Contents

[AZURE MONITOR AND BACKUP 2](#_Toc156832972)

[AZURE MONITORS 2](#_Toc156832973)

[KEY FEATURES OF AZURE MONITORS 2](#_Toc156832974)

[AZURE MONITORING – METRICES 2](#_Toc156832975)

[AZURE MONITORING – ACTIVITY LOGS 4](#_Toc156832976)

[AZURE MONITORING – ALERTS 4](#_Toc156832977)

[LOG ANALYTICS WORKSPACE 7](#_Toc156832978)

[CREATING A LOG ANALYTICS WORKSPACE 8](#_Toc156832979)

[SENDING DATA TO LOG ANALYTICS 9](#_Toc156832980)

[CREATING DATA COLLECTION 9](#_Toc156832981)

[CONNECTING A VM TO LOG ANALYTICS WORKSPACE 12](#_Toc156832982)

[CONNECTING ANOTHER VMs TO LOG ANALYTICS WORKSPACE 13](#_Toc156832983)

[LOG ANALYTICS QUERIES 15](#_Toc156832984)

[CUSTOM LOGS 15](#_Toc156832985)

[AZURE BACKUP 19](#_Toc156832986)

[BACKUP PROCESS 19](#_Toc156832987)

[AZURE SITE RECOVERY 28](#_Toc156832988)

# AZURE MONITOR AND BACKUP

## AZURE MONITORS

* Azure Monitoring is a service in Microsoft Azure that provides comprehensive monitoring and diagnostics capabilities for your applications, infrastructure, and services deployed in Azure.
* It helps us gain insights into the performance, health, and availability of your resources, enabling you to proactively identify and resolve issues.

### KEY FEATURES OF AZURE MONITORS

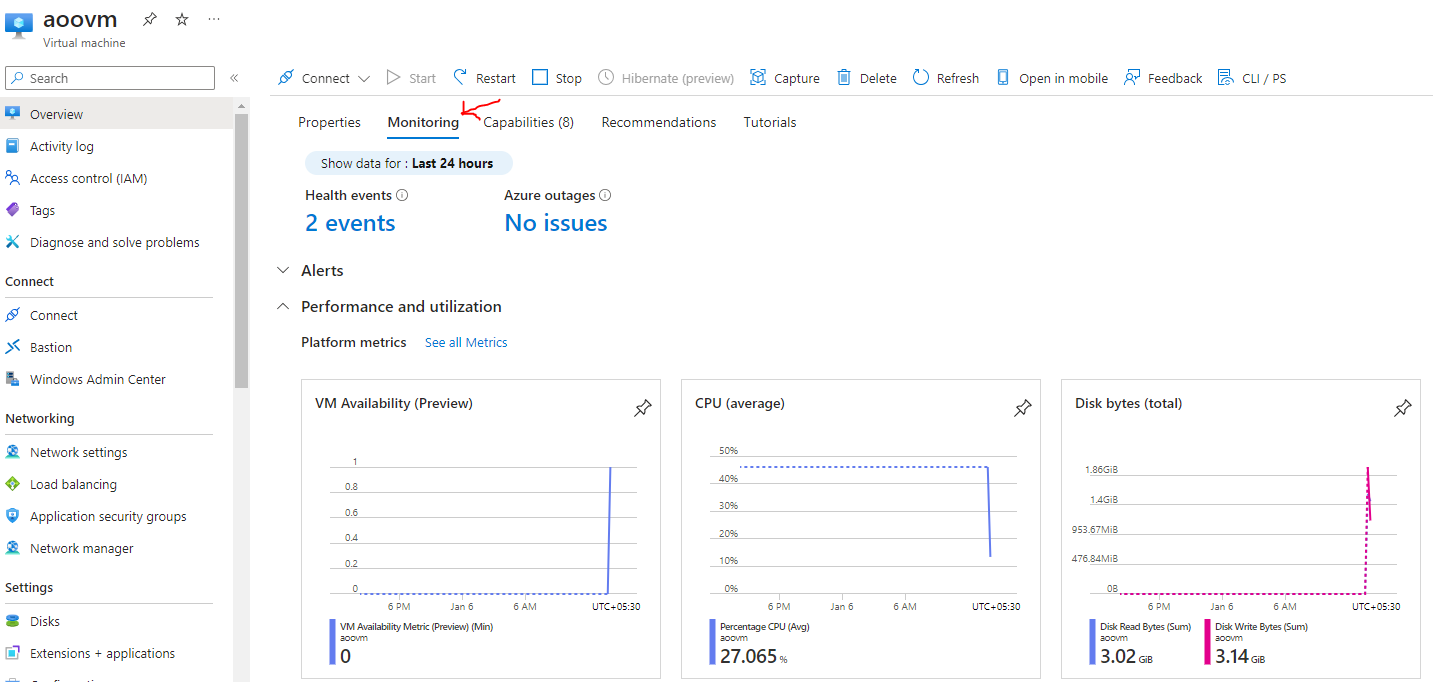
* METRICS AND LOGS
  + Azure Monitoring collects and analyzes metrics and logs from various Azure services, virtual machines, and custom applications.
  + It provides a centralized view of performance data, allowing us to monitor resource utilization, detect anomalies, and troubleshoot issues.
* ALERTS AND NOTIFICATIONS
  + **We can configure alerts based on predefined conditions or custom queries to be notified when certain events or metrics exceed defined thresholds.**
  + Azure Monitoring can send notifications via email, SMS, or integrate with other communication channels like Azure Logic Apps or Microsoft Teams.
* APPLICATION INSIGHTS
  + Application Insights, a component of Azure Monitoring, provides application performance monitoring (APM) capabilities.
  + It helps us to monitor the performance and availability of the web applications, track user sessions, detect failures, and analyze application dependencies.
* LOG ANALYTICS
  + Azure Monitoring includes Log Analytics, which allows us to collect, analyze, and visualize log data from various sources, including Azure resources, virtual machines, and custom applications.
  + It supports powerful query capabilities and offers insights into system behavior and application logs.
* AZURE MONITOR FOR CONTAINERS
  + Azure Monitor for containers helps us to monitor the performance and health of your containerized applications running on Azure Kubernetes Service (AKS) or Azure Container Instances (ACI).
  + It provides metrics, logs, and diagnostics specific to container workloads.
* AZURE MONITOR FOR VMS
  + Azure Monitor for VMs provides monitoring and diagnostics capabilities for virtual machines (VMs) running in Azure.
  + It helps us track VM performance, detect issues, and troubleshoot problems related to CPU, memory, disk, and network usage.

