

Azure Portfolio Projects

Project 3 – Monitoring, Backup, and Recovery

Overview:

Each project in this 5-project portfolio is designed to demonstrate my hands-on experience with Azure and cloud technologies. The projects cover core aspects such as compute and identity management, networking and storage, monitoring, backup and recovery, identity integration, and app service deployment.

03 – Azure Monitoring, Backup, and Recovery

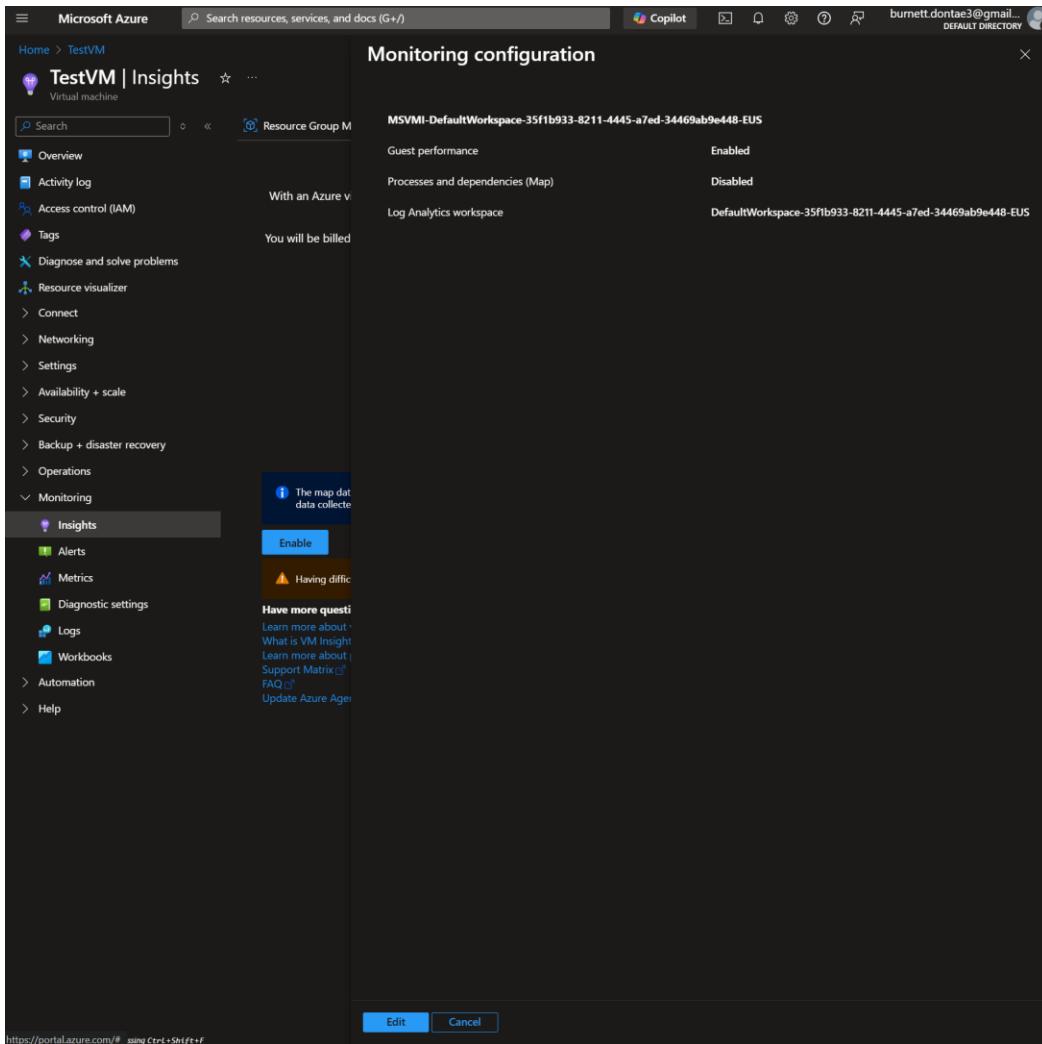
Project Summary

In this project, I implemented Azure's built-in monitoring, backup, and disaster recovery services to ensure operational visibility and business continuity. The setup includes VM insights, log analytics, alerting, backup automation, and site recovery, all with security best practices in mind.

