

Azure Monitor Project

Project Summary

Configuring monitoring of various workloads and infrastructure services using Azure Monitor

- Deploying and configuring Log Analytics.
- Configuring monitoring for Web apps.
- Monitoring compute and networking services.
- Configuring alerts.

Task	Task List
Deploy Log Analytics	<ul style="list-style-type: none">• Create a Log Analytics workspace.• Configure Log Analytics data retention and archive policies.• Enable access to a Log Analytics workspace.
Monitor web apps	<ul style="list-style-type: none">• Enable Application Insights.• Disable logging for .NET core snapshot debugger.• Configure Web apps to be written to a Log Analytics workspace.• Enable file and configuration tracking for web apps.
Configure monitoring for compute services	<ul style="list-style-type: none">• 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.
Configure alerts	<ul style="list-style-type: none">• Create an action group to send an email.• Create an alert for VM CPU utilization.

Tasks 1: Prepare your Azure environment

- **Create App Log Examiners security Group**
- **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 sidebar with navigation links like Home, Resource groups, Default Directory, Create, Manage view, Delete resource group, Refresh, Export to CSV, Open query, and JSON View. The main area is titled "rg-alpha" and shows the "Overview" tab. It displays basic information: Subscription (Pay-As-You-Go), Subscription ID (8148d5d5-df15-44ef-beb3-5960d3dc42eb), and Location (East US). There are sections for "Essentials" (Deployment, Access control (IAM), Tags, Resource visualizer, Events) and "Resources". The "Resources" section has filters for Type (equals all), Location (equals all), and a dropdown for List view. Below the filters, it says "Showing 0 to 0 of 0 records." and "No resources match your filters". It includes a "Clear filters" button and a "Learn more" link. At the bottom right, 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 ...

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

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

Home > Default Directory | Groups >

Groups | All groups ...

Default Directory - Microsoft Entra ID

All groups Deleted groups Diagnose and solve problems

New group Download groups Refresh Manage view Delete Got feedback?

Azure Active Directory is now Microsoft Entra ID. Learn more

Search Add filter

Search mode Contains

1 group found

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

All groups Deleted groups Diagnose and solve problems

General Expiration Naming policy

Privileged Identity Management Access reviews Audit logs Bulk operation results

New support request

Next step creates windows VM

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

Home > Virtual machines >

Create a virtual machine ...

⚠️ Changing Basic options may reset selections you have made. Review all options prior to creating the 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

Instance details

Virtual machine name: WS-VM1

Region: (US) East US

Availability options: No infrastructure redundancy required

Security type: Standard

Image: Windows Server 2022 Datacenter: Azure Edition - x64 Gen2

VM architecture: Arm64 (selected), x64

Arm64 is not supported with the selected image.

Review + create < Previous Next : Disks > Give feedback

One VM Created go to networking and add following rule.

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

WS-VM1 | Networking ⚡

Virtual machine

Search Feedback Attach network interface Detach network interface

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

Settings

Networking (selected)

Connect Windows Admin Center Disks Size Microsoft Defender for Cloud Advisor recommendations Extensions + applications Availability + scaling Configuration Identity Properties Locks

Operations

Bastion Auto-shutdown Backup Disaster recovery Updates

<https://portal.azure.com/#home>

Add inbound security rule

WS-VM1-nsg

Source: Any

Source port ranges: *

Destination: Any

Service: HTTP

Destination port ranges: 80

Protocol: TCP

Action: Allow

Priority: 310

Name: AllowAnyHTTPinbound

Description: AllowAnyHTTPinbound

Add Cancel Give feedback

Microsoft Azure Search resources, services, and docs (G+/-) vikaramtirat@outlook.com DEFAULT DIRECTORY

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

WS-VM1 | Networking

Virtual machine

Search Feedback Attach network interface Detach network interface

ws-vm1609

IP configuration ipconfig1 (Primary)

Network Interface: ws-vm1609 Effective security rules Troubleshoot VM connection issues Topology

Virtual network/subnet: WS-VM1-vnet/default NIC Public IP: 20.232.113.215 NIC Private IP: 10.0.0.4 Accelerated networking: Enabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group WS-VM1-nsg (attached to network interface: ws-vm1609) Impacts 0 subnets, 1 network interfaces Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action
300	RDP	3389	TCP	Any	Any	Allow
310	AllowAnyHTTPInbound	80	TCP	Any	Any	Allow
65000	AllowNetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

Need help?

Understand Azure load balancing Learn more

Quickstart: Create a public load balancer to load balance Virtual Machines Learn more

Quickstart: Direct web traffic with Azure Application Gateway Learn more

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 Change

Just-in-time policy Unsupported by plan Change

Most common

Native RDP
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

Connect from your local machine (Windows)

Switch local machine OS

1 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

2 Open Remote Desktop Connection (on Windows)

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

3 Download and open the RDP file

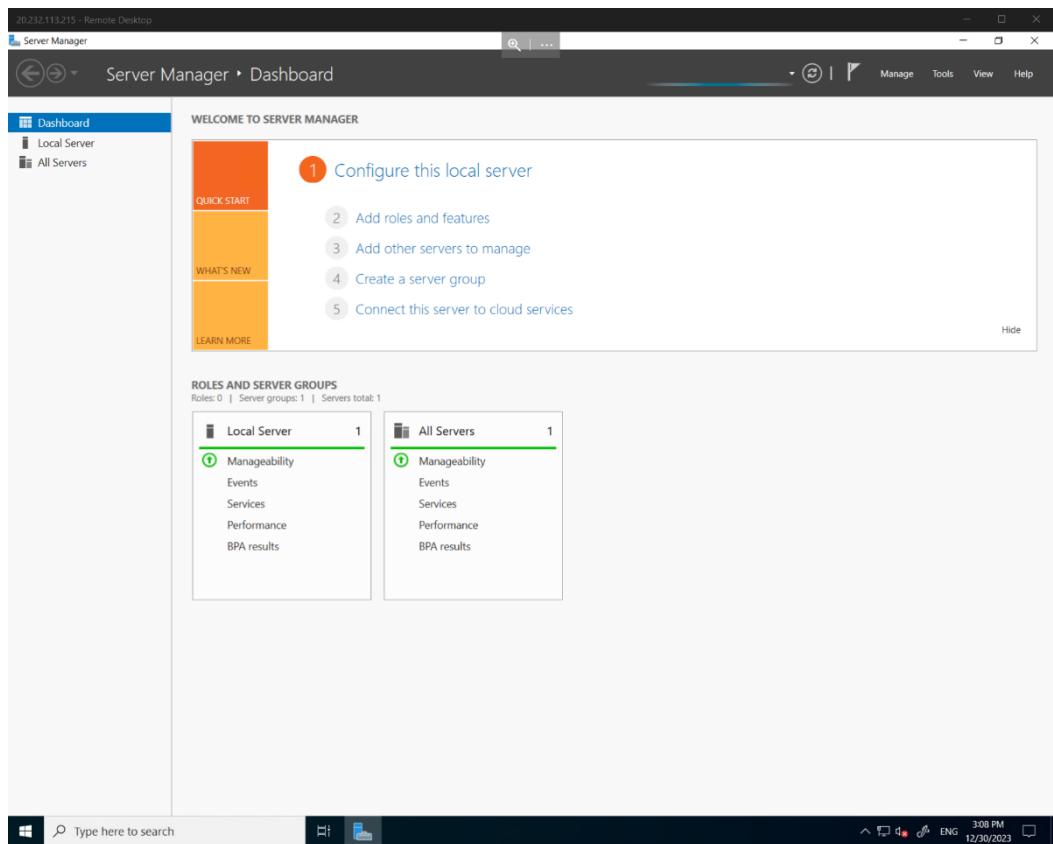
Download and open the RDP file to connect to the virtual machine.