|  |  |
| --- | --- |
| METRICES | * We can view the metrices of Azure resources. For example – For Azure VM , we can view CPU usage, Disk metrices , Network stats etc.. * We can create alerts of these metrices (For example – Sending an alert when CPU utilization go beyond certain threshold for a VM) |
| ACTIVITY LOGS | * Activity logs are generated for management activities on the Azure resource like Starting / Stopping the VMs, Creating VMs etc. * We can create alerts based on these activities |
| LOGS ANALYTICS WORKSPACE | * This the centralized solution for all logs in Azure * We can send application and resource logs to Log analytics workspace |
| APPLICATION INSIGHT | * Performance Management system of the live application. For example - Performance of the web app |

### AZURE MONITORING – METRICES

#### AZURE MONITORING – RESOURCE LEVEL

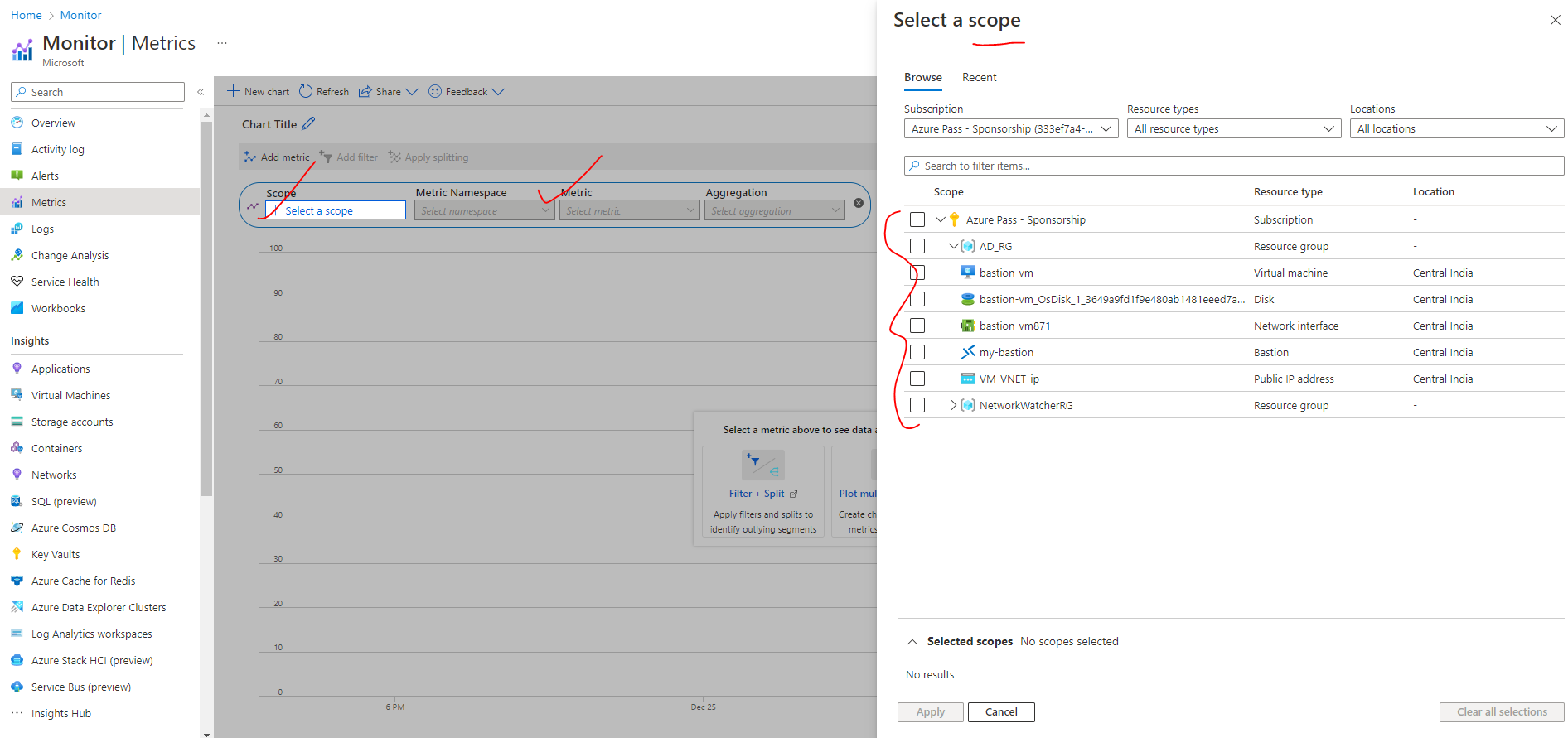
* Monitoring can be done on resource level itself. For example – Metrices for a VM can be captured from VM level itself