Project Tasks

Task 1: Configure Azure Monitor for VMs

- Step 1: Enable VM Insights via Monitoring > Insights
- Step 2: Configure performance alerts for high CPU usage (Threshold: 80%)
- Step 3: Set up Action Groups for notifications



The screenshot shows the Microsoft Azure portal interface for managing a virtual machine named 'TestVM'. The left sidebar is open, showing various monitoring and diagnostic tools. The 'Monitoring' section is expanded, and the 'Insights' option is selected, which is highlighted with a dark background. The main content area is titled 'Monitoring configuration' and displays several configuration items:

- MSVMI-DefaultWorkspace-35f1b933-8211-4445-a7ed-34469ab9e448-EUS**
- Guest performance**: Enabled
- Processes and dependencies (Map)**: Disabled
- Log Analytics workspace**: DefaultWorkspace-35f1b933-8211-4445-a7ed-34469ab9e448-EUS

A tooltip for 'The map data collect' is displayed over the 'Processes and dependencies (Map)' setting. At the bottom of the configuration pane, there are 'Edit' and 'Cancel' buttons.

Microsoft Azure Search resources, services, and docs (G+) Copilot Home > TestVM TestVM | Alerts Virtual machine

Set up recommended alert rules

Select alert rules

- > Percentage CPU is greater than 80 %
- > Available Memory Bytes is less than 1 GB
- > Data Disk IOPS Consumed Percentage is greater than 95 %
- > OS Disk IOPS Consumed Percentage is greater than 95 %
- > Network In Total is greater than 500 GB
- > Network Out Total is greater than 200 GB
- > VmAvailabilityMetric is less than 1

Notify me by

Email

Email Azure Resource Manager Role

Azure mobile app notification

Set Use an existing action group

Add imp

More alerting options Estimated monthly total: 0.10 USD

Save Cancel

Add or remove favorites by pressing Ctrl + Shift + F

The screenshot shows the Azure portal interface for managing alerts on a virtual machine named 'TestVM'. On the left, a navigation sidebar is visible with categories like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, Insights, Alerts (which is selected), Metrics, Diagnostic settings, Logs, Workbooks, Automation, and Help. The main content area is titled 'Set up recommended alert rules' and displays a list of pre-configured alert rules. Each rule includes a description, a condition (e.g., 'Percentage CPU is greater than 80 %'), and a toggle switch to enable or disable it. Below the rules, there are sections for 'Notify me by' (Email, Azure Resource Manager Role, Azure mobile app notification) and a checkbox for 'Use an existing action group'. At the bottom, there are 'Save' and 'Cancel' buttons, along with a note about estimated monthly costs (0.10 USD).

The screenshot shows the Microsoft Azure portal interface for a virtual machine named 'TestVM'. The main page displays the 'Alerts' section, which is currently empty ('No alerts found'). The left sidebar lists various monitoring and diagnostic options like Metrics, Diagnostic settings, Logs, and Workbooks. A notifications sidebar on the right shows a success message: 'Create recommended alert rule created successfully' a few seconds ago.

Task 2: Set Up Azure Backup

- Step 1: Create a Recovery Services Vault
- Step 2: Define and apply a daily backup policy with 7-day retention
- Step 3: Enable encryption for backups
- Step 4: Perform and verify a manual backup

Microsoft Azure Search resources, services, and docs (G+) Copilot 🔍 Notifications burnett.dontae3@gmail... DEFAULT DIRECTORY

Home > Recovery Services vaults >

Create Recovery Services vault

Basics Redundancy Encryption Vault properties Networking Tags Review + create

Project Details
Select the subscription and the resource group in which you want to create the vault.

