

# Azure Monitor Project

## Tasks 1: Prepare your Azure environment

- **Create App Log Examiners security**
- **Deploy and configure WS-VM1**
- **Deploy and configure LX-VM2**
- **Deploy a web app with an SQL Database**
- **Deploy a Linux web app**

### Create resource group

The screenshot shows the Azure Resource Groups blade. On the left, there's a navigation pane with sections like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings (with sub-options like Deployments, Security, Deployment stacks, Policies, Properties, Locks), Cost Management (Cost analysis, Cost alerts (preview), Budgets, Advisor recommendations), Monitoring (Insights (preview), Alerts, Metrics, Diagnostic settings, Logs, Advisor recommendations), and Workbooks. The main area is titled 'rg-alpha' and shows the 'Essentials' tab. It displays information such as Subscription (move), Pay-As-You-Go, Subscription ID (8148d5d5-df15-44ef-beb3-5960d3dc42eb), and Tags (edit, Add tags). Below this is the 'Resources' section, which is currently empty, indicated by the message 'No resources match your filters'. There are filter options for Type (all) and Location (all), and a 'Clear filters' button. At the bottom right of the main area, there's a 'Give feedback' link.

# Create App Log Examiners security group

Create secure group in Entra ID called App Log Examiners with deceptions as App Log Examiners

Home > Default Directory | Groups > Groups | All groups >

New Group ... X

Got feedback?

Group type \*  Security

Group name \*  App Log Examiners

Group description  App Log Examiners

Membership type  Assigned

Owners  
No owners selected

Members  
No members selected

Create

Groups created

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (vikaramtirat@outlook.com). Below the navigation bar, the breadcrumb path 'Home > Default Directory | Groups' is visible. The main title 'Groups | All groups' is displayed above a table. The table has columns: Name, Object Id, Group type, and Membership type. One group, 'App Log Examiners', is listed with the following details:

| Name                 | Object Id                            | Group type | Membership type |
|----------------------|--------------------------------------|------------|-----------------|
| AL App Log Examiners | d0acc8d8-3a22-4259-906a-f80994371fdf | Security   | Assigned        |

The left sidebar contains several sections: 'All groups' (selected), 'Deleted groups', 'Diagnose and solve problems', 'Settings' (with 'General', 'Expiration', 'Naming policy'), 'Activity' (with 'Privileged Identity Management', 'Access reviews', 'Audit logs', 'Bulk operation results'), and 'Troubleshooting + Support' (with 'New support request').

## Next step creates windows VM

### Deploy and configure vm name - WS-VM1 Allow RDP 3389

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (vikaramtirat@outlook.com). The breadcrumb path 'Home > Virtual machines' is visible. The main title 'Create a virtual machine' is displayed above the configuration form.

The form consists of several tabs: Basics, Disks, Networking, Management, Monitoring, Advanced, Tags, and Review + create. The 'Basics' tab is selected. The 'Project details' section includes fields for Subscription (Pay-As-You-Go) and Resource group (rg-alpha). The 'Instance details' section includes fields for Virtual machine name (WS-VM1), Region ((US) East US), Availability options (No infrastructure redundancy required), Security type (Standard), and Image (Windows Server 2022 Datacenter: Azure Edition - x64 Gen2). The 'VM architecture' section shows options for Arm64 and x64, with a note that Arm64 is not supported with the selected image. At the bottom, there are buttons for 'Review + create' and 'Next : Disks >'.

One VM Created go to networking and add following rule.

WS-VM1 | Networking

**Add inbound security rule**

Source: Any  
Source port ranges: \*  
Destination: Any  
Service: HTTP  
Destination port ranges: 80  
Protocol: TCP  
Action: Allow  
Priority: 310  
Name: AllowAnyHTTPInbound  
Description: AllowAnyHTTPInbound

**Inbound port rules**

| Priority | Name                          | Port |
|----------|-------------------------------|------|
| 300      | RDP                           | 3389 |
| 65000    | AllowVnetInBound              | Any  |
| 65001    | AllowAzureLoadBalancerInBound | Any  |
| 65500    | DenyAllInBound                | Any  |

WS-VM1 | Networking

**Inbound port rules**

| Priority | Name                          | Port | Protocol | Source            | Destination    | Action |
|----------|-------------------------------|------|----------|-------------------|----------------|--------|
| 300      | RDP                           | 3389 | TCP      | Any               | Any            | Allow  |
| 310      | AllowAnyHTTPInbound           | 80   | TCP      | Any               | Any            | Allow  |
| 65000    | AllowVnetInBound              | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  |
| 65001    | AllowAzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer | Any            | Allow  |
| 65500    | DenyAllInBound                | Any  | Any      | Any               | Any            | Deny   |

Next RDP onto Windows VM to Install IIS webserver to host basic site.

Home > CreateVm-MicrosoftWindowsServer.WindowsServer-202-20231230145453 | Overview > WS-VM1

## WS-VM1 | Connect

Virtual machine

Search

Refresh Troubleshoot More Options Feedback

Connecting using Public IP address | 20.232.113.215

Admin username prime  
port (change) 3389 Check access

Just-in-time policy Unsupported by plan

Most common

Native RDP Local machine

Connect via native RDP without any additional software needed. Recommended for testing only.

Public IP address (20.232.113.215)

Select Download RDP file

More ways to connect (4)

Native RDP

Configure prerequisites for Native RDP

Azure needs to configure some features in order to connect to the VM.

Prerequisites configured

Port 3389 access

Port 3389 on this virtual machine is accessible from the local machine IP (82.10.15.118). Learn more ⓘ

Change the port for connecting to this virtual machine on the Connect page of the virtual machine.

Public IP address: 20.232.113.215

A public IP address is required to connect via this connection method.

Configured

Open Remote Desktop Connection (on Windows)

Open Remote Desktop Connection. Or change your local machine operating system to view more instructions. Learn more ⓘ

Download and open the RDP file

Download RDP file

Other Information

Forgot password? Reset password

Close Troubleshooting Give feedback

20.232.113.215 - Remote Desktop

Server Manager Server Manager • Dashboard

Dashboard Local Server All Servers

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

Roles: 0 | Server groups: 1 | Servers total: 1

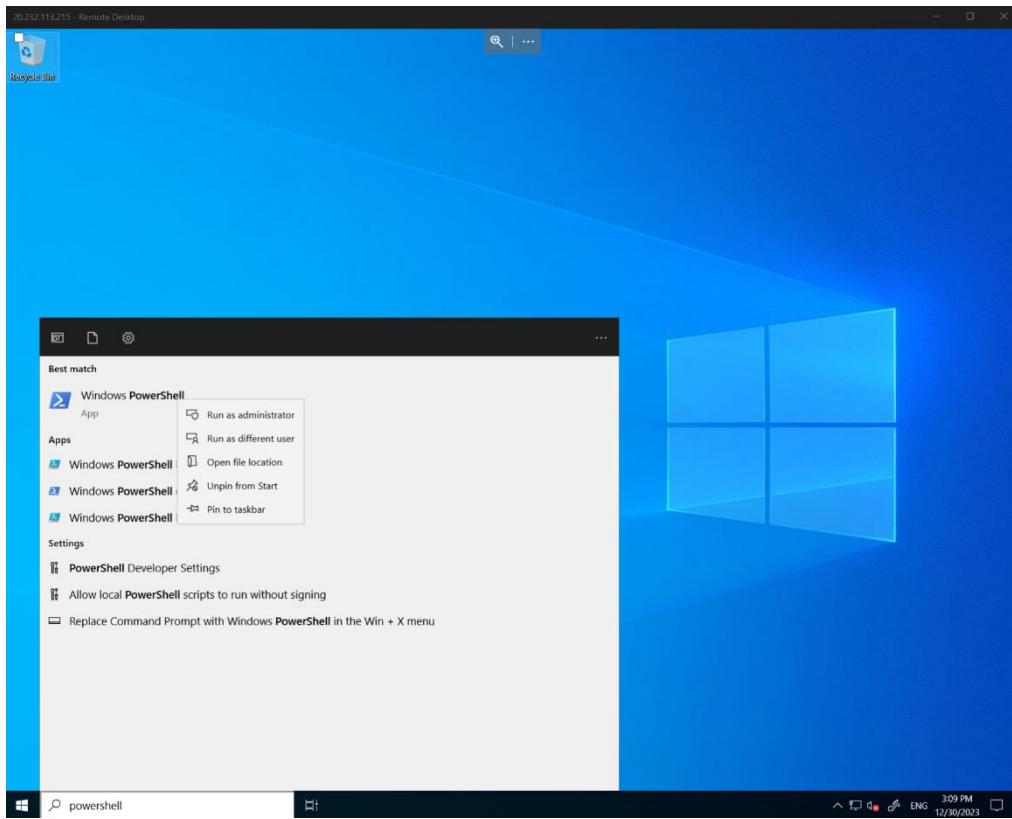
| Local Server  | 1 |
|---------------|---|
| Manageability |   |
| Events        |   |
| Services      |   |
| Performance   |   |
| BPA results   |   |

| All Servers   | 1 |
|---------------|---|
| Manageability |   |
| Events        |   |
| Services      |   |
| Performance   |   |
| BPA results   |   |

Type here to search

3:08 PM ENG 12/30/2023

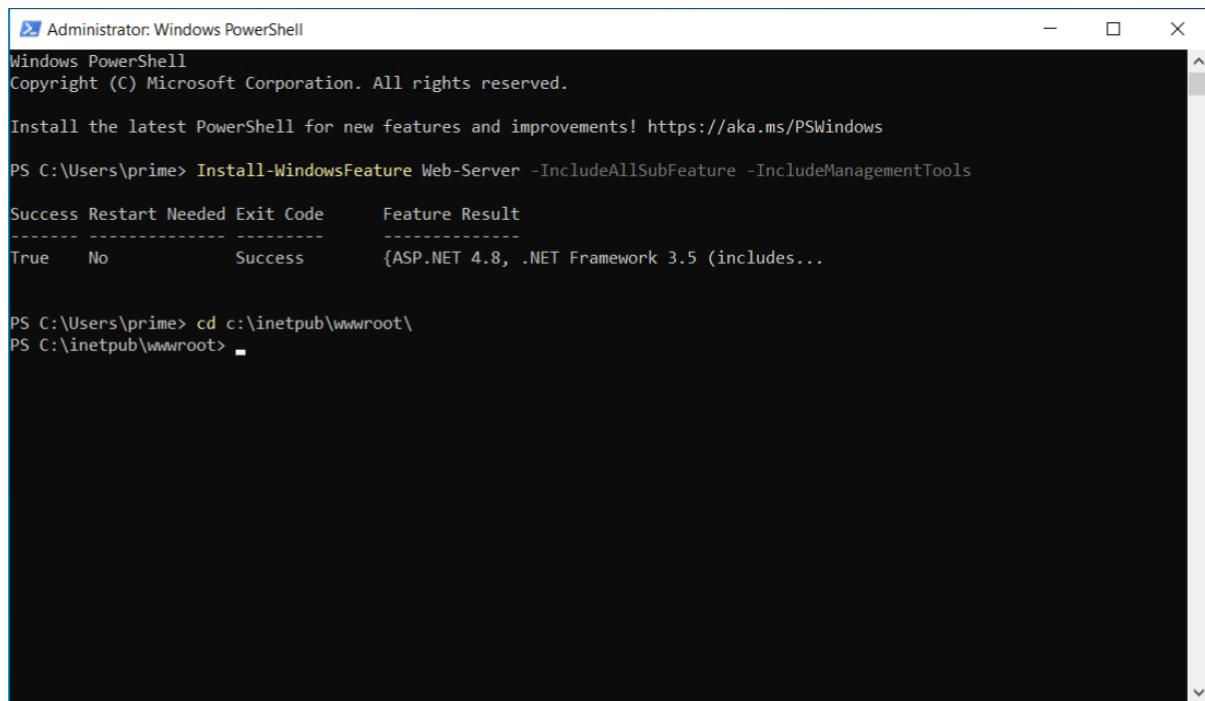
To start the webserver set up run PowerShell as admin



At the elevated command prompt, type the following command and press **Enter**.  
`Install-WindowsFeature Web-Server -IncludeAllSubFeature -IncludeManagementTools`

A screenshot of a Windows PowerShell window titled 'Administrator: Windows PowerShell'. The window shows the command 'Install-WindowsFeature Web-Server -IncludeAllSubFeature -IncludeManagementTools' being run. The output is a table with four columns: 'Success', 'Restart Needed', 'Feature', and 'Result'. The table has one row with the values 'True', 'No', 'Success', and '{ASP.NET 4.8, .NET Framework 3.5 (includes...)}'.