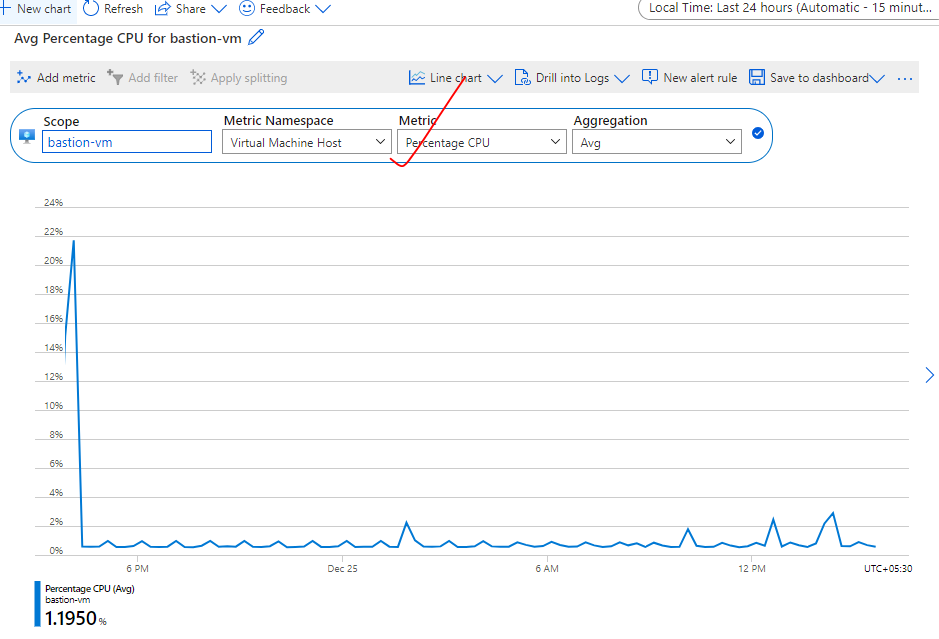


#### METRICES FROM MONITORING SERVICES

To monitor any azure resources based on some metrices

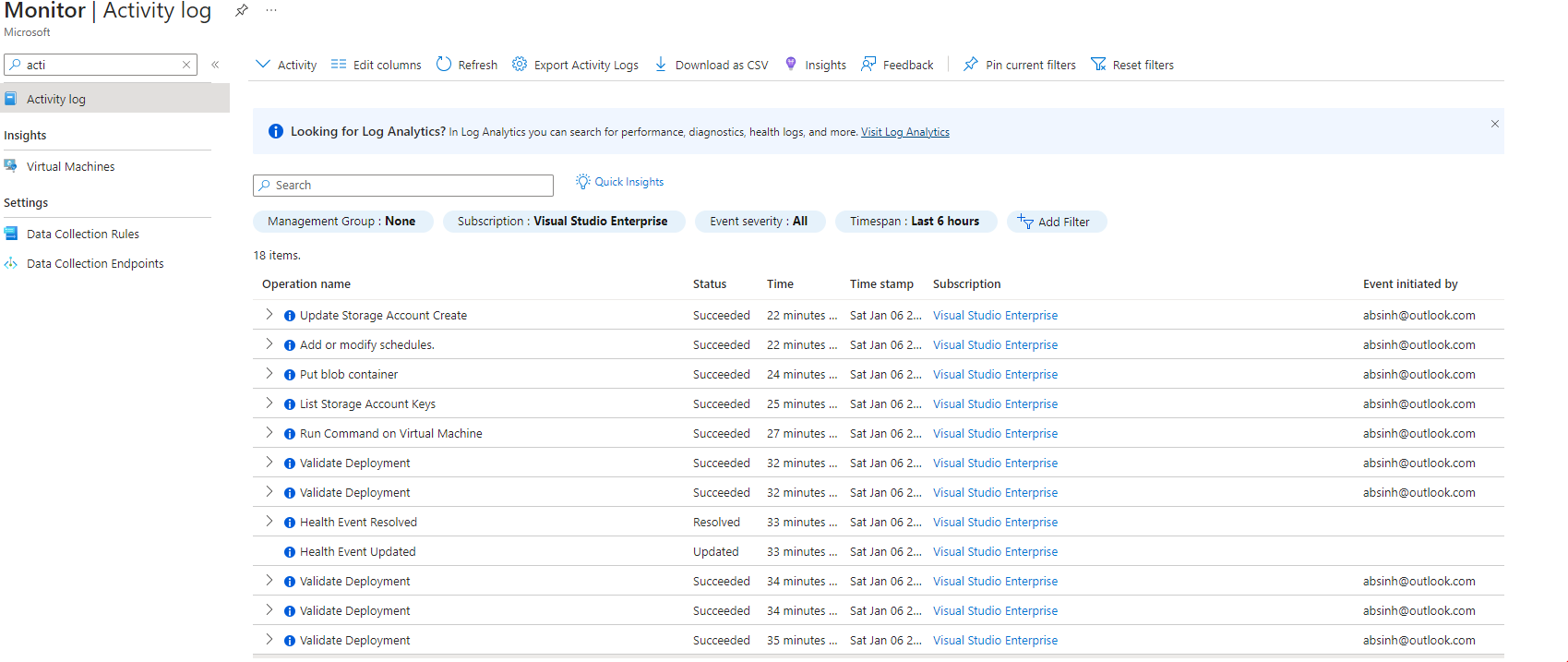
* Select the scope (The resources of which we want to graph / monitor the service)
* Select the metric which we want to capture for a given resource (like CPU Percentage etc..)