Subscription Azure for Students Resource group AzureProject1 Create new

Instance Details

Vault name Test3 Region East US

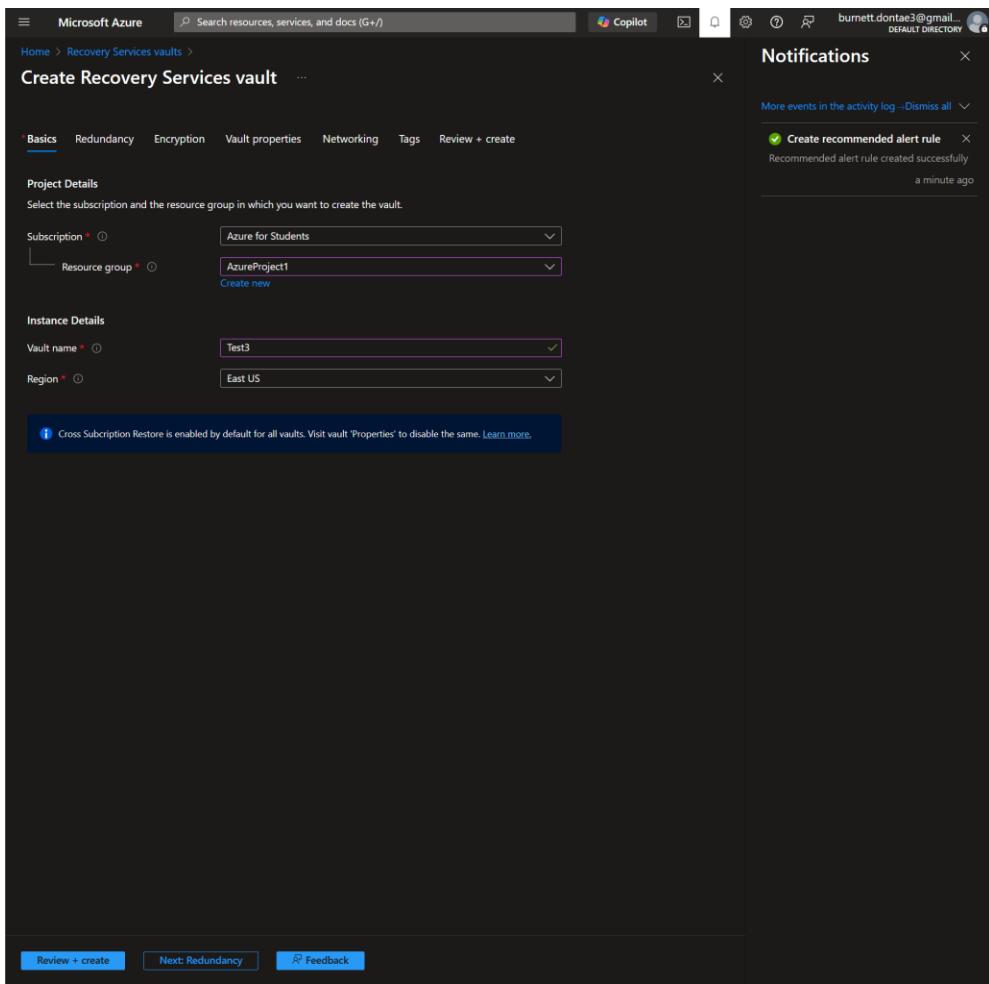
ⓘ Cross Subscription Restore is enabled by default for all vaults. Visit vault 'Properties' to disable the same. [Learn more](#).

Review + create Next: Redundancy Feedback

Notifications

More events in the activity log -Dismiss all

✓ Create recommended alert rule Recommended alert rule created successfully a minute ago



Microsoft Azure Search resources, services, and docs (G+) Copilot Home > Microsoft.RecoveryServicesV2-1746497138549 | Overview

Deployment

Overview Deployment

Search Delete Cancel Redeploy Download Refresh

Your deployment is complete

Deployment name : Microsoft.RecoveryServicesV2... Start time : 5/5/2025, 9:05:57 PM
Subscription : Azure for Students Correlation ID : 3f4a9ed4-4e1-4536-8471-087...
Resource group : AzureProject1

Deployment details Next steps Go to resource

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 >

Add or remove favorites by pressing Ctrl + Shift F4.