When the installation completes run the following command to change to the web server root directory. cd c:\inetpub\wwwroot\



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

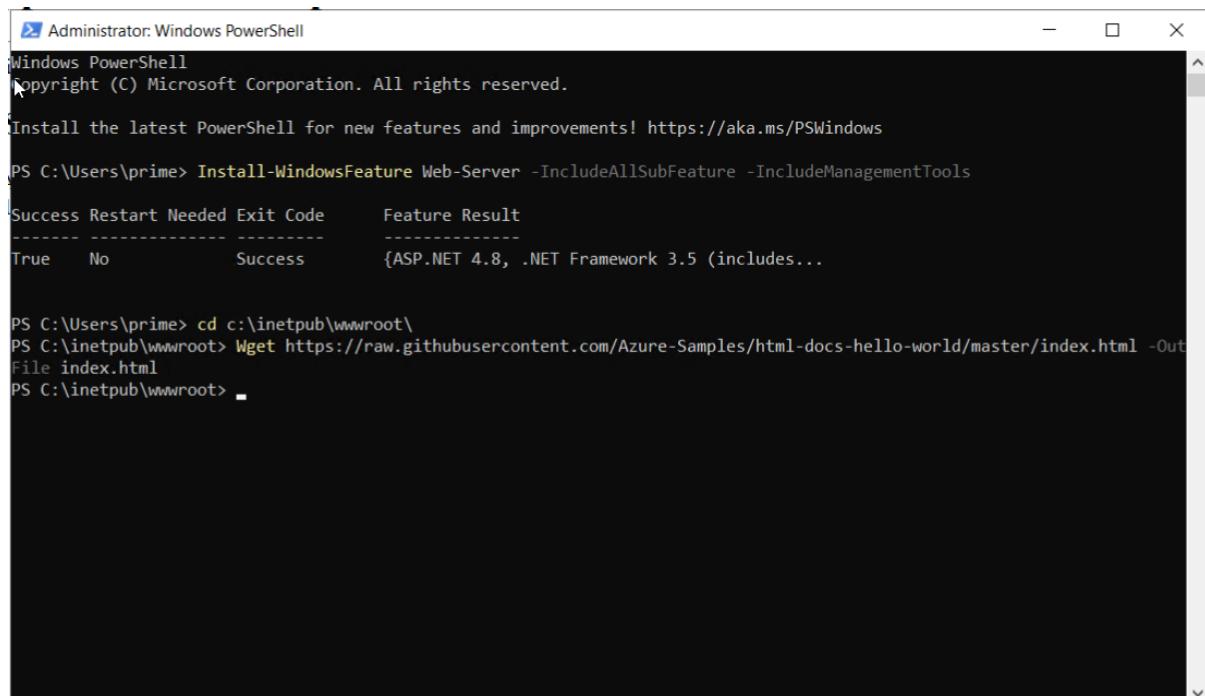
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\prime> Install-WindowsFeature Web-Server -IncludeAllSubFeature -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
----- ----- ----- -----
True    No          Success        {ASP.NET 4.8, .NET Framework 3.5 (includes...}

PS C:\Users\prime> cd c:\inetpub\wwwroot\
PS C:\inetpub\wwwroot>
```

To get a basic website run the command Wget <https://raw.githubusercontent.com/Azure-Samples/html-docs-hello-world/master/index.html> -OutFile index.html



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

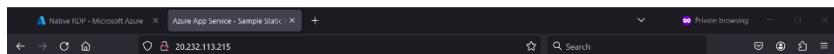
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\prime> Install-WindowsFeature Web-Server -IncludeAllSubFeature -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
----- ----- ----- -----
True    No          Success        {ASP.NET 4.8, .NET Framework 3.5 (includes...}

PS C:\Users\prime> cd c:\inetpub\wwwroot\
PS C:\inetpub\wwwroot> Wget https://raw.githubusercontent.com/Azure-Samples/html-docs-hello-world/master/index.html -OutFile index.html
PS C:\inetpub\wwwroot>
```

Browse to public ip of VM to confirm web server running and outputting sample web page



## Azure App Service - Sample Static HTML Site

Azure App Service Web Apps

### Azure App Service Web Apps

App Service Web Apps is a fully managed compute platform that is optimized for hosting websites and web applications. This platform-as-a-service (PaaS) offering of Microsoft Azure lets you focus on your business logic while Azure takes care of the infrastructure to run and scale your app.

## Deploy and configure linux server vm - LX-VM2

Home > Virtual machines >

### Create a virtual machine

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* Pay-As-You-Go

Resource group \* rg-alpha [Create new](#)

**Instance details**

Virtual machine name \* Linux-VM2

Region \* (US) East US

Availability options No infrastructure redundancy required

Security type Standard

Image \* Ubuntu Server 22.04 LTS - x64 Gen2 [See all images](#) | [Configure VM generation](#)

This image is compatible with additional security features. [Click here to swap to the Trusted launch security type.](#)

VM architecture  x64

Run with Azure Spot discount

Size \* Standard\_D2s\_v3 - 2 vcpus, 8 GiB memory (US\$70.08/month) [See all sizes](#)

Enable live migration [Learn more](#)

[Review + create](#) [Next : Disks >](#) [Give feedback](#)

Inbound port allow SSH(22)

**Administrator account**

Authentication type  SSH public key  Password

Username \*  ✓

Password \*  ✓

Confirm password \*  ✓

**Inbound port rules**

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \*  None  Allow selected ports

Select inbound ports \*

! All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Home >

**CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20231230152133 | Overview** ✓ ...

! Deployment

<> Delete Cancel Redeploy Download Refresh

✓ **Your deployment is complete**

! Deployment name: CreateVm-canonical.0001-com-ubuntu-server-j... Start time: 30/12/2023, 15:27:32  
Subscription: Pay-As-You-Go Correlation ID: 9432dd1a-93ca-4276-ba17-84ccb6c

✓ Deployment details

✓ Next steps

Setup auto-shutdown Recommended Monitor VM health, performance and network dependencies Recommended Run a script inside the virtual machine Recommended

Go to resource Create another VM

Give feedback Tell us about your experience with deployment

\$ **Cost Management**  
Get notified to stay within your budget and prevent unexpected charges on your bill.  
[Set up cost alerts >](#)

! **Microsoft Defender for Cloud**  
Secure your apps and infrastructure  
[Go to Microsoft Defender for Cloud >](#)

? **Free Microsoft tutorials**  
[Start learning today >](#)

? **Work with an expert**  
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.  
[Find an Azure expert >](#)

Once the VM deploys, open the VM properties page and choose Extensions + Applications under Settings.

Install an Extension ...

The screenshot shows the Azure portal interface for installing a VM extension. On the left, there's a search bar with 'network watcher' typed in. Below it, a card for 'Network Watcher Agent for Linux' by Microsoft Corp. is displayed, with a brief description of its function. On the right, the extension details page for 'Network Watcher Agent for Linux' is shown, including its publisher (Microsoft Corp.), an 'Overview' section with a description of Azure Network Watcher, and a note about accepting terms. A 'Create' button is visible at the bottom of this panel.

Choose Add and select the Network Watcher Agent for Linux. Choose Next and then choose Review and Create. Choose Create.

The screenshot shows the 'Extensions + applications' blade for a virtual machine named 'Linux-VM2'. The 'Extensions' tab is selected. On the left, a sidebar lists various management options like Networking, Connect, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, and more. The 'Extensions + applications' option is highlighted. The main area shows a table of installed extensions:

| Name                         | Type                       | Version | Status                 | Automatic upgrade status |
|------------------------------|----------------------------|---------|------------------------|--------------------------|
| AzureNetworkWatcherExtension | Microsoft.Azure.Network... | 1.*     | Provisioning succeeded | Disabled                 |

Configure the AzureNetworkWatcherExtension and the OmsAgentForLinux extension so that they automatically upgrade.

Home > Linux-VM2

## Linux-VM2 | Extensions + applications

Virtual machine

Extensions

VM Applications

+ Add    Refresh    Feedback

Search to filter items...

Sorting all 1 items

| Name                         | Type                                     |
|------------------------------|--|
| AzureNetworkWatcherExtension | Microsoft.Azure.NetworkWatcherAgentLinux |

**AzureNetworkWatcherExtension**

Enable automatic upgrade    Uninstall

Type: Microsoft.Azure.NetworkWatcher.NetworkWatcherAgentLinux

Version: 1.4.3147.1

Status: Provisioning succeeded

Status level: Info

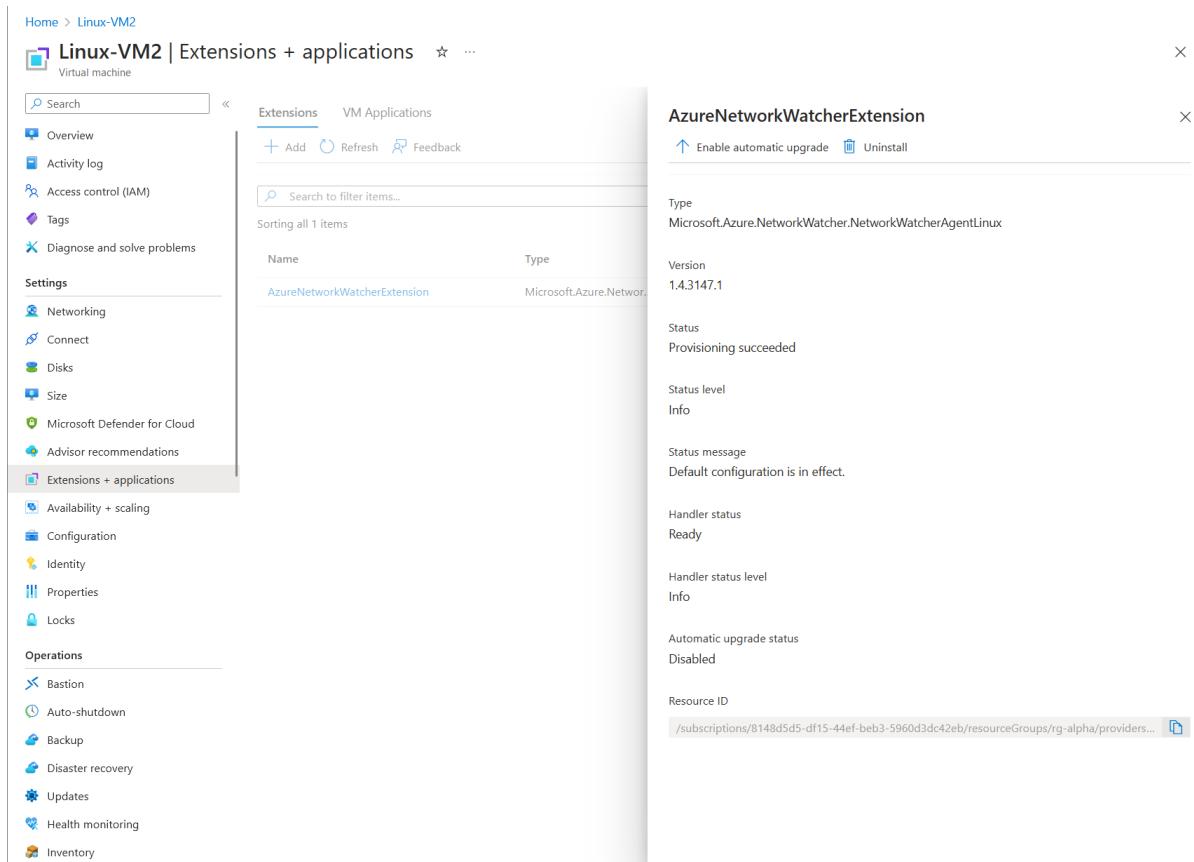
Status message: Default configuration is in effect.

Handler status: Ready

Handler status level: Info

Automatic upgrade status: Disabled

Resource ID: /subscriptions/8148d5d5-df15-44ef-beb3-5960d3dc42eb/resourceGroups/rg-alpha/providers...



One enabled you should see Automatic upgrade status changed to enabled

Home > Linux-VM2

## Linux-VM2 | Extensions + applications

Virtual machine

Extensions

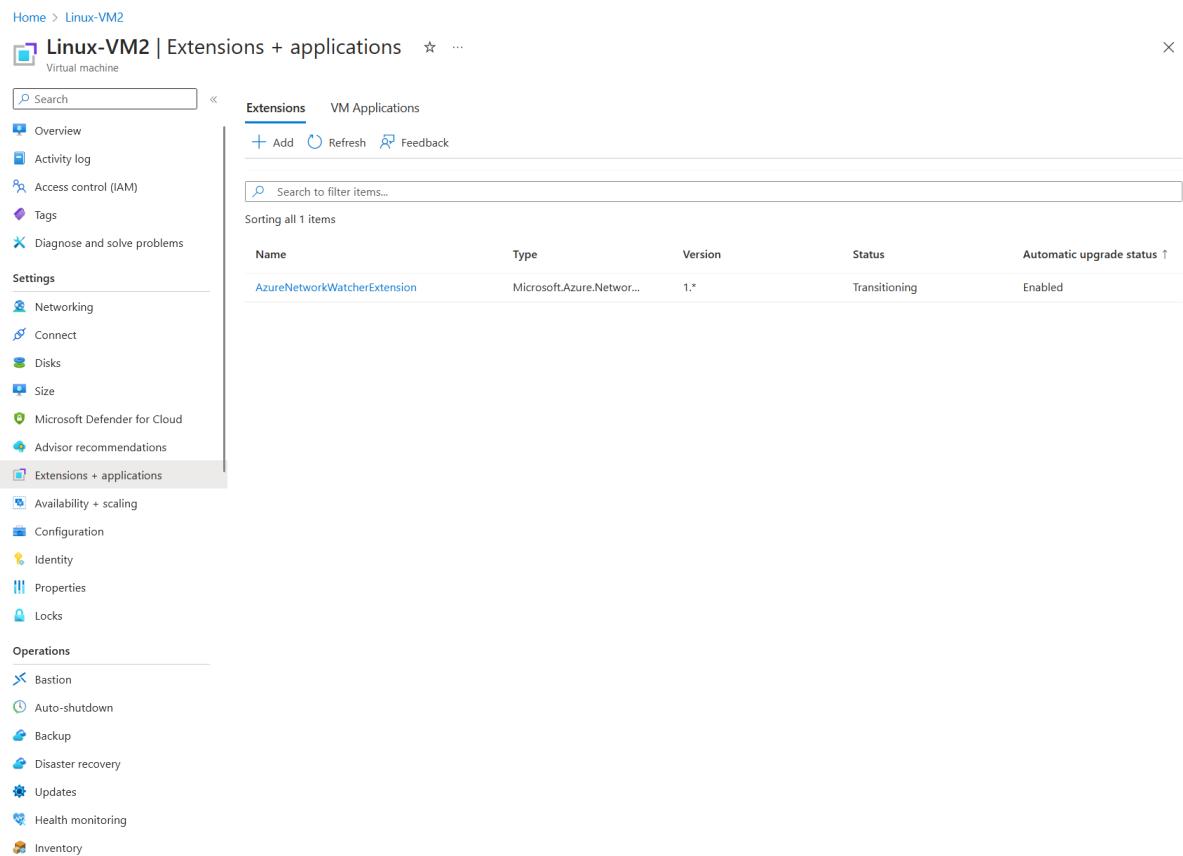
VM Applications

+ Add    Refresh    Feedback

Search to filter items...

