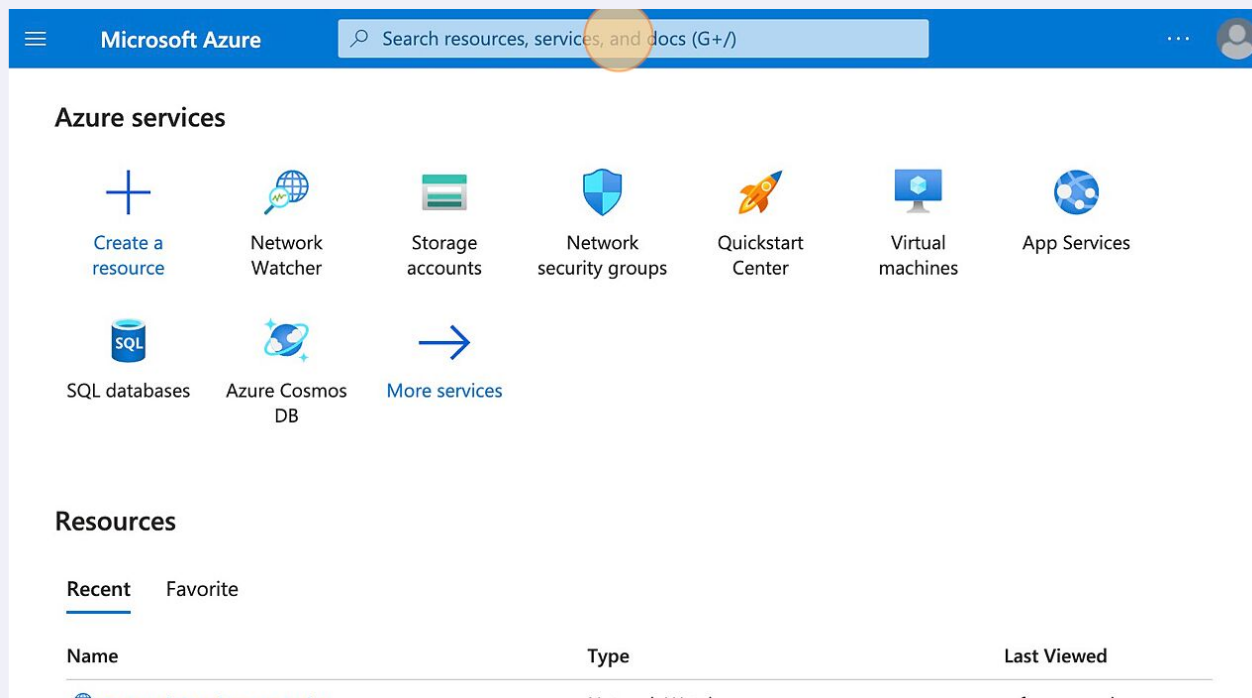


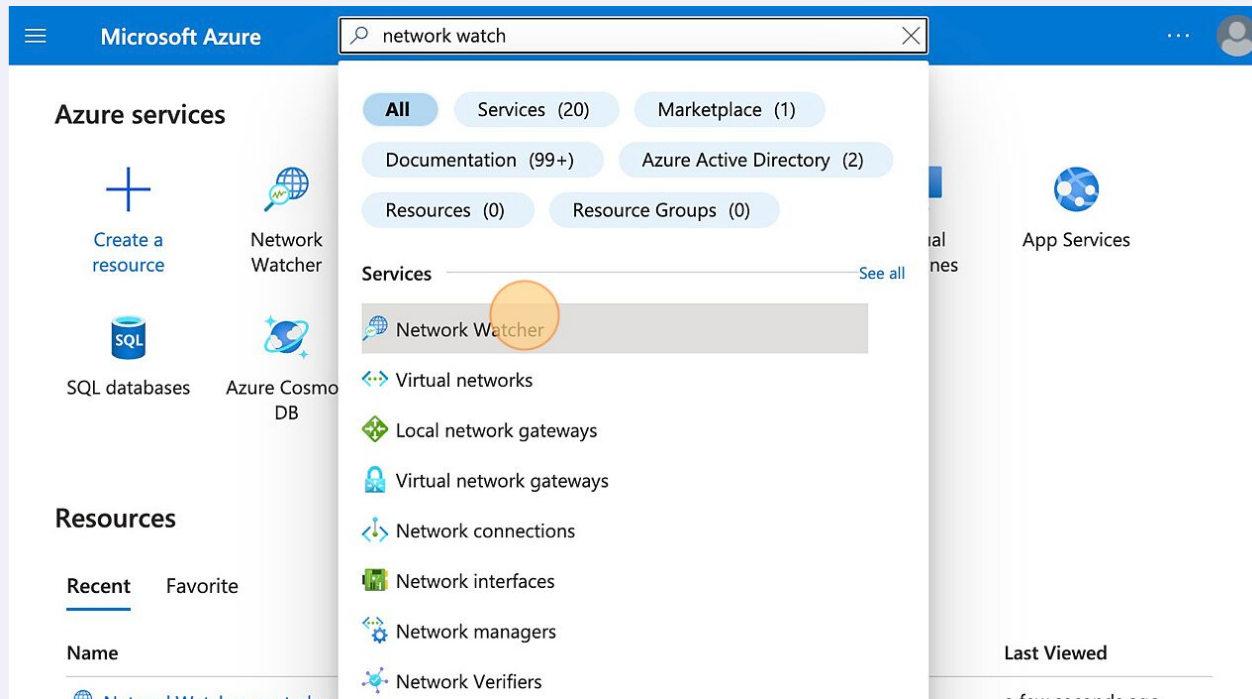
Enabling Azure Flow Logs for Prisma Cloud