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

Home > ConfigureProtection-1746497485140 | Overview

Deployment

Search | Delete | Cancel | Redeploy | Download | Refresh

Overview

Your deployment is complete

Deployment name : ConfigureProtection-1746497485140

Subscription : Azure for Students

Resource group : AzureProject1

Start time : 5/5/2025, 9:11:25 PM

Correlation ID : 047fe8d2-ba0d-43ef-9975-7b11e2bbe136

Deployment details

Resource	Type	Status	Operat
Test3/Azure/IaaSVM	Backup Item	OK	Operat

Next steps

Go to resource

Notifications

More events in the activity log -Dismiss all

Deployment succeeded Deployment 'ConfigureProtection-1746497485140' to resource group 'AzureProject1' was successful.

Go to res... Go to resource ... a few seconds ago

Deployment succeeded Deployment 'Microsoft.RecoveryServicesV2-1746497485140' to resource group 'AzureProject1' was successful.

Go to res... Pin to dash... 5 minutes ago

Create recommended alert rule Recommended alert rule created successfully

10 minutes ago

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 >

https://portal.azure.com/#blade/Microsoft_Azure_ActivityLog/ActivityLogBlade/queryInputs/%7B%22user%22%3A%22donte3%22%7D

The screenshot shows the Microsoft Azure portal interface for managing a virtual machine named 'TestVM'. The left sidebar contains a navigation menu with various options such as Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings, Availability + scale, Security, Backup + disaster recovery (which is currently selected), Disaster recovery, Restore point, Operations, Monitoring, Insights, Metrics, Diagnostic settings, Logs, Workbooks, Automation, and Help.

In the main content area, under the 'Backup' section, there is a 'Pre-Check' status message indicating 'Passed'. Below this, there are sections for 'Subscription (move)', 'Subscription ID', and 'Alerts (in last 24 hours)'. A 'Recovery points' section states 'No restore points available.'

A notification on the right side of the screen shows a success message: 'Triggering backup for TestVM' was triggered successfully a few seconds ago.

Task 3: Implement Azure Site Recovery

- Step 1: Enable disaster recovery for the VM
- Step 2: Configure replication to a secondary region
- Step 3: Test failover and monitor replication health

Microsoft Azure Search resources, services, and docs (G+) Copilot DEFAULT DIRECTORY

Home > TestVM

TestVM | Disaster recovery

Virtual machine

Basics Advanced settings Review + Start replication

Welcome to Azure Site Recovery

You can replicate your virtual machines to another Azure region for business continuity and disaster recovery needs. [Learn more about Azure Site Recovery.](#)

Disaster recovery between availability zones? * No Yes

Target region * South Central US East US

World map showing regions: Source region (East US), Selected target region (South Central US), Available target regions

Azure Site Recovery support for Trusted launch VMs is generally available. Click [here](#) for more details.

Review + Start replication Previous Next : Advanced settings Give Feedback

Add or remove favorites by pressing Ctrl + Shift + F

Task 4: Query Logs in Azure Monitor

- Step 1: Access Log Analytics Workspace

Visualize results as charts for insights. In my case there was nothing to show

The screenshot shows the Microsoft Azure Log Analytics workspace interface. The left sidebar lists various logs and monitoring options. The main area displays a KQL query being run:

```
1 Perf  
2 | where ObjectName == "Processor" and CounterName == "% Processor Time"  
3 | summarize Avg_CPU = avg(CounterValue) by bin(TimeGenerated, 5m)  
4
```

The query is set to run over the last 24 hours and shows 1000 results. A progress bar indicates the query is running. At the bottom, there are navigation links for Results and Chart.

Task 5: Secure Backup and Recovery

- Step 1: Verify encryption settings in Recovery Services Vault

Encryption with Microsoft-Managed Keys (MMK):

- Azure Recovery Services Vault uses encryption-at-rest by default with Microsoft-managed keys.
- You can view and confirm the encryption settings by navigating to: Recovery Services Vault > Properties > Encryption Settings.

- This ensures all backup data is protected without the need for manual key management.