Sorting all 1 items

| Name                         | Type                                     | Version | Status        | Automatic upgrade status ↑ |
|------------------------------|--|---------|---------------|----------------------------|
| AzureNetworkWatcherExtension | Microsoft.Azure.NetworkWatcherAgentLinux | 1.*     | Transitioning | Enabled                    |



## Deploy a web app with an SQL Database

In your browser, open a new browser tab and navigate to <https://github.com/Azure/azure-quickstart-templates/tree/master/quickstarts/microsoft.web/web-app-sql-database>

The screenshot shows the GitHub repository page for 'web-app-sql-database'. The repository has 935 issues, 71 pull requests, and 16k forks. The README.md file contains a table with deployment details:

| description   | page_type | products                       | urlFragment          | languages    |
|---|-----------|--------------------------------|----------------------|--------------|
| This template provisions a Web App, a SQL Database, AutoScale settings, Alert rules, and App Insights. It configures a connection string in the web app for the database. | sample    | azure   azure-resource-manager | web-app-sql-database | json   bicep |

Below the table, there is a section titled 'Provision a Web App with a SQL Database' with two green 'pass' status indicators for Azure Public Test Date (2023.11.23) and Azure US Gov Test Date (2023.12.29).

On the GitHub page, choose Deploy to Azure

The screenshot shows the 'Provision a Web App with a SQL Database' template page. It includes sections for Microsoft App Services, Microsoft SQL, and Microsoft Learn Resources, each with links to pricing information. A note states: 'This sample creates a free Azure Web App and SQL Database at the "Basic" service level. The template can support other tiers of service, details for each service can be found here:'. At the bottom, there is a 'Tags' section listing: Microsoft.Sql/servers, Microsoft.Sql/servers/databases, Microsoft.Sql/servers/firewallRules, Microsoft.Web/serverfarms, Microsoft.Web/sites, Microsoft.Web/sites/config, SQLAzure, Microsoft.Insights/components.

Click review and create

Home >

## Provision a Web App with a SQL Database

Azure quickstart template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

**Basics** Review + create

**Template**

web-app-sql-database 7 resources

Edit template Edit parameters Visualize

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* Pay-As-You-Go

Resource group \* rg-alpha Create new

**Instance details**

Region \* (US) East US

Sku Name F1

Sku Capacity 1

Sql Administrator Login \* prime

Sql Administrator Login Password \* [REDACTED]

Location [resourceGroup().location]

Previous Next Review + create

## After the deployment completes, choose Go to resource group

Home > Microsoft.Template-20231230154256 | Overview >

rg-alpha Resource group

Search Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete ...

Overview

- Activity log
- Access control (IAM)
- Tags
- Resource visualizer
- Events

Settings

- Deployments
- Security
- Deployment stacks
- Policies
- Properties
- Locks

Cost Management

- Cost analysis
- Cost alerts (preview)
- Budgets
- Advisor recommendations

Monitoring

- Insights (preview)
- Alerts
- Metrics
- Diagnostic settings

Logs

Advisor recommendations

Workbooks

Essentials

Subscription (move) : Pay-As-You-Go Deployments : 4 Succeeded

Subscription ID : 8148d5d5-df15-44ef-beb3-5960d3dc42eb Location : East US

Tags (edit) : Add tags

Resources Recommendations

Filter for any field... Type equals all Location equals all Add filter

| Name   | Type                   | Location |
|--|------------------------|----------|
| AppInsightswebsitefqyp73mfn5xq4                  | Application Insights   | East US  |
| hostingplanfqyp73mfn5xq4                         | App Service plan       | East US  |
| Linux-VM2  | Virtual machine        | East US  |
| Linux-VM2-ip                                     | Public IP address      | East US  |
| Linux-VM2-nsg                                    | Network security group | East US  |
| linux-vm2129                                     | Network Interface      | East US  |
| Linux-VM2_disk1_9c3afed3d41346b3a64876858c08fa3c | Disk                   | East US  |
| sampledbsq1Serverfqyp73mfn5xq4/sampledbs         | SQL database           | East US  |
| sqlserverfqyp73mfn5xq4                           | SQL server             | East US  |
| websitefqyp73mfn5xq4                             | App Service            | East US  |
| WS-VM1   | Virtual machine        | East US  |
| WS-VM1-ip  | Public IP address      | East US  |
| WS-VM1-nsg                                       | Network security group | East US  |
| WS-VM1-vnet                                      | Virtual network        | East US  |

< Previous Page 1 of 1 Next >

Give feedback

# Deploy a Linux web app

open a new browser tab and navigate to <https://learn.microsoft.com/en-us/samples/azure/azure-quickstart-templates/webapp-basic-linux/>

The screenshot shows a Microsoft Learn page for a code sample titled "Deploy a basic Linux web app". The page includes a "Browse code" button, deployment status cards for Azure Public Test Date (2023.12.29) and Azure US Gov Test Date (2023.12.21), and links for Best Practice Check (pass), CredScan Check (Not Tested), and Bicep Version (0.24.24). It also features three deployment buttons: "Deploy to Azure", "Deploy to Azure Gov", and "Visualize". Below the buttons, a description states: "This template allows you to deploy an app service plan and a basic Linux web app." A "Tags" section lists "Microsoft.Web/serverfarms" and "Microsoft.Web/sites".

On the GitHub page, choose Deploy to Azure

The screenshot shows the Azure portal's "Deploy a basic Linux web app" template creation interface. It starts with a "Template" section showing a "webapp-basic-linux" template with 2 resources, and options to "Edit template", "Edit parameters", or "Visualize". The "Project details" section asks to select a subscription and resource group; "Pay-As-You-Go" is selected under "Subscription" and "rg-alpha" is selected under "Resource group". The "Instance details" section includes fields for Region (US East US), Web App Name (AzureLinuxApp2023), Sku (S1), Linux Fx Version (php7.4), and Location ([resourceGroup().location]). At the bottom, there are "Previous" and "Next" buttons, and a prominent blue "Review + create" button.

Review the information and choose Create

The screenshot shows the Azure portal interface for deploying a basic Linux web app. At the top, there's a navigation bar with 'Home >' and the title 'Deploy a basic Linux web app'. Below the title, it says 'Azure quickstart template'. The main area has tabs 'Basics' and 'Review + create' (which is underlined, indicating it's active). Under 'Basics', there's a 'Summary' section showing a resource group named 'webapp-basic-linux' with 2 resources. Below that is a 'Terms' section with links to 'Azure Marketplace Terms' and 'Azure Marketplace'. A note about legal terms follows. Then there's a note about Microsoft's responsibility for third-party templates. Below that is a note about Azure Marketplace offerings. Another note states that neither subscription credits nor monetary commitment funds can be used to purchase non-Microsoft offerings. If any Microsoft products are included, they are licensed by Microsoft. The configuration section shows the following parameters:

|                  |                            |
|------------------|----------------------------|
| Subscription     | Pay-As-You-Go              |
| Resource group   | rg-alpha                   |
| Region           | East US                    |
| Web App Name     | AzureLinuxApp2023          |
| Sku              | S1                         |
| Linux Fx Version | php[7.4]                   |
| Location         | [resourceGroup()].location |

At the bottom, there are 'Previous' and 'Next' buttons, and a prominent blue 'Create' button.

## Tasks 2 - Deploy Log Analytics

- **Create a Log Analytics workspace**
- **Configure Log Analytics data retention and archive policies**
- **Enable access to a Log Analytics workspace**

## Create a Log Analytics workspace

Azure Portal Search Bar, enter **Log Analytics** and select **Log Analytics workspaces** from the list of results

On the Log Analytics workspaces page, choose Create

Enter the following info and review and create

Home > Log Analytics workspaces >

## Create Log Analytics workspace

Basics Tags Review + Create

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* Pay-As-You-Go

Resource group \* rg-alpha

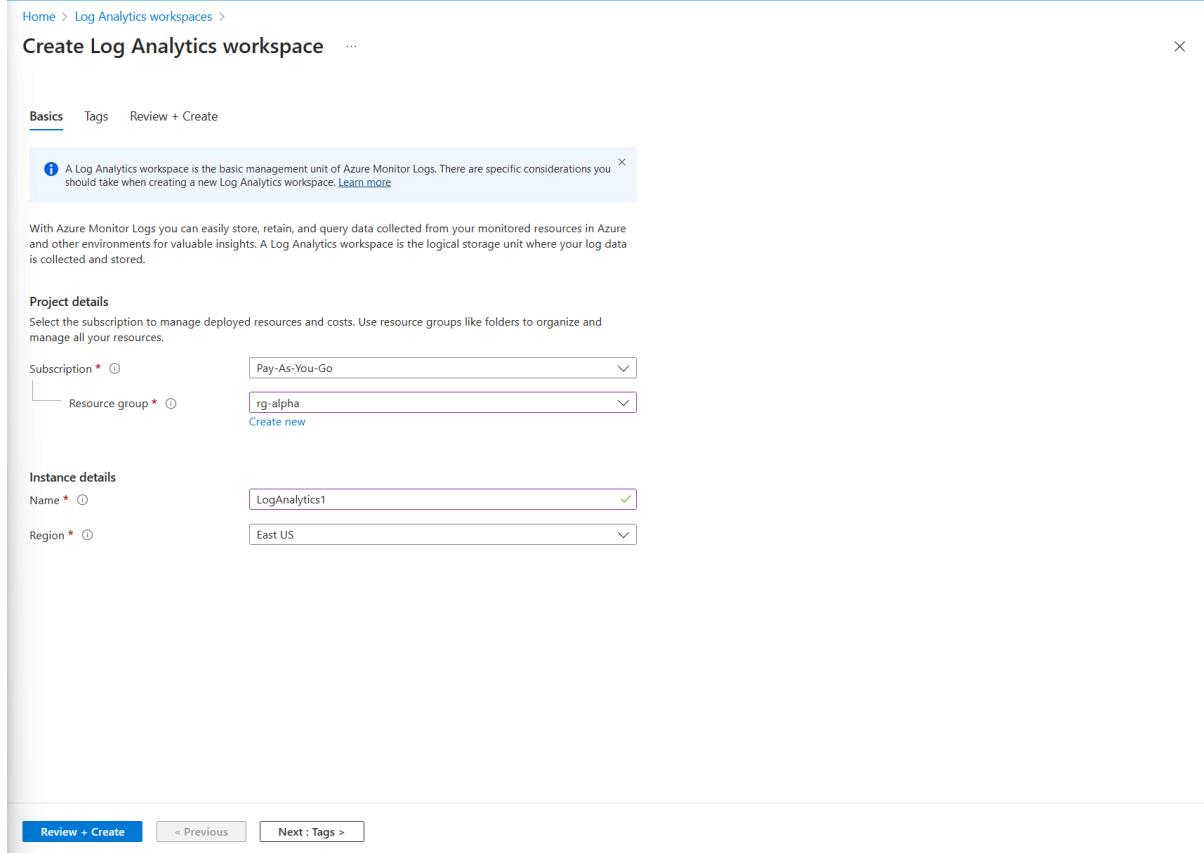
Create new

**Instance details**

Name \* LogAnalytics1

Region \* East US

[Review + Create](#) [« Previous](#) [Next : Tags >](#)



## Configure Log Analytics data retention and archive policies

In the Azure Portal Search Bar, enter Log Analytics and select Log Analytics workspaces from the list of results

Home >

## Log Analytics workspaces

Default Directory

Create Open recycle bin Manage view Refresh Export to CSV Open query Assign tags

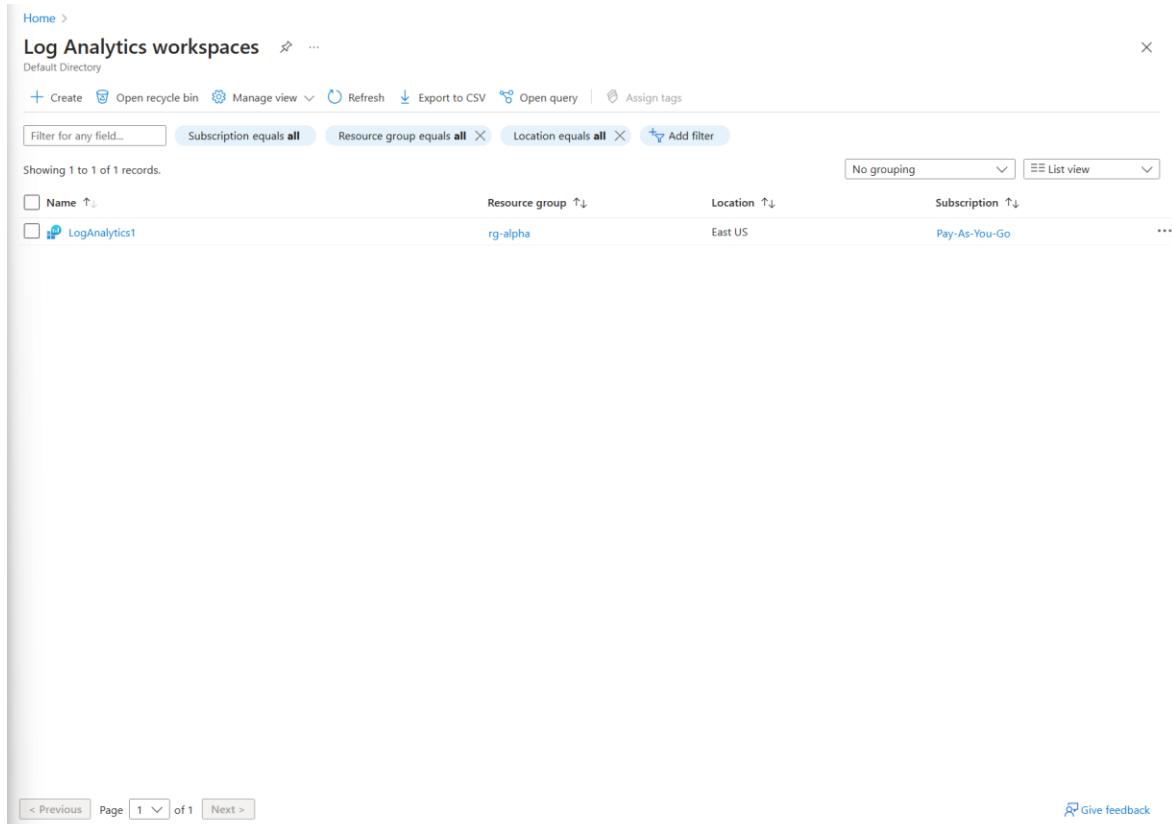
Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

No grouping List view

Showing 1 to 1 of 1 records.

| Name          | Resource group | Location | Subscription  |
|---------------|----------------|----------|---------------|
| LogAnalytics1 | rg-alpha       | East US  | Pay-As-You-Go |

< Previous Page 1 of 1 Next > Give feedback



On the Log Analytics workspaces page, choose LogAnalytics1

On the Log Analytics workspace page for LogAnalytics1, choose Usage and estimated costs

The screenshot shows the Azure portal's Log Analytics workspaces page. A sidebar on the left lists workspaces: Default Directory, Create, Open recycle bin, and LogAnalytics1 (selected). The main area shows the LogAnalytics1 workspace details. The 'Essentials' section includes: Resource group (move), Status (Active), Location (East US), Subscription (Pay-As-You-Go), and Tags (tg-alpha). It also shows Workspace Name (LogAnalytics1), Workspace ID (7dfe60e-3312-4d79-bebd-e6b2dd2bd935), Pricing tier (Pay-as-you-go), Access control mode (Use resource or workspace permissions), and Operational issues (OK). Below this is a 'Get started with Log Analytics' section with three steps: 1. Connect a data source (with options for Azure virtual machines (VMs), Windows and Linux Agents management, Storage account log, and System Center Operations Manager), 2. Configure monitoring solutions (with a link to View solutions), and 3. Monitor workspace health (with a link to Learn more about monitor workspace health). At the bottom right, a 'Select Data' button is highlighted.

