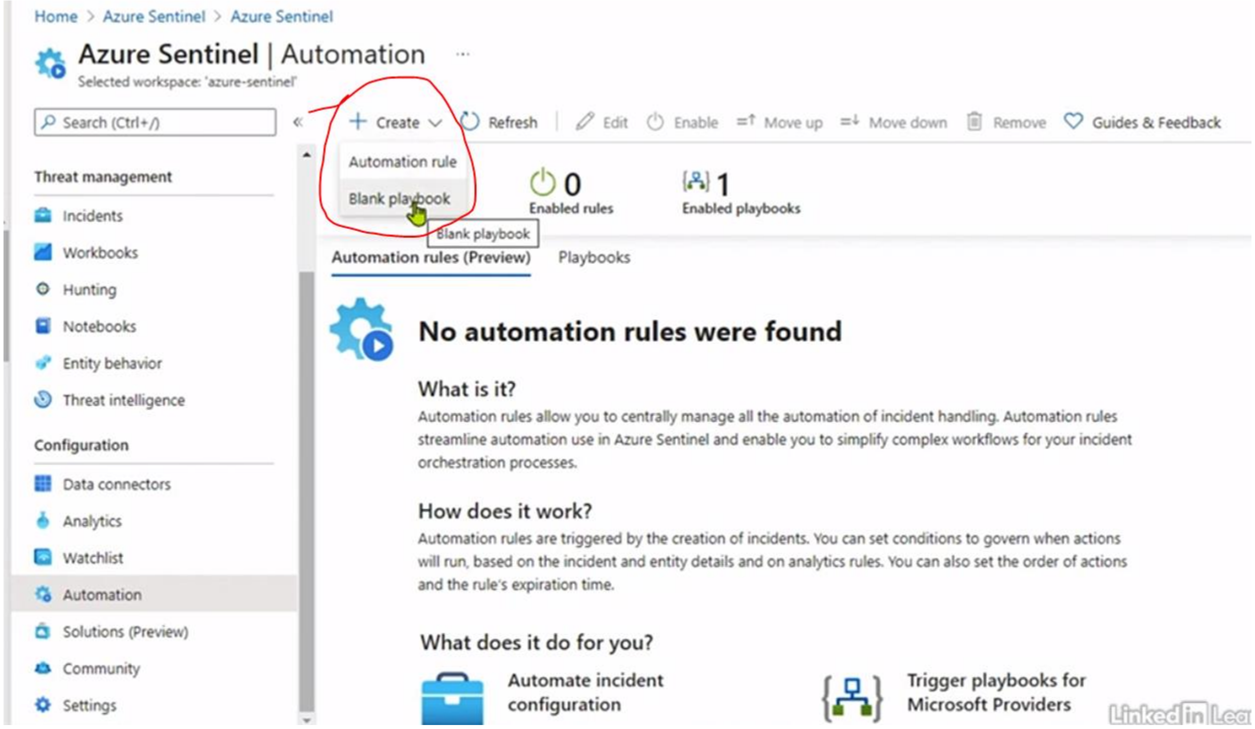
What is it?

Automation rules allow you to centrally manage all the automation of incident handling. Automation ru
streamline automation use in Azure Sentinel and enable you to simplify complex workflows for your inci
orchestration processes.

How does it work?

Automation rules are triggered by the creation of incidents. You can set conditions to govern when acti
will run, based on the incident and entity details and on analytics rules. You can also set the order of act
and the rule's expiration time.

What does it do for you?



Azure Sentinel | Automation

Selected workspace: 'azure-sentinel'

No automation rules were found

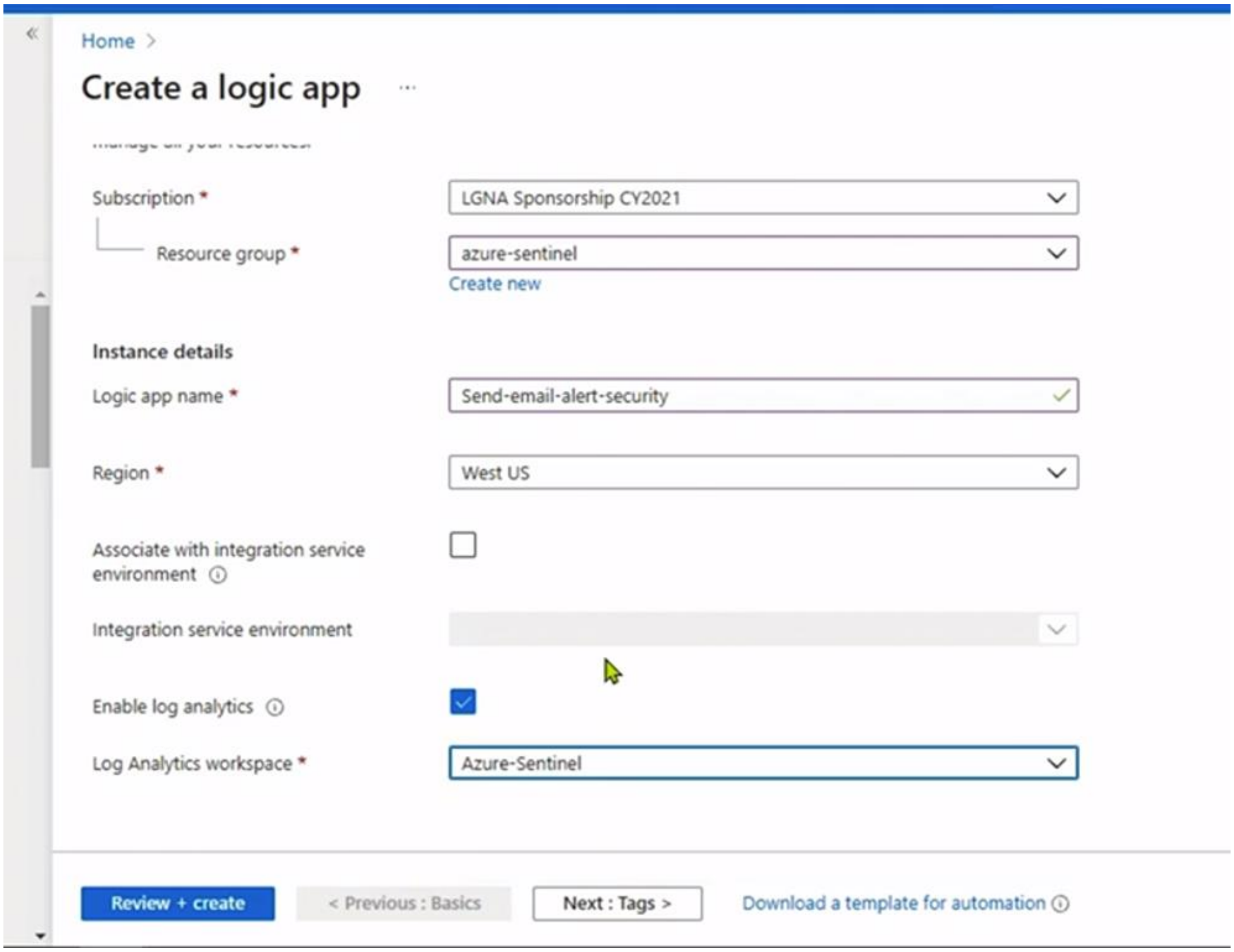
What is it?