### AZURE MONITORING – ACTIVITY LOGS

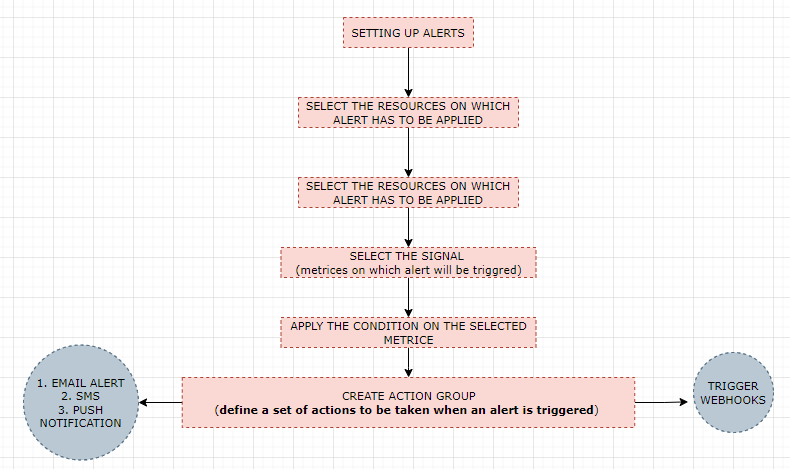
* Logs of control plane activity (administrator activity) for example Starting / Stopping /Deleting VM or deleting Storage Account. All these admin activities are recorded in the activity logs



