Student Name: **Weight: 3%**

Student ID: **Marks: /10**

Lab: Azure Performance Tools

Lab Objectives

In this lab you'll explore how to use the Azure fault and performance tools. You will:

1. View the Azure Monitor tools.
2. Monitor a virtual machine.
3. Create an alert.
4. Run a query in the Log Analytics workspace.
5. Back up and restore a VM.
6. Replicate Azure VMs.
7. Create a Load Balancer.

Lab Requirements

- Up to date web browser
- Azure account

Instructions

1. Working individually, follow the procedure below.
2. Take screenshots, as described in the *Marking Criteria* section.
3. Create a document that includes all screenshots appropriately titled and described, and then upload it to the Lab assignment drop box.
4. Be sure to include your name and student ID in the document.

Marking Criteria

Screenshots	Marks
CPU % alert	/2
Log Analytics query	/2
Successful VM restore	/2
Successful VM replication failover	/2
Created public load balancer with the CLI	/2
Total	**/10**

Note: This icon indicates when a screenshot is required.

📷

Source: Flatiron.com, Freepik, Image: screenshot_983871

Procedure

IT system performance can be quite complex and involve a number of monitoring, fault tolerance and disaster recovery tools. The key topics discussed in this lab are:

- Monitoring – monitoring logs and alerts
- Fault tolerance – replication and load balancing
- Disaster recovery – backups

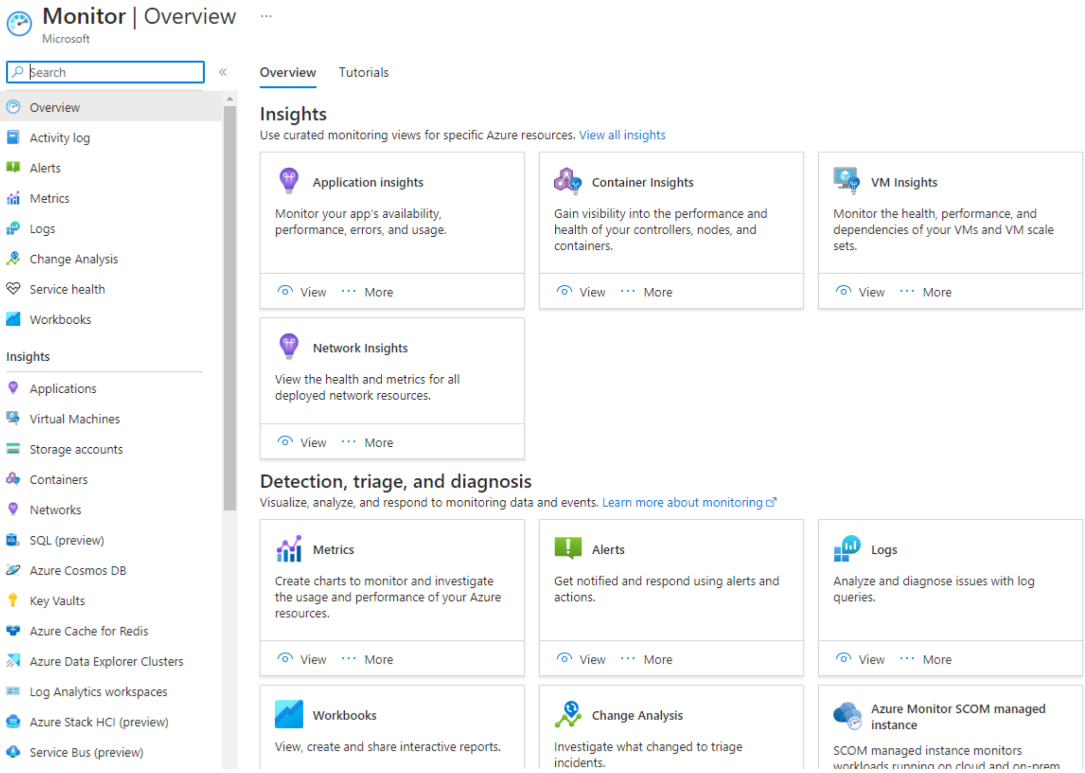
Part 1: View the Azure Monitor Tools

All of Azure’s several monitoring tools are found under the name Azure Monitor.

☐ Read: Azure Monitor Overview (https://learn.microsoft.com/en-us/azure/azure-monitor/overview).

☐ Search for and navigate to **Monitor** in the portal.

☐ On the main page, browse the various tools to get an idea of what’s available.



Use curated monitoring views for specific Azure resources.

Monitor your app’s availability, performance, errors, and usage.

Gain visibility into the performance and health of your controllers, nodes, and containers.

Monitor the health, performance, and dependencies of your VMs and VM scale sets.

View the health and metrics for all deployed network resources.

Visualize, analyze, and respond to monitoring data and events.

Create charts to monitor and investigate the usage and performance of your Azure resources.

Get notified and respond using alerts and actions.

Analyze and diagnose issues with log queries.

View, create and share interactive reports.

Investigate what changed to triage incidents.

SCOM managed instance monitors workloads running on cloud and on-prem

© 2023, Microsoft Azure. Used with permission from Microsoft.

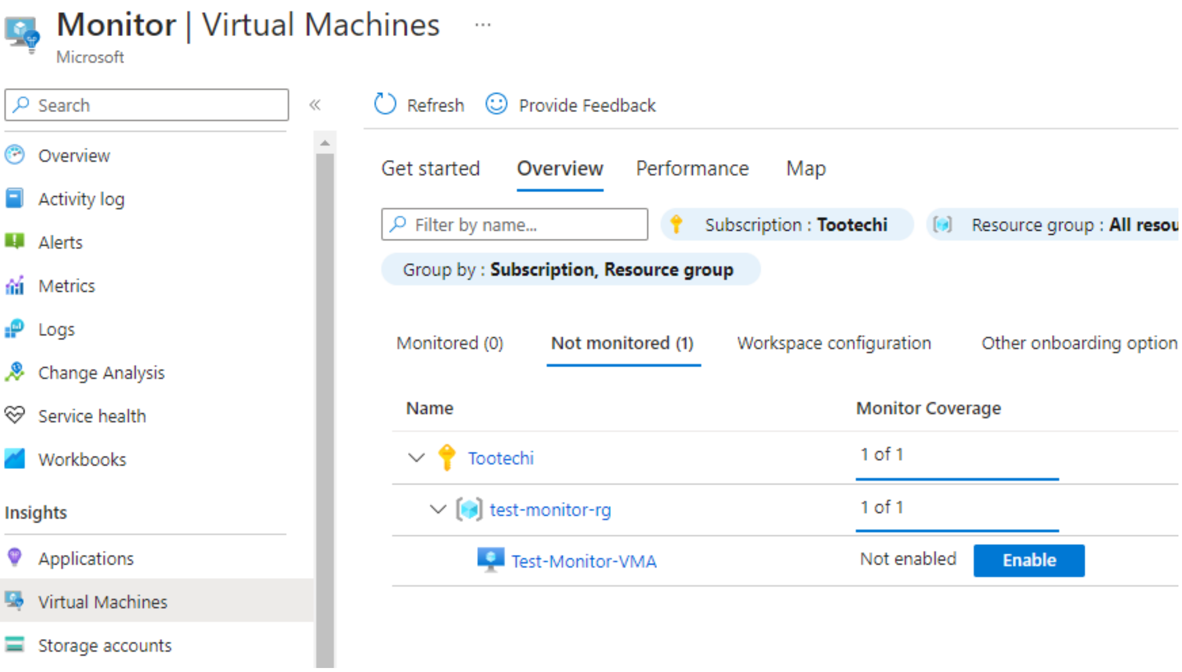
Part 2: Monitor a Virtual Machine

□ Create an inexpensive virtual machine.

□ Navigate to the **Monitor** tool in the portal and select the **VM Insights** tool.

□ Click the **Configure Insights** button.

□ You should be able to see your subscription, resource group and VM.