Automation rules allow you to centrally manage all the automation of incident handling. Automation rules streamline automation use in Azure Sentinel and enable you to simplify complex workflows for your incident orchestration processes.

How does it work?

Automation rules are triggered by the creation of incidents. You can set conditions to govern when actions will run, based on the incident and entity details and on analytics rules. You can also set the order of actions and the rule's expiration time.

What does it do for you?



Home >

Create a logic app ···

Subscription * LGNA Sponsorship CY2021

Resource group * azure-sentinel

Create new

Instance details

Logic app name * Send-email-alert-security

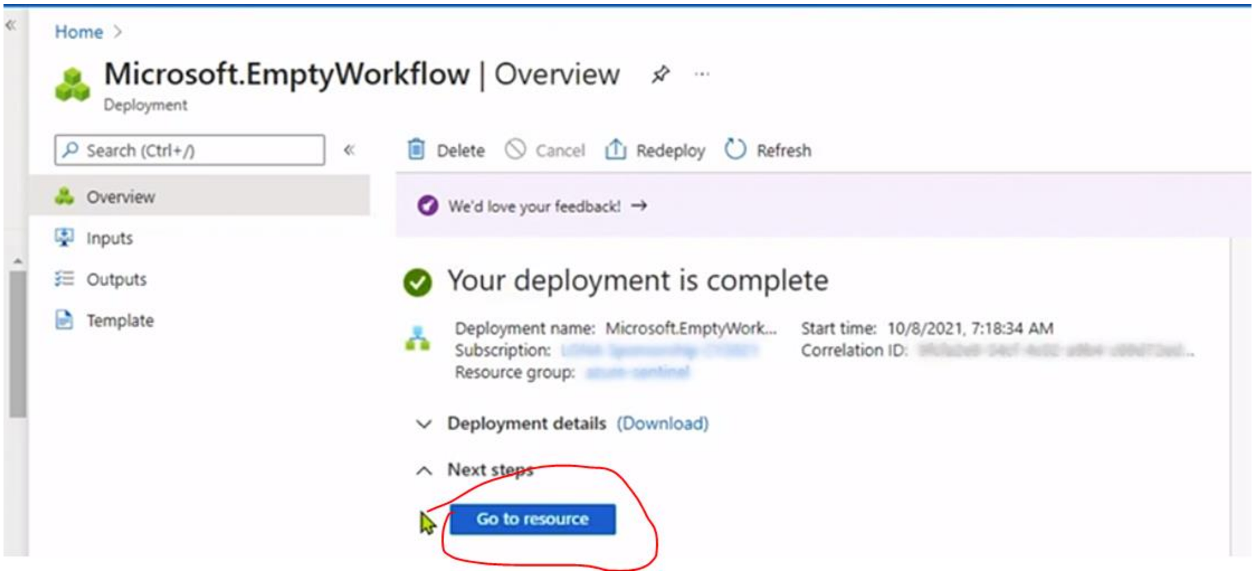