Username prime Download RDP file

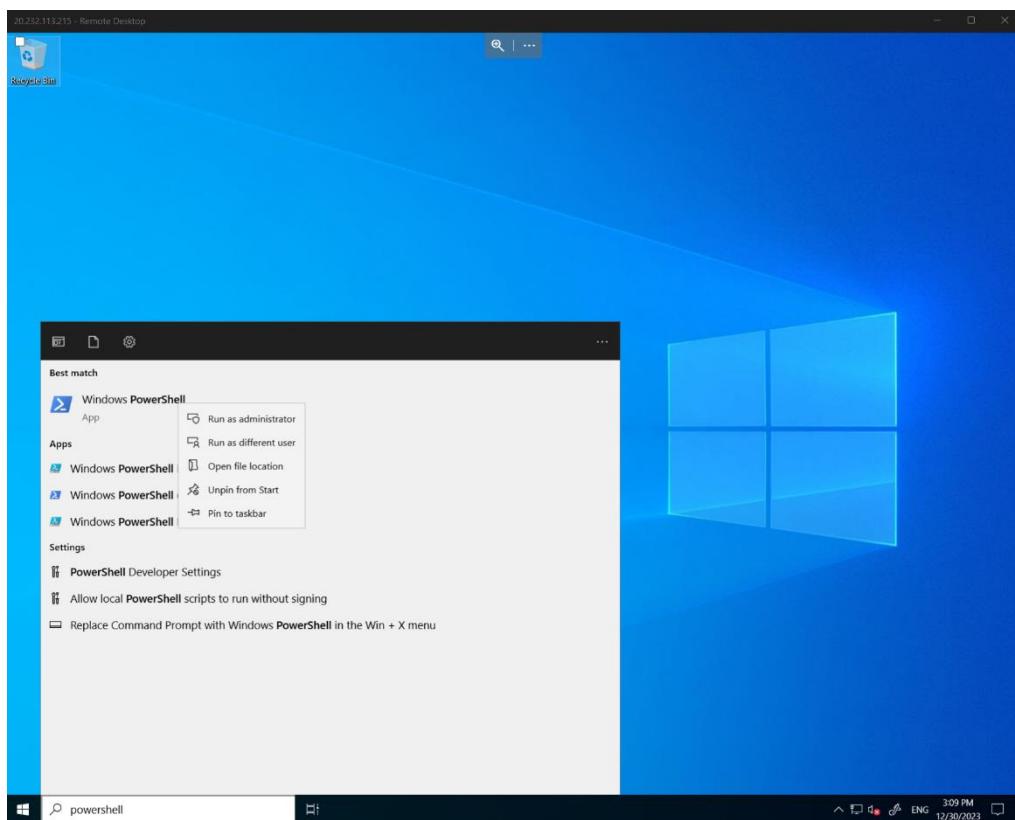
Other Information

Forgot password? Reset password

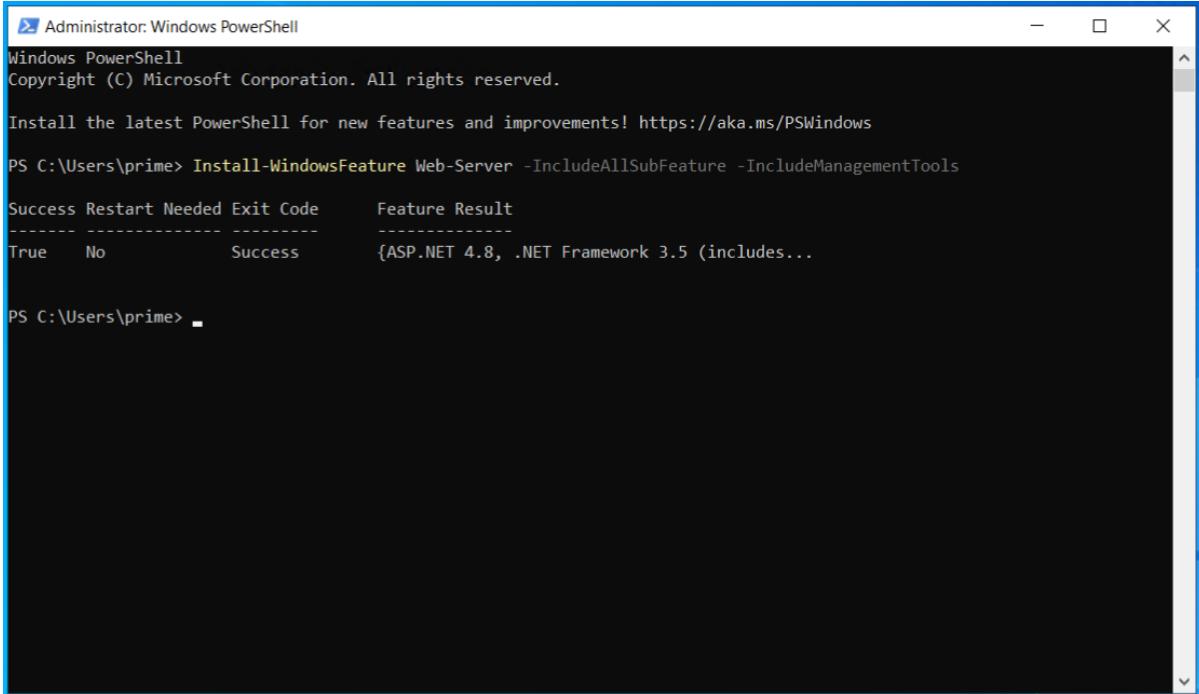
Close Troubleshooting Give feedback



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



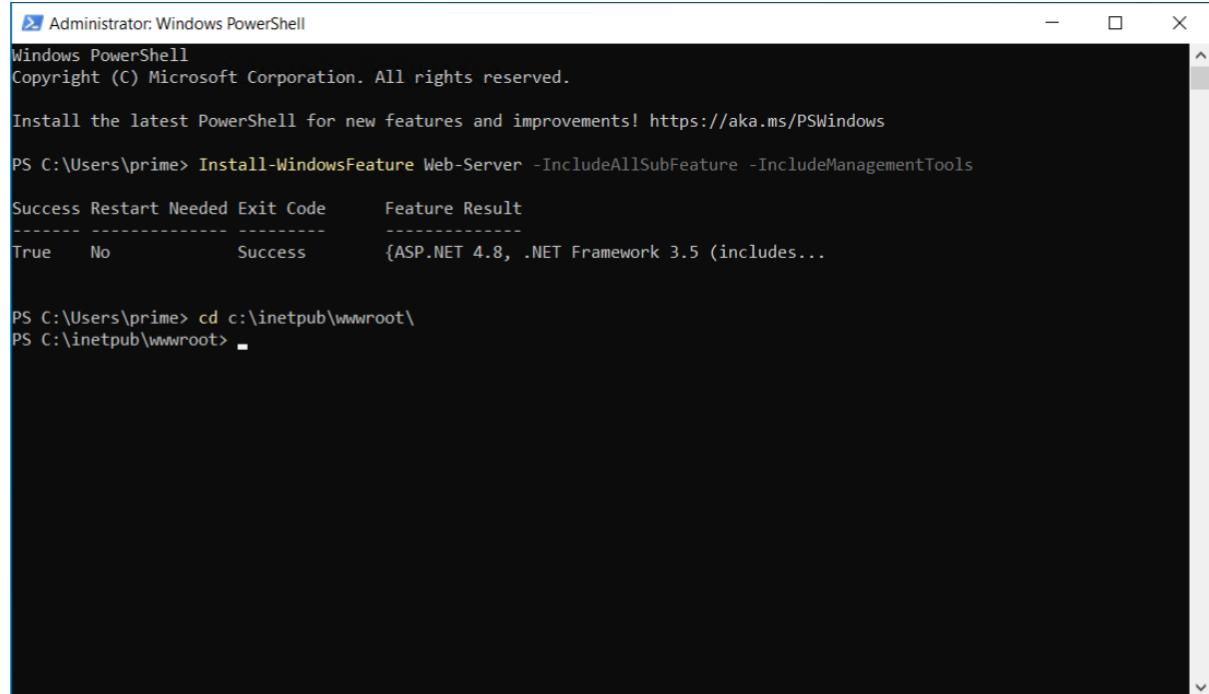
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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...
```

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.

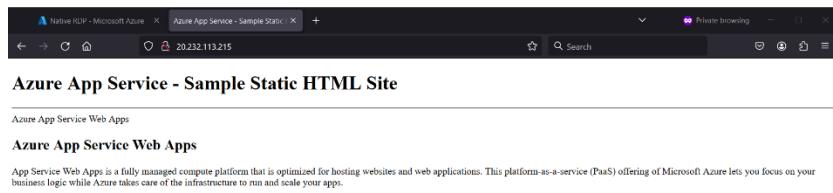
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

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



Deploy and configure linux server vm - LX-VM2

Home > Virtual machines >

Create a virtual machine ...

X

[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 * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Virtual machine name * ⓘ

Region * ⓘ

Availability options ⓘ

Security type ⓘ

Image * ⓘ

[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 ⓘ Arm64 x64

Run with Azure Spot discount ⓘ

Size * ⓘ [See all sizes](#)

[Enable Linux maintenance mode](#)

[Review + create](#)

[< Previous](#)

[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.

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

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

network watcher

Network Watcher Agent for Linux

Microsoft Corp.

Azure Network Watcher is a network performance monitoring, diagnostic and analytics service that enables you to monitor your network in Azure

Network Watcher Agent for Linux

Publisher: Microsoft Corp.

Overview

Azure Network Watcher is a service that helps you monitor, diagnose, and gain insights to your network performance and health. This virtual machine extension enables you to capture network traffic and leverage other advanced functionality provided by the Network Watcher service.

By clicking the Create button, I acknowledge that I am getting this software from Microsoft Corp. and that the [legal terms](#) of Microsoft Corp. apply to it.

Next

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

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.Network...	1.1*	Provisioning succeeded	Disabled

Settings

- Networking
- Connect
- Disks
- Size
- Microsoft Defender for Cloud
- Advisor recommendations
- Extensions + applications**
- Availability + scaling
- Configuration
- Identity
- Properties
- Locks

Operations

- Bastion
- Auto-shutdown
- Backup
- Disaster recovery
- Updates
- Health monitoring
- Inventory

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.Network...

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/r-g-alpha/providers...`

One enabled you should see Automatic upgrade status changed to enabled

The screenshot shows the Azure portal interface for a virtual machine named "Linux-VM2". The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Networking, Connect, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations), Extensions + applications (selected), Availability + scaling, Configuration, Identity, Properties, Locks, and Operations (Bastion, Auto-shutdown, Backup, Disaster recovery, Updates, Health monitoring, Inventory). The main content area is titled "Extensions + applications" and shows a table with one item:

Name	Type	Version	Status	Automatic upgrade status
AzureNetworkWatcherExtension	Microsoft.Azure.Network... (1.0)	1.0	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 a GitHub repository page for "azur... / azure-quickstart-templates" with the "Code" tab selected. The repository has 935 issues, 71 pull requests, 11 actions, 1 project, 1 wiki, 1 security, and 13.5k stars. The "web-app-sql-database" branch is selected. The README.md file content is as follows:

```
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.
```

The repository also contains files like README.md, azuredeploy.json, azuredeploy.parameters.json, main.bicep, and metadata.json. The metadata.json file contains the following table:

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

On the GitHub page, choose Deploy to Azure

Provision a Web App with a SQL Database

Azure Public Test Date 2023.11.23 Azure Public Test Result pass
Azure US Gov Test Date 2023.12.29 Azure US Gov Test Result pass
Best Practice Check fail CredScan Check Not Tested
Bicep Version 0.24.24

[Deploy to Azure](#) [Deploy to Azure Gov](#) [Visualize](#)

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:

Microsoft App Services

- [App Service Pricing](#)

Microsoft SQL

- [SQL Database Pricing](#)

For more information about using this template, see [Provision a web app with a SQL Database](#).

Microsoft Learn Resources

- [Learn SQL Server](#)
- [Learn App Services](#)

Tags: 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 * [*****](#)
Location [\[resourceGroup\(\).location\]](#)

[Previous](#) [Next](#) [Review + create](#)

After the deployment completes, choose Go to resource group

The screenshot shows the Azure Resource Group Overview page for 'rg-alpha'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Deployments, Security, Deployment stacks, Policies, Properties, Locks, Cost Management, Monitoring, Insights (preview), Alerts, Metrics, Diagnostic settings, Logs, Advisor recommendations, and Workbooks. The main content area displays the 'Essentials' section with details about the subscription (move to Pay-As-You-Go, ID: 8148d5d5-df15-44ef-beb3-5960d3dc42eb), deployments (4 succeeded), and location (East US). Below this is the 'Resources' section, which lists 16 resources. The table includes columns for Name, Type, and Location. Resources listed include Application Insights, App Service plan, Virtual machine, Public IP address, Network security group, Network Interface, Disk, SQL database, SQL server, App Service, Virtual machine, Public IP address, Network security group, and Virtual network. All resources are located in East US.

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 the Microsoft Learn - Code Samples page for the 'Deploy a basic Linux web app' code sample. The top navigation bar includes links for Microsoft, Learn, Documentation, Training, Credentials, Q&A, Code Samples, Assessments, and Shows. A search bar and sign-in link are also present. The main content area features a large heading 'Deploy a basic Linux web app' with a 'Code Sample' link and a '11/30/2022' timestamp. Below the heading are several status indicators: 'Azure Public Test Date' (2023.12.29), 'Azure Public Test Result' (pass); 'Azure US Gov Test Date' (2023.12.21), 'Azure US Gov Test Result' (pass); 'Best Practice Check' (pass); 'CredScan Check' (Not Tested); and 'Bicep Version' (0.24.24). At the bottom of the page, there are three buttons: 'Deploy to Azure', 'Deploy to Azure Gov', and 'Visualize'. A note below the buttons states: 'This template allows you to deploy an app service plan and a basic Linux web app.' A 'Tags' box at the bottom lists 'Microsoft.Web/serverfarms, Microsoft.Web/sites'.

On the GitHub page, choose Deploy to Azure

Home >

Deploy a basic Linux web app

Azure quickstart template

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

Basics Review + create

Template

webapp-basic-linux 2 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

Web App Name AzureLinuxApp2023

Sku S1

Linux Fx Version php|7.4

Location [resourceGroup().location]

Previous Next Review + create

Review the information and choose Create

Home >

Deploy a basic Linux web app