Retention and set the slider to 60 days. Choose OK

The screenshot shows the Log Analytics workspace page for LogAnalytics1. The 'Usage and estimated costs' section is selected in the sidebar. The main area displays 'Data Retention' settings. It states that 31 days of retention is included with the pricing plan, and longer retention incurs additional charges. It allows configuration for specific data types. A slider for 'Data Retention (Days)' is set to 60. Below this, it notes that Application Insights data types default to 90 days. It also mentions configuration for tables and data archive on a per-table basis. An 'OK' button is at the bottom right.

## Data Retention

31 days of retention is included with your pricing plan. Longer retention will incur additional charges. Retention can also be configured individually for specific data types.

Data Retention (Days)

60

Retention for Application Insights data types default to 90 days and will get the workspace retention if it is over 90 days. To set the retention on these types to be less than 90 days, set the retention on each of these data types. [Learn more](#).

In addition to setting the default retention for tables in this workspace here, you can configuration data retention and data archive on a per-table basis on the [Tables](#) page of this workspace.

OK

On the Log Analytics workspace page for LogAnalytics1, choose Usage and estimated costs.

Select Daily cap. Choose On. Set the daily cap to 10 GB and choose OK

The screenshot shows the Azure portal interface for a Log Analytics workspace named 'LogAnalytics1'. On the left, there's a navigation sidebar with various options like Overview, Activity log, Tags, Diagnose and solve problems, Logs, Settings, Tables, Agents, and Usage and estimated costs (which is selected). The main content area displays 'Usage details', 'Cost optimization', and 'Insights' tabs. A 'Pricing Tiers' section is visible, showing the 'Pay-as-you-go' tier as the recommended choice. To the right, a modal window titled 'Daily cap' is open, explaining how it controls costs by applying a daily data ingestion limit. It shows a current limit of 10 GB/day and a note that the limit will be set at 22:00 UTC. The 'ON' button is selected, and the 'OK' button is at the bottom.

## Enable access to a Log Analytics workspace

Enter Log Analytics and select Log Analytics workspaces from the list of results

On the Log Analytics workspaces page, choose LogAnalytics1

Home >

## Log Analytics workspaces

Default Directory

+ Create Open recycle bin Manage view Refresh Export to CSV Open query Assign tags

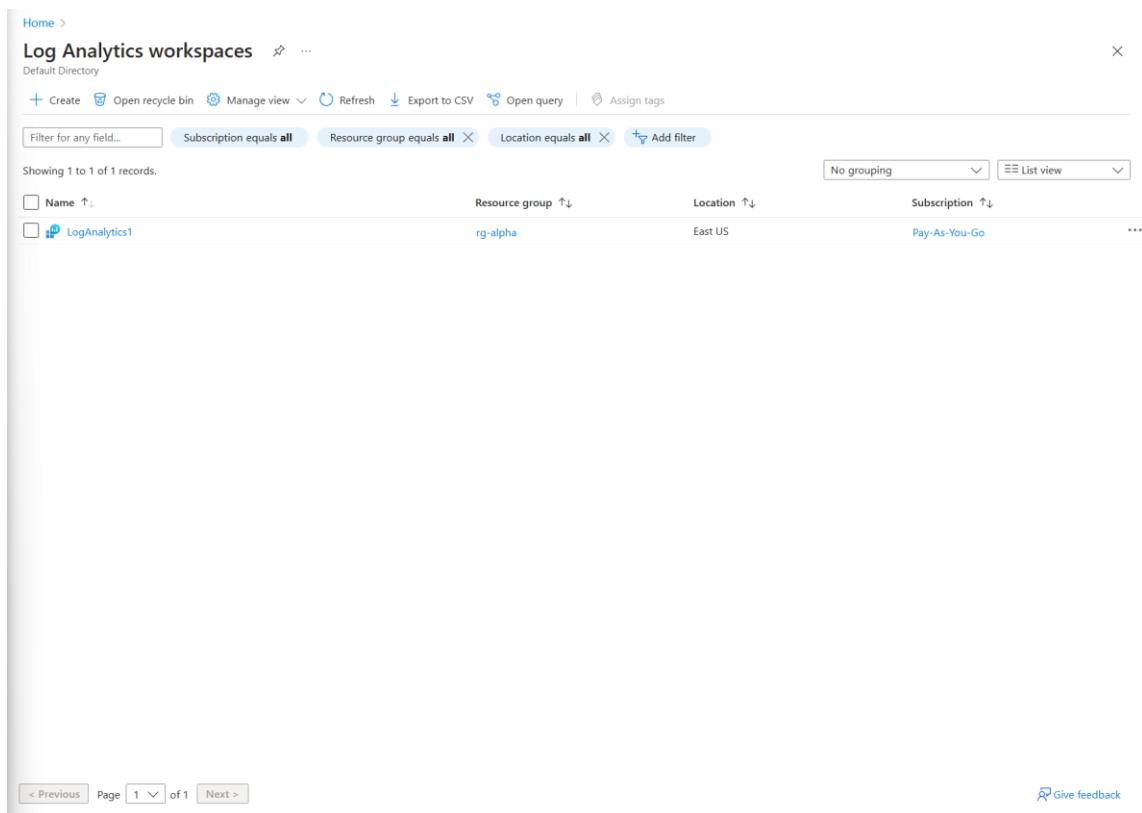
Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

No grouping List view

Showing 1 to 1 of 1 records.

| Name          | Resource group | Location | Subscription  |
|---------------|----------------|----------|---------------|
| LogAnalytics1 | rg-alpha       | East US  | Pay-As-You-Go |

< Previous Page 1 of 1 Next > Give feedback



## Select Access control (IAM)

Home > Log Analytics workspaces > LogAnalytics1

## LogAnalytics1 | Access control (IAM)

Log Analytics workspace

+ Create Open recycle bin ...

Filter for any field...

Name

|               |
|---------------|
| LogAnalytics1 |
|---------------|

Access control (IAM) Tags Diagnose and solve problems Logs Settings Tables Agents Usage and estimated costs Data export Network isolation Linked storage accounts Properties Locks Classic Legacy agents management Legacy activity log connector Legacy storage account logs Legacy computer groups Legacy solutions System center Workspace summary (deprecated) Service map (deprecated) Virtual machines (deprecated) Scope configurations (deprecated)

Check access Role assignments Roles Deny assignments Classic administrators

My access View my access

Check access Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Check access

Grant access to this resource

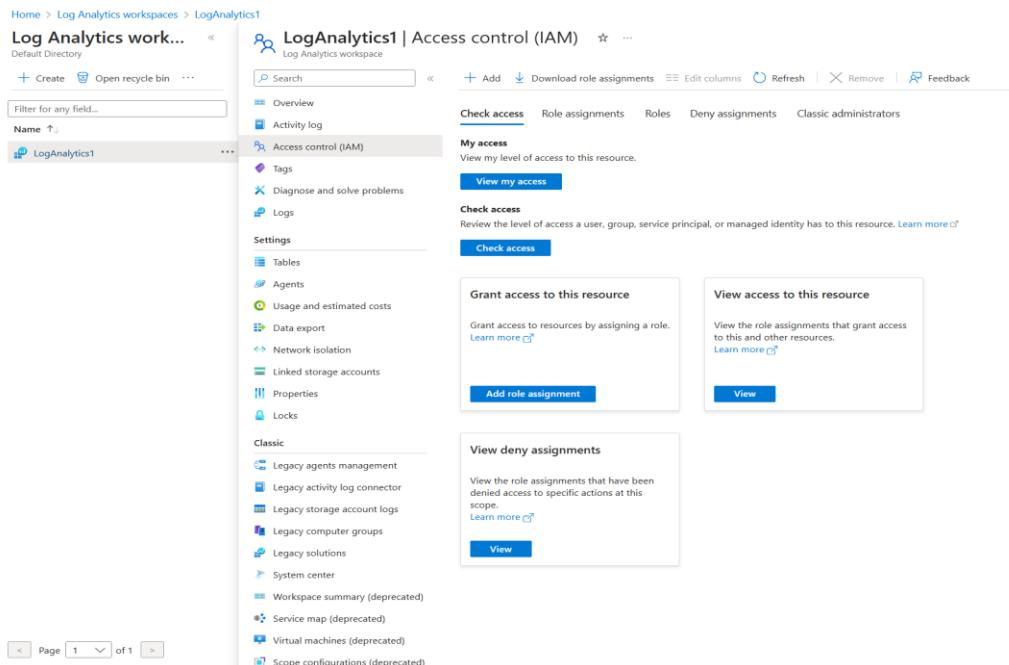
View access to this resource

View deny assignments

Add role assignment View

View

< Previous Page 1 of 1 Next >



Choose Add and then choose Add role assignment

On the list of roles, select Log Analytics Reader and choose Next

| Name ↑                                  | Description ↑  | Type ↑↓     | Category ↑↓           | Details |
|---|--|-------------|-----------------------|---------|
| Reader                                  | View all resources, but does not allow you to make any changes.  | BuiltInRole | General               | View    |
| App Compliance Automation Administrator | Create, read, download, modify and delete reports objects and related other resource objects.                | BuiltInRole | None                  | View    |
| App Compliance Automation Reader        | Read, download the reports objects and related other resource objects.                                       | BuiltInRole | None                  | View    |
| Automation Contributor                  | Manage azure automation resources and other resources using azure automation.                                | BuiltInRole | None                  | View    |
| Data Purger                             | Can purge analytics data   | BuiltInRole | Analytics             | View    |
| LocalNGFWAdministrator role             | Allows user to create, modify, describe, or delete NGFirewalls.  | BuiltInRole | None                  | View    |
| Log Analytics Contributor               | Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring s... | BuiltInRole | Analytics             | View    |
| <b>Log Analytics Reader</b>             | Log Analytics Reader can view and search all monitoring data as well as and view monitoring settings, inc... | BuiltInRole | Analytics             | View    |
| Managed Application Contributor Role    | Allows for creating managed application resources.   | BuiltInRole | Management + Gover... | View    |
| Managed Application Operator Role       | Lets you read and perform actions on Managed Application resources   | BuiltInRole | Management + Gover... | View    |
| Managed Applications Reader             | Lets you read resources in a managed app and request JIT access.   | BuiltInRole | Management + Gover... | View    |
| Microsoft Sentinel Contributor          | Microsoft Sentinel Contributor   | BuiltInRole | Security              | View    |
| Microsoft Sentinel Reader               | Microsoft Sentinel Reader  | BuiltInRole | Security              | View    |
| Microsoft Sentinel Responder            | Microsoft Sentinel Responder   | BuiltInRole | Security              | View    |
| Monitoring Contributor                  | Can read all monitoring data and update monitoring settings.   | BuiltInRole | Monitor               | View    |
| Monitoring Metrics Publisher            | Enables publishing metrics against Azure resources   | BuiltInRole | Monitor               | View    |
| Monitoring Reader                       | Can read all monitoring data.  | BuiltInRole | Monitor               | View    |

On the Members page, choose Select Members and choose the App Log Examiners security group. Choose Select

Home > Log Analytics workspaces > LogAnalytics1 | Access control (IAM) >

### Add role assignment ...

**Role** **Members** \* **Review + assign**

**Selected role** Log Analytics Reader

**Assign access to**  User, group, or service principal  Managed identity

**Members** [+ Select members](#)

| Name                | Object ID | Type |
|---------------------|-----------|------|
| No members selected |           |      |

**Description** Optional

[Review + assign](#) [Previous](#) [Next](#) [Select](#) [Close](#)

### Select members

Select ⓘ

bob.hotel bob.hotel@vikaramtiratoutlook.onmicrosoft.com

Vikar Ramtirat vikaramtirat\_outlook.com#EXT#@vikaramtiratoutlook...

Selected members:

App Log Examiners [Remove](#)

### On the Members space, choose Review + Assign

Home > Log Analytics workspaces > LogAnalytics1 | Access control (IAM) >

### Add role assignment ...

**Role** **Members** **Review + assign**

**Selected role** Log Analytics Reader

**Assign access to**  User, group, or service principal  Managed identity

**Members** [+ Select members](#)

| Name              | Object ID                            | Type  |
|-------------------|--------------------------------------|-------|
| App Log Examiners | d0acc8d8-3a22-4259-906a-f80994371fdf | Group |

**Description** Optional

[Review + assign](#) [Previous](#) [Next](#) [Feedback](#)

The role with security group has been added under role assignments

Home > Log Analytics workspaces > LogAnalytics1

## Log Analytics workspace

Default Directory

+ Create Open recycle bin ...

Filter for any field... Name ↑

LogAnalytics1

...