Region * West US

Associate with integration service environment ⓘ □

Integration service environment

Enable log analytics ⓘ ☑

Log Analytics workspace * Azure-Sentinel



Home >

Microsoft.EmptyWorkflow | Overview

Deployment

Your deployment is complete

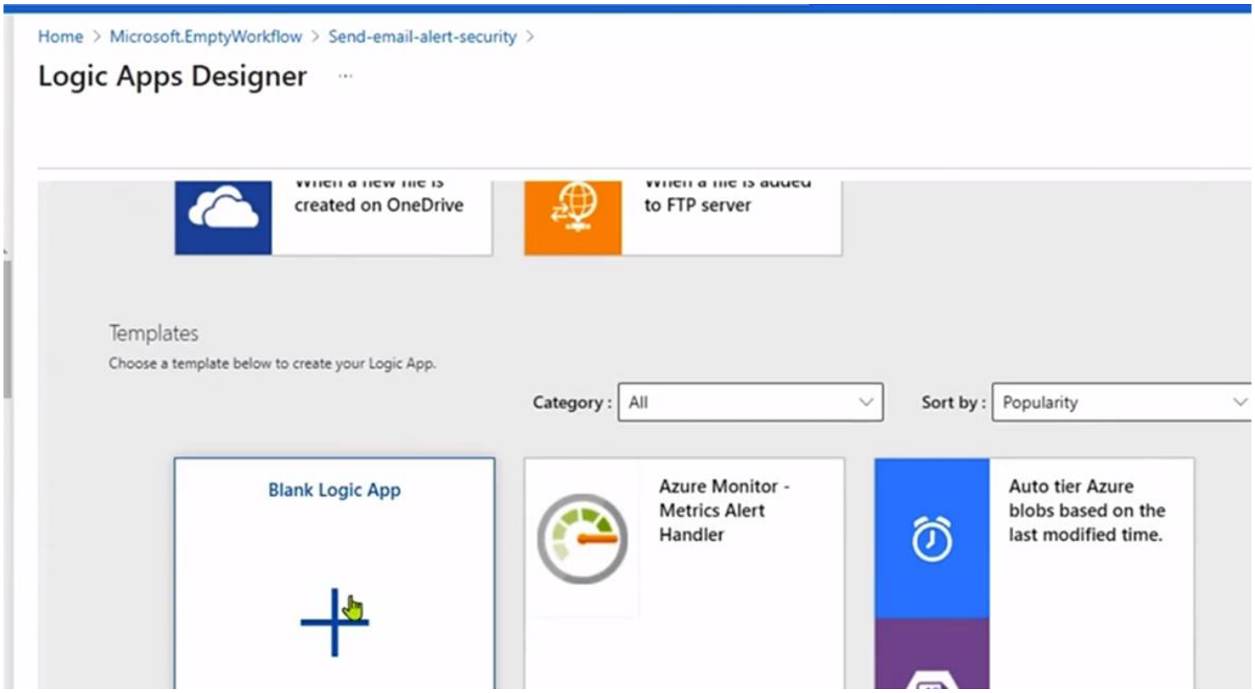
Deployment name: Microsoft.EmptyWork... Start time: 10/8/2021, 7:18:34 AM

Subscription: [redacted] Correlation ID: [redacted]

Resource group: [redacted]

Deployment details (Download)

Next steps



Home > Microsoft.EmptyWorkflow > Send-email-alert-security >

Logic Apps Designer ···

When a new file is created on OneDrive
When a file is added to FTP server

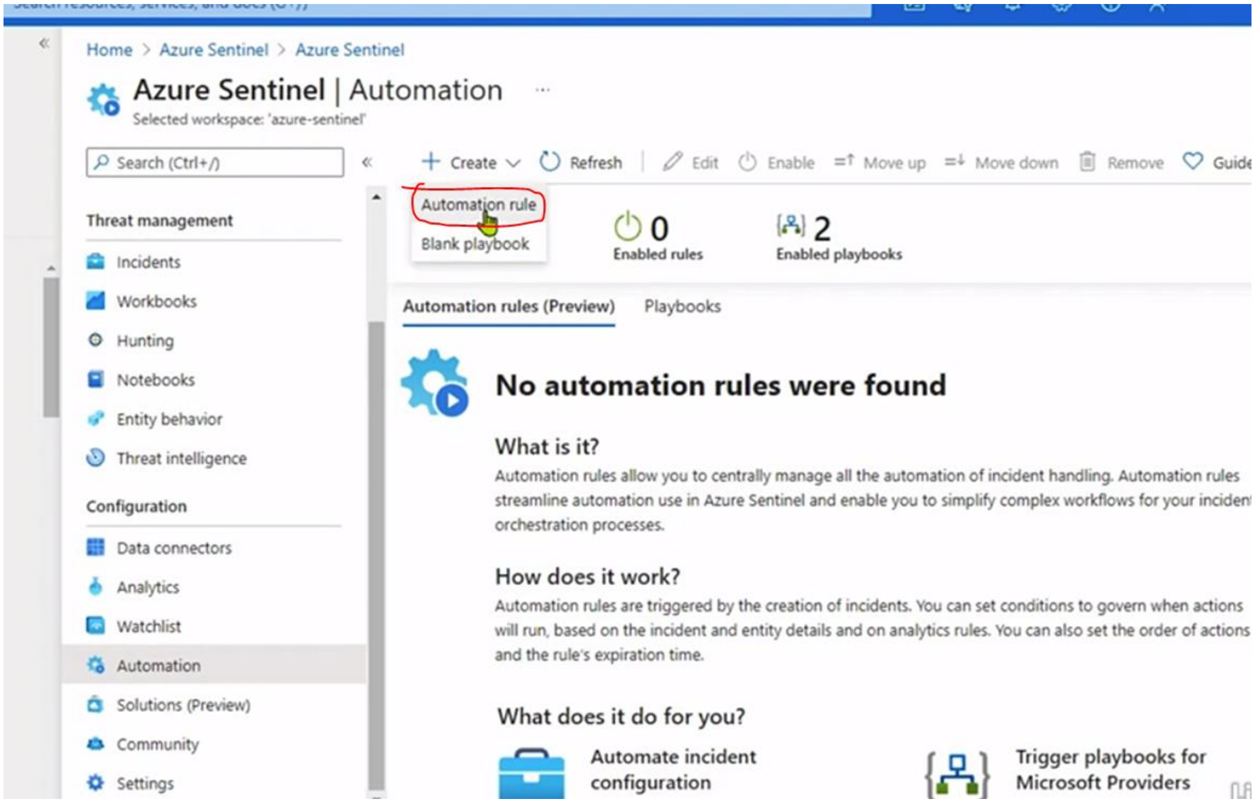
Templates

Choose a template below to create your Logic App.