Subscription : **Tootechi**

Resource group : **All resou**

Group by : **Subscription, Resource group**

Name	Monitor Coverage
Tootechi	1 of 1
test-monitor-rg	1 of 1
Test-Monitor-VMA	Not enabled Enable

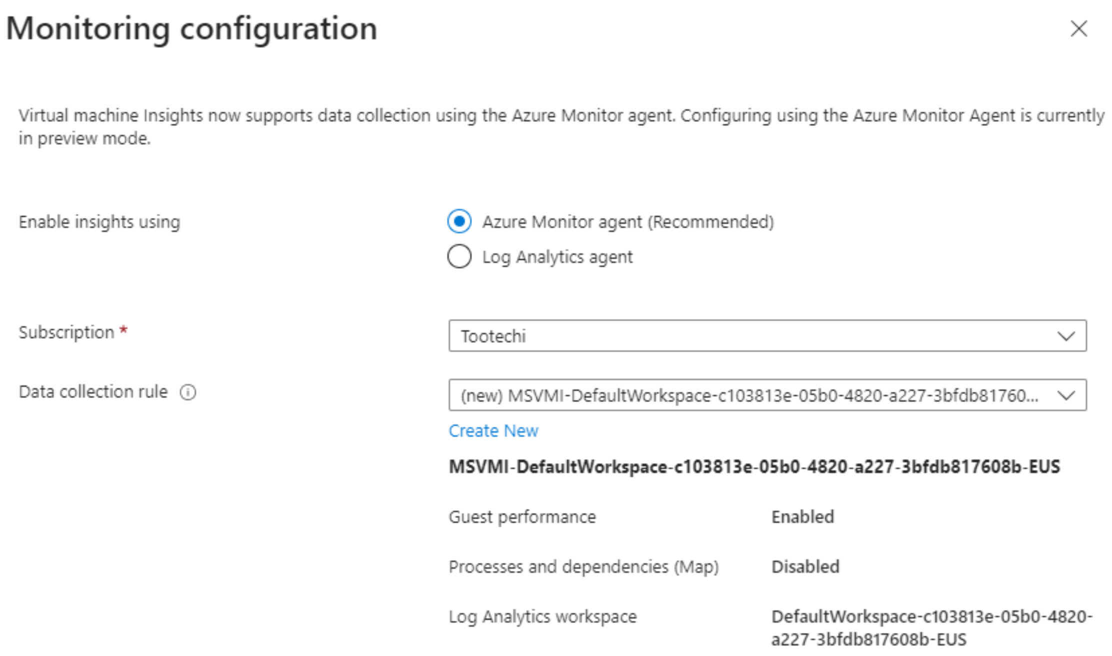
© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Click the **Enable** button beside your virtual machine and enable the monitor.

The *Monitoring configuration* window opens.

□ Select the **Azure Monitor Agent** and your subscription.

A default name is created for the Data Collection rule.



Monitoring configuration

Virtual machine Insights now supports data collection using the Azure Monitor agent. Configuring using the Azure Monitor Agent is currently in preview mode.

Enable insights using: ● Azure Monitor agent (Recommended) ○ Log Analytics agent

Subscription *: Tootechi

Data collection rule: (new) MSVMI-DefaultWorkspace-c103813e-05b0-4820-a227-3bfdb81760...

Create New

MSVMI-DefaultWorkspace-c103813e-05b0-4820-a227-3bfdb817608b-EUS

Guest performance: Enabled

Processes and dependencies (Map): Disabled

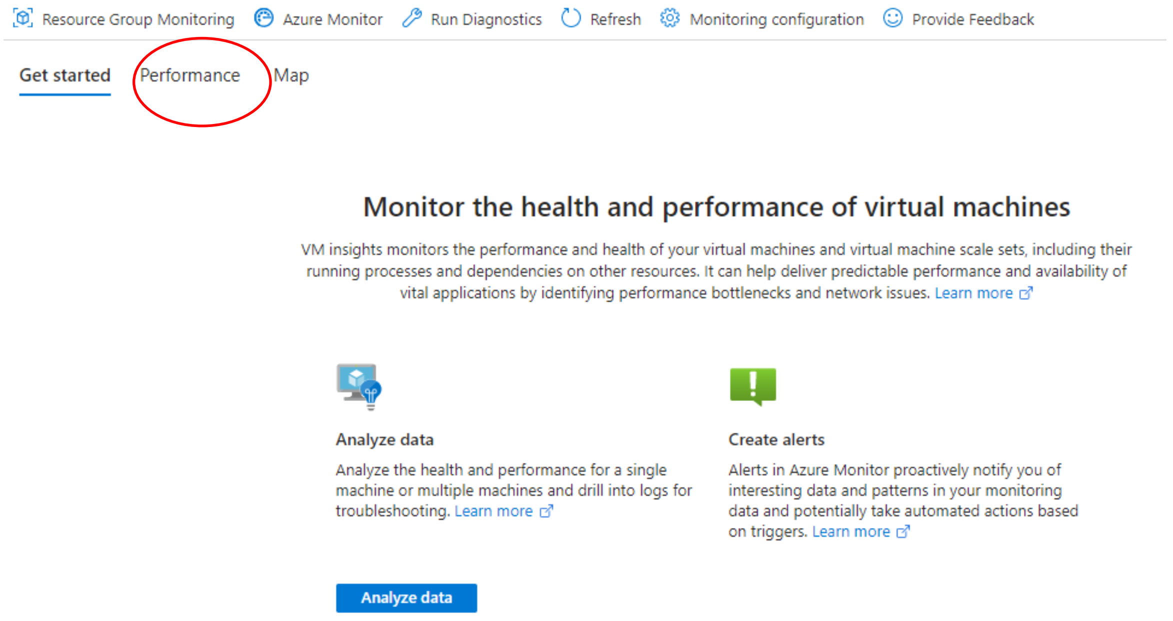
Log Analytics workspace: DefaultWorkspace-c103813e-05b0-4820-a227-3bfdb817608b-EUS

© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Complete the configuration.

□ When the resource is created, go to the virtual machine and select **Insights** from the blade menu.

Note: You may need to refresh the screen.



Monitor the health and performance of virtual machines

VM insights monitors the performance and health of your virtual machines and virtual machine scale sets, including their running processes and dependencies on other resources. It can help deliver predictable performance and availability of vital applications by identifying performance bottlenecks and network issues. Learn more

Analyze data

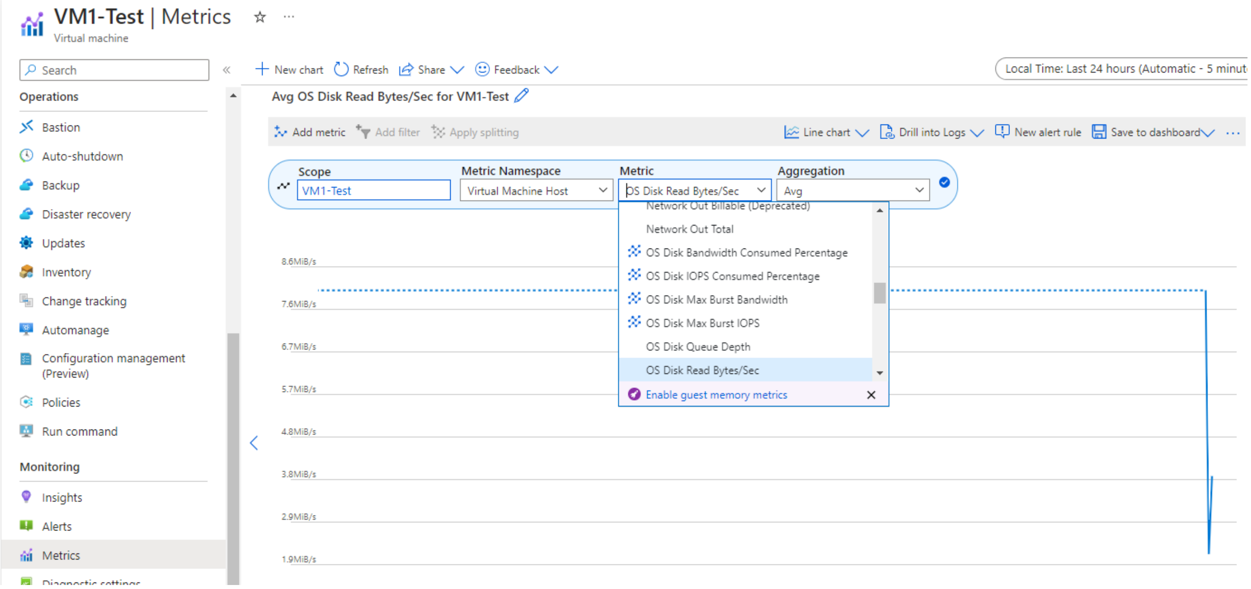
Analyze the health and performance for a single machine or multiple machines and drill into logs for troubleshooting. Learn more

Create alerts

Alerts in Azure Monitor proactively notify you of interesting data and patterns in your monitoring data and potentially take automated actions based on triggers. Learn more

© 2023, Microsoft Azure. Used with permission from Microsoft.