LogAnalytics1 | Access control (IAM)

Log Analytics workspace

Search Add Download role assignments Edit columns Refresh Remove Feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Logs

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription 1 4000 Privileged 0

View assignments

All Job function (1) Privileged (0)

Search by name or email Type : All Role : All Scope : All scopes Group by : Role

| Name                     | Type  | Role                 | Scope         | Condition |
|--------------------------|-------|----------------------|---------------|-----------|
| Log Analytics Reader (1) | Group | Log Analytics Reader | This resource | None      |

Page 1 of 1 >

Legacy agents management Legacy activity log connector Legacy storage account logs Legacy computer groups Legacy solutions System center Workspace summary (deprecated) Service map (deprecated) Virtual machines (deprecated) Scope configurations (deprecated)

## Tasks 3 - Monitor web apps

- **Enable Application Insights**
- **Disable logging for .NET core snapshot debugger**
- **Configure web app HTTP logs to be written to a Log Analytics workspace**
- **Configure SQL Insights data to be written to a Log Analytics workspace**
- **Enable file and configuration change tracking for web apps**

## Enable Application Insights

In the Azure Portal Search Bar, enter rg-alpha and select rg-alpha from the list of results

The screenshot shows the Azure Portal interface for the 'rg-alpha' resource group. The left sidebar contains various navigation links such as Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Logs, and Workbooks. The main content area is titled 'Essentials' and shows basic information about the resource group, including Subscription (move) to Pay-As-You-Go, Subscription ID, Tags, Deployments (1 Failed, 7 Succeeded), and Location (East US). Below this, there is a table listing 22 resources, each with a name, type, location, and three-dot ellipsis menu. The resources include Application Insights, Action groups, App Service plans, App Service plans, App Services, Smart detector alert rules, App Service plans, Virtual machines, Public IP addresses, Network security groups, Network interfaces, Disks, Log Analytics workspaces, and SQL databases.

| Name   | Type                      | Location | Actions |
|--|---------------------------|----------|---------|
| AppInsightswebsitefyp73mfn5xq4                     | Application Insights      | East US  | ...     |
| Application Insights Smart Detection               | Action group              | Global   | ...     |
| AppServicePlan-AzureLinuxApp2023                   | App Service plan          | East US  | ...     |
| AppServicePlan-AzureLinuxAppny2024                 | App Service plan          | East US  | ...     |
| AzureLinuxAppny2024-webapp                         | App Service               | East US  | ...     |
| Failure Anomalies - AppInsightswebsitefyp73mfn5xq4 | Smart detector alert rule | Global   | ...     |
| hostingplanfyqp73mfn5xq4                           | App Service plan          | East US  | ...     |
| Linux-VM2  | Virtual machine           | East US  | ...     |
| Linux-VM2-ip                                       | Public IP address         | East US  | ...     |
| Linux-VM2-nsg                                      | Network security group    | East US  | ...     |
| linux-vm2129                                       | Network Interface         | East US  | ...     |
| Linux-VM2_disk1_9c3afed3d41346b3a64876858c08fa3c   | Disk                      | East US  | ...     |
| LogAnalytics1                                      | Log Analytics workspace   | East US  | ...     |
| sampledb (sqlServerfyp73mfn5xq4/sampledb)          | SQL database              | East US  | ...     |

From the list of items in the resource group, choose App Services for the Web App with an SQL Database

The screenshot shows the Azure portal interface for managing a web application named 'AzureLinuxAppny2024-webapp'. The left sidebar contains a navigation menu with various options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Microsoft Defender for Cloud, Events (preview), Deployment slots, Deployment Center, Configuration, Authentication, Application Insights, Identity, Backups, Custom domains, Certificates, Networking, Scale up (App Service plan), Scale out (App Service plan), Service Connector, Locks, App Service plan, and Quotas. The 'Application Insights' option is highlighted. The main panel displays the 'Essentials' section with details such as Resource group (rg-alpha), Status (Running), Location (East US), Subscription (Pay-As-You-Go), Subscription ID (8148d5d5-df15-44ef-beb3-5960d3dc42eb), and Tags (Add tags). It also shows the 'Properties' tab with settings for the Web app (Name: AzureLinuxAppny2024-webapp, Publishing model: Code, Runtime Stack: PHP - 7.4), Domains (Default domain: azurelinuxappny2024-webapp.azurewebsites.net, Custom domain: Add custom domain), and Hosting (Plan Type: App Service plan, Name: AppServicePlan-AzureLinuxAppny2024, Operating System: Linux, Instance Count: 1, SKU and size: Standard (S1) Scale up). The 'Deployment Center' tab is visible at the bottom.

## Under Settings choose Application Insights

The screenshot shows the same Azure portal interface as the previous one, but with a different focus. The 'Application Insights' option in the left sidebar is now highlighted. The main panel displays the 'Turn on Application Insights' button, indicating that Application Insights are currently disabled. The rest of the interface remains the same, showing the 'Essentials' section with the same details as the previous screenshot.

## On the Application Insights page, choose Turn On Application Insights

Home > rg-alpha > AzureLinuxAppny2024-webapp

AzureLinuxAppny2024-webapp | Application Insights

Web App

Application Insights

Collect application monitoring data using Application Insights

Enable  Disable  Feedback

Link to an Application Insights resource

Your app will be connected to an auto-created Application Insights resource: **AzureLinuxAppny2024-webapp**. Instrumentation key will be added to App Settings. This will overwrite any instrumentation key value in web app configuration files.

As part of using Application Insights instrumentation, we collect and send diagnostic data to Microsoft. This data helps us run and improve Application Insights. You have the option to disable non-essential data collection. [Learn more](#)

Change your resource

Create new resource

Application insights and workspace resources are created in current subscription and resource group scope. If you want to choose a different scope, please create a new AI component by visiting: [Create a new Application Insights resource](#) and then return to this page.

New resource name \*

Location \*

Log Analytics Workspace  (new) DefaultWorkspace-8148d5d5-df15-44ef-beb3-5960d3dc42eb-EUS [eastus]

Select existing resource   
select a subscription

Top 5 relevant resources - Relevance is determined by resource group, location, or in alphabetical order.

Apply

On the Application Insights page, ensure that Create a new resource is selected and that the Log Analytics Workspace is set to LogAnalytics1 and choose Apply

Home > rg-alpha > AzureLinuxAppny2024-webapp

AzureLinuxAppny2024-webapp | Application Insights

Web App

Application Insights

Collect application monitoring data using Application Insights

Enable  Disable  Feedback

Link to an Application Insights resource

Your app will be connected to an auto-created Application Insights resource: **AzureLinuxAppny2024-webapp**. Instrumentation key will be added to App Settings. This will overwrite any instrumentation key value in web app configuration files.

As part of using Application Insights instrumentation, we collect and send diagnostic data to Microsoft. This data helps us run and improve Application Insights. You have the option to disable non-essential data collection. [Learn more](#)

Change your resource

Create new resource

Application insights and workspace resources are created in current subscription and resource group scope. If you want to choose a different scope, please create a new AI component by visiting: [Create a new Application Insights resource](#) and then return to this page.

New resource name \*

Location \*

Log Analytics Workspace  LogAnalytics1 [eastus]

Select existing resource   
select a subscription

Top 5 relevant resources - Relevance is determined by resource group, location, or in alphabetical order.

Apply

On the Apply monitoring settings dialog, choose Yes

The screenshot shows the Azure portal interface for a web application named 'AzureLinuxAppny2024-webapp'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Microsoft Defender for Cloud, Events (preview), Deployment slots, Deployment Center, Configuration, Authentication, Application Insights (which is selected), Identity, Backups, Custom domains, Certificates, Networking, Scale up (App Service plan), Scale out (App Service plan), Service Connector, Locks, App Service plan, and Quotas. The main content area shows the Application Insights settings, including fields for 'New resource name \*' (set to 'AzureLinuxAppny2024-webapp') and 'Location \*' (set to 'East US'). Below these are dropdown menus for 'Log Analytics Workspace' (set to 'LogAnalytics1 [eastus]') and 'Select existing resource' (with a search bar). A table lists one resource: 'Name' (AppInsightswebsitefyp73mfn5xq4), 'Resource Group' (rg-alpha), and 'Location' (East US). A modal dialog titled 'Apply monitoring settings' is displayed, containing the message: 'We will now apply changes to your app settings and install our tools to link your Application Insights resource to the web app. This will restart the site. Do you want to continue?'. It has 'Yes' and 'No' buttons, with 'Yes' being the active button.

## Disable logging for .NET core snapshot debugger

Go back to the rg-alpha resource group and from the list of items in the resource group, choose App Services for the Web App with an SQL Database.

Under Settings choose Application Insights

The screenshot shows the Azure portal interface for the same web application. The left sidebar includes the 'Application Insights' section. The main content area displays the Application Insights settings, specifically the 'Instrument your application' section. It features a 'View Application Insights data' button and a 'Disable' button for Application Insights. A note states: 'Your app is connected to Application Insights resource: AzureLinuxAppny2024-webapp'. Another note explains: 'As part of using Application Insights instrumentation, we collect and send diagnostic data to Microsoft. This data helps us run and improve Application Insights. You have the option to disable non-essential data collection.' Below this is a 'Change your resource' section and an 'Instrument your application' section with tabs for Info, .NET, .NET Core, Node.js, Java, and Python. An 'Apply' button is at the bottom.

Under Instrument your application, choose .NET Core and then set the Snapshot Debugger setting to Off. Choose Apply.

## Configure web app HTTP logs to be written to a Log Analytics workspace

Go to rg-alpha resource group

Choose App Services for the Web App with an SQL Database

Under Monitoring, choose Diagnostic settings

The screenshot shows the Azure portal interface for managing diagnostic settings for an App Service. The left sidebar navigation includes sections for App Service plan, Quotas, Change App Service plan, Development Tools (SSH, Advanced Tools), API (API Management, API definition, CORS), Monitoring (Alerts, Metrics, Logs, Advisor recommendations, Health check, Diagnostic settings, App Service logs, Log stream), Automation (Tasks (preview), Export template), and Support + troubleshooting (Resource health, Support + Troubleshooting). The main content area is titled "AzureLinuxAppny2024-webapp | Diagnostic settings". It displays a table for "Diagnostic settings" with columns for Name, Storage account, Event hub, Log Analytics workspace, Partner solution, and Edit setting. A note states "No diagnostic settings defined" and provides a link to "+ Add diagnostic setting". Below this, a list of data types to collect is shown, including HTTP logs, App Service Console Logs, App Service Application Logs, Access Audit Logs, IPSecurity Audit logs, App Service Platform logs, and AllMetrics. The "Diagnostic settings" link in the sidebar is highlighted.

On the Diagnostic settings page, select + Add diagnostic settings

On the Diagnostic settings page, choose the following and select Save.

| Property                | Value                           |
|-------------------------|---------------------------------|
| Diagnostic setting name | httplogs                        |
| Categories              | HTTP logs                       |
| Destination details     | Send to Log Analytics workspace |
| Subscription            | Your subscription               |
| Log Analytics workspace | LogAnalytics1                   |

Home > Resource groups > rg-alpha > AzureLinuxAppny2024-webapp | Diagnostic settings >

Diagnostic setting ... X

Save  Discard  Delete  Feedback JSON View

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 setting name \*  ✓

Logs Destination details

Categories

HTTP logs  Send to Log Analytics workspace

App Service Console Logs Subscription

App Service Application Logs Log Analytics workspace

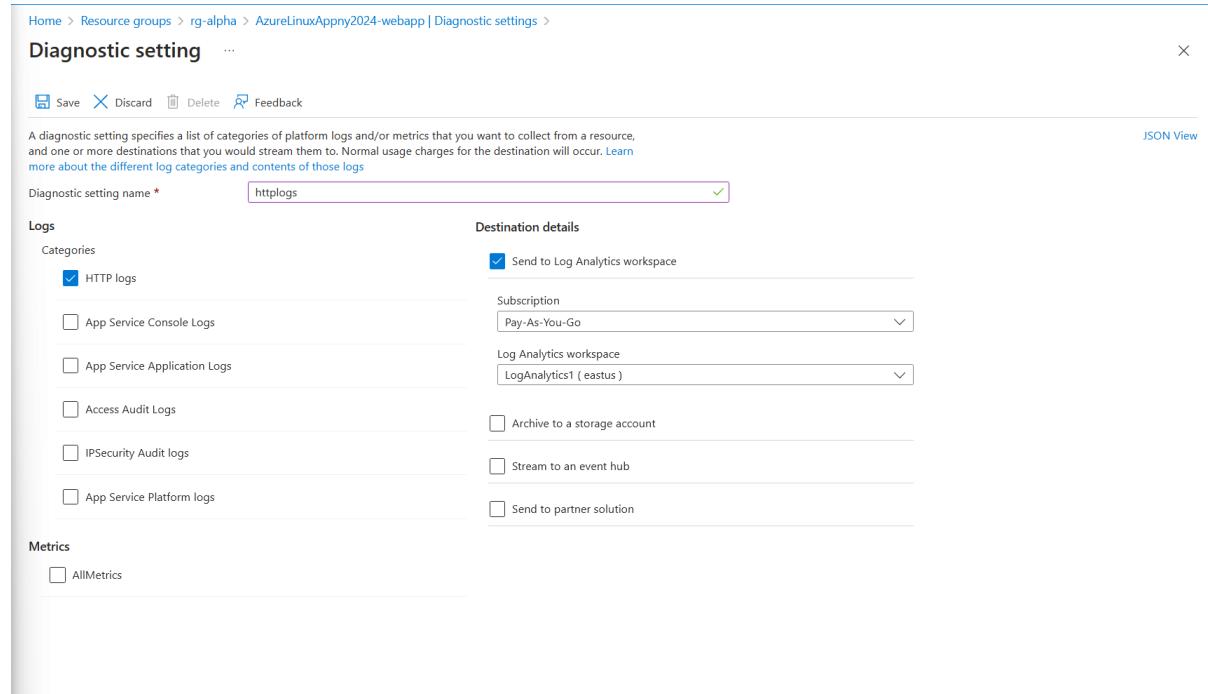
Access Audit Logs  Archive to a storage account

IP Security Audit logs  Stream to an event hub

App Service Platform logs  Send to partner solution

Metrics

AllMetrics



# Configure SQL Insights data to be written to a Log Analytics workspace

Go to rg-alpha resource group and choose the sample SQL database

The screenshot shows the Azure portal interface for the 'sampledb' resource group under 'rg-alpha'. The left sidebar lists various service categories like Activity log, Tags, Diagnose and solve problems, Query editor (preview), Compute + storage, Connection strings, Properties, Locks, Data management, Replicas, Sync to other databases, Azure Synapse Link, Stream analytics (preview), Add Azure AI Search, Power BI, Power Apps, Power Automate, Auditing, Ledger, and Data Discovery & Classification. The main content area displays the database's properties, including its resource group (rg-alpha), status (Online), location (East US), and subscription information. It also shows connection strings and pricing tier. Below the properties, there are sections for 'Getting started' (with links to 'Configure access', 'Connect to application', and 'Start developing'), 'Start working with your database' (with a link to 'Learn more'), and a 'Start developing' section with links to 'Open Azure Data Studio', 'Open in Visual Studio', and 'Open in Visual Studio Code'.