Azure quickstart template

Basics Review + create

Summary

webapp-basic-linux 2 resources

Terms

Azure Marketplace Terms | Azure Marketplace

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

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

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

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

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Basics

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]

Previous Next Create

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

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

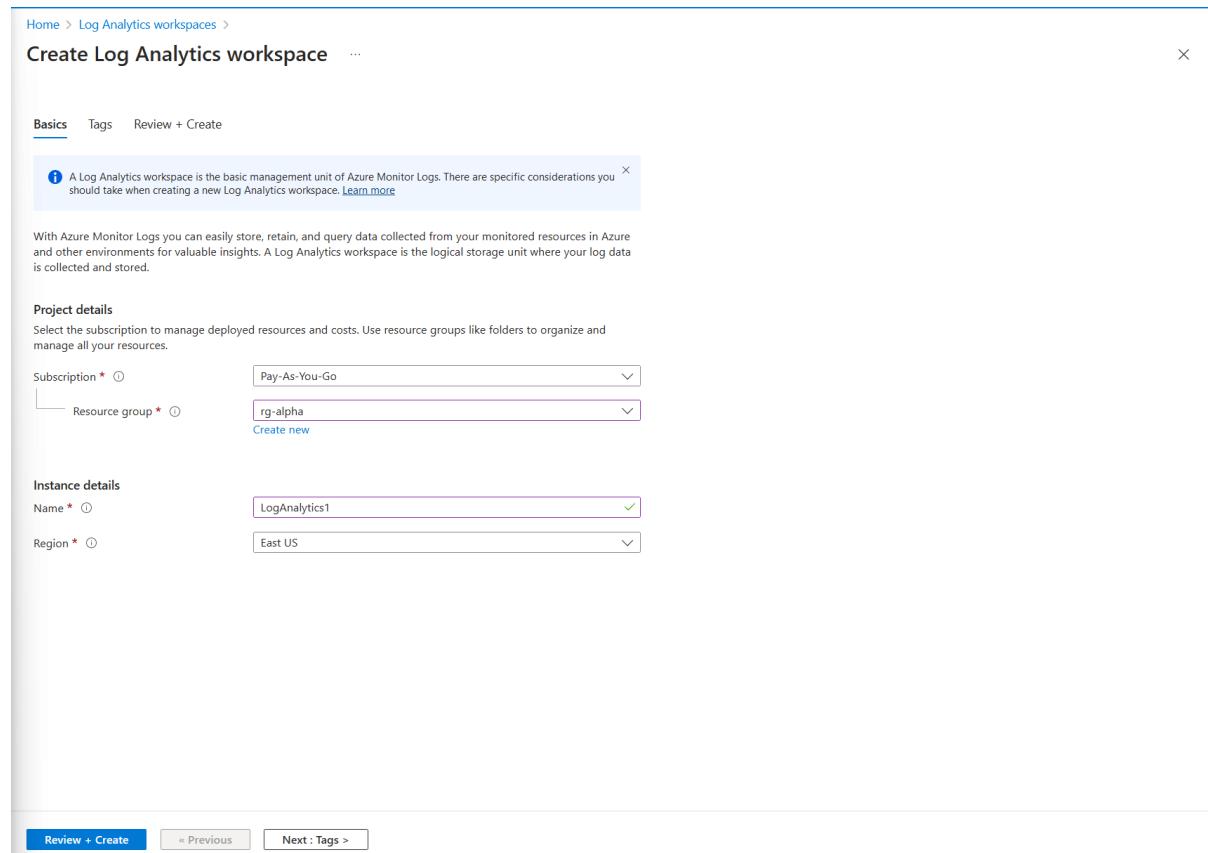
Create new

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

The screenshot shows the 'Log Analytics workspaces' page in the Azure portal. A single workspace, 'LogAnalytics1', is listed. It is associated with a resource group 'rg-alpha', located in 'East US', and is part of the 'Pay-As-You-Go' subscription. The page includes standard filtering and sorting options, and a 'Give feedback' link at the bottom right.

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 'LogAnalytics1' workspace overview page. The 'Usage and estimated costs' section is selected. It displays the workspace's name, location (East US), and subscription information. A note indicates that MMAOMS support will end on August 31, 2024. The page also includes sections for 'Essentials', 'Get started with Log Analytics', and 'Select Data' (which is highlighted).

Retention and set the slider to 60 days. Choose OK

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

Daily cap

You can control your costs by applying a cap to the amount of data that you collect per day. Note that there can be some latency in applying the daily cap, so stopping data ingestion precisely at the specified cap cannot be guaranteed.

ON OFF

⚠ Be sure to create an alert so you know if your workspace is capped. [Learn more](#)

The daily volume cap is:

10 GB/day

Daily limit will be set at: 22:00 UTC

OK

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

The screenshot shows the 'Log Analytics workspaces' page in the Azure portal. The search bar at the top contains 'Log Analytics workspaces'. Below the search bar, there are several filter buttons: 'Subscription equals all', 'Resource group equals all', 'Location equals all', and 'Assign tags'. The main table displays one record: 'LogAnalytics1'. The columns for this record are: Name (LogAnalytics1), Resource group (rg-alpha), Location (East US), and Subscription (Pay-As-You-Go). The table has sorting icons for each column. At the bottom of the page, there are navigation links for 'Page 1 of 1' and a 'Give feedback' button.

Select Access control (IAM)

The screenshot shows the 'Access control (IAM)' page for the LogAnalytics1 workspace. The left sidebar lists various workspace settings like Overview, Activity log, Tags, and Logs. The 'Access control (IAM)' option is selected and highlighted. The main content area is titled 'LogAnalytics1 | Access control (IAM)'. It features a navigation bar with 'Check access', 'Role assignments', 'Roles', 'Deny assignments', and 'Classic administrators'. The 'Check access' tab is active. Below it, there's a section for 'My access' with a 'View my access' button. Another section for 'Check access' allows reviewing access levels for users, groups, service principals, or managed identities. There are three boxes: 'Grant access to this resource' (with a 'Add role assignment' button), 'View access to this resource' (with a 'View' button), and 'View deny assignments' (with a 'View' button). At the bottom of the page, there are navigation links for 'Page 1 of 1'.

Choose Add and then choose Add role assignment