- □ Select **Performance** from the top menu.
- □ You should be able to see graphs like CPU utilization and Disk IOPS.
- □ Restart the VM and go back to see the changes in the graphs.
- □ Select **Metrics** from the blade menu.
- □ Under the *Metric* column, you can choose different types of information to monitor (see image). Try viewing the different metrics.



VM1-Test | Metrics

Virtual machine

Avg OS Disk Read Bytes/Sec for VM1-Test

Scope: VM1-Test

Metric Namespace: Virtual Machine Host

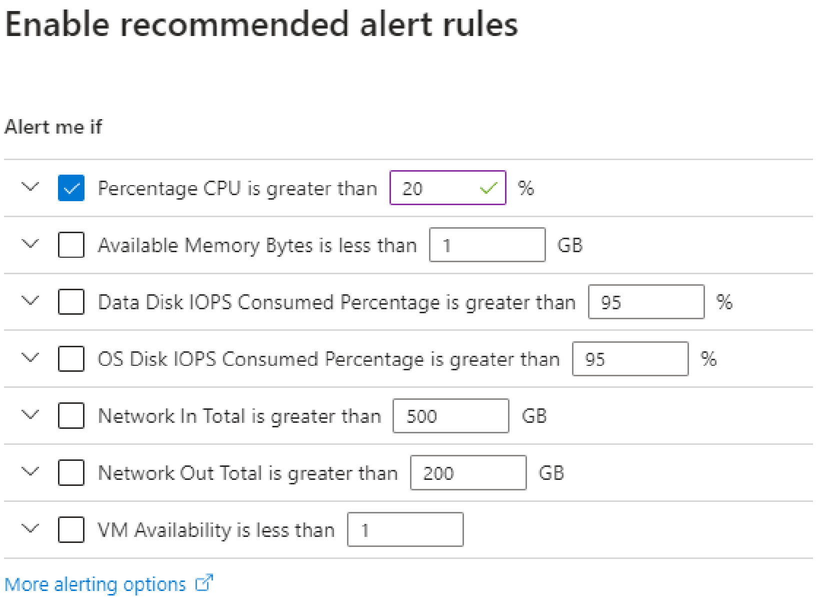
Metric: OS Disk Read Bytes/Sec

Aggregation: Avg

© 2023, Microsoft Azure. Used with permission from Microsoft.

Part 3: Create an Alert

- □ Select **Alerts** from the blade menu.
- □ Click the **Enable Recommended Alert rules** button.
- □ Deselect everything except **the Percentage CPU** and set it to **20%**.
- □ Enter your email and enable the alert.



Enable recommended alert rules

Alert me if

☑ Percentage CPU is greater than 20 %

□ 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

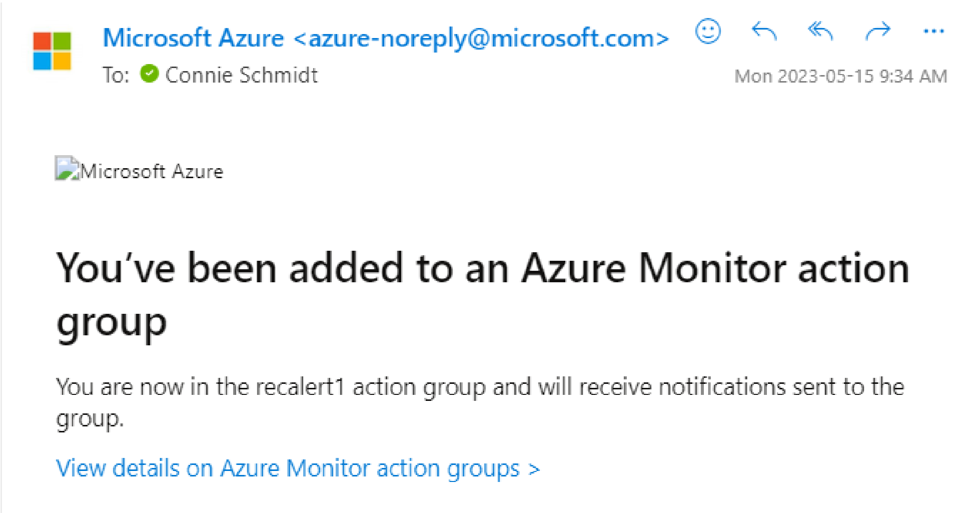
□ Network Out Total is greater than 200 GB

□ VM Availability is less than 1

More alerting options

© 2023, Microsoft Azure. Used with permission from Microsoft.

When the alert is complete, you'll receive an email indicating that you have been added to an action group.



Microsoft Azure <azure-noreply@microsoft.com>

To: Connie Schmidt

Mon 2023-05-15 9:34 AM

Microsoft Azure

You've been added to an Azure Monitor action group

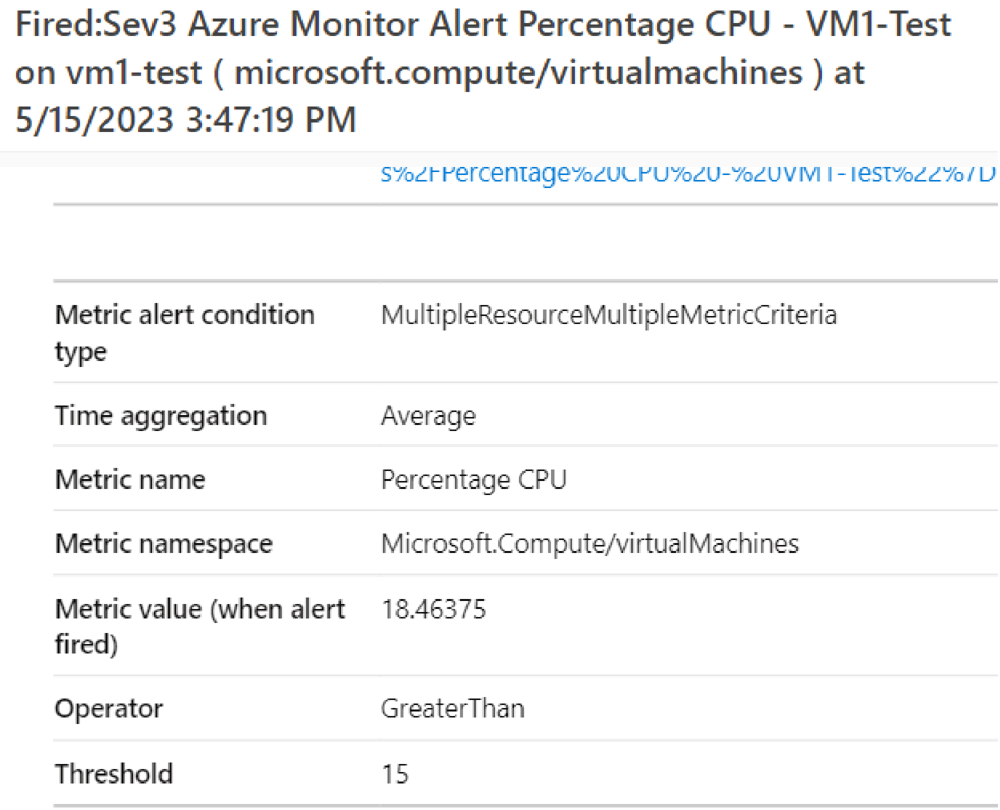
You are now in the recalert1 action group and will receive notifications sent to the group.

View details on Azure Monitor action groups >

© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Reboot the VM

You may have to wait some time but you should receive an email with the alert.