1 Navigate to portal.azure.com/#home

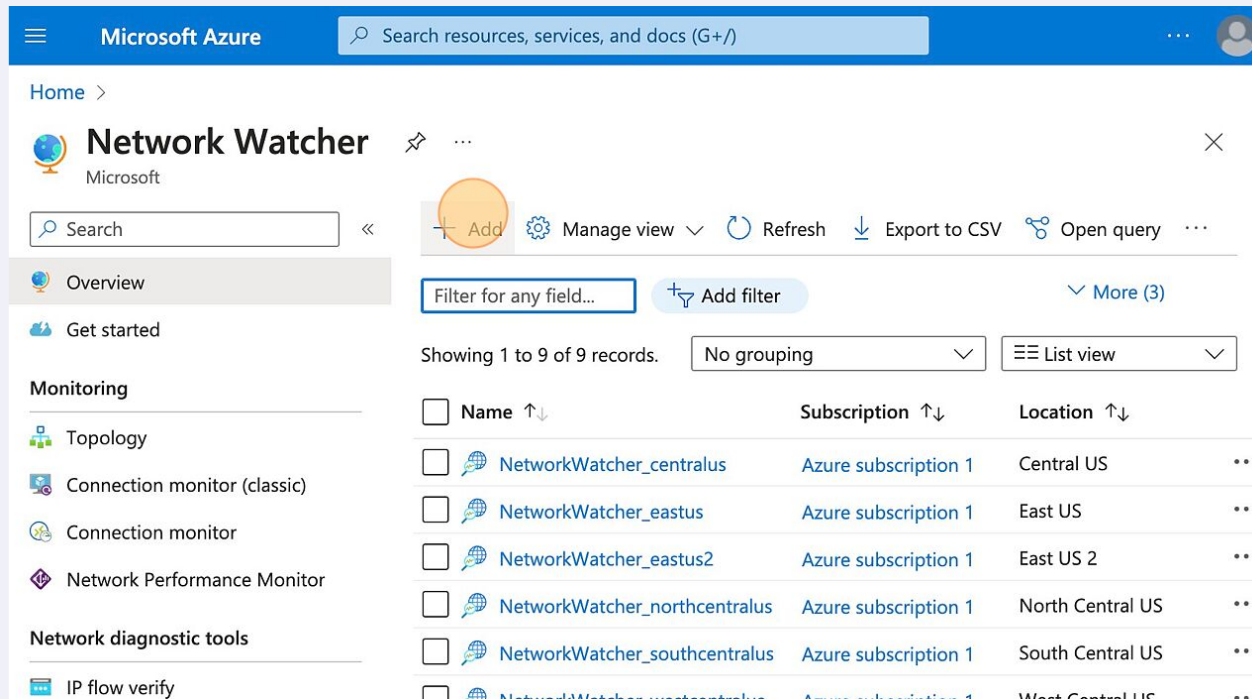
2 Click the "Search resources, services, and docs (G+)" and search for Network watcher



3 Click "Network Watcher"



4 Create a new network watcher



5 Create the watcher in the region you want the flow logs collected

Home > **Network Watcher** Microsoft

Search

Overview

Get started

Monitoring

- Topology
- Connection monitor (classic)
- Connection monitor
- Network Performance Monitor

Network diagnostic tools

- IP flow verify
- NSG diagnostics

Filter for any field...

Showing 1 to 9 of 9 records

<input type="checkbox"/>	Name ↑↓
<input type="checkbox"/>	NetworkWatch
<input type="checkbox"/>	NetworkWatch
<input type="checkbox"/>	NetworkWatch
<input type="checkbox"/>	NetworkWatch
<input type="checkbox"/>	NetworkWatch
<input type="checkbox"/>	NetworkWatch
<input type="checkbox"/>	NetworkWatch
<input type="checkbox"/>	NetworkWatch
<input type="checkbox"/>	NetworkWatch