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

Log Analytics work... Default Directory

+ Create Open recycle bin ...

Filter for any field... Name ↑

LogAnalytics1

Access control (IAM) Overview Activity log Add role assignment Add co-administrator

Tags Diagnose and solve problems Logs 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

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)

Page 1 of 1

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

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

Add role assignment ...

Role Members Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Assignment type

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Search by role name, description, or ID Type : All Category : All

Name ↑	Description ↑	Type ↑	Category ↑	Details
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
App Compliance Automation Administr...	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
LocalNGFirewallAdministrator 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
Log Analytics Reader	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

Review + assign Previous Next Feedback

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

The screenshot shows the 'Add role assignment' page in the Azure portal. The 'Members' tab is selected. The 'Selected role' is set to 'Log Analytics Reader'. Under 'Assign access to', 'User, group, or service principal' is selected. The 'Members' section shows a table with columns: Name, Object ID, and Type. A note says 'No members selected'. Below the table is a 'Description' field with 'Optional' entered. On the right, a modal window titled 'Select members' lists two users: 'bob.hotel' and 'Vikar Ramtirat'. 'Vikar Ramtirat' is highlighted with a pink circle. The 'Selected members' section contains 'App Log Examiners' with a red square icon. Buttons at the bottom include 'Review + assign', 'Previous', 'Next', 'Select', and 'Close'.

On the Members space, choose Review + Assign

The screenshot shows the 'Add role assignment' page in the Azure portal. The 'Review + assign' tab is selected. The 'Selected role' is set to 'Log Analytics Reader'. Under 'Assign access to', 'User, group, or service principal' is selected. The 'Members' section shows a table with one entry: 'App Log Examiners' (Object ID: d0acc8d8-3a22-4259-906a-f80994371fd, Type: Group). Below the table is a 'Description' field with 'Optional' entered. At the bottom, there are buttons for 'Review + assign', 'Previous', 'Next', and 'Feedback'.

The role with security group has been added under role assignments

Home > Log Analytics workspaces > LogAnalytics1

Log Analytics work... Default Directory

LogAnalytics1 | Access control (IAM)

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

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
App Log Examiner	Group	Log Analytics Reader	This resource	None

Page 1 of 1

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

Home > rg-alpha < ...

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

Overview

Essentials

Subscription (move) : Pay-As-You-Go
Subscription ID : 8148d5d5-df15-44ef-beb3-5960d3dc42eb
Tags (edit) : Add tags

Deployments : 1 Failed 7 Succeeded
Location : East US

Resources Recommendations

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

No grouping List view

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	...
Failure Anomalies - AppInsightswebsitefyp73mfn5xq4	Smart detector alert rule	Global	...
hostingplanfyp73mfn5xq4	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	...
sampledbs (sqlServerfyp73mfn5xq4/sampledbs)	SQL database	East US	...

< Previous Page 1 of 1 Next >

Give feedback