Fired:Sev3 Azure Monitor Alert Percentage CPU - VM1-Test on vm1-test (microsoft.compute/virtualmachines) at 5/15/2023 3:47:19 PM

s%2FPercentage%20CPU%20-%20VM1-Test%22%7D

Metric alert condition type	MultipleResourceMultipleMetricCriteria
Time aggregation	Average
Metric name	Percentage CPU
Metric namespace	Microsoft.Compute/virtualMachines
Metric value (when alert fired)	18.46375
Operator	GreaterThan
Threshold	15

© 2023, Microsoft Azure. Used with permission from Microsoft.

Part 4: Run a Query in the Log Analytics Workspace

The **Log Analytics Workspace** stores data from Azure Monitor, Sentinel, Defender and other services. You can use the Kusto query language to query your logs.

☐ Search for and navigate to the **Log Analytics Workspace** tool.

☐ Select the resource group and region, and then give it a name.

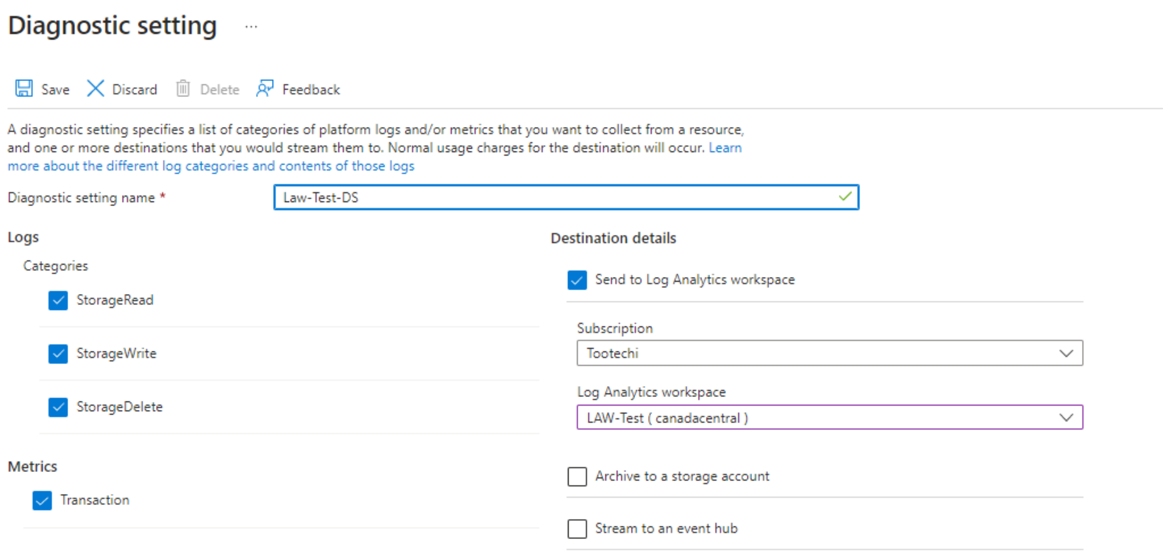
☐ Review and create the workspace.

☐ Create a standard storage account.

☐ When the resource is completed, go to the main page and select **Diagnostic Settings** from the blade menu.

☐ Click the **Blob** icon, and then select **+ Add Diagnostic Setting**.

☐ Select the logs and send them to your log analytics workspace.



Diagnostic setting

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 * Law-Test-DS

Logs

Categories

☑ StorageRead

☑ StorageWrite

☑ StorageDelete

Metrics

☑ Transaction

Destination details

☑ Send to Log Analytics workspace

Subscription: Tootechi

Log Analytics workspace: LAW-Test (canadacentral)

☐ Archive to a storage account

☐ Stream to an event hub

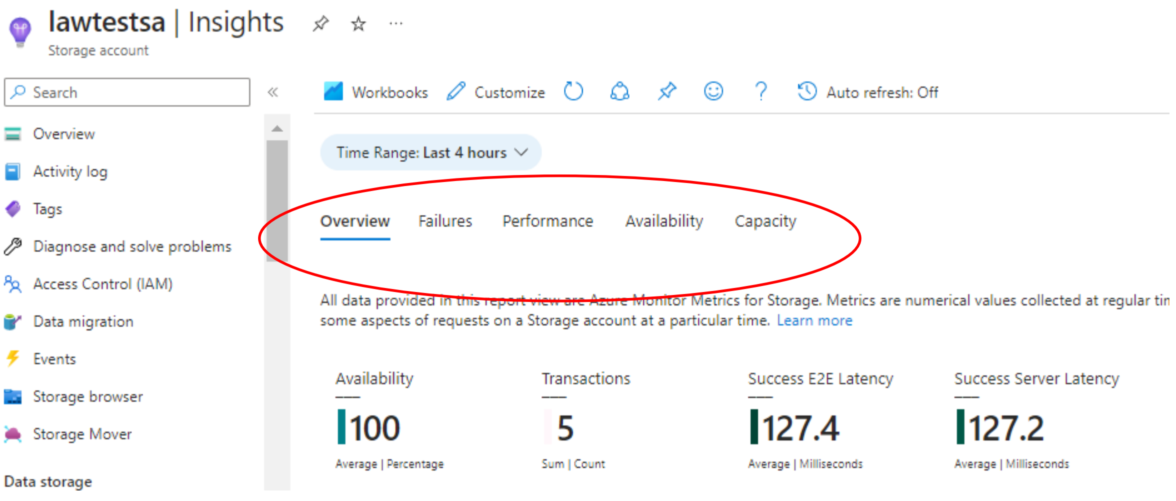
© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Click the **Save** button.

□ Go to the **Monitor** tool and select **Storage Accounts** from the blade menu.

□ Select your storage account.

The *Insights* menu for the storage account appears.



lawtestsa | Insights

Storage account

All data provided in this report view are Azure Monitor Metrics for Storage. Metrics are numerical values collected at regular tin some aspects of requests on a Storage account at a particular time. Learn more

Availability	Transactions	Success E2E Latency	Success Server Latency
100	5	127.4	127.2
Average | Percentage	Sum | Count	Average | Milliseconds	Average | Milliseconds

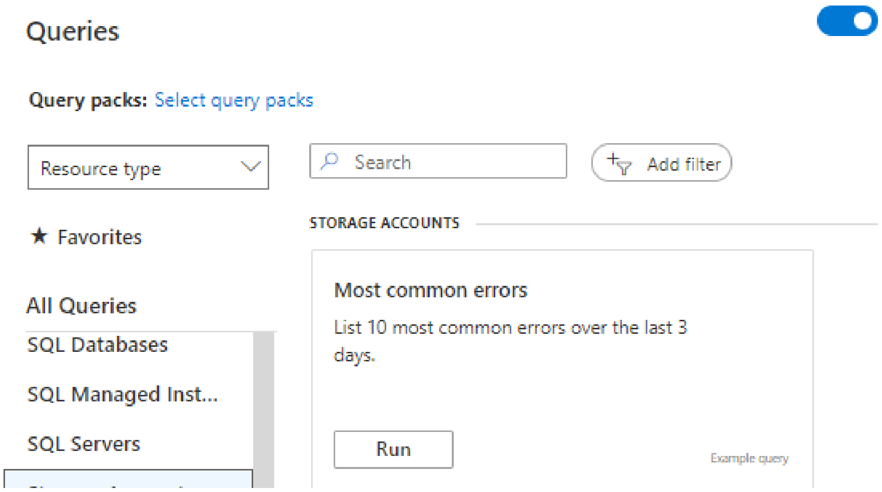
© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Review the information available in the menus along the top.

□ From the main page of the log analytics workspace, select **Logs**.

□ Under **Category**, select **Resource Type**, and then scroll down and select **Storage Accounts**.

☐ Select and run the **Most Common Errors** query.



Queries

Query packs: Select query packs

Resource type

Search

Add filter

★ Favorites

All Queries

SQL Databases

SQL Managed Inst...

SQL Servers

STORAGE ACCOUNTS

Most common errors

List 10 most common errors over the last 3 days.

Run

Example query

© 2023, Microsoft Azure. Used with permission from Microsoft.

☐ Complete the Log Analytics tutorial (https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-tutorial).

☐ On the demo from the log analytics tutorial, run a query with the following options:

- Under **LogManagement**
- Storage Blob Logs
- Location contains “westus”
- Authentication Type = SAS
- Does a count

📷

☐ Delete your resources to avoid accruing costs.