Add network watcher

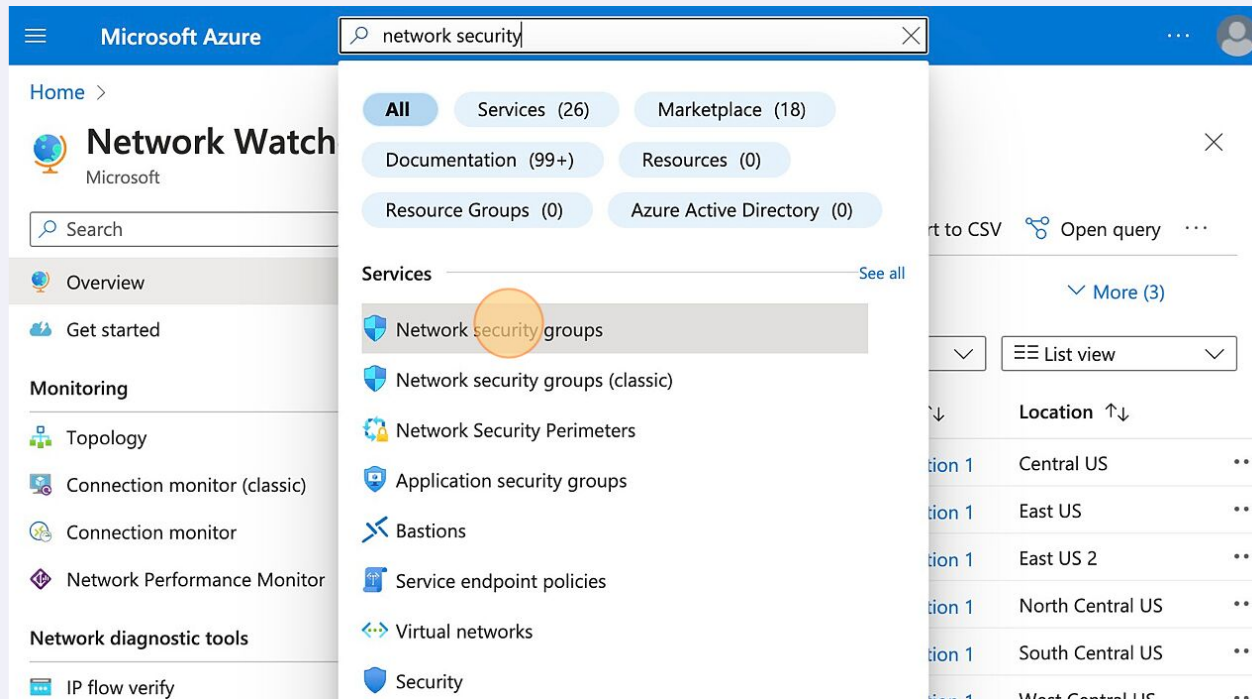
Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level. [Learn more.](#)