Under Monitoring, choose Diagnostic settings

The screenshot shows the 'Diagnostic settings' page for the 'sampledb' resource group. The left sidebar includes sections for Power Automate, Security (Auditing, Ledger, Data Discovery & Classification, Dynamic Data Masking, Microsoft Defender for Cloud, Identity, Data Encryption), Intelligent Performance (Performance overview, Performance recommendations, Query Performance Insight, Automatic tuning), Monitoring (Alerts, Metrics, Diagnostic settings, Logs), Automation (Tasks (preview), Export template), Help (Resource health, Support + Troubleshooting), and a 'Diagnostic settings' section which is currently selected. The main content area provides information about diagnostic settings and a table for managing them. The table has columns for Name, Storage account, Event hub, Log Analytics workspace, Partner solution, and Edit setting. A note at the bottom of the table area says 'Click 'Add diagnostic setting' above to configure the collection of the following data:' followed by a bulleted list of data types: SQL Insights, Automatic tuning, Query Store Runtime Statistics, Query Store Wait Statistics, Errors, Database Wait Statistics, Timeouts, Blocks, Deadlocks, Basic, InstanceAndAppAdvanced, and WorkloadManagement.

On the Diagnostic settings page, choose Add diagnostic setting

On the **Diagnostic setting page**, provide the following information and choose **Save**.

| Property                | Value                           |
|-------------------------|---------------------------------|
| Diagnostic setting name | InsightLogAnalytics             |
| Categories              | SQL Insights                    |
| Destination details     | Send to Log Analytics workspace |
| Subscription            | Your subscription               |
| Log Analytics workspace | LogAnalytics1                   |

Home > Resource groups > rg-alpha > sampledb (sqlServerfyqp73mfn5xq4/sampledb) | Diagnostic settings >

**Diagnostic setting** ... X

Save Discard Delete Feedback JSON View

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 setting name \*  ✓

**Logs**

Category groups (1)

allLogs  audit

Categories

SQL Insights  Automatic tuning  Query Store Runtime Statistics  Query Store Wait Statistics  Errors  Database Wait Statistics  Timeouts  Blocks  Deadlocks

Metrics

Basic  InstanceAndAppAdvanced  WorkloadManagement

**Destination details**

Send to Log Analytics workspace

Subscription

Log Analytics workspace

Archive to a storage account  Stream to an event hub  Send to partner solution

## Enable file and configuration change tracking for web apps

Go to rg-alpha resource group and choose AzureLinuxAppny2024-webapp

Choose Diagnose and Solve Problems.

The screenshot shows the Azure portal interface for the 'AzureLinuxAppny2024-webapp' under the 'rg-alpha' resource group. The left sidebar contains navigation links for Overview, Activity log (selected), Access control (IAM), Tags, Diagnose and solve problems (selected), Microsoft Defender for Cloud, Events (preview), Deployment slots, Deployment Center, Configuration, Authentication, Application Insights, Identity, Backups, Custom domains, Certificates, Networking, Scale up (App Service plan), Scale out (App Service plan), Service Connector, Locks, and App Service plan. The main content area is titled 'App Service Diagnostics - Investigate how your app is performing, diagnose issues, and discover how to improve your application.' It features a search bar, a 'Risk alerts' section with 2 Critical availability issues, and four troubleshooting categories: Availability and Performance, Configuration and Management, Diagnostic Tools, and Load Test your App. Each category has associated sub-links. A 'Popular troubleshooting tools' section lists Application Logs, Web App Down, and Linux Web App Slow. The URL at the bottom is <https://portal.azure.com/#@vikaramtiratoutlook.onmicrosoft.com/resource/subscriptions/8148d5d5-dff5-44ef-beb3-5960d3dc42eb/resourceGroups/rg-alpha/providers/Microsoft.Web/sites/AzureLinuxAppny2024-webapp/eventLogs>.

In the search dialog box, type Application Changes

In the search dialog box, type Application Changes.

On the Change Analysis page, choose Configure.

On the Enable file and configuration change tracking page, change the Status slider to On and then choose Save

The screenshot shows the 'Enable file and configuration change tracking' dialog box. At the top left, there's a back button labeled 'Home > Resource groups > rg-alpha'. To its right is the title 'Change Analysis' with a 'Configure' link. Below the title are buttons for 'Refresh', 'Edit columns', and a 'Filter changes...' search bar. A note says 'Subscription : Pay-As-You-Go'. It also mentions '0 changes from 29/12/2023, 16:59:33 GM' and 'Some types of resource configuration set'. On the far left, there's a vertical sidebar with a 'Changes' tab. The main area has a header 'Enable file and configuration change tracking' and a note: 'If you just enabled or disabled an App Services resource for in-guest changes collection and don't see latest status reflected, please come back in a few minutes. The resources will take some time to update. Learn more at <https://aka.ms/changeanalysis/app-service-enablement>'. Below this is a table with one row:

| Name                       | Type             | Resource Group | Status                                 |
|----------------------------|------------------|----------------|--|
| > hostingplanfyqp73mfn5xq4 | App Service Plan | rg-alpha       | <input checked="" type="checkbox"/> On |

At the bottom of the dialog are 'Save' and 'Discard' buttons.

## Tasks 4 - Configure monitoring for compute services

- create a data collection endpoint
- Create a data collection rule
- Add an IIS log collection to an existing data collection rule
- Configure Network Connection Monitor for a Linux IaaS virtual machine

### Create a data collection endpoint

In the Azure Portal Search Bar, enter Monitor and select Monitor from the list of results

The screenshot shows the Azure Monitor Overview page. On the left, there's a navigation sidebar with sections like Overview, Insights, Detection, triage, and diagnosis, and Settings. The main area displays various monitoring views: Application Insights, Container Insights, VM Insights, Network Insights, Metrics, Alerts, Logs, Workbooks, Change Analysis, and Diagnostic Settings. A prominent message at the top states: "The Log Analytics agents, used by VM Insights, won't be supported as of August 31, 2024. Plan to migrate to VM Insights on Azure Monitor agent prior to this date." There are also links to "View all insights" and "Learn more about monitoring".

In the Monitor page, under Settings, choose Data Collection Endpoints

The screenshot shows the Azure Monitor Data Collection Endpoints page. The left sidebar includes sections for Storage accounts, Containers, Networks, SQL (preview), Azure Cosmos DB, Key Vaults, Azure Cache for Redis, Azure Data Explorer Clusters, Log Analytics workspaces, Azure Stack HCI, Service Bus (preview), Insights Hub, Managed Services (with sub-options for Managed Prometheus, Azure Managed Grafana, and Azure Monitor SCOM managed instance), Settings (with sub-options for Diagnostic settings, Data Collection Rules, and Data Collection Endpoints), Autoscale, Private Link Scopes, Support + Troubleshooting (with sub-options for Advisor recommendations and New support request), and a "Give feedback" link. The main content area displays a message: "No data collection endpoints to display. Try changing or clearing your filters." It features a blue circular icon with a green center and arrows pointing outwards.

On the **Data Collection Endpoints** page, choose **Create**.

On the Create Data Collection Endpoint page, provide the following settings and then choose Review + Create.

| Property       | Value                    |
|----------------|--------------------------|
| Endpoint name  | IaaSVMCollectionEndpoint |
| Subscription   | Your subscription        |
| Resource Group | rg-alpha                 |
| Region         | East US                  |

Review the settings and choose **Create**.

Home > Monitor | Data Collection Endpoints >

Create data collection endpoint ... X

[Basics](#) [Tags](#) [Review + create](#)

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. [Learn more](#)

**Endpoint details**

Endpoint Name \*  ✓

Subscription \* ⓘ  ▾

Resource Group \* ⓘ  ▾  
[Create new](#)

Region \* ⓘ  ▾

[Review + create](#) [< Previous](#) [Next : Tags >](#)

The screenshot shows the Azure Monitor interface for Data Collection Endpoints. On the left, there's a sidebar with navigation links like Home, Monitor, Storage accounts, Containers, Networks, SQL (preview), Azure Cosmos DB, Key Vaults, Azure Cache for Redis, Azure Data Explorer Clusters, Log Analytics workspaces, Azure Stack HCI, Service Bus (preview), Insights Hub, Managed Services (with options for Managed Prometheus, Azure Managed Grafana, and Azure Monitor SCOM managed instance), Settings (with options for Diagnostic settings, Data Collection Rules, and Data Collection Endpoints - which is currently selected and highlighted in grey), and Support + Troubleshooting (with Advisor recommendations and New support request). At the top, there's a search bar and several filter buttons: 'Subscription equals all', 'Resource group equals all', 'Location equals all', 'Add filter', 'No grouping', and 'List view'. The main area displays a table with one record: 'IaaSVMCollectionEndpoint' under 'Name', 'Pay-As-You-Go' under 'Subscription', 'rg-alpha' under 'Resource group', and 'East US' under 'Location'. Below the table are buttons for '< Previous', 'Page', 'of 0', and 'Next >'. In the bottom right corner, there's a 'Give feedback' link.

## Create a data collection rule

Go to Monitor

In the Monitor page, under Settings, choose Data Collection Rules

On the Data Collection Rules page, choose Create

On the **Create Data Collection Rule** page, configure the following settings and choose **Next**.

| Property     | Value             |
|--------------|-------------------|
| Rule name    | WinVMDCR          |
| Subscription | Your subscription |

| Property                 | Value                    |
|--------------------------|--------------------------|
| Resource Group           | rg-alpha                 |
| Region                   | East US                  |
| Platform type            | Windows                  |
| Data collection endpoint | IaaSVMCollectionEndpoint |

Home > Monitor | Data Collection Rules >

## Create Data Collection Rule ...

X

Data collection rule management

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

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. [Learn more](#)

### Rule details

|                          |  |
|--------------------------|--|
| Rule Name *              | WinVMDCR   |
| Subscription *           | Pay-As-You-Go  |
| Resource Group *         | rg-alpha   |
| Region *                 | East US  |
| Platform Type *          | <input checked="" type="radio"/> Windows<br><input type="radio"/> Linux<br><input type="radio"/> All |
| Data Collection Endpoint | IaaSVMCollectionEndpoint   |

[Review + create](#)

[< Previous](#)

[Next : Resources >](#)

On the Resources page, choose Add Resources

On the Select a scope page, enable the WS-VM1 checkbox and choose Apply

The screenshot shows the 'Create Data Collection Rule' wizard in the Azure portal. On the left, the 'Resources' tab is selected. A note says: 'This will also enable System Assigned Managed Identity on these machines, in addition to the existing User Assigned Managed Identity.' Below it are 'Add resources' and 'Create endpoint' buttons. A note below says: 'Only virtual machines in the same region can be assigned to the same endpoint.' On the right, the 'Select a scope' dialog is open, showing a table of resources:

| Scope                                      | Resource type   | Location |
|--|-----------------|----------|
| <input type="checkbox"/> Pay-As-You-Go     | Subscription    | -        |
| <input type="checkbox"/> rg-alpha          | Resource group  | -        |
| <input checked="" type="checkbox"/> WS-VM1 | Virtual machine | East US  |

At the bottom of the dialog are 'Apply' and 'Cancel' buttons.

On the Create Data Collection Rule page, choose Next.

On the Collect and Deliver page, choose Add data source.

On the **Add data source** page, select **Windows Event Logs**. In the **Application** category enable the **Critical** and **Error** categories. In the **Security** category, choose the **Audit Failure** category. In the **System** category, enable the **Critical** and **Error** categories.

Choose Next

Screenshot on next page

On the **Destination** page, configure the following settings:

| Property             | Value              |
|----------------------|--------------------|
| Destination type     | Azure Monitor Logs |
| Subscription         | Your subscription  |
| Account or namespace | LogAnalytics1      |

The screenshot shows the 'Create Data Collection Rule' wizard in the Azure portal. The left sidebar shows 'Home > Monitor | Data Collection Rules > Create Data Collection Rule'. The main area has tabs for 'Basics', 'Resources', 'Collect and deliver' (which is selected), 'Tags', and 'Review + create'. Under 'Collect and deliver', it says 'Configure which data sources to collect, and where to send the data to.' There's a button '+ Add data source' and a note 'No standard data sources or destinations found.' The right side is titled 'Add data source' with a 'Destination' tab selected. It asks to 'Select the destination(s) for where the data will be delivered. Normal usage charges for the destination will occur.' It includes fields for 'Destination type' (set to 'Azure Monitor Logs'), 'Subscription' (set to 'Pay-As-You-Go'), and 'Account or namespace' (set to 'LogAnalytics1 (rg-alpha)'). A note at the bottom left says '✖ This data collection rule doesn't have any data sources or destinations selected.' At the bottom, there are buttons for 'Review + create', '< Previous', 'Next : Tags >', 'Add data source', '< Previous', and 'Cancel'.

Choose Add data source

Choose Review + Create and then choose Create

# Add an IIS log collection to an existing data collection rule

## Select Monitor

In the Monitor page, under Settings, choose Data Collection Rules

The screenshot shows the Microsoft Azure Monitor Data Collection Rules page. The left sidebar includes sections for Storage accounts, Containers, Networks, SQL (preview), Azure Cosmos DB, Key Vaults, Azure Cache for Redis, Azure Data Explorer Clusters, Log Analytics workspaces, Azure Stack HCI, Service Bus (preview), and Insights Hub. Under Managed Services, there are links for Managed Prometheus, Azure Managed Grafana, and Azure Monitor SCOM managed instance. The main content area displays a table of data collection rules. One rule is selected, showing details: WinVMDCR, Pay-As-You-Go, rg-alpha, East US, Windows Event Logs, Azure Monitor Logs, and Windows. The table has columns for Name, Subscription, Resource group, Location, Data sources, Destinations, and Kind. There are filters at the top: Subscription equals all, Resource group equals all, Location equals all, and Add filter. The bottom of the page shows navigation links for Previous, Page 1 of 1, and Next.