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, which is prominently featured. 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 managing 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 displays the Application Insights settings, including fields for 'New resource name' (set to 'AzureLinuxAppny2024-webapp') and 'Location' (set to 'East US'). Below these fields is a dropdown for 'Log Analytics Workspace' containing 'LogAnalytics1 [eastus]'. A note at the top states: '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.' A modal dialog titled 'Apply monitoring settings' is overlaid on the page, containing the text: '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?' with 'Yes' and 'No' buttons, and an 'Apply' button at the bottom.

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 managing 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 displays the Application Insights settings, including tabs for 'Info', '.NET', '.NET Core', 'Node.js', 'Java', and 'Python'. A note at the top of the 'Info' tab states: 'Your app is connected to Application Insights resource: AzureLinuxAppny2024-webapp'. Another note below it says: '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](#)'.

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

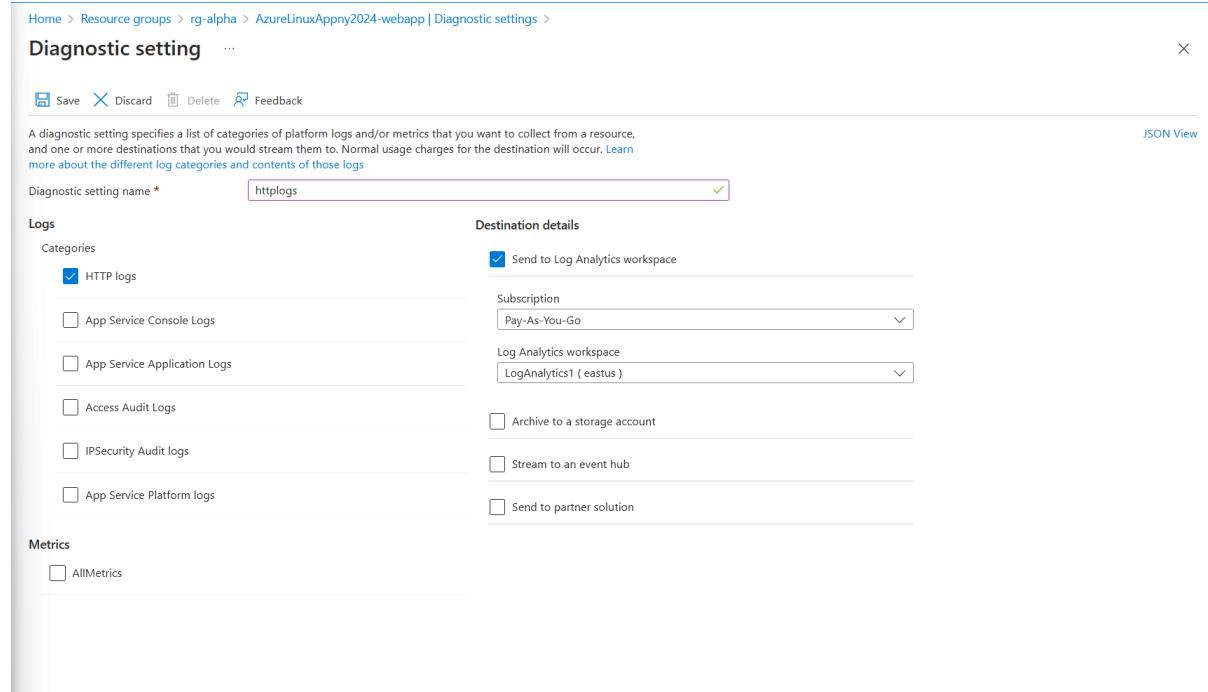
Access Audit Logs Archive to a storage account

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'), 'Monitoring' (with links to 'Open Azure Data Studio', 'Open in Visual Studio', and 'Open in Visual Studio Code'), and a 'Start working with your database' section.

Under Monitoring, choose Diagnostic settings

The screenshot shows the 'Diagnostic settings' configuration 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' link which is highlighted. The main content area explains what diagnostic settings are used for and provides a table to add new settings. A note at the bottom lists the types of logs and metrics that can be collected, such as SQL Insights, Automatic tuning, Query Store Runtime Statistics, Errors, Database Wait Statistics, 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

The screenshot shows the 'Diagnostic setting' configuration page for a resource group. At the top, there are buttons for Save, Discard, Delete, and Feedback. To the right, there is a 'JSON View' link. The main area is divided into sections: 'Logs' and 'Metrics'. Under 'Logs', there are 'Category groups' (allLogs, audit) and 'Categories' (SQL Insights, Automatic tuning, Query Store Runtime Statistics, Query Store Wait Statistics, Errors, Database Wait Statistics, Timeouts, Blocks, Deadlocks). Under 'Metrics', there are Basic, InstanceAndAppAdvanced, and WorkloadManagement. On the right side, under 'Destination details', there is a section for 'Subscription' (Pay-As-You-Go) and 'Log Analytics workspace' (LogAnalytics1 (eastus)). There are also checkboxes for 'Send to Log Analytics workspace', 'Archive to a storage account', 'Stream to an event hub', and '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). The main content area displays a table with one record: 'IaaSVMCollectionEndpoint'. The table has columns for Name, Subscription, Resource group, and Location. The row for 'IaaSVMCollectionEndpoint' shows 'Name' as 'IaaSVMCollectionEndpoint', 'Subscription' as 'Pay-As-You-Go', 'Resource group' as 'rg-alpha', and 'Location' as 'East US'. There are also filter buttons at the top and bottom of the table, and a 'Give feedback' link at the bottom right.

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 <input type="radio"/> Linux <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 the endpoints 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

Home > Monitor | Data Collection Rules >

Create Data Collection Rule