Subscription *
Azure subscription 1

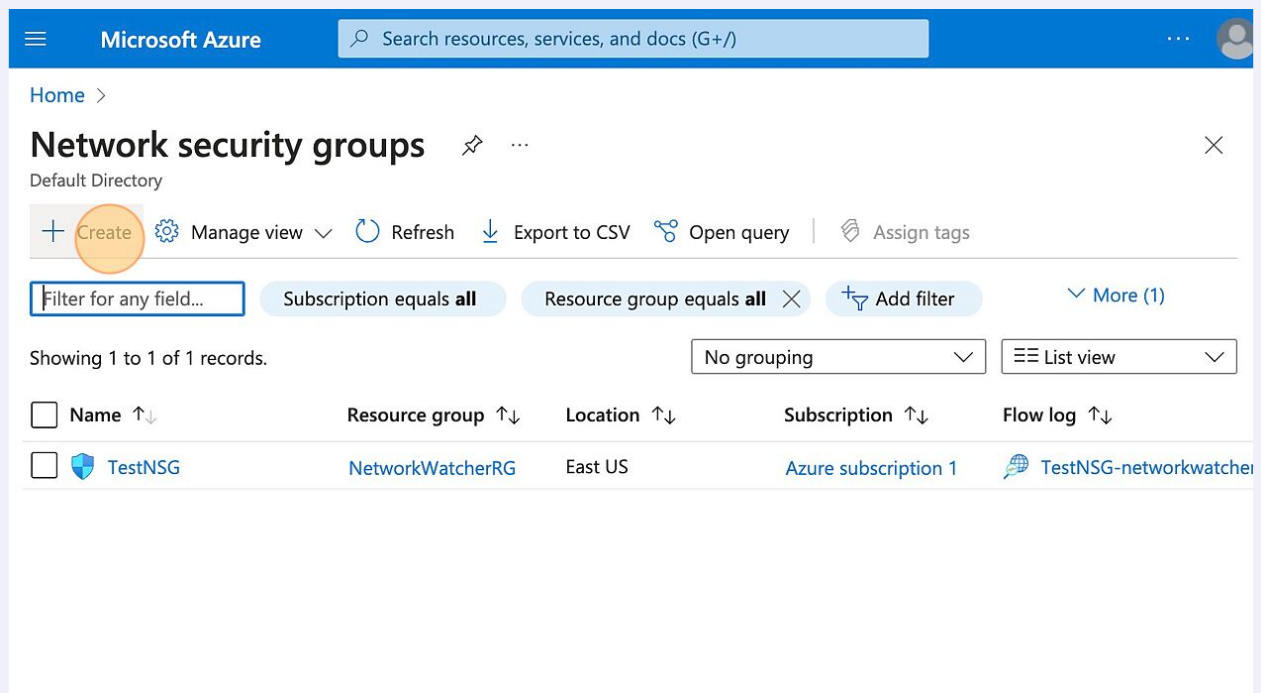
Region * ⓘ
0 selected

6 Switch to tab "Azure Cloud Account Onboarding Checklist"

7 Search for network security groups



8 Create new NSG, preferably in the same resource group as your network watcher



9 Leave everything as default and click create

The screenshot shows the Microsoft Azure portal interface. At the top, the header bar includes the Microsoft Azure logo, a search bar with the placeholder text "Search resources, services, and docs (G+ /)", and a user profile icon. Below the header, the left sidebar contains navigation links: "Home >", "Overview", "Inputs", "Outputs", and "Template". The main content area displays the deployment details for "Microsoft.NetworkSecurityGroup-20230319225121". A green checkmark icon indicates that the deployment is complete. A notification banner at the top right states "Deployment succeeded" and provides details about the deployment to the resource group "NetworkWatcherRG". Below the notification, a large green checkmark and the text "Your deployment is complete" are displayed. The deployment details include the name, subscription, resource group, start time, and correlation ID. A "Go to resource" button is visible at the bottom of the deployment details section.

Microsoft Azure

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

Home >

Microsoft.NetworkSecurityGroup-20230319225121

Deployment

Search

Overview

Inputs

Outputs

Template

Deployment succeeded

Deployment 'Microsoft.NetworkSecurityGroup-20230319225121' to resource group 'NetworkWatcherRG' was successful.

Go to resource

Pin to dashboard

✓ Your deployment is complete

Deployment name: Microsoft.NetworkSecurityGroup-20230319225121

Subscription: [Azure subscription 1](#)

Resource group: [NetworkWatcherRG](#)

Start time: 3/19/2023, 10:51:59 PM

Correlation ID: 4ea9de4b-abc5-42b5-a5e2-23a08ed8d3d6

Deployment details

Next steps

Go to resource

10 Next search for "Storage accounts"

The screenshot shows the Microsoft Azure portal interface with the search bar at the top. The search bar contains the text "storag". Below the search bar, a dropdown menu displays search results. The results are categorized into "All", "Services (16)", "Marketplace (18)", "Documentation (99+)", "Resources (0)", "Resource Groups (1)", and "Azure Active Directory (5)". Under the "Services" category, the search results are listed: "Storage accounts", "Storage browser", "Storage movers", "Storage accounts (classic)", "Storage Sync Services", "Data Lake Storage Gen1", "Azure Native Qumulo Scalable File Service", and "Azure Managed Lustre". The "Storage accounts" result is highlighted with a green background and a blue icon. A "See all" link is visible next to the "Services" category.

Microsoft Azure

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

Home >

Microsoft.NetworkSecurityGroup-20230319225121

Deployment

Search

Overview

Inputs

Outputs

Template

Storage accounts

Storage browser

Storage movers

Storage accounts (classic)

Storage Sync Services

Data Lake Storage Gen1

Azure Native Qumulo Scalable File Service

Azure Managed Lustre

See all

11 Create new Storage account

Home >

Storage accounts

Default Directory

+ Create Restore Manage view Refresh Export to CSV Open query Assign tags Delete

Filter for any field... Subscription equals all Add filter More (2)

Showing 1 to 1 of 1 records. No grouping List view

Name ↑↓	Type ↑↓	Kind ↑↓	Resource group ↑↓	Location ↑↓
<input type="checkbox"/> cs710032002875e794c	Storage account	StorageV2	cloud-shell-storage-s...	South Central US

12 Preferably in the same resource group as your NSG and NW

Subscription * Azure subscription 1

Resource group * NetworkWatcherRG
[Create new](#)

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ *

Region ⓘ * (US) East US
[Deploy to an edge zone](#)

Performance ⓘ * ☒ Standard: Recommended for most scenarios (general-purpose v2 account)

[Give feedback](#)

13 Click "Next : Advanced >"

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ *

Region ⓘ *

[Deploy to an edge zone](#)


Performance ⓘ *

☒ **Standard:** Recommended for most scenarios (general-purpose v2 account)

☐ **Premium:** Recommended for scenarios that require low latency.

Redundancy ⓘ *

☒ Make read access to data available in the event of regional unavailability.