Choose the WinVMDCR rule in rg-alpha

Under Configuration, choose Data Sources

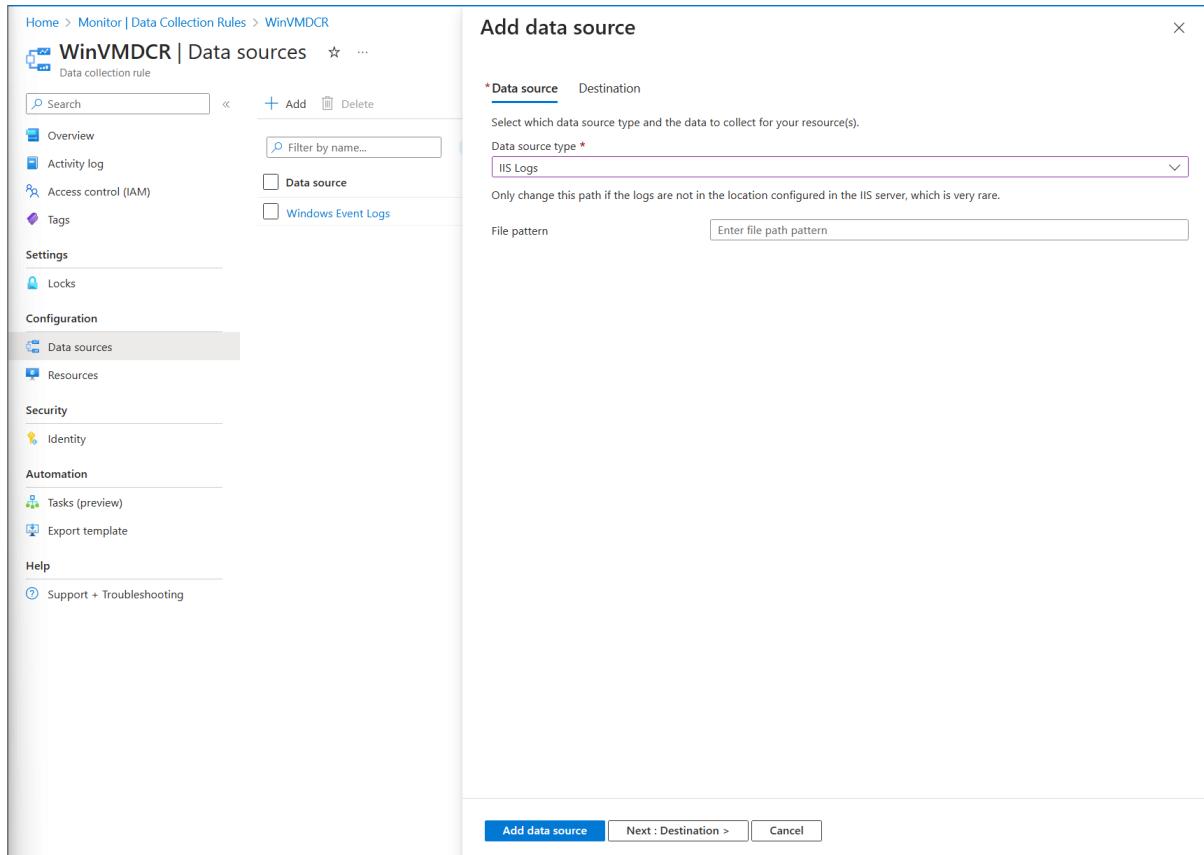
The screenshot shows the WinVMDCR Data sources configuration page. The left sidebar includes sections for Overview, Activity log, Access control (IAM), Tags, Settings (Locks), Configuration (Data sources, Resources), Security (Identity), Automation (Tasks (preview), Export template), and Help (Support + Troubleshooting). The main content area shows a table of data sources. One source is selected, showing details: Data source (checkbox) and Destination(s) (checkbox) Azure Monitor Logs. The table has columns for Data source and Destination(s). There is a filter bar at the top labeled 'Filter by name...' and 'Destination: all'. The bottom of the page shows navigation links for Previous, Page 1 of 1, and Next.

Under Configuration, choose Data Sources.

On the Data Sources page, choose Add.

On the Add Data Source page, select IIS Logs.

Choose Next



On the **Destination** page, configure the following settings:

| Property             | Value              |
|----------------------|--------------------|
| Destination type     | Azure Monitor Logs |
| Subscription         | Your subscription  |
| Account or namespace | LogAnalytics1      |

Choose **Add data source**.

The screenshot shows the Azure Monitor Data Collection Rules interface for a resource named 'WinVMDCR'. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Tags, Settings (Locks), Configuration (Data sources, Resources), Security (Identity), Automation (Tasks (preview), Export template), and Help (Support + Troubleshooting). The 'Data sources' option under Configuration is currently selected.

The main area is titled 'Add data source' and has a tab bar with 'Data source' (selected) and 'Destination'. Below the tabs, it says 'Select the destination(s) for where the data will be delivered. Normal usage charges for the destination will occur.' with a link to 'Learn more about pricing.' There's a button '+ Add destination' and a section for 'Destination type', 'Subscription', and 'Account or namespace'. The 'Destination type' dropdown is set to 'Azure Monitor Logs', 'Subscription' to 'Pay-As-You-Go', and 'Account or namespace' to 'LogAnalytics1 (rg-alpha)'. At the bottom right of the dialog are 'Save', '< Previous', and 'Cancel' buttons.

## Configure Network Connection Monitor for a Linux IaaS virtual machine

### Go to Network Watcher

The screenshot shows the Microsoft Azure Network Watcher interface. At the top, there's a header with the Microsoft Azure logo, a search bar, and user information ('vikaramtirat@outlook.com', 'DEFAULT DIRECTORY (VIKARRA...)'). Below the header is a toolbar with buttons for Create, Add, Manage view, Refresh, Export to CSV, Open query, Assign tags, and Disable.

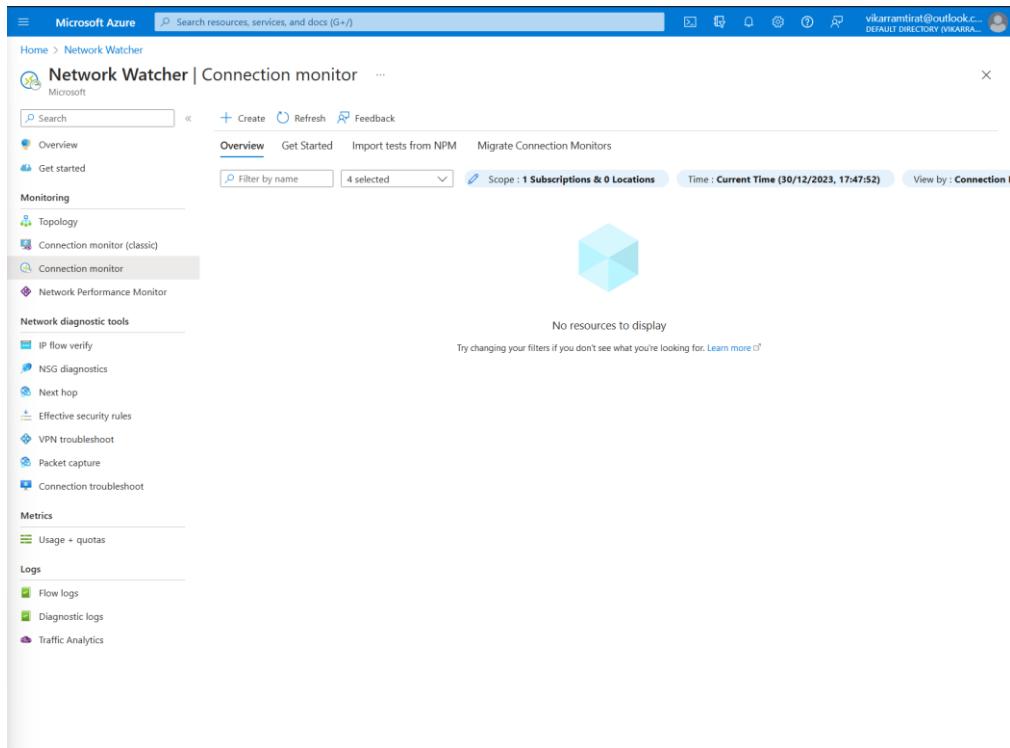
The main content area is titled 'Network Watcher' and shows a list of resources. It includes filters for 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. The results table shows one record: 'Name' is 'NetworkWatcher\_eastus', 'Subscription' is 'Pay-As-You-Go', and 'Location' is 'East US'. There are buttons for 'Edit' and 'Delete' next to the resource name.

The sidebar on the left contains several sections:

- Monitoring**: Topology, Connection monitor (classic), Connection monitor, Network Performance Monitor.
- Network diagnostic tools**: IP flow verify, NSG diagnostics, Next hop, Effective security rules, VPN troubleshoot, Packet capture, Connection troubleshoot.
- Metrics**: Usage + quotas.
- Logs**: Flow logs, Diagnostic logs, Traffic Analytics.

At the bottom of the page, there are navigation links for '< Previous', 'Page 1 of 1', 'Next >', and a 'Give feedback' button.

Under Monitoring, choose Connection Monitor



On the Connection Monitor page, choose Create

On the **Basics** page of the **Create Connection Monitor** wizard, provide the following information and choose **Next**.

| Property                | Value             |
|-------------------------|-------------------|
| Connection Monitor name | LinuxVMPubIP      |
| Subscription            | Your subscription |
| Region                  | East US           |
| Workspace               | LogAnalytics1     |

On the Add test group details page, enter the name LinuxIPTest and choose Add sources.

On the Add Sources page, select Azure Endpoints and set the type to Virtual machines. Select Subnet and then enable the Linux-VM checkbox. Choose Add Endpoints.

Choose Add Test Configuration.

On the Add Test Configuration page, enter the name DefaultHTTP and then choose Add Test Configuration.

Choose Add Destinations. Select Azure Endpoints and set the type to Virtual machines. Select Subnet and then enable the WS-VM1 checkbox. Select Add Endpoints.

Choose Add Test Group.

Choose Review and Create and then choose Create.

The screenshot shows the 'Create Connection Monitor' wizard in the Azure portal. The current step is 'Add test group details'. The 'Test groups' tab is selected. On the left, there's a summary of what a test group does and a note about monitoring extensions. The main area shows the configuration for the 'LinuxIPTest' test group:

- Sources:** 1 Item, Azure endpoints (default(rg-alpha), Subscription: Pay-As-You-Go, Resource group: rg-alpha). An 'Edit' link is present.
- Test configurations:** 1 Item, DefaultHTTP. A 'Delete' link is present.
- Destinations:** 1 Item, Azure endpoints (default(rg-alpha), Subscription: Pay-As-You-Go, Resource group: rg-alpha). An 'Edit' link is present.

At the bottom, there are buttons for 'Add sources', 'Add Test configuration', and 'Add destinations'. Below these are navigation buttons: '<< Previous', 'Next : Workspace >>', 'Review + create', 'Cancel', and a large blue 'Add Test Group' button.

## Add work space

Home > Network Watcher | Connection monitor >

### Create Connection Monitor ...

Microsoft

Basics Test groups **Workspace** Create alert Review + create

You can use this section to setup granular control over where you wish to store all the monitoring data generated as part of monitoring tests. [Learn more](#)

Workspace \*  Default (Recommended)  Custom Workspace

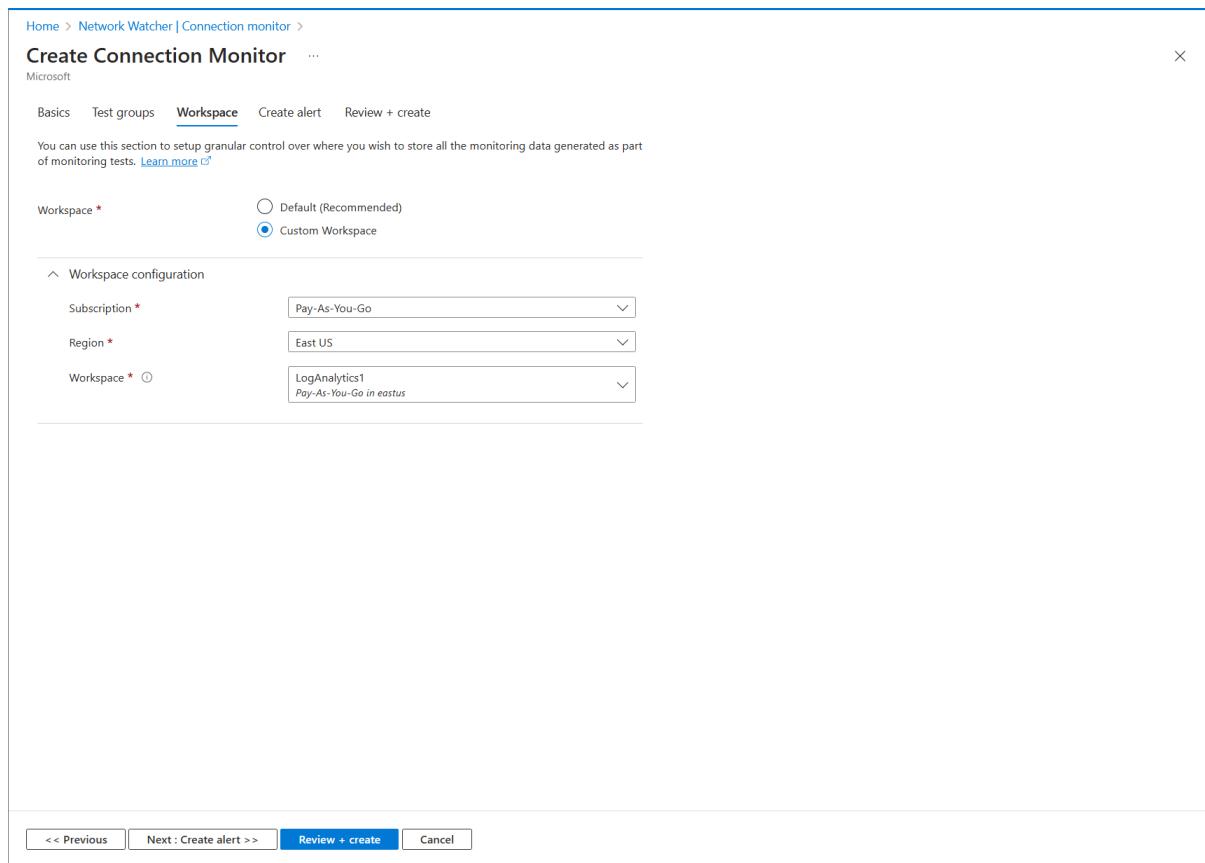
Workspace configuration

Subscription \* Pay-As-You-Go

Region \* East US

Workspace \* LogAnalytics1  
Pay-As-You-Go in eastus

<< Previous Next : Create alert >> **Review + create** Cancel



Click create

Home > Network Watcher | Connection monitor >

## Create Connection Monitor

Microsoft

Basics Test groups Workspace Create alert Review + create

**Primary details**

**Essentials**

|  |                           |
|--|---------------------------|
| Connection Monitor Name : LinuxVMPubIP | Status : Enabled          |
| Subscription : Pay-As-You-Go           | Workspace : LogAnalytics1 |
| Region : East US                       |                           |

**Test groups (1)**

| Name        | Sources ↓         | Destinations ↓    | Test Configurations ↑↓ | Current Cost/Month ↑↓ | Estimated Cost/Mo... ↑↓ | Status ↑↓ | Extension Status ↑↓   |
|-------------|-------------------|-------------------|------------------------|-----------------------|-------------------------|-----------|-----------------------|
| LinuxIPTest | default(rg-alpha) | default(rg-alpha) | DefaultHTTP            | 0                     | \$1.2                   | Enabled   | 1 Auto Enablement *** |

<< Previous Create Cancel Download template

Home > Network Watcher

## Network Watcher | Connection monitor

Microsoft

Search < + Create Refresh Feedback

Overview Get Started Import tests from NPM Migrate Connection Monitors

Newly created Connection Monitors may take 3-5 mins to get monitoring data and show up in the dashboard.