Category : All

Sort by : Popularity

Blank Logic App
Azure Monitor - Metrics Alert Handler
Auto tier Azure blobs based on the last modified time.



Home > Azure Sentinel > Azure Sentinel

Azure Sentinel | Automation ···

Selected workspace: 'azure-sentinel'

No automation rules were found

What is it?

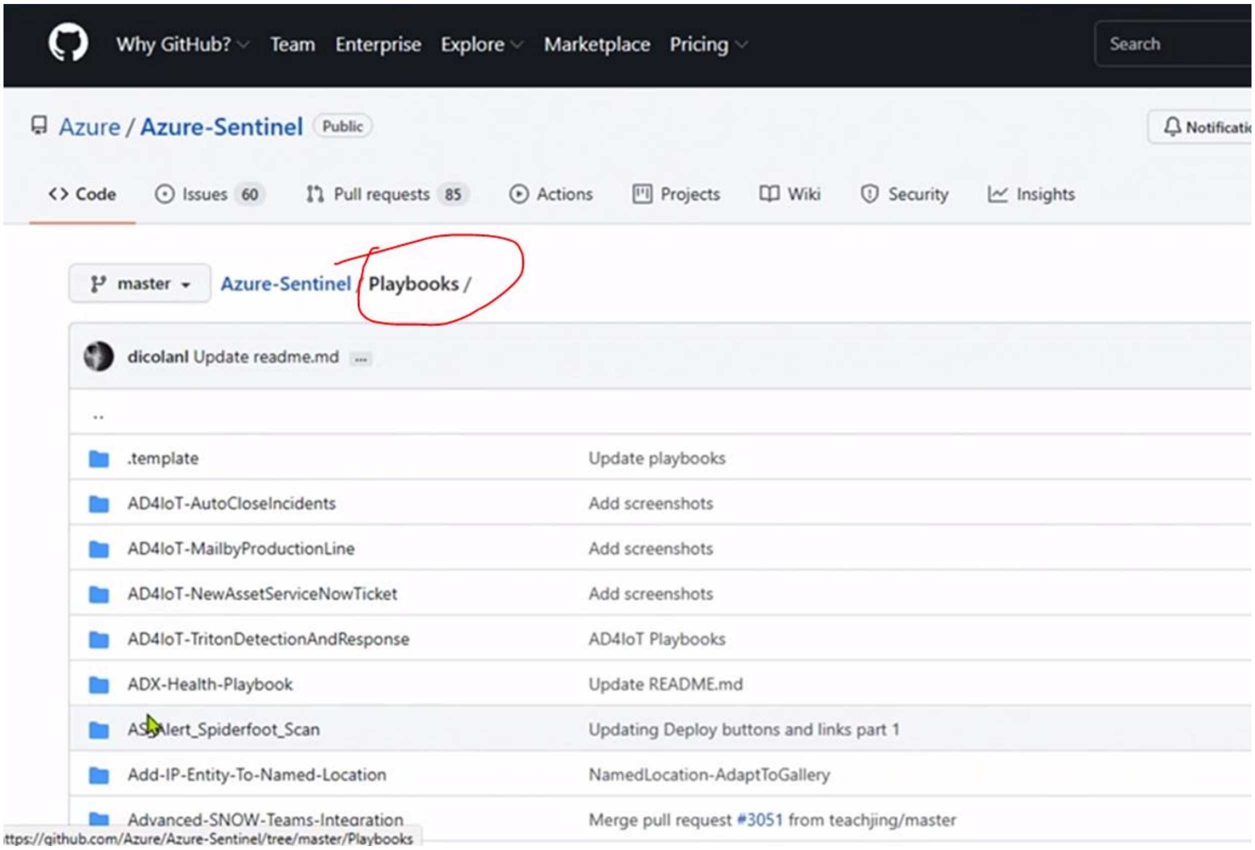
Automation rules allow you to centrally manage all the automation of incident handling. Automation rules streamline automation use in Azure Sentinel and enable you to simplify complex workflows for your inciden orchestration processes.

How does it work?

Automation rules are triggered by the creation of incidents. You can set conditions to govern when actions will run, based on the incident and entity details and on analytics rules. You can also set the order of actions and the rule's expiration time.

What does it do for you?