Part 5: Back Up and Restore a VM

Azure backup services can apply to a number of resources, including:

- Disks
- File shares
- Virtual machines
- Blobs
- Databases
- On-prem files and folders

Before you can create a backup, you need to create a Recovery Services Vault, which stores the backups and has the tools for recovery.

☐ Create an inexpensive virtual machine.

☐ Search for and navigate to the **Recovery Services Vault** tool, and then click **+ Create**.

☐ Enter the resource group, name and region.

☐ Review and create the vault.

☐ When the resource has been created, go to the vault and select **Backup** from the blade menu.

The two selections here are the location of the resource (where is the workload running) and the type of resource.

☐ Select **On-Premises** as the workload type, and then use the drop-down arrow to see the types of on-prem resources that can be backed up to Azure.

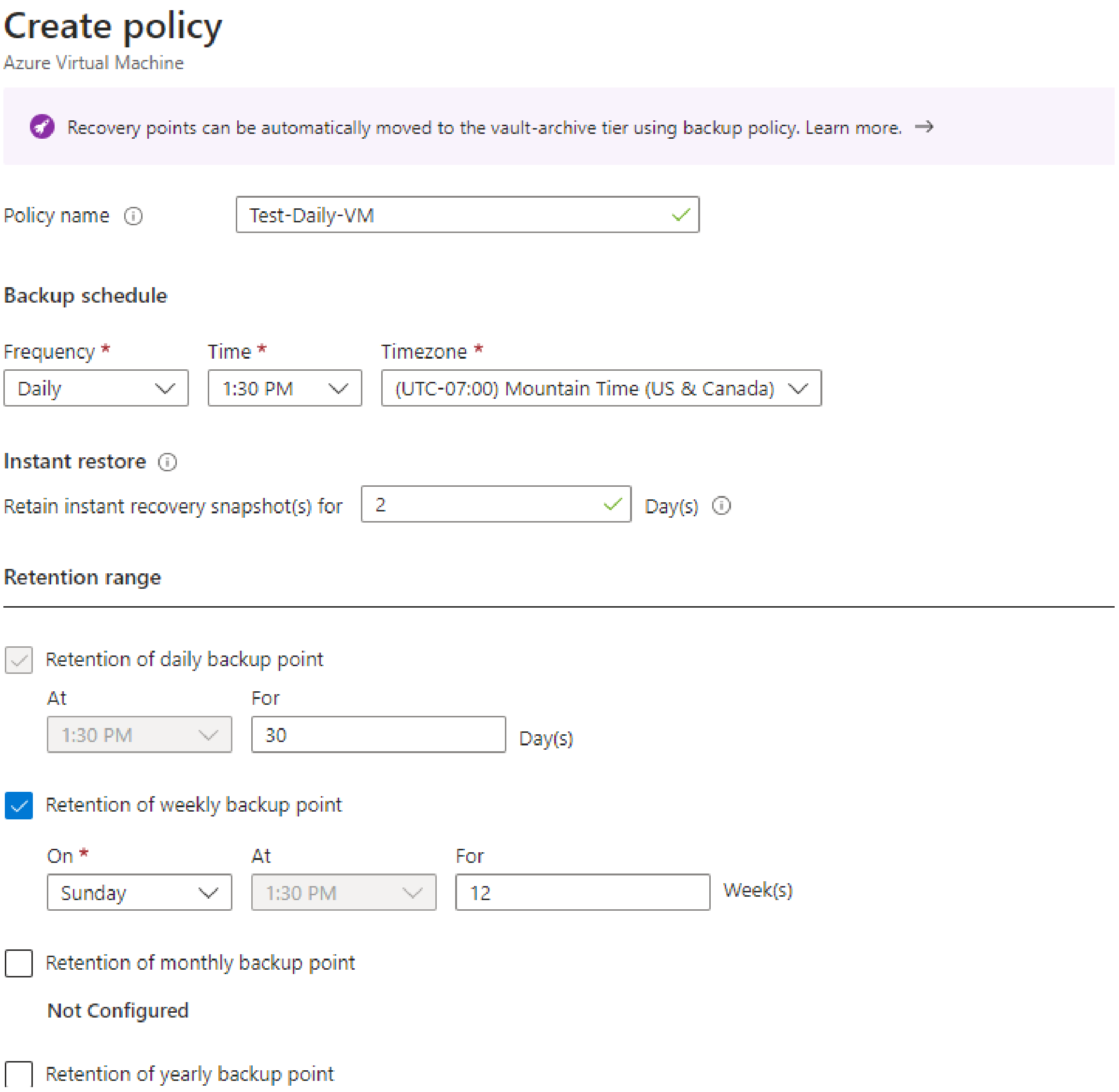
☐ Select **Azure** as the workload type and **Virtual Machine** as the resource you want to back up.

☐ Click the **Backup** button.

☐ Note the differences between the **Standard** and the **Enhanced** policy types.

☐ Leave the policy type as **Standard** and click **Create a New Policy**.

☐ Create a new policy that will run ten or fifteen minutes from the current time, and then click **OK**.



Create policy

Azure Virtual Machine

Recovery points can be automatically moved to the vault-archive tier using backup policy. Learn more. →

Policy name: Test-Daily-VM

Backup schedule

Frequency *: Daily

Time *: 1:30 PM

Timezone *: (UTC-07:00) Mountain Time (US & Canada)

Instant restore

Retain instant recovery snapshot(s) for: 2 Day(s)

Retention range

☑ Retention of daily backup point

At: 1:30 PM

For: 30 Day(s)

☑ Retention of weekly backup point

On *: Sunday

At: 1:30 PM

For: 12 Week(s)

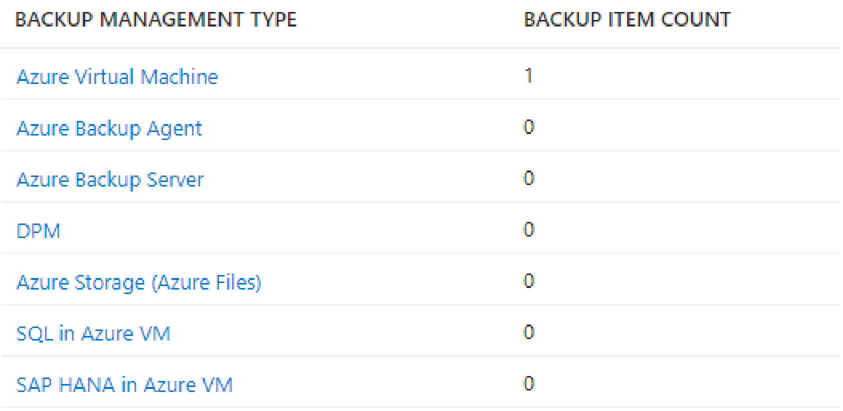
☐ Retention of monthly backup point

Not Configured

☐ Retention of yearly backup point

© 2023, Microsoft Azure. Used with permission from Microsoft.

- ☐ Click the **Add** button and add your VM to the backup.
- ☐ Click the **Enable Backup** button.
- ☐ When the resource has completed, return to the recovery services vault and select **Backup Items** from the blade menu.



BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	1
Azure Backup Agent	0
Azure Backup Server	0
DPM	0
Azure Storage (Azure Files)	0
SQL in Azure VM	0
SAP HANA in Azure VM	0

© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Select the VM backup. A message may appear saying “Warning (Initial backup pending)” until the backup is complete.

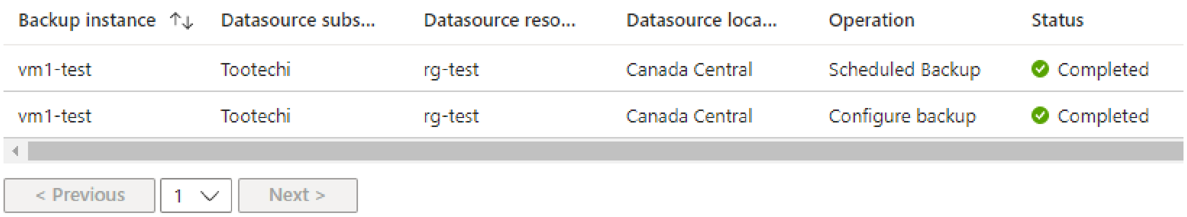
The backup has two stages:

1. Take a snapshot
2. Send the data to the vault

□ Search for and navigate to the **Backup Center** tool.