Filter by name 4 selected Scope : 1 Subscriptions & 0 Locations Time : Current Time (30/12/2023, 18:02:22) View by : Connection Monitor

| Fail | Warning | Indeterminate | Not running | Pass        | Alerts fired        |
|------|---------|---------------|-------------|-------------|---------------------|
| 0    | 0       | 1  out of 1   | 0           | 0  out of 1 | 0  out of 0 created |

Connection Monitor Test configurati... Ale.. Protocol Status Reason Last polled

> LinuxVMPubIP ? \*\*\*

- Monitoring
  - Topology
  - Connection monitor (classic)
  - Connection monitor**
  - Network Performance Monitor
- Network diagnostic tools
  - IP flow verify
  - NSG diagnostics
  - Next hop
  - Effective security rules
  - VPN troubleshoot
  - Packet capture
  - Connection troubleshoot
- Metrics
  - Usage + quotas
- Logs
  - Flow logs
  - Diagnostic logs
  - Traffic Analytics

## Tasks 5 - Configure alerts

- Create an action group to send an email
- Create an alert for virtual machine CPU utilization

### Go to Monitor

The screenshot shows the Microsoft Azure Monitor Overview page. On the left, there is a navigation menu with sections like Overview, Activity log, Alerts, Metrics, Logs, Change Analysis, Service health, and Workbooks. Under Insights, there are links for Applications, Virtual Machines, Storage accounts, Containers, Networks, SQL (preview), Azure Cosmos DB, Key Vaults, Azure Cache for Redis, Azure Data Explorer Clusters, Log Analytics workspaces, Azure Stack HCI, Service Bus (preview), Insights Hub, Managed Services, Managed Prometheus, and Azure Managed Grafana. The main content area is titled 'Insights' and 'Detection, triage, and diagnosis'. It features several cards: Application insights, Container Insights, VM Insights, Network Insights, Metrics, Alerts, Logs, Workbooks, Change Analysis, and Diagnostic Settings. A message at the top right states: 'The Log Analytics agents, used by VM Insights, won't be supported as of August 31, 2024. Plan to migrate to VM Insights on Azure Monitor agent prior to this date.'

### Select Alerts in the navigation menu

The screenshot shows the Microsoft Azure Monitor Alerts page. The navigation menu on the left includes the 'Alerts' option under the Insights section. The main area displays a search bar, a subscription ID (8148d5d5-df15-44ef-beb3-5960d3dc42eb), a time range (Past 24 hours), and a 'No grouping' dropdown. Below this, there are filters for Name, Severity, Affected resource, Alert condition, User response, and Fire time. A large green exclamation mark icon indicates 'No alerts found'. A note below it says: 'Try changing your search or choose a different scope level if you don't see what you're looking for.' There is also a 'Clear filters' button.

### Choose Action Groups

The screenshot shows the Azure portal's 'Action groups' page. At the top, there are navigation links: 'Home > Monitor | Alerts > Action groups'. Below the header are several buttons: '+ Create', 'Columns', 'Refresh', 'Open query', 'Delete', 'Enable', 'Disable', and 'Test action group'. A search bar is followed by filters: 'Subscription: Pay-As-You-Go', 'Resource group: all', 'Location: all', 'Status: Enabled', 'Add tag filter', and a dropdown for 'No grouping'. The main table has columns: 'Name ↑↓', 'Short name ↑↓', 'Resource group ↑↓', 'Subscription ↑↓', 'Actions', and 'Status ↑↓'. One row is visible: 'Application Insights Smart Detect...' (Short name: 'SmartDetect'), 'rg-alpha' (Resource group), 'Pay-As-You-Go' (Subscription), '2 Email Azure Resource Manager ...' (Actions), and 'Enabled' (Status). At the bottom left, it says 'Showing 1 - 1 of 1 results.' and at the bottom right is a 'Give feedback' link.

On the **Action Groups** page, choose **Create**.

On the **Basics** page of the Create Action Group wizard, configure the following settings and choose **Next**.

| Property          | Value             |
|-------------------|-------------------|
| Subscription      | Your subscription |
| Resource Group    | rg-alpha          |
| Region            | Global            |
| Action group name | NotifyCPU         |
| Display Name      | NotifyCPU         |

Home > Monitor | Alerts > Action groups >

### Create action group ...

[Basics](#) [Notifications](#) [Actions](#) [Tags](#) [Review + create](#)

An action group invokes a defined set of notifications and actions when an alert is triggered. [Learn more](#)

**Project details**

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription [Pay-As-You-Go](#) [rg-alpha](#) [Create new](#)

Region [Global](#)

**Instance details**

Action group name \* [NotifyCPU](#)

Display name \* [NotifyCPU](#) The display name is limited to 12 characters

[Review + create](#) [Previous](#) [Next: Notifications >](#)

On the Notifications page, set the notification type to Email/SMS message/Push/Voice and the Name to NotificationEmail. Choose the Edit (pencil) icon

On the Email/SMS message/Push/Voice enable the email checkbox and enter the address prime@fabrikam.com. Choose OK.

Home > Monitor | Alerts > Action groups >

### Create action group ...

[Basics](#) [\*\*Notifications\*\*](#) [Actions](#) [Tags](#) [Review + create](#)

Choose how to get notified when the action group is triggered. This step is optional.

| Notification type            | Name | Selected |
|------------------------------|------|----------|
| Email/SMS message/Push/Voice |      |          |
|                              |      |          |

**Email/SMS message/Push/Voice**

Add or edit Email/SMS message/Push/Voice action

Email  
Email \* prime@fabrikam.com

SMS (Carrier charges may apply)  
Country code 1  
Phone number

Azure mobile app notification  
Azure account email

Voice  
Country code 1  
Phone number

Enable the common alert schema. [Learn more](#)

Yes  No

**OK**

[Review + create](#) [Previous](#) [Next: Actions >](#)

Enable the common alert schema. [Learn more](#)

Yes  No

**OK**

## Choose Review and Create. Choose Create

Home > Monitor | Alerts >

### Action groups

| Action groups  |               |  |   |                                    |   |  |
|--|---------------|--|---|------------------------------------|---|---|
|  Create  Columns  Refresh  Open query  Delete  Enable  Disable  Test action group  |               |  |   |                                    |   |   |
|  Search  Subscription : Pay-As-You-Go  Resource group : all  Location : all  Status : Enabled  Add tag filter  No grouping  |               |  |   |                                    |   |   |
| Name ↑↓  | Short name ↑↓ | Resource group ↑↓  | Subscription ↑↓   | Actions                            | Status ↑↓   |   |
| <input type="checkbox"/> Application Insights Smart Detecti...   | SmartDetect   |  rg-alpha |  Pay-As-You-Go | 2 Email Azure Resource Manager ... |  Enabled |  |

## Create an alert for virtual machine CPU utilization

### Go to rg-alpha resource group

Microsoft Azure  vikaramtirat@outlook.c... DEFAULT DIRECTORY VIKARRA... 

Home > rg-alpha   

 rg-alpha  Resource group

  Manage view  Refresh  Export to CSV  Open query  Assign tags  Move  Delete 

 Overview  JSON View

Subscription (move) : Pay-As-You-Go Deployments : 1 Failed 12 Succeeded

Subscription ID : 8148d5d5-df15-44ef-beb3-5960d3dc42eb Location : East US

Tags (edit) : Add tags

 Resources  Recommendations

Filter for any field... Type equals all × Location equals all ×  Add filter  

Showing 1 to 27 of 27 records.  Show hidden types 

| Name ↑↓  | Type ↑↓                   | Location ↑↓ |
|--|---------------------------|-------------|
|  AppInsightswebsitefyp73mfn5xq4                     | Application Insights      | East US     |
|  Application Insights Smart Detection               | Action group              | Global      |
|  AppServicePlan-AzureLinuxApp2023                   | App Service plan          | East US     |
|  AppServicePlan-AzureLinuxAppny2024                 | App Service plan          | East US     |
|  AzureLinuxAppny2024-webapp                         | App Service               | East US     |
|  AzureLinuxAppny2024-webapp                         | Application Insights      | East US     |
|  Failure Anomalies - AppInsightswebsitefyp73mfn5xq4 | Smart detector alert rule | Global      |
|  Failure Anomalies - AzureLinuxAppny2024-webapp     | Smart detector alert rule | Global      |
|  hostingplanfyp73mfn5xq4                            | App Service plan          | East US     |
|  IaaSVMCollectionEndpoint                           | Data collection endpoint  | East US     |
|  Linux-VM2  | Virtual machine           | East US     |
|  Linux-VM2-ip                                       | Public IP address         | East US     |
|  Linux-VM2-nsg                                      | Network security group    | East US     |
|  linux-vm2129                                       | Network Interface         | East US     |

< Previous Page 1 of 1 Next > 

choose Linux-VM2

On the Linux-VM2 properties page, choose Alerts under Monitoring

The screenshot shows the Azure portal interface for a virtual machine named 'Linux-VM2'. The left sidebar has sections for Configuration management, Policies, Run command, Monitoring (with Insights and Alerts selected), Workbooks, Automation (Tasks (preview) and Export template), and Help (Resource health, Boot diagnostics, Performance diagnostics, VM Inspector (Preview), Reset password, Redeploy + reapply, Ubuntu Advantage support plan, Serial console, Connection troubleshoot, and Support + Troubleshooting). The main content area is titled 'Set up recommended alert rules' and includes a sub-section for 'Add commonly-used alert rules for resources like this to get notified on important events happening on this resource.' It features two buttons: 'View + set up' and 'Create custom alert rule'. A large green speech bubble icon with an exclamation mark is overlaid on the main content area.

On the Alerts page, choose Create and then choose Alert rule

On the Condition page of the Create an Alert Rule wizard, set the Signal name to Percentage CPU. Use the default settings and choose Next.

The screenshot shows the 'Create an alert rule' wizard on the 'Condition' page. The top navigation bar includes 'Scope', 'Condition' (which is selected), 'Actions', 'Details', 'Tags', and 'Review + create'. Below this, a note says 'Configure when the alert rule should trigger by selecting a signal and defining its logic.' A 'Signal name' dropdown is set to 'Percentage CPU'. To the right, a 'Preview' section shows a line chart titled '\$0.10 USD/month' with the Y-axis ranging from 0% to 90%. The X-axis shows dates from 13 to 17. A red dashed horizontal line is at 80%, and a blue line series shows values like 0.31% and 0.32%. Below the preview are sections for 'Alert logic' (with a note about automatic configuration), 'When to evaluate' (Check every 1 minute, Lookback period 5 minutes), and a '+ Add condition' button. At the bottom are 'Review + create', 'Previous', and 'Next: Actions >' buttons.

On the Actions page, choose Select Action Group

On the Select Action Groups page, choose NotifyCPU and choose Select.

The screenshot shows two overlapping windows. The background window is titled 'Create an alert rule' and has tabs for Scope, Condition, Actions, Details, Tags, and Review + create. The 'Actions' tab is selected. Below it, there's a note: 'An action group is a set of actions that can be applied to an alert rule. [Learn more](#)'. It has buttons for '+ Select action groups' and '+ Create action group'. A note at the bottom says 'No action group selected yet'. The foreground window is titled 'Select action groups' and contains the following text: 'Select up to five action groups to attach to this rule.' It shows a subscription dropdown set to 'Pay-As-You-Go' and a search bar. A table lists action groups: one row for 'Application Insights Smart Det...' (rg-alpha) with 2 Email Azure Resource Manag... Global, and one row for 'NotifyCPU' (rg-alpha) with 1 Email Global. The 'NotifyCPU' row has a checked checkbox. At the bottom right of the dialog is a 'Select' button. Navigation buttons at the bottom of the dialog are 'Review + create', 'Previous', 'Next: Details >', and a URL 'https://portal.azure.com/#'

On the Details page enter the Alert rule name HighCPU. Choose Review and Create and then choose Create.

The screenshot shows the 'Create an alert rule' page with the 'Details' tab selected. It has sections for 'Project details' and 'Alert rule details'. In 'Project details', 'Subscription' is set to 'Pay-As-You-Go' and 'Resource group' is set to 'rg-alpha'. In 'Alert rule details', 'Severity' is set to '2 - Warning', 'Alert rule name' is set to 'HighCPU', and 'Alert rule description' is set to 'HighCPU'. There's a 'Advanced options' section with a collapsed arrow. Navigation buttons at the bottom are 'Review + create', 'Previous', 'Next: Tags >', and a URL 'https://portal.azure.com/#'