Automate incident configuration
Trigger playbooks for Microsoft Providers



Azure / Azure-Sentinel Public

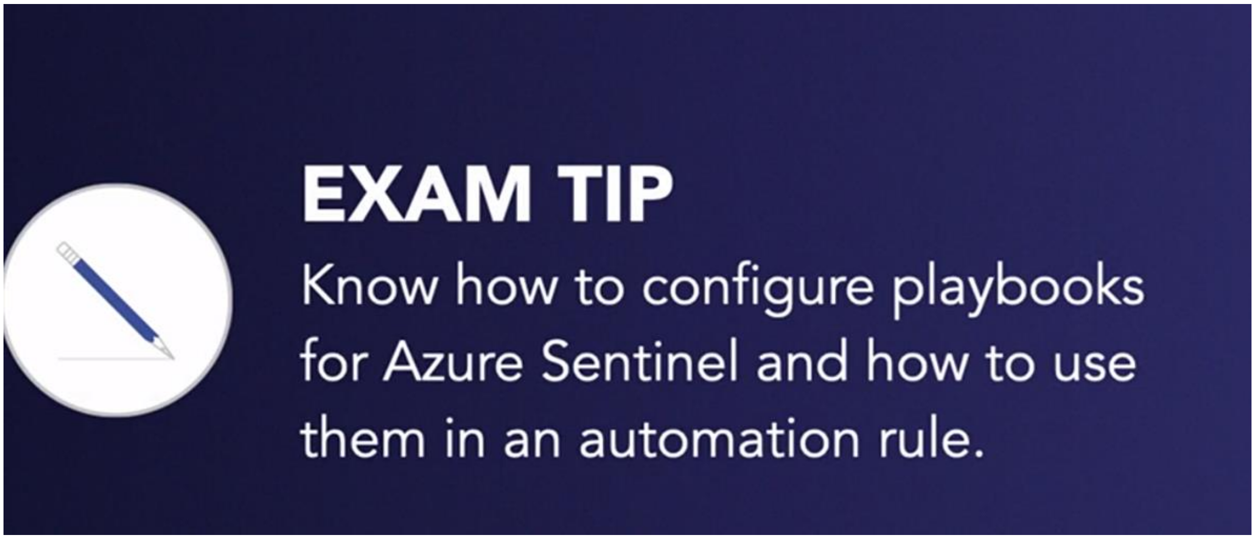
Azure-Sentinel / Playbooks /

dicolanl Update readme.md …

..

.template	Update playbooks
AD4IoT-AutoCloseIncidents	Add screenshots
AD4IoT-MailbyProductionLine	Add screenshots
AD4IoT-NewAssetServiceNowTicket	Add screenshots
AD4IoT-TritonDetectionAndResponse	AD4IoT Playbooks
ADX-Health-Playbook	Update README.md
ASAlert_Spiderfoot_Scan	Updating Deploy buttons and links part 1
Add-IP-Entity-To-Named-Location	NamedLocation-AdaptToGallery
Advanced-SNOW-Teams-Integration	Merge pull request #3051 from teachjing/master

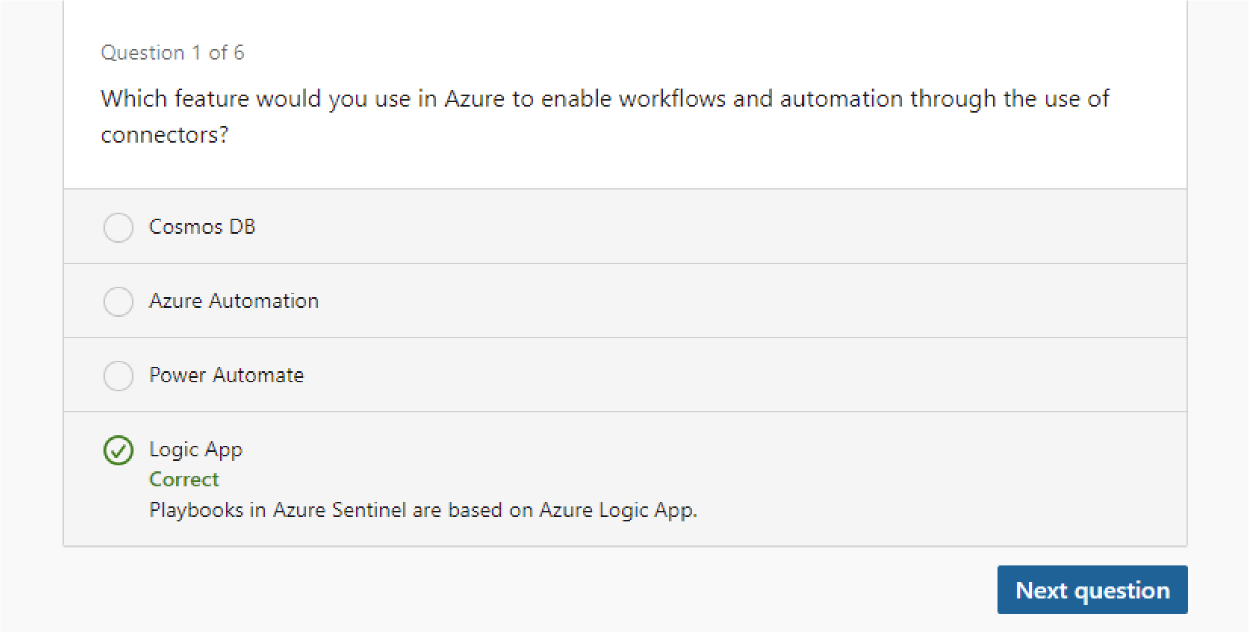
ttps://github.com/Azure/Azure-Sentinel/tree/master/Playbooks



EXAM TIP

Know how to configure playbooks for Azure Sentinel and how to use them in an automation rule.

3.8 Quiz



Question 1 of 6

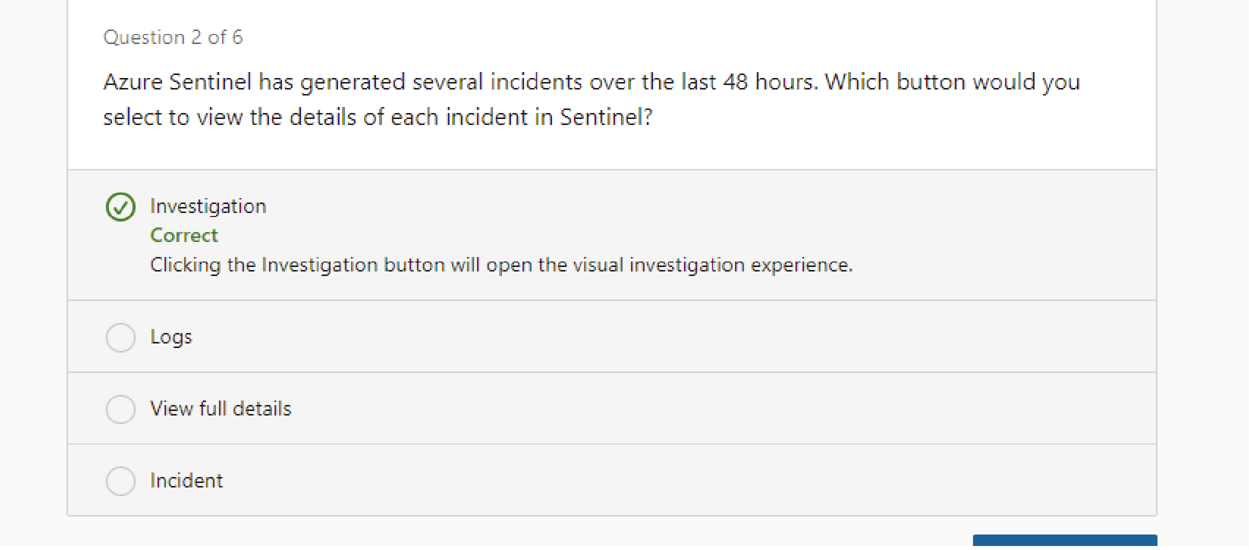
Which feature would you use in Azure to enable workflows and automation through the use of connectors?