 [Give feedback](#)

14 Click "Disable public access and use private access"

Create a storage account ... ×

Basics Advanced Networking Data protection Encryption Tags Review

Network access *

☐ Enable public access from all networks

☒ Enable public access from selected virtual networks and IP addresses

☒ Disable public access and use private access

Virtual networks

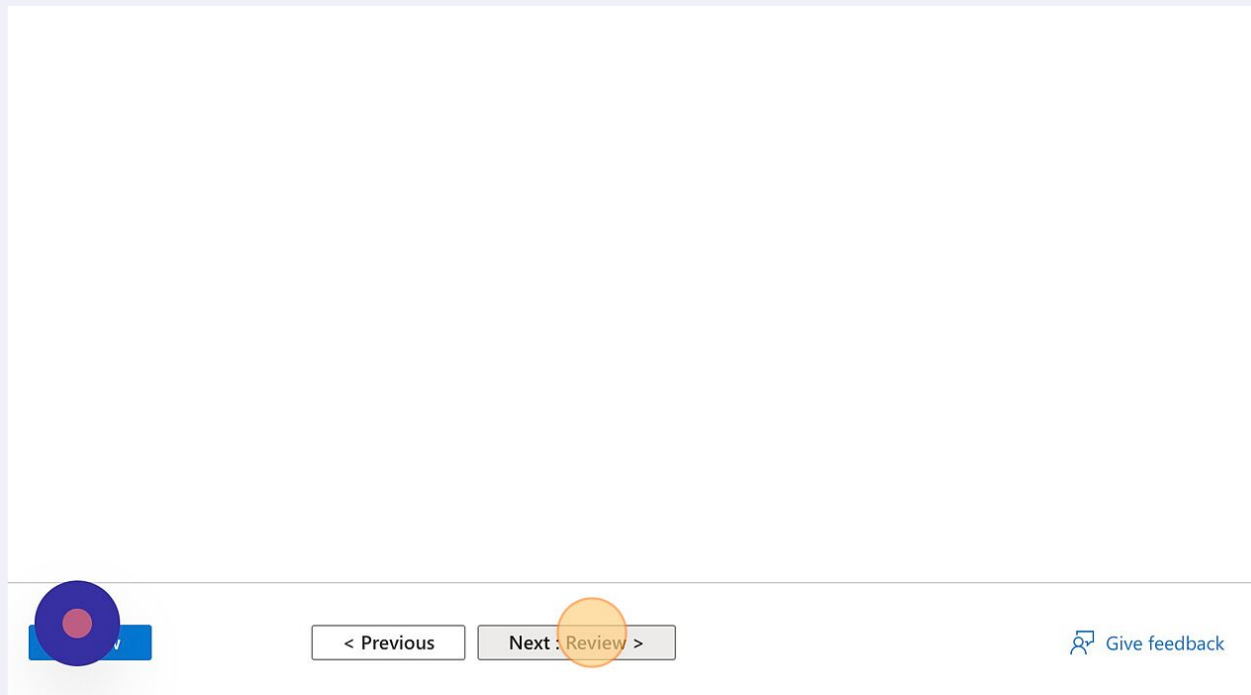
Only the selected network will be able to access this storage account. [Learn more](#)