...
Data collection rule management

Basics Resources **Collect and deliver** Tags Review + create

Configure which data sources to collect, and where to send the data to.

+ Add data source

Data source	Destination(s)
No standard data sources or destinations found.	

✖ This data collection rule doesn't have any data sources or destinations selected.

Add data source

* Data source **Destination**

Select the destination(s) for where the data will be delivered. Normal usage charges for the destination will occur. [Learn more about pricing.](#)

+ Add destination

* Destination type Subscription Account or namespace

Azure Monitor Logs Pay-As-You-Go LogAnalytics1 (rg-alpha)

Review + create < Previous Next : Tags > Add data source < Previous 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 shows a table with one record: WinVMDCR, Pay-As-You-Go, rg-alpha, East US, Windows Event Logs, Azure Monitor Logs, and Windows. The 'Data Collection Rules' link in the sidebar is highlighted.

Choose the WinVMDCR rule in rg-alpha

Under Configuration, choose Data Sources

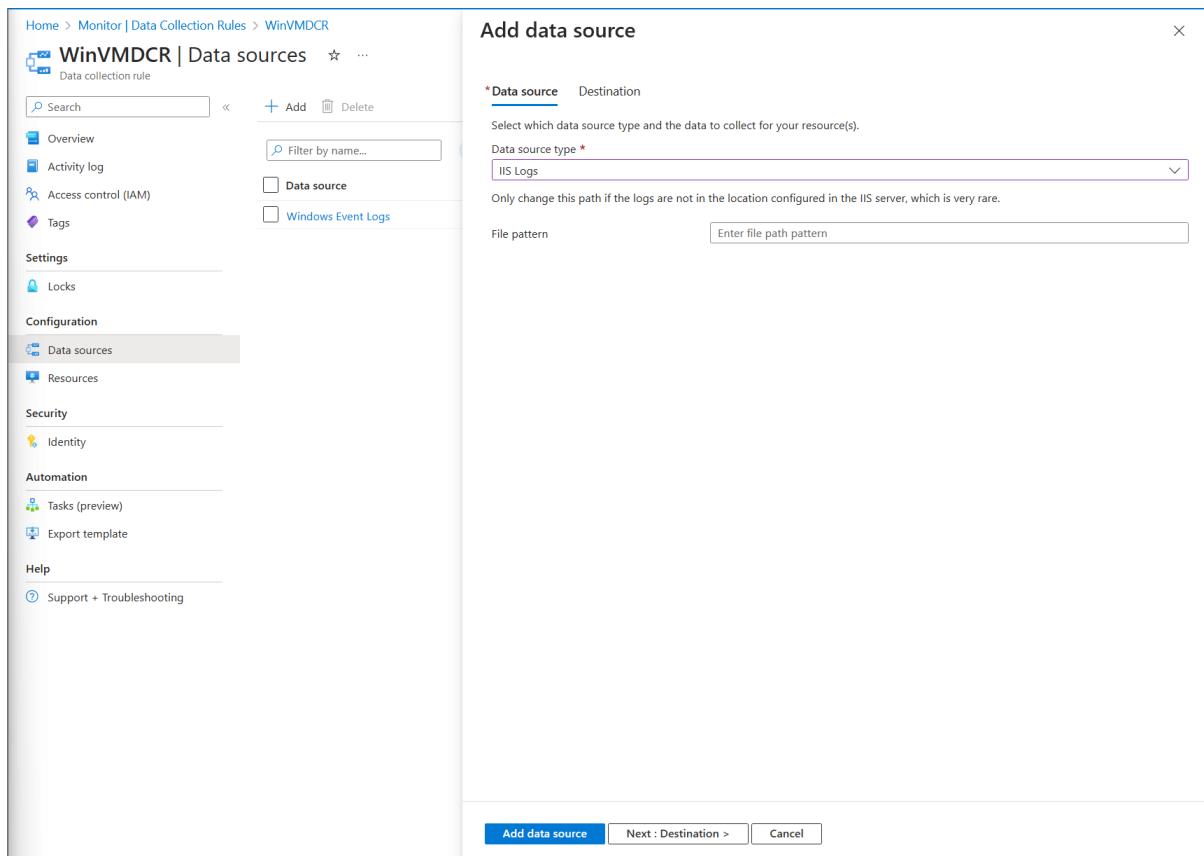
The screenshot shows the WinVMDCR Data sources configuration page. The left sidebar has sections for Overview, Activity log, Access control (IAM), Tags, Settings (Locks), Configuration (Data sources, Resources), Security (Identity), Automation (Tasks (preview), Export template), and Help (Support + Troubleshooting). The 'Data sources' link in the Configuration section is highlighted. The main content area shows a table with two rows: 'Data source' (selected) and 'Windows Event Logs'. The 'Destination(s)' column shows 'Azure Monitor Logs' for both rows. A 'Filter by name...' search bar and a 'Destination : all' dropdown are also present.

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 navigation sidebar with sections 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' section is currently selected.

The main area is titled 'Add data source' and has a tab bar with 'Data source' (selected) and 'Destination'. Below this, 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 table for selecting destinations:

* Destination type	Subscription	Account or namespace
Azure Monitor Logs	Pay-As-You-Go	LogAnalytics1 (rg-alpha)

At the bottom 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 search bar and a user profile. The main area has a title 'Network Watcher' with a 'Microsoft' logo. Below it is a toolbar with buttons for 'Create', 'Add', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', and 'Disable'.

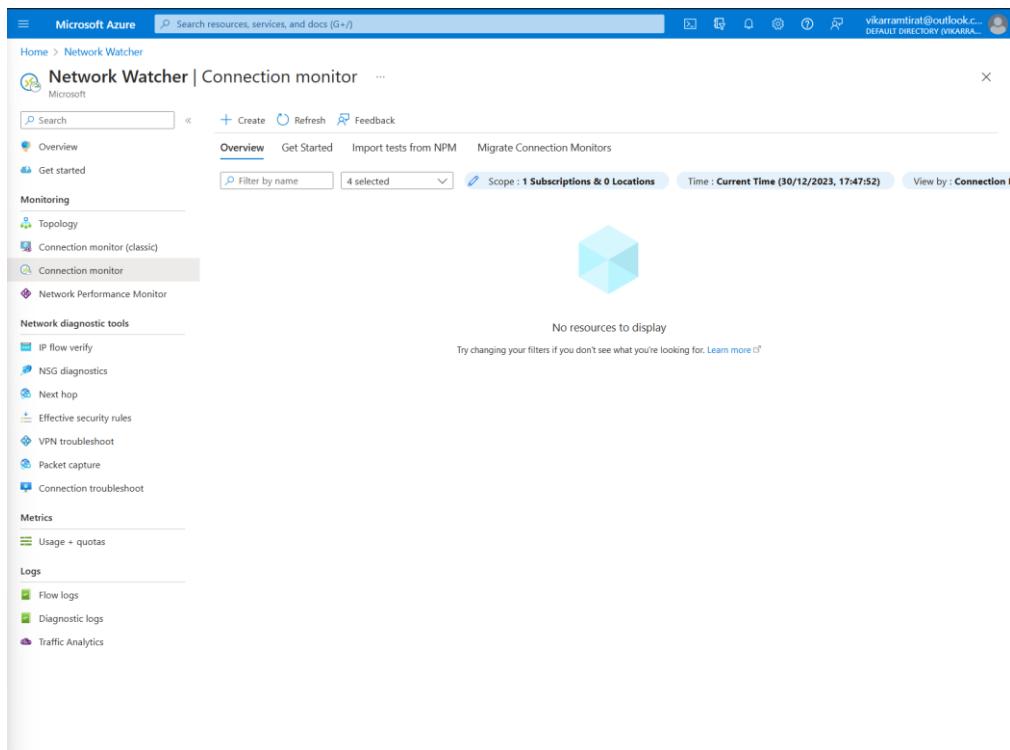
The main content area has a table header with filters: 'Filter for any field...', 'Subscription equals all', 'Resource group equals all', 'Location equals all'. It shows one record: 'Name' is 'NetworkWatcher_eastus', 'Subscription' is 'Pay-As-You-Go', and 'Location' is 'East US'. There are buttons for 'No grouping' and 'List view'.

The left sidebar 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, 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. In the center, the 'Test group name' is set to 'LinuxIPTest'. Below it, under 'Sources', there's one item: 'Azure endpoints' (default(rg-alpha), Subscription: Pay-As-You-Go, Resource group: rg-alpha). Under 'Test configurations', there's one item: 'DefaultHTTP'. Under 'Destinations', there's one item: 'Azure endpoints' (default(rg-alpha), Subscription: Pay-As-You-Go, Resource group: rg-alpha). At the bottom, there are buttons for 'Add sources', 'Add Test configuration', and 'Add destinations'. At the very bottom, there are 'Review + create' and 'Cancel' buttons, with 'Add Test Group' being the primary action 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