□ Select **Backup Jobs** from the blade menu to see the details of your backups.

□ Eventually, the backup completes.



Backup instance ↑↓	Datasource subs...	Datasource reso...	Datasource loca...	Operation	Status
vm1-test	Tootechi	rg-test	Canada Central	Scheduled Backup	✓ Completed
vm1-test	Tootechi	rg-test	Canada Central	Configure backup	✓ Completed

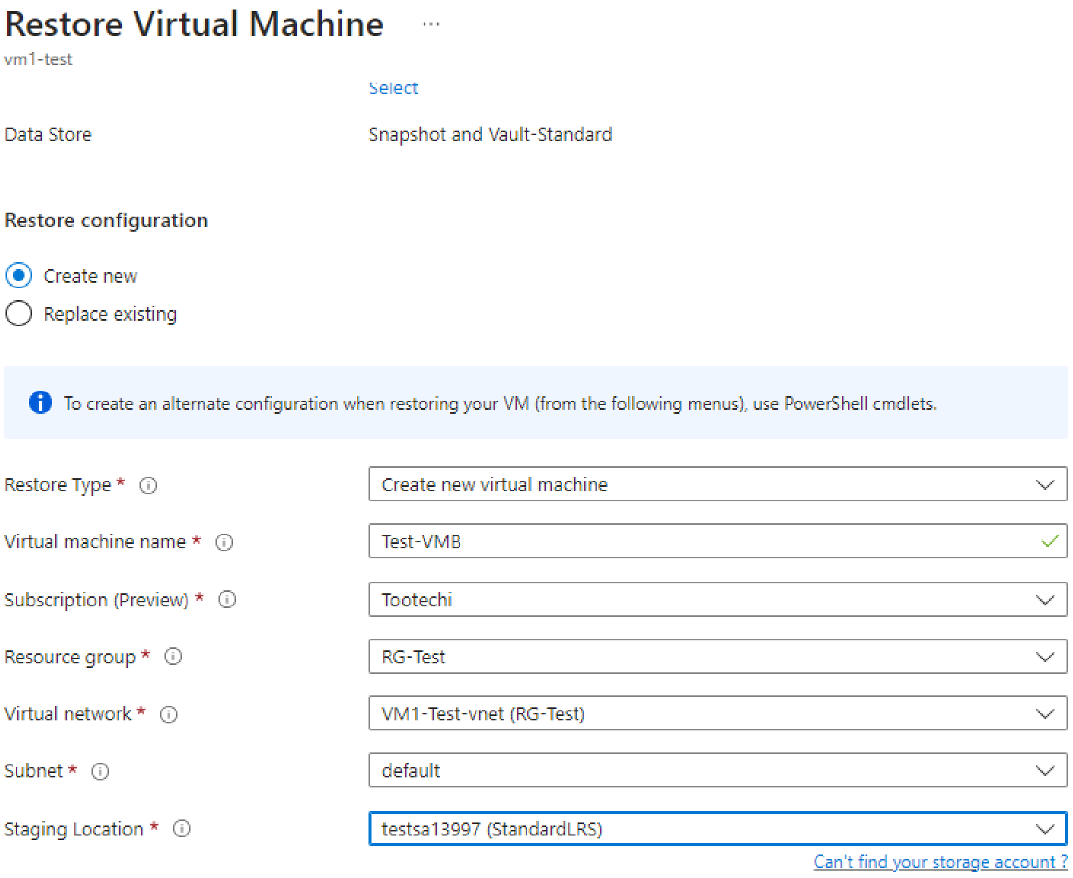
© 2023, Microsoft Azure. Used with permission from Microsoft.

□ In the Backup Center tool, select **Backup Instances** from the blade menu to get your restore point.

□ To restore the VM, you need a storage account as a staging area for the data. Create a standard storage account.

□ In the Backup Center tool, on the **Overview** page, select **Restore** from the top menu.

- □ Select **Azure Virtual Machine** as the data source type, and then click **Select Backup Instance**.
- □ Choose the VM and click the **Select** button.
- □ Click **Continue**, select the restore point and click **OK**.
- □ You are going to use the restore point to create a new VM, so give it a name and select your resource group, networks and storage account.



Restore Virtual Machine ···

vm1-test

Select

Data Store Snapshot and Vault-Standard

Restore configuration

● Create new

○ Replace existing

To create an alternate configuration when restoring your VM (from the following menus), use PowerShell cmdlets.

Restore Type *	Create new virtual machine
Virtual machine name *	Test-VMB ✓
Subscription (Preview) *	Tootechi
Resource group *	RG-Test
Virtual network *	VM1-Test-vnet (RG-Test)
Subnet *	default
Staging Location *	testsa13997 (StandardLRS)

Can't find your storage account ?

© 2023, Microsoft Azure. Used with permission from Microsoft.

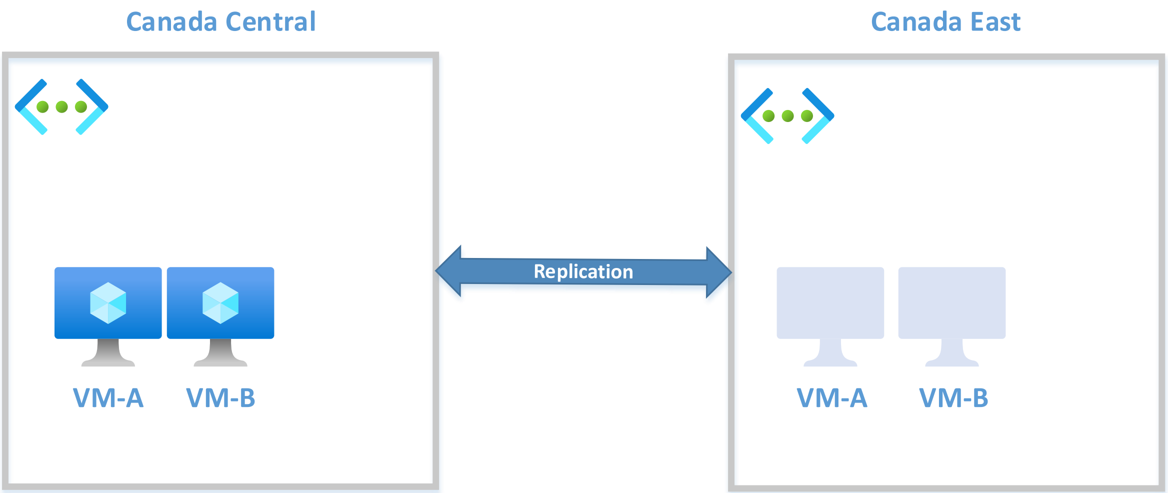
- □ Click the **Restore** button.
- □ When the deployment is complete, you should be able to see your second virtual machine.

- □ To delete the backup and recovery services vault, go to the backup item and stop the backup first.
- □ Delete your resources to avoid accruing costs.

Part 6: Replicate Azure VMs

Azure site recovery is a disaster recovery solution that provides replication of workloads running on physical and virtual machines, on-prem and in the cloud.