Virtual network subscription ⓘ

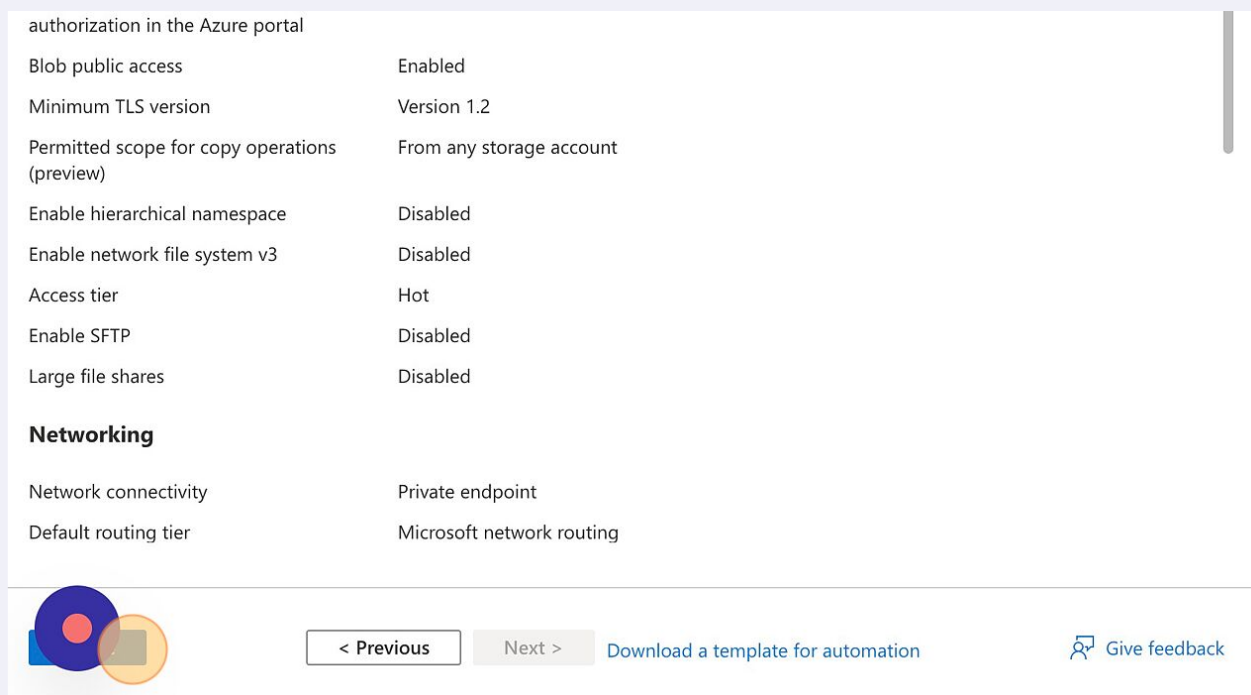
Virtual network ⓘ

[Create virtual network](#)

15 Leave all settings at default



16 Click "Create"



17 Click "Go to resource"

Microsoft Azure

Search resources, services, and docs (G+)

Home >

flowlogbuc12344556_1679284389263 | Overview

Deployment

Search

Delete Cancel Redeploy

Go to resource Pin to dashboard

Deployment succeeded

Deployment 'flowlogbuc12344556_1679284389263' to resource group 'NetworkWatcherRG' was successful.

Your deployment is complete

Deployment name: flowlogbuc12344556_1679284389263
Subscription: [Azure subscription 1](#)
Resource group: [NetworkWatcherRG](#)
Start time: 3/19/2023, 10:53:12 PM
Correlation ID: b6cf52c7-dee4-486b-b960-562c0ffbfe50

Deployment details

Next steps

Go to resource

18 Click "Networking"

Data storage

- Containers
- File shares
- Queues
- Tables

Security + networking

- Networking**
- Azure CDN
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

Subscription ID b2648256-a087-4e63-b0e2-a1c899793573 **Created** 3/19/2023, 10:53:26 PM

Disk state
Primary: Available, Secondary: Available

Tags ([edit](#))
[Click here to add tags](#)

Properties Monitoring Capabilities (7) Recommendations (0)

Tutorials Tools + SDKs

Blob service

- Hierarchical namespace [Disabled](#)
- Default access tier [Hot](#)
- Blob public access [Enabled](#)
- Blob soft delete

Security

- Require secure transfer for REST API operations [Enabled](#)
- Storage account key access [Enabled](#)
- Minimum TLS version [Version 1.2](#)

19 Click "Enabled from selected virtual networks and IP addresses"

Firewalls and virtual networks Private endpoint connections Custom domain

Save Discard Refresh

Public network access to this storage account has been disabled. Please create a private endpoint connection to grant access.

Public network access

- ☐ Enabled from all networks
- ☒ Enabled from selected virtual networks and IP addresses
- ☐ Disabled

Configure network security for your storage accounts. [Learn more](#)

Network Routing

Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.

Routing preference * ⓘ

- ☒ Microsoft network routing
- ☐ Internet routing

Publish route-specific endpoints ⓘ

☐ Microsoft network routing

20 Click on the link below and select the corresponding IP addresses for the Prisma tenant you're on

docs.paloaltonetworks.com/prisma/prisma-cloud/p...

21 Copy all the IP addresses

deployments communications. For sending alerts to your environment, you'd add an inbound security rule to the Ingress IP address 104.198.109.73.



To install Prisma Cloud Defenders in Kubernetes cluster, in addition to being able to connect to the Prisma Cloud Compute Console, the nodes in your cluster must be able to access the Prisma Cloud cloud registry at registry-auth.twistlock.com.

Prisma Cloud URL (AWS Region)	Source IP Address to Allow	Compute SaaS Console Region (GCP)	DR IP Address to Allow
app.prismacloud.io us-east-1 (N.Virginia)	3.217.51.44	us-east1 (South Carolina) Egress: 34.75.54.101 Ingress: 34.74.84.51	52.25.108.159/32
	3.218.144.244		34.213.129.111/32
	34.199.10.120		44.242.81.208/32
	34.205.176.82		52.40.100.6/32
	34.228.96.118		54.71.172.241/32
	52.201.19.205		44.236.217.120/32
	Only required for Code Security integrations with on-premises environments		

22 Paste them in the "IP address or CIDR" field.

Data storage

Containers

File shares

Queues

Tables

Security + networking

Networking

Azure CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Management

Redundancy

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status
No network selected.			

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more](#).

☐ Add your client IP address ('165.1.177.233') ⓘ

Address range

IP address or CIDR

Resource instances

Specify resource instances that will have access to your storage account based on their system-assigned managed identity.