○ Cosmos DB

○ Azure Automation

○ Power Automate

✓ Logic App
Correct
Playbooks in Azure Sentinel are based on Azure Logic App.



Question 2 of 6

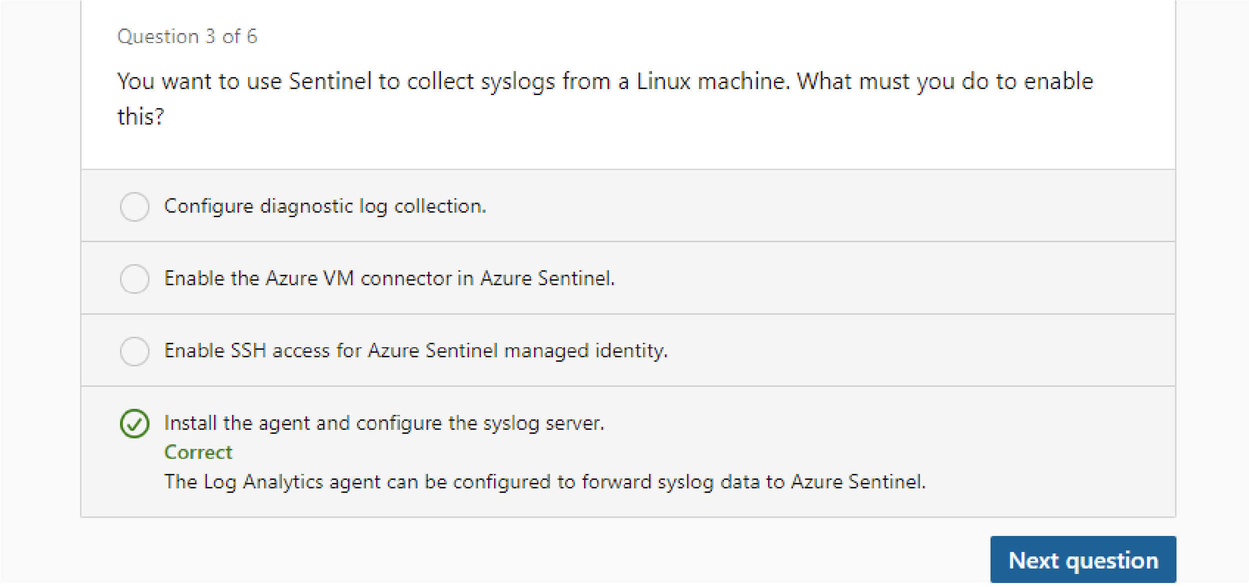
Azure Sentinel has generated several incidents over the last 48 hours. Which button would you select to view the details of each incident in Sentinel?

✓ Investigation
Correct
Clicking the Investigation button will open the visual investigation experience.

○ Logs

○ View full details

○ Incident



Question 3 of 6

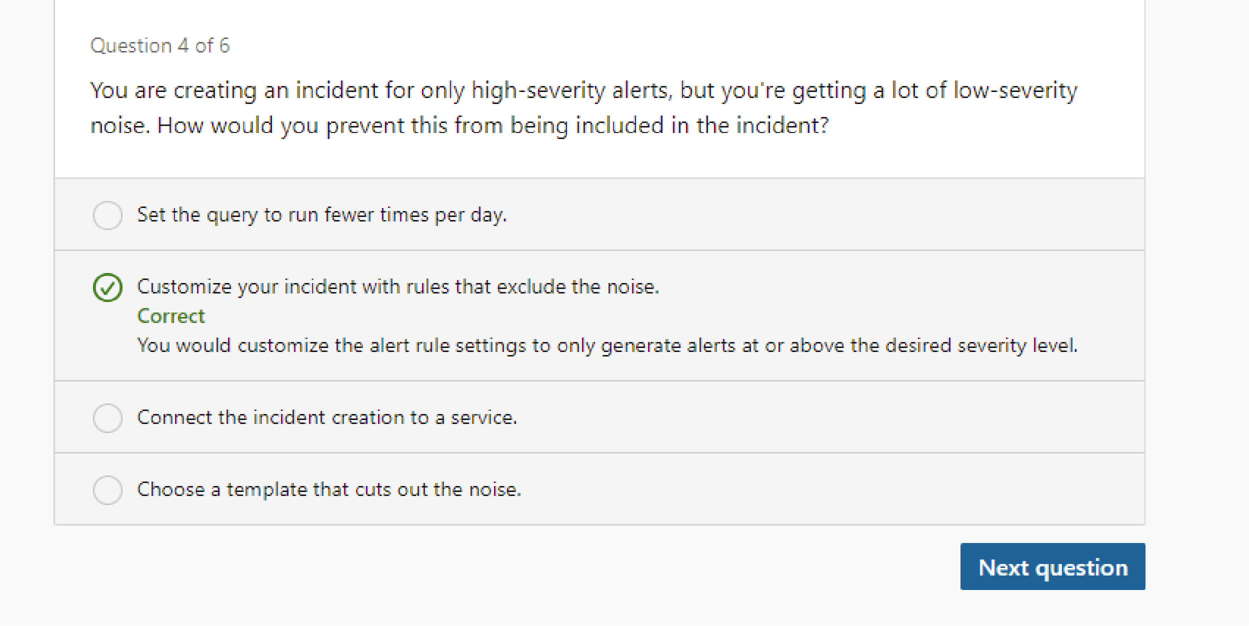
You want to use Sentinel to collect syslogs from a Linux machine. What must you do to enable this?