### AZURE MONITORING – ALERTS

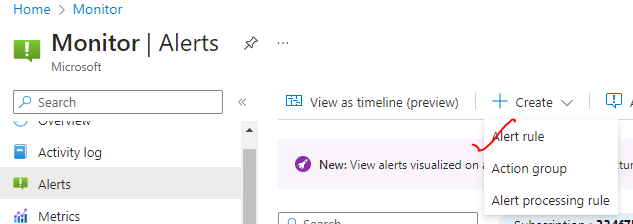
* We can create logs based on metrices or activity logs



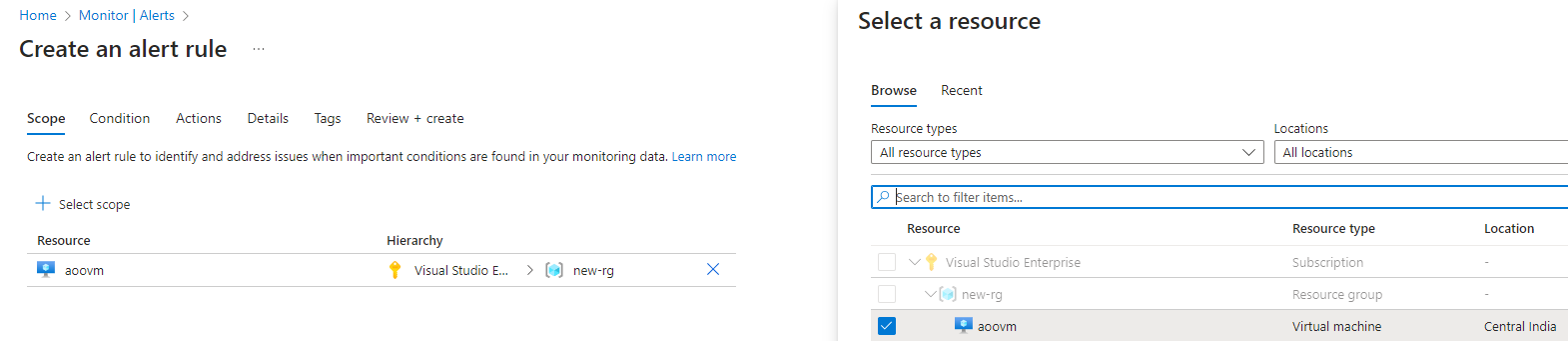


CREATE ALERT RULE

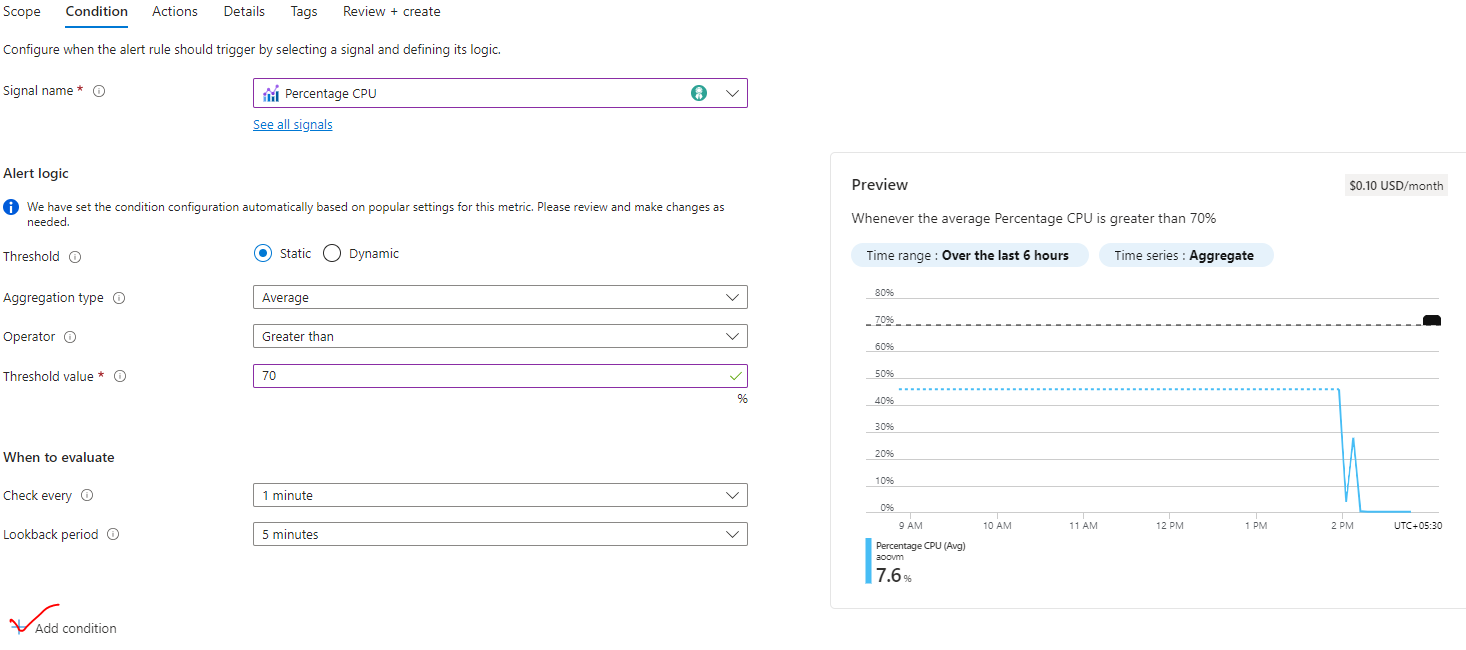
* Navigate to Monitor Service 🡪 Alerts -🡪 Alert Rule