Resource type	Instance name
Select a resource type	Select one or more instances

23 Should look like this when done

Data storage

Containers	3.217.51.44	
File shares	3.218.144.244	
Queues	34.199.10.120	
Tables	34.205.176.82	
	34.228.96.118	

Security + networking

Networking

IP address or CIDR

Resource instances

Specify resource instances that will have access to your storage account based on their system-assigned managed identity.

Resource type	Instance name
Select a resource type	Select one or more instances

Exceptions

- ☒ Allow Azure services on the trusted services list to access this storage account. ⓘ
- ☐ Allow read access to storage logging from any network

24 Ensure you save the new config

Microsoft Azure

Search resources, services, and docs (G+)

Home > flowlogbuc12344556

flowlogbuc12344556 | Networking

Storage account

Search

Firewalls and virtual networks Private endpoint connections Custom domain

Public network access

- ☐ Enabled from all networks
- ☒ Enabled from selected virtual networks and IP addresses
- ☐ Disabled

Configure network security for your storage accounts. [Learn more](#)

25 Return to your NSG




Network security groups

Default Directory

[+ Create](#) [Manage view](#) [Refresh](#) [Export to CSV](#) [Open query](#) [Assign tags](#)

Filter for any field... [Subscription equals all](#) [Add filter](#) [More \(2\)](#)

Showing 1 to 2 of 2 records. [No grouping](#) [List view](#)

<input type="checkbox"/> Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓	Flow log ↑↓
<input type="checkbox"/>  Flowlogtest	NetworkWatcherRG	East US	Azure subscription 1	
<input type="checkbox"/>  TestNSG	NetworkWatcherRG	East US	Azure subscription 1	 TestNSG-networkwatcher

26 Click "NSG flow logs"

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

D diagnostic settings

Logs

NSG flow logs

Automation

Tasks (preview)

Export template

Effective security rules

[Port == all](#) [Protocol == all](#) [Source == all](#) [Destination == all](#)

[Action == all](#)

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓
Inbound Security Rules			
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalan...	Any	Any
65500	DenyAllInBound	Any	Any
Outbound Security Rules			
65000	AllowVnetOutBound	Any	Any
65001	AllowInternetOutBound	Any	Any
65500	DenyAllOutBound	Any	Any

27 Create a new one

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets
- Properties
- Locks

Monitoring

- Alerts
- Diagnostic settings
- Logs
- NSG flow logs

Automation

- Tasks (preview)



No flow logs match your filters

Try changing or clearing your filters.

Create flow log

Clear filters

[Learn more](#)

28 Click on select resource

Basics Configuration Tags Review + create

Flow logs allow you to view information about ingress and egress IP traffic through a Network Security Group. [Learn more](#)

Project details

Subscription * ⓘ

Azure subscription 1

+ Select resource

Instance details

Select storage account

i You'll be charged normal data rates for storage and transactions when you send data to a storage account.

Location

Subscription

Azure subscription 1

29

Select the NSG you'd like to use and confirm your selection at the bottom of the screen

[Home](#) > [Network security groups](#) > [Flowlogtest | NSG flow logs](#) > [Create a flow log](#) >

Select network security group ...



Select one NSG or multiple NSGs in the same location to create flow logs.

Name : all X

Location : all X

Resource Group : all X

<input type="checkbox"/>	Name ↑	Location	Resource Group	Subscription
<input checked="" type="checkbox"/>	Flowlogtest	eastus	NetworkWatcherRG	b2648256-a087-4e63-b...

30

Your storage account will get auto-populated. Enter a desired number for the retention days and click through to "Create"

Instance details

Select storage account

You'll be charged normal data rates for storage and transactions when you send data to a storage account.

Location

Subscription

Storage Accounts *

[Create a new storage account](#)

Retention (days) *



Now + create

< Previous

Next : Configuration >

[Download a template for automation](#)

31 Click here.

Configuration

Flow Logs Version	2
Enable Traffic Analytics	No

Tags

None



< Previous

Next >

[Download a template for automation](#)

32 Switch to your Prisma Cloud tenant

33 Click on the edit icon for the concerned Azure account

Account ID	Cloud	Name	Actions
302746826271	aws	AWS Account	
154600454722	aws	AWS: RedLock Demo Account	
006106178103	aws	AWS: RedLock Demo Account	
943d9682-fd7e-4520-975b-905b1e94118d	Azure	Azure: RedLock Demo Account	
bfe8ce1b-ec1d-4e99-80ba-d20747afc867	Azure	Azure: RedLock Demo Account	
b2648256-a087-4e63-b0e2-a1c899793573	Azure	DayoSEAZtest	
se-customer-facing-demo	GCP	GCP: RedLock Demo Account	
ocid1.tenancy.oc1..aaaaaaaq7kshmgpstonwu3hwpmpn5h2vbe2...	Oracle	Oracle Cloud Demo Account	
240075317252	aws	PureSec Demo Account	
cto-demos-245420	GCP	cto-demos	