○ Configure diagnostic log collection.

○ Enable the Azure VM connector in Azure Sentinel.

○ Enable SSH access for Azure Sentinel managed identity.

✓ Install the agent and configure the syslog server.
Correct
The Log Analytics agent can be configured to forward syslog data to Azure Sentinel.



Question 4 of 6

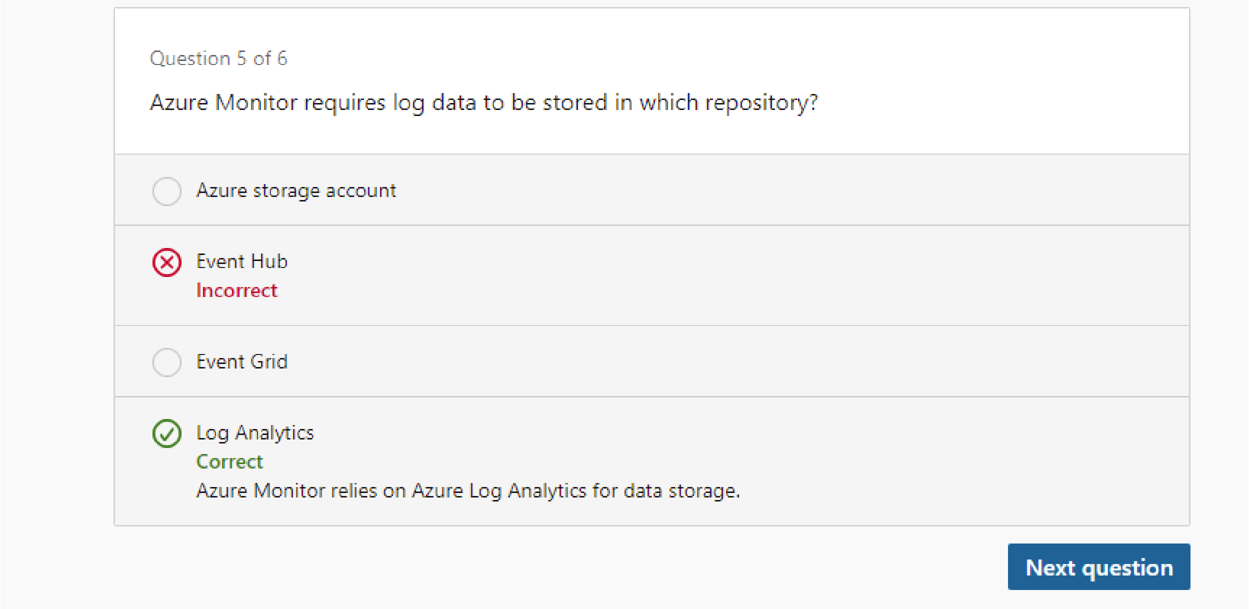
You are creating an incident for only high-severity alerts, but you're getting a lot of low-severity noise. How would you prevent this from being included in the incident?

○ Set the query to run fewer times per day.

✓ Customize your incident with rules that exclude the noise.
Correct
You would customize the alert rule settings to only generate alerts at or above the desired severity level.

○ Connect the incident creation to a service.

○ Choose a template that cuts out the noise.



Question 5 of 6

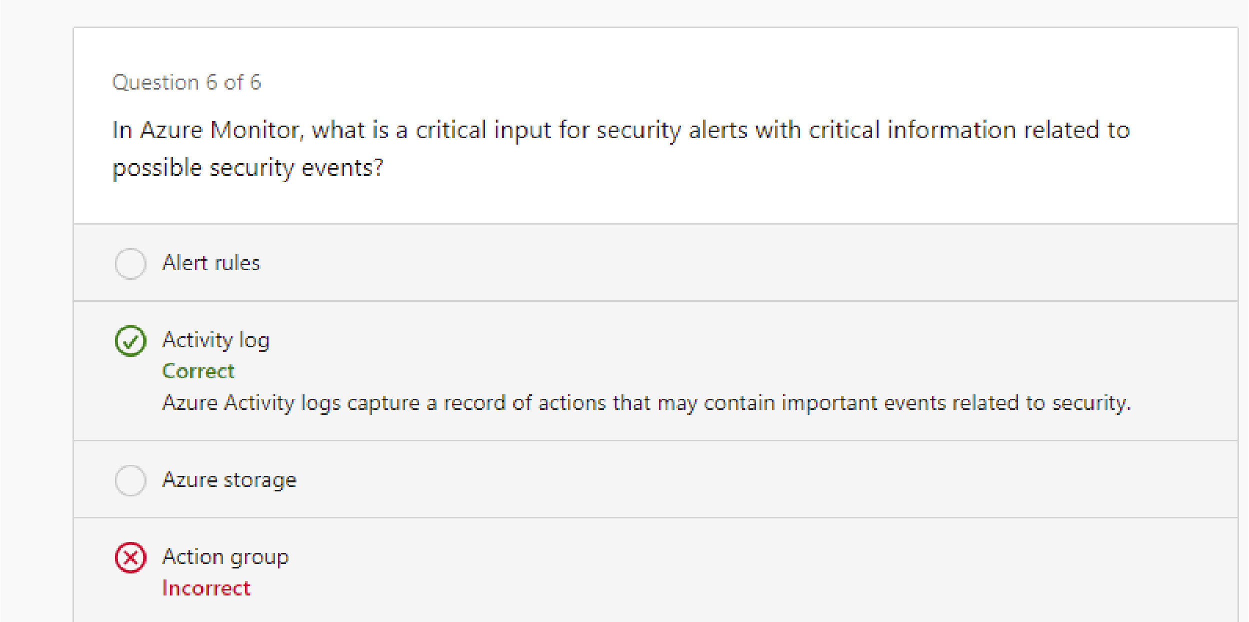
Azure Monitor requires log data to be stored in which repository?