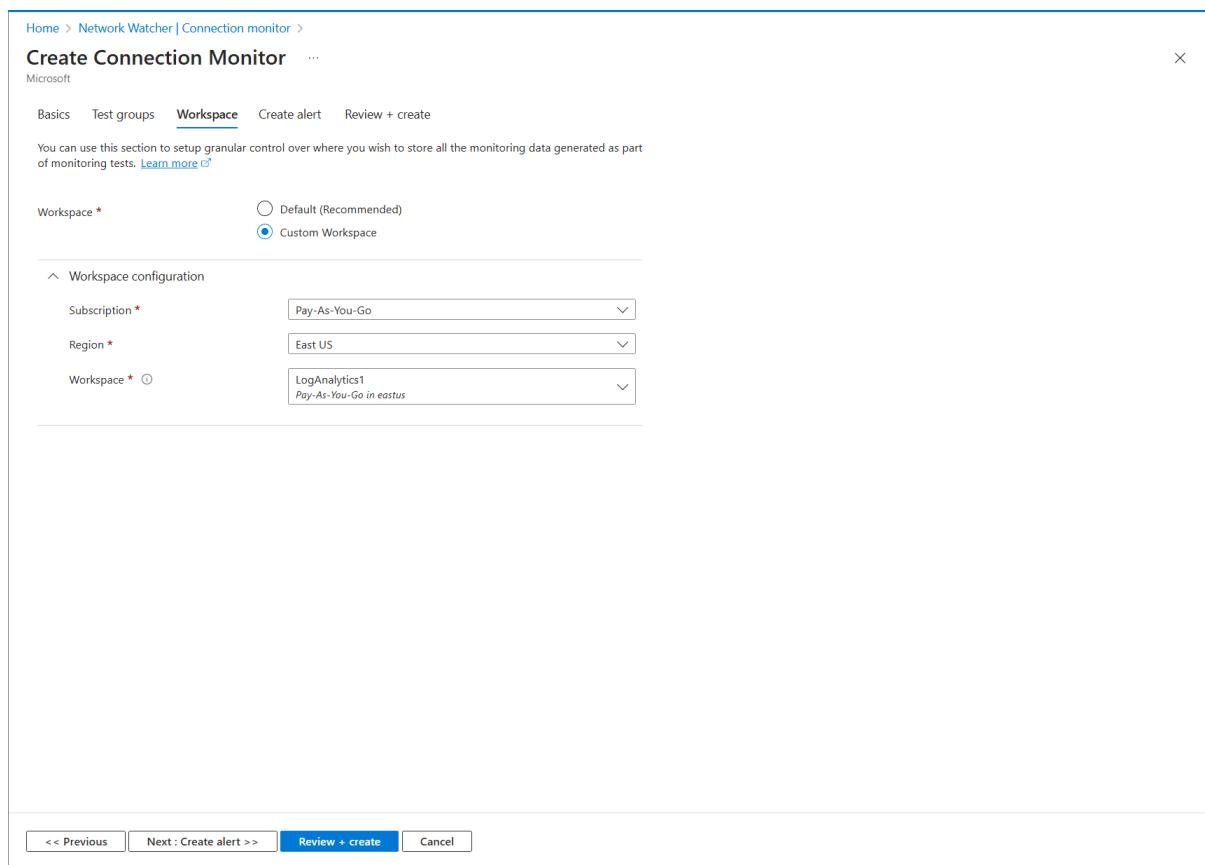
Workspace configuration

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

Review + create

Some selected endpoints do not have the monitoring extension enabled. They will be automatically enabled during the creation of the connection monitor. If you do not wish to automatically enable the extensions, kindly deselect the endpoints before proceeding further.

This Connection Monitor's estimated monthly cost is \$0 [Learn more](#)

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](#) Create alert ?

- 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 Alerts, which is currently selected. The main area displays a summary of alerts: Total alerts (1 Critical, 0 Error, 0 Warning, 1 Informational, 0 Verbose). It also shows a timeline view with a green exclamation mark icon and the message 'No alerts found'. Below this, there is a note: 'Try changing your search or choose a different scope level if you don't see what you're looking for.' and 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 this is a toolbar with buttons for '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', and 'Add tag filter'. A dropdown menu shows '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

Resource group: 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 >

Choose Review and Create. Choose Create

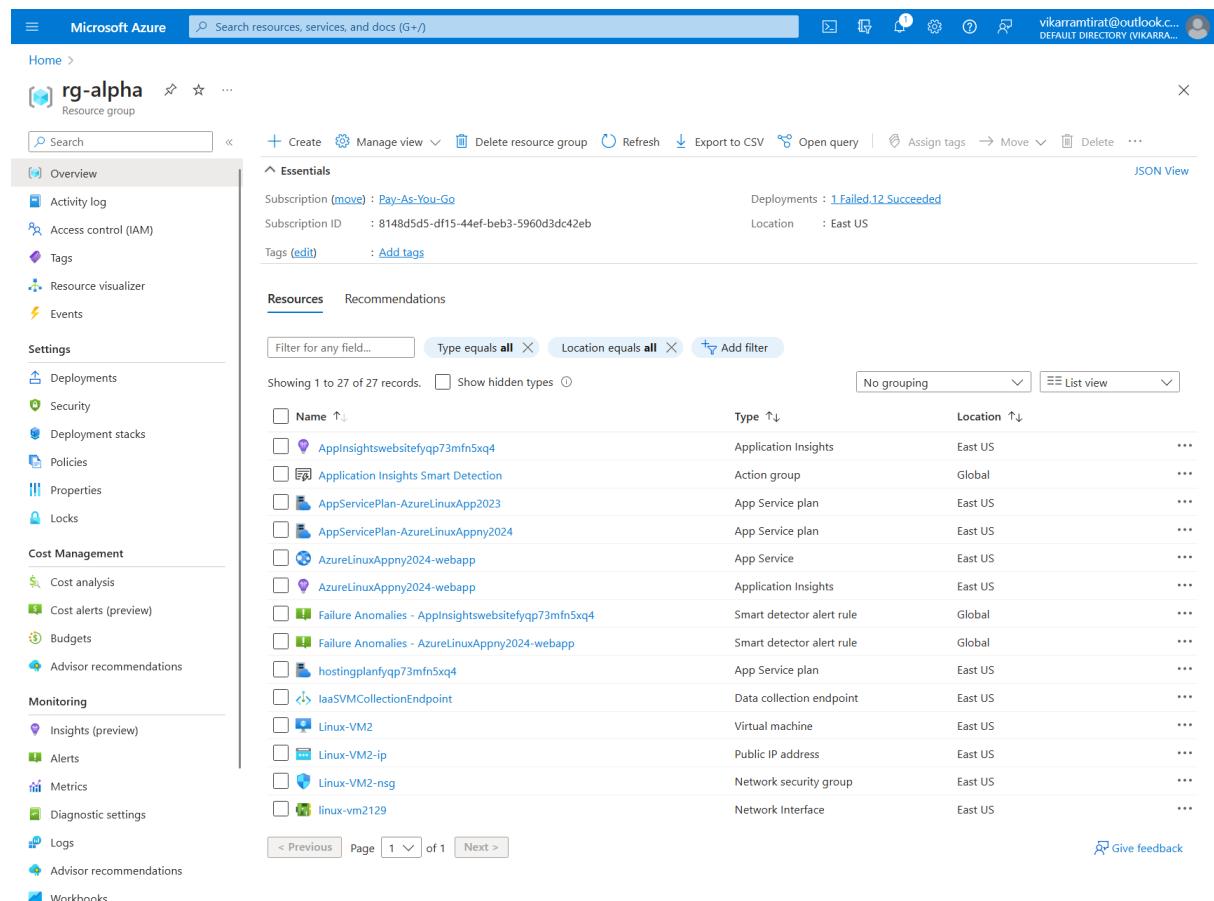
Home > Monitor | Alerts >

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

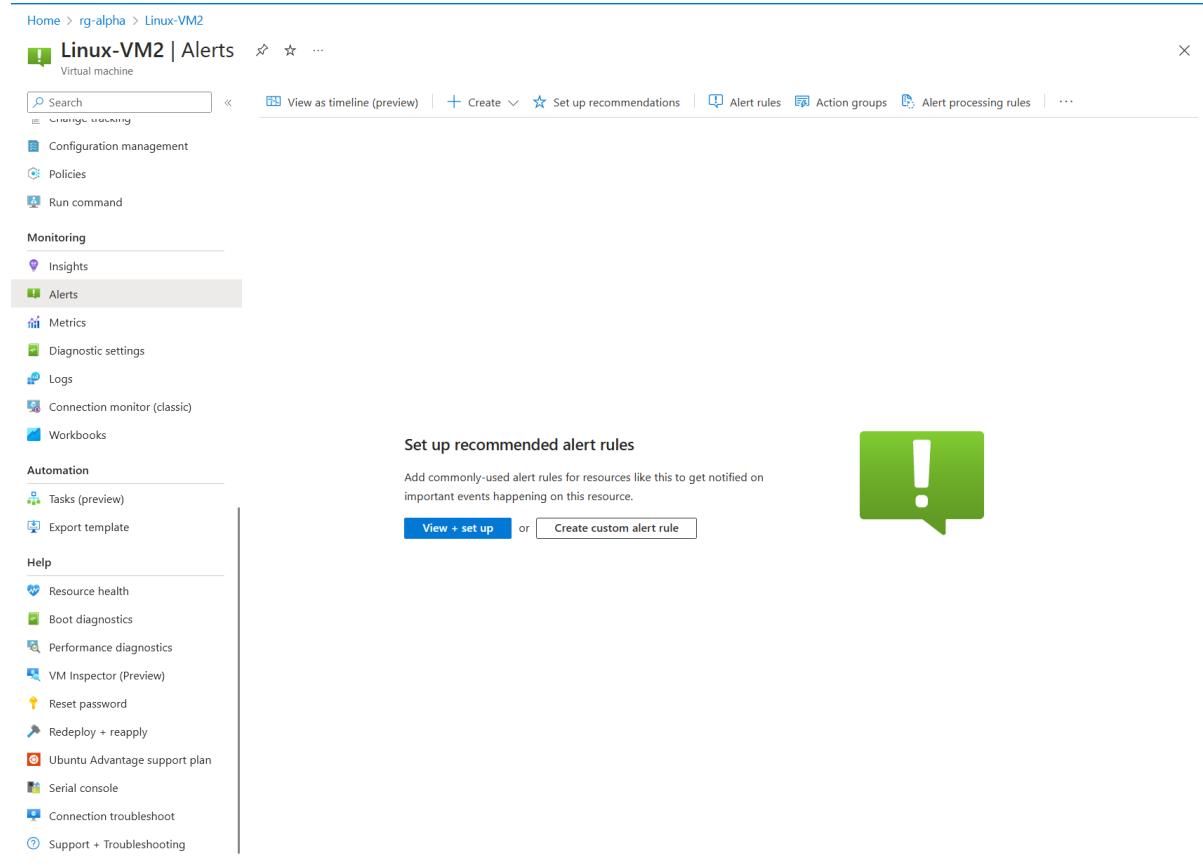


The screenshot shows the Microsoft Azure portal interface for the 'rg-alpha' resource group. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings (Deployments, Security, Deployment stacks, Policies, Properties, Locks), Cost Management (Cost analysis, Cost alerts (preview), Budgets, Advisor recommendations), Monitoring (Insights (preview), Alerts, Metrics, Diagnostic settings, Logs, Advisor recommendations, Workbooks), and a 'Resources' section. The main content area displays the 'Essentials' section with details like Subscription (Pay-As-You-Go), Deployment status (1 Failed, 12 Succeeded), and Location (East US). Below this is a 'Resources' table listing 27 records, including Application Insights, Action groups, App Service plan, App Service, Application Insights, Smart detector alert rule, and various VMs and network components. The table includes columns for Name, Type, and Location.

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

choose Linux-VM2

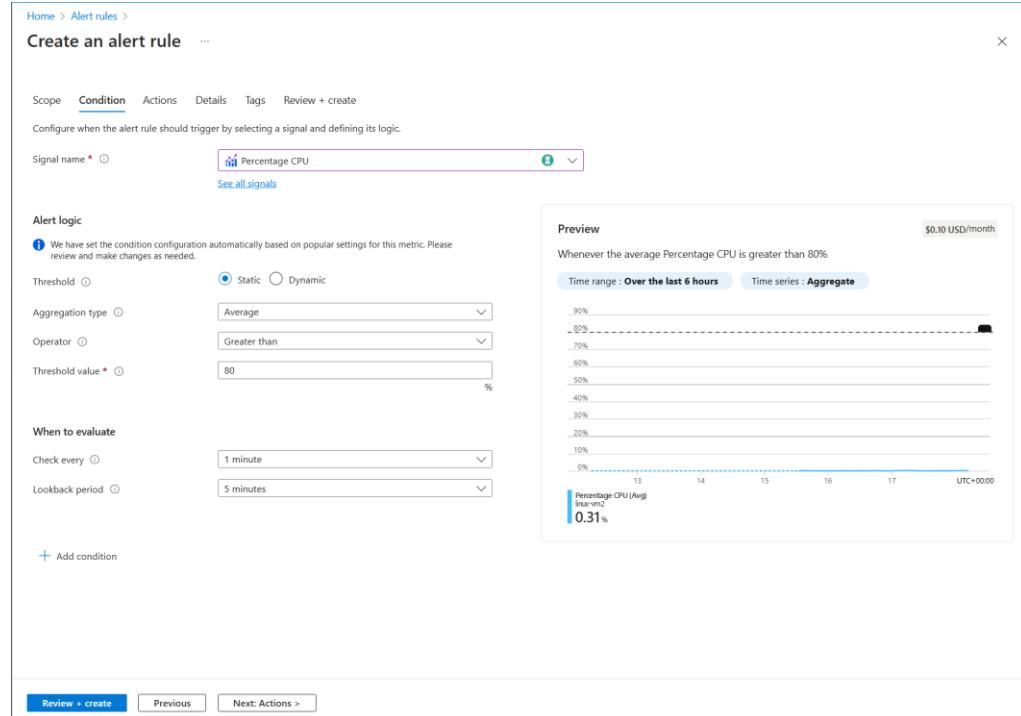
On the Linux-VM2 properties page, choose Alerts under Monitoring



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 right side of the main content.

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 chart shows data for 'Percentage CPU (Avg)' over the time range 'Over the last 6 hours' with 'Time series: Aggregate'. A red dashed horizontal line is drawn at the 80% mark, and a blue line shows values starting around 0.31%. At the bottom of the wizard, there are buttons for 'Review + create', 'Previous', and 'Next: Actions >'.

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 instructions: '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 named 'Application Insights Smart Det...' and another named 'NotifyCPU' (which is checked). The table columns are Action group name, Resource group, Contains actions, and Location.

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' (Subscription: Pay-As-You-Go, Resource group: rg-alpha) and 'Alert rule details' (Severity: 2 - Warning, Alert rule name: HighCPU, Alert rule description: HighCPU). At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next: Tags >'. The URL https://portal.azure.com/# is visible at the bottom left.