34 Still shows "Ingestion Failed"

Remediation: Disabled

Enterprise Application Object ID: 75bb819f-2ece-451f-bd85-6ae3b711e7fc

Account Groups: [View Details](#)

Last Modified: 6 minutes ago

Last Modified By: aogunleke@paloaltonetworks.com

Compute Workload Protection

Workload Discovery

Discover all compute workloads in your account and build serverless radar.
(Permissions granted, and Enabled)

Default

[Scan Settings](#)

Agentless Workload Scanning

Scan hosts & containers for vulnerabilities & compliance risks without

Enabled ☒

Logs: Operational

Workload Discovery: Operational

Config: Operational

Serverless Function Scanning: Operational

Flow Logs: [Ingestion Failed](#)

35 Click the edit icon

Cloud Accounts > Account Overview

DayoSEAZtest Enabled

Account ID	b2648256-a087-4e63-b0e2-a1c899793573	Tenant ID	9bb43885-ca0e-4129-9534-8c514be54c02
Account Type	Account	Client ID	5095d93b-76d4-4764-92a9-2a2321406bfd
Deployment Type	Global	Enterprise Application Object ID	75bb819f-2ece-451f-bd85-6ae3b711e7fc
Remediation	Disabled		
Account Groups	View Details		
Last Modified	6 minutes ago		
Last Modified By	aogunleke@paloaltonetworks.com		

Status

- Agentless Workload Scanning Operational
- Audit Logs Operational
- Workload Discovery Operational
- Config Operational
- Serverless Function Scanning Operational

Compute Workload Protection

36 Make Prisma Cloud update the settings by clicking "Next" till you reach the "Review Status" page

For product documentation please click [here](#)

Next

Agentless Workload Scanning

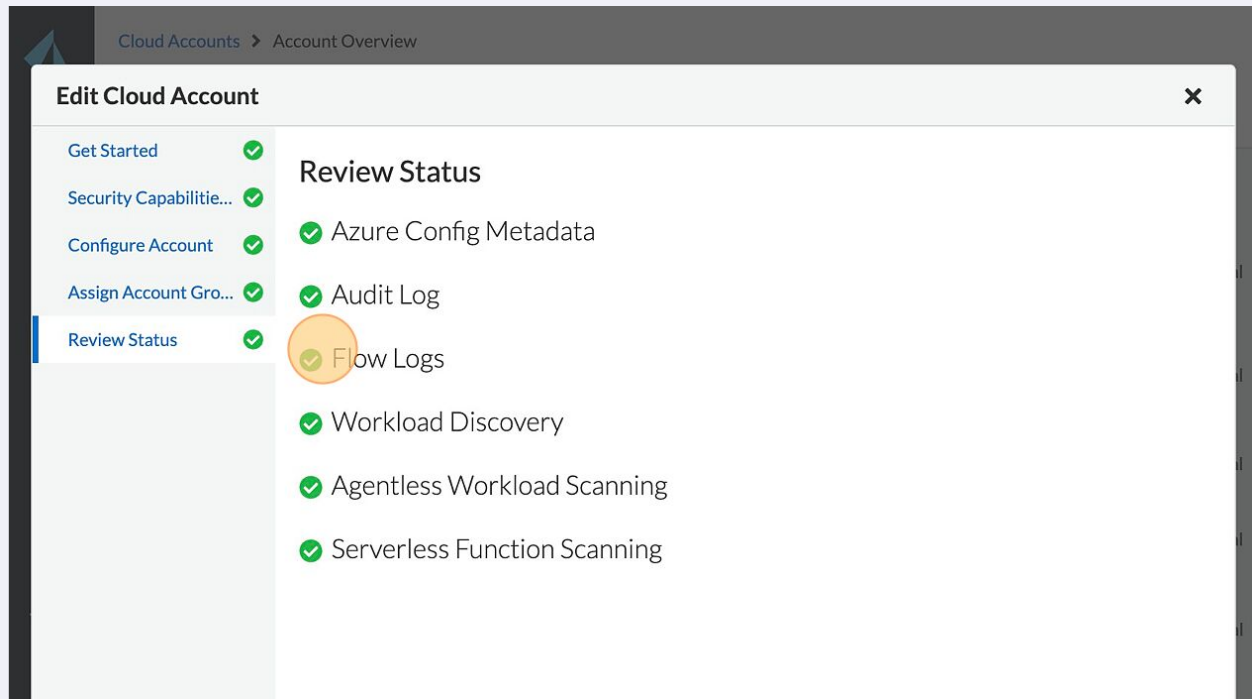
Scan hosts & containers for vulnerabilities & compliance risks without deploying agents. Enabled

(Permissions granted, and Enabled)

[Scan Settings](#)

37

Prisma Cloud will take a few seconds to update after which your Flow log will be onboarded



38

Click "Save"