In this section, you'll create a replication set of virtual machines in a different region, as shown below. If the Canada Central region fails, the virtual machines and their workloads will be fully replicated and available in the Canada East region.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

☐ Create two inexpensive Windows VMs with the following settings:

- Resource group – Source-RG
- Region – **Canada Central**
- No infrastructure redundancy
- Security type – Standard
- Ports – RDP and HTTPS
- Both in the same subnet

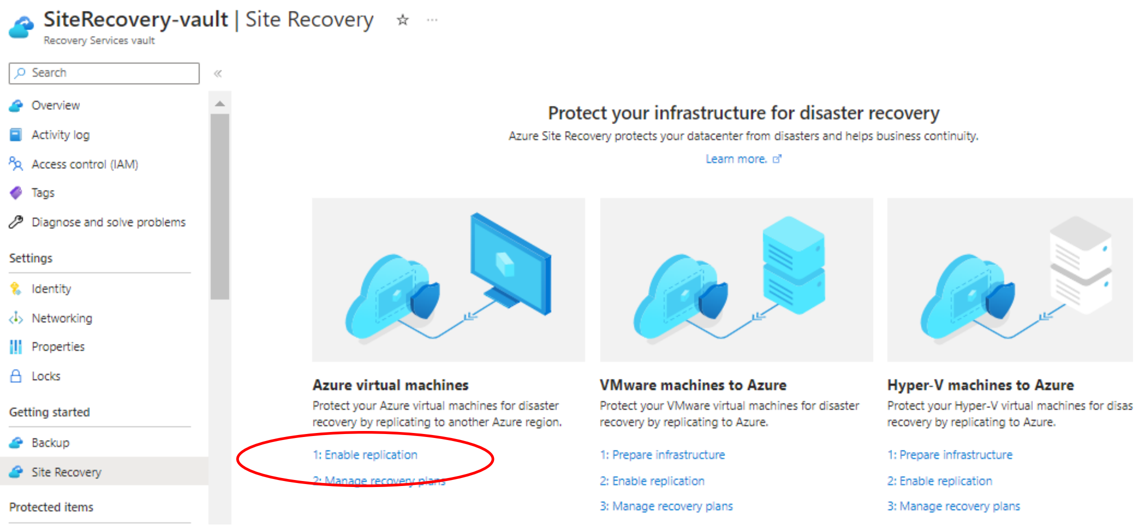
☐ When the resources are created, update the operating systems and reboot.

Note: The most updated root certificates are required.

☐ Create a recovery services vault in a resource group called **Destination-RG** in the **Canada East** region.

☐ When the vault is complete, go to the main page and select **+ Enable Site Recovery** from the top menu.

☐ Under the *Azure virtual machines* section, select **1. Enable replication**.



Protect your infrastructure for disaster recovery

Azure Site Recovery protects your datacenter from disasters and helps business continuity.

Learn more.

Azure virtual machines

Protect your Azure virtual machines for disaster recovery by replicating to another Azure region.

1: Enable replication

2: Manage recovery plans

VMware machines to Azure

Protect your VMware virtual machines for disaster recovery by replicating to Azure.

1: Prepare infrastructure

2: Enable replication

3: Manage recovery plans

Hyper-V machines to Azure

Protect your Hyper-V virtual machines for disas recovery by replicating to Azure.

1: Prepare infrastructure

2: Enable replication

3: Manage recovery plans

© 2023, Microsoft Azure. Used with permission from Microsoft.

First, select what you want to replicate.

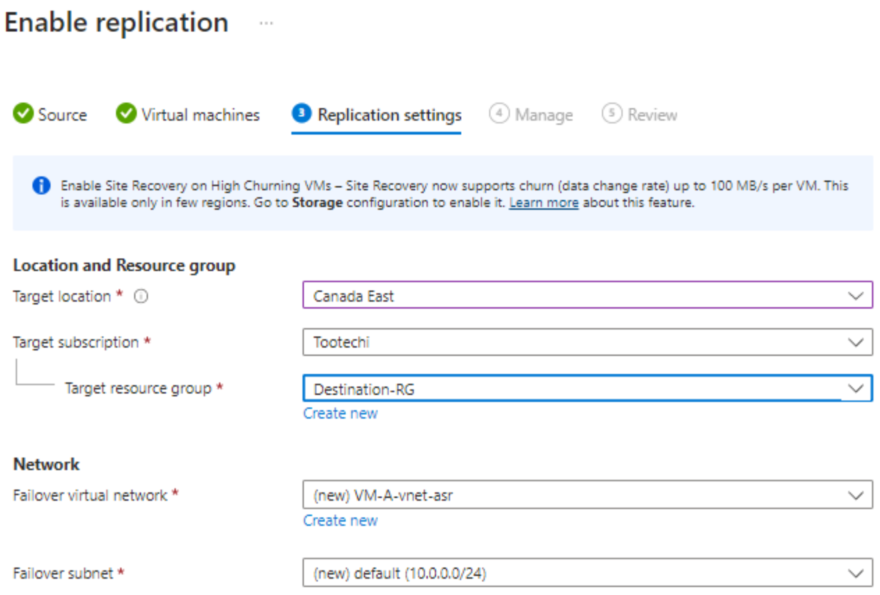
☐ Select **Canada Central** as the region, the source resource group for your virtual machines. The deployment model should be **Resource Manager** and the availability zones setting should be **No**.

☐ Click the **Next** button.

☐ Select both of your VMs and click **Next**.

Now, select where you want to replicate.

☐ Select **Canada East** as the region, and then complete the configuration as shown below.



Enable Site Recovery on High Churning VMs – Site Recovery now supports churn (data change rate) up to 100 MB/s per VM. This is available only in few regions. Go to **Storage** configuration to enable it. Learn more about this feature.

Location and Resource group

Target location *	Canada East
Target subscription *	Tootechi
Target resource group *	Destination-RG

Network

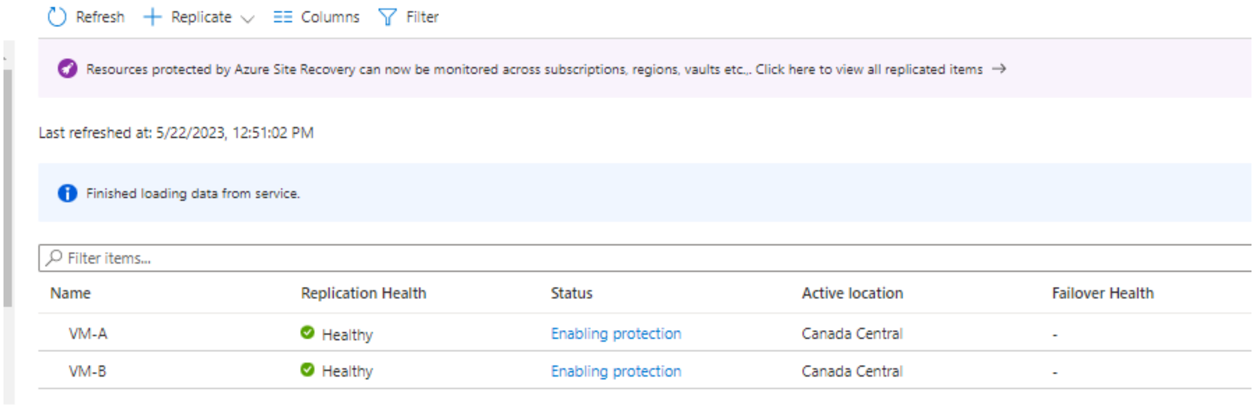
Failover virtual network *	(new) VM-A-vnet-asr
Failover subnet *	(new) default (10.0.0.0/24)

© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Review the other options and click the **Next** button.

□ Review the default management selections, click **Next** and enable replication.

□ When the resource is complete, select **Replicated Items** from the main page. You should see your VMs.



Resources protected by Azure Site Recovery can now be monitored across subscriptions, regions, vaults etc.. Click here to view all replicated items →

Last refreshed at: 5/22/2023, 12:51:02 PM

Finished loading data from service.

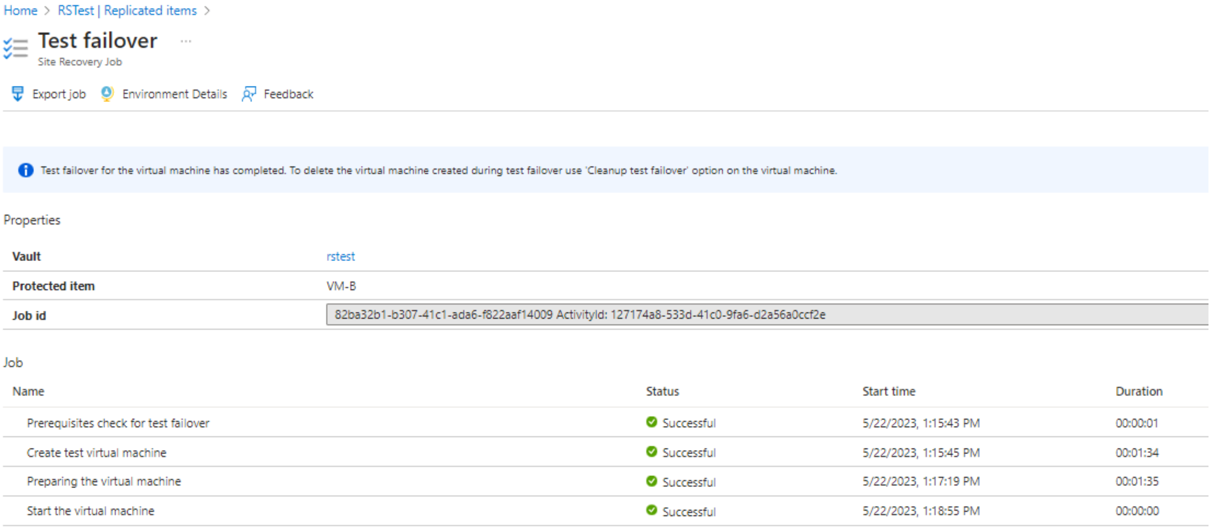
Filter items...