○ Azure storage account

⊗ Event Hub
Incorrect

○ Event Grid

✓ Log Analytics
Correct
Azure Monitor relies on Azure Log Analytics for data storage.



Question 6 of 6

In Azure Monitor, what is a critical input for security alerts with critical information related to possible security events?

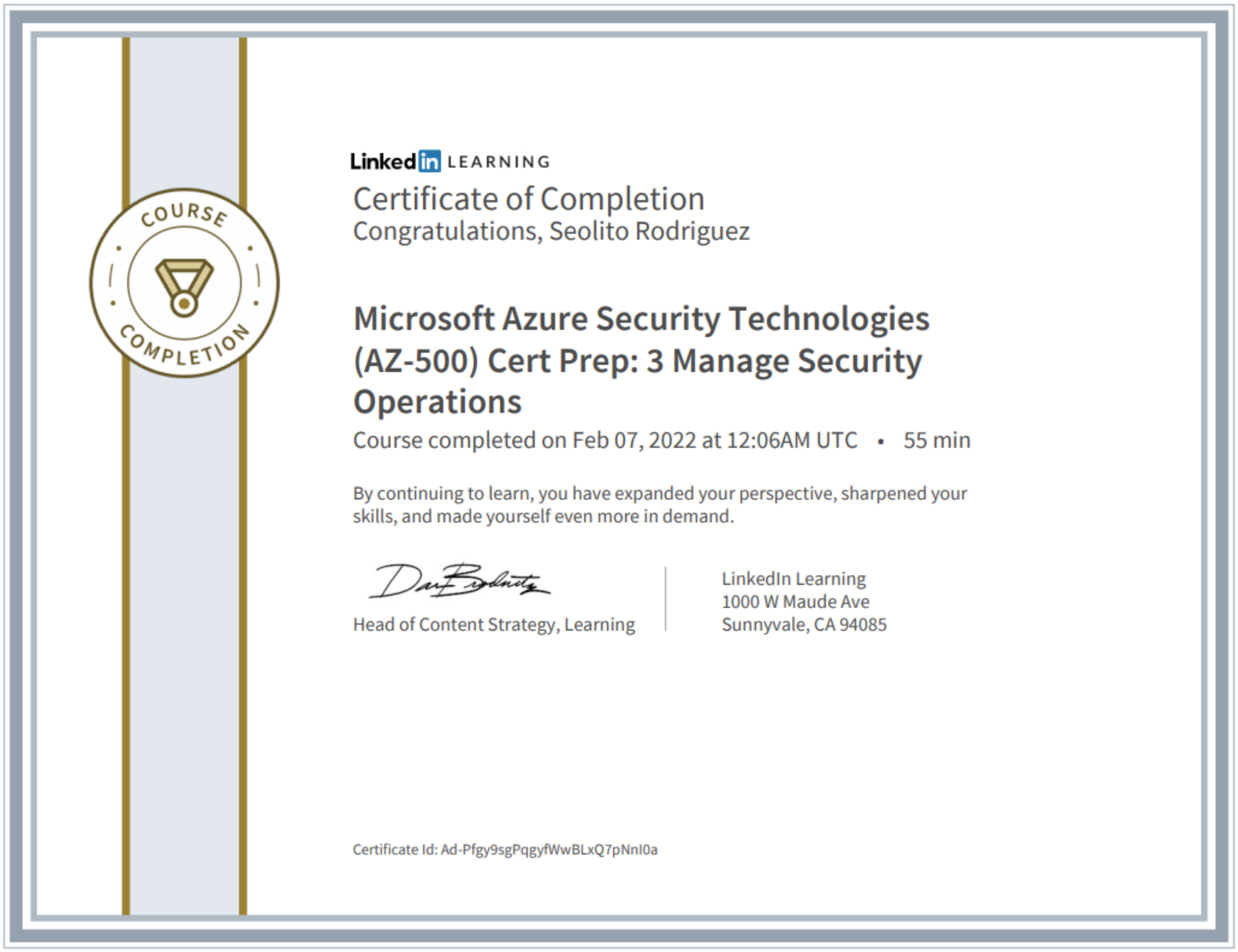
○ Alert rules

✓ Activity log
Correct
Azure Activity logs capture a record of actions that may contain important events related to security.

○ Azure storage

⊗ Action group
Incorrect

Certificate



COURSE
COMPLETION

Linked in LEARNING

Certificate of Completion

Congratulations, Seolito Rodriguez

Microsoft Azure Security Technologies (AZ-500) Cert Prep: 3 Manage Security Operations

Course completed on Feb 07, 2022 at 12:06AM UTC • 55 min

By continuing to learn, you have expanded your perspective, sharpened your skills, and made yourself even more in demand.

Head of Content Strategy, Learning

LinkedIn Learning
1000 W Maude Ave
Sunnyvale, CA 94085

Certificate Id: Ad-PfgygsgPqgyfWwBLxQ7pNnI0a

References