Name	Replication Health	Status	Active location	Failover Health
VM-A	✓ Healthy	Enabling protection	Canada Central	-
VM-B	✓ Healthy	Enabling protection	Canada Central	-

© 2023, Microsoft Azure. Used with permission from Microsoft.

It may take some time to fully replicate the VMs, but the Status should say **protected** when completed.

□ Select one of your VMs and click **Test Failover**.



Test failover

Site Recovery Job

Test failover for the virtual machine has completed. To delete the virtual machine created during test failover use 'Cleanup test failover' option on the virtual machine.

Properties

Vault	rstest
Protected item	VM-B
Job id	82ba32b1-b307-41c1-ada6-f822aaf14009 ActivityId: 127174a8-533d-41c0-9fa6-d2a56a0ccf2e

Job

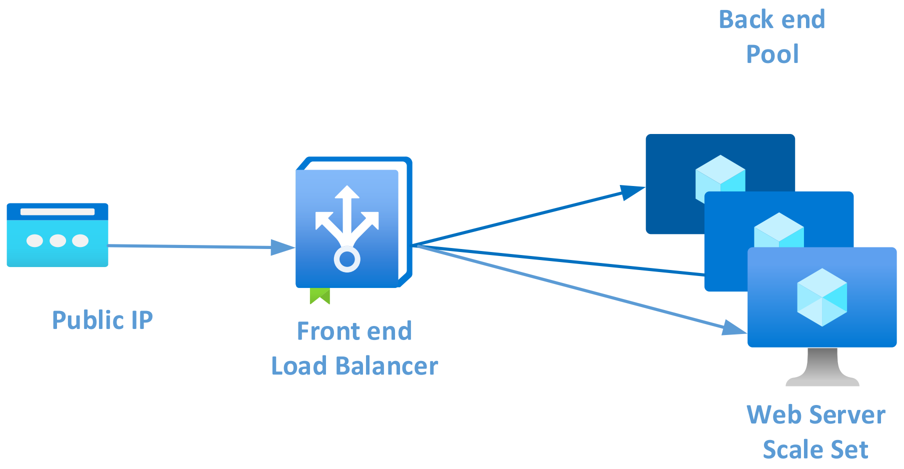
Name	Status	Start time	Duration
Prerequisites check for test failover	✓ Successful	5/22/2023, 1:15:43 PM	00:00:01
Create test virtual machine	✓ Successful	5/22/2023, 1:15:45 PM	00:01:34
Preparing the virtual machine	✓ Successful	5/22/2023, 1:17:19 PM	00:01:35
Start the virtual machine	✓ Successful	5/22/2023, 1:18:55 PM	00:00:00

© 2023, Microsoft Azure. Used with permission from Microsoft.

Part 7: Create a Load Balancer

In the compute section of this course, you discussed scale sets: automatically increasing or decreasing the number of identical VMs based on a schedule or a change in the load. For example, if you sell products on a website that runs on an Az VM, and traffic to the website increases in the evenings and decreases overnight, scale sets allow you to have the right amount of processing power. But you wouldn't want clients using different IP addresses to access different servers. You want your clients to see the scale set as a single site and have your service redirect them to the best server. This is done using load balancers.

A load balancer can have a single, public-facing IP address and redirect the requests to the servers based on the load balancing rules. It can also monitor the health of the servers.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

☐ Open the **Virtual Machine Scale Set** tool and select **Create a Virtual Machine Scale Set**.

☐ Fill in the resource group, name and region.

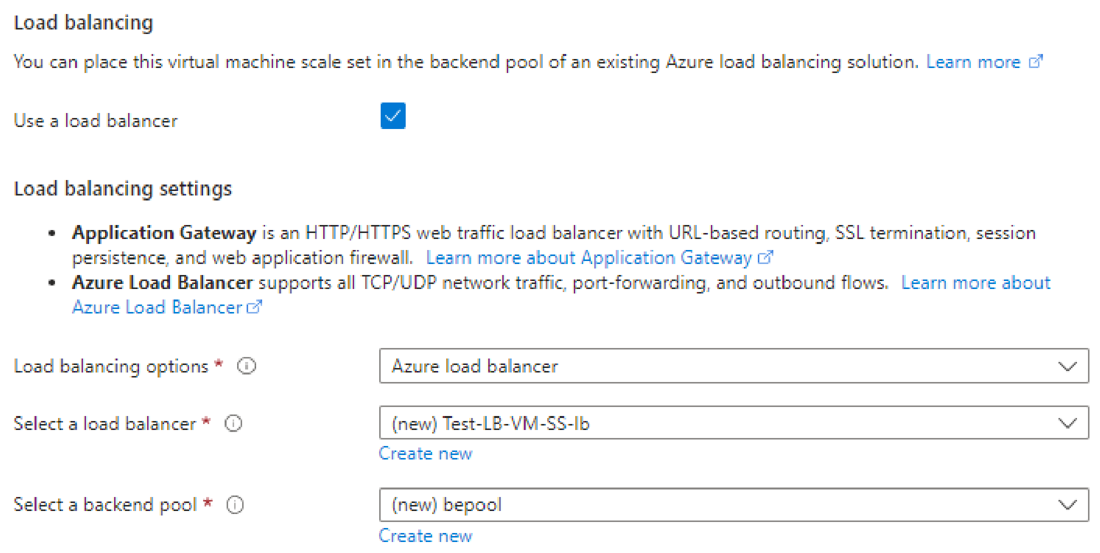
☐ Select **Flexible** orchestration mode, enter your username and password and forward to the networking page.

☐ There will be a NIC associated with the VNet. Click the pencil icon to edit it.

☐ Change the Public IP Address to **disabled** and click **OK**.

☐ Select **Use a Load Balancer**.

Load balancing options appear.



Load balancing

You can place this virtual machine scale set in the backend pool of an existing Azure load balancing solution. Learn more

Use a load balancer ☑

Load balancing settings

- **Application Gateway** is an HTTP/HTTPS web traffic load balancer with URL-based routing, SSL termination, session persistence, and web application firewall. Learn more about Application Gateway
- **Azure Load Balancer** supports all TCP/UDP network traffic, port-forwarding, and outbound flows. Learn more about Azure Load Balancer

Load balancing options * : Azure load balancer

Select a load balancer * : (new) Test-LB-VM-SS-lb
Create new

Select a backend pool * : (new) bepool
Create new

© 2023, Microsoft Azure. Used with permission from Microsoft.

Azure has three load balancer SKUs:

- Basic – for small-scale applications that don't need high availability or redundancy.
- Standard – for low-latency, high-performance network layer traffic
- Gateway – makes routing decisions based on attributes of HTTP request

Note: You can read more about the SKUs at: Azure Load Balancer SKUs (https://learn.microsoft.com/en-us/azure/load-balancer/skus).

☐ In the **Load Balancing Options** select **Azure Load Balancer**.

☐ Review and create the set.

☐ When the resources are finished, go to the resource group and select the load balancer.

☐ Read the document describing the components of the system at: Azure Load Balancer components (https://learn.microsoft.com/en-us/azure/load-balancer/components).

☐ Find each of the components on the blade menu and review the default settings.

☐ Using the tutorial: Quickstart: Create a public load balancer to load balance VMs using the Azure CLI (https://learn.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-cli), create a public load balancer to load balance VMs using the Azure CLI.