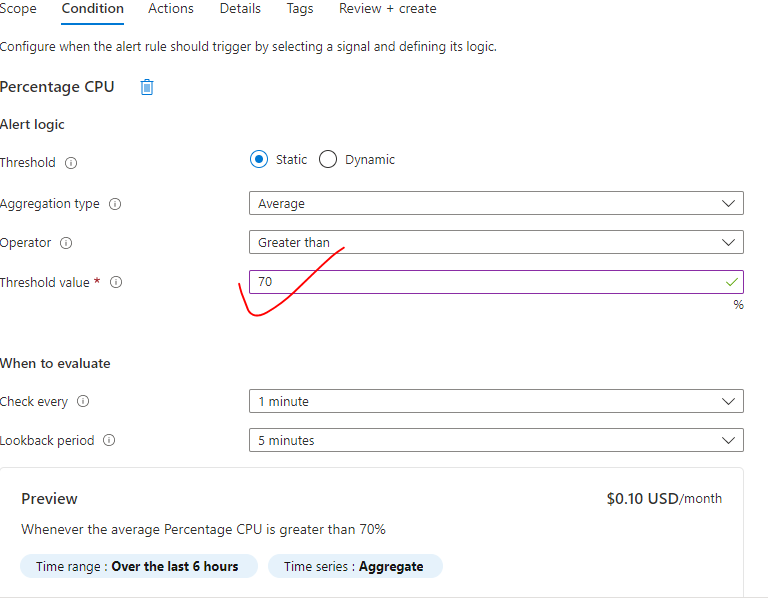
* STEP 1: SELECT THE SCOPE (AZURE RESOURCE TO BE MONITORED)



* **STEP 2: CREATE THE SIGNAL NAME AND THE CONDITION ON WHICH WE WANT TO TRIGGER THE ALERT**



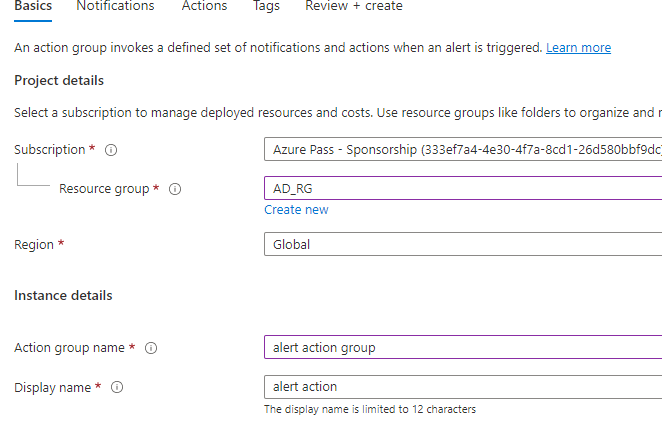
Step 3: Based on metrices (example – if want to trigger the alert when CPU percentage go beyond 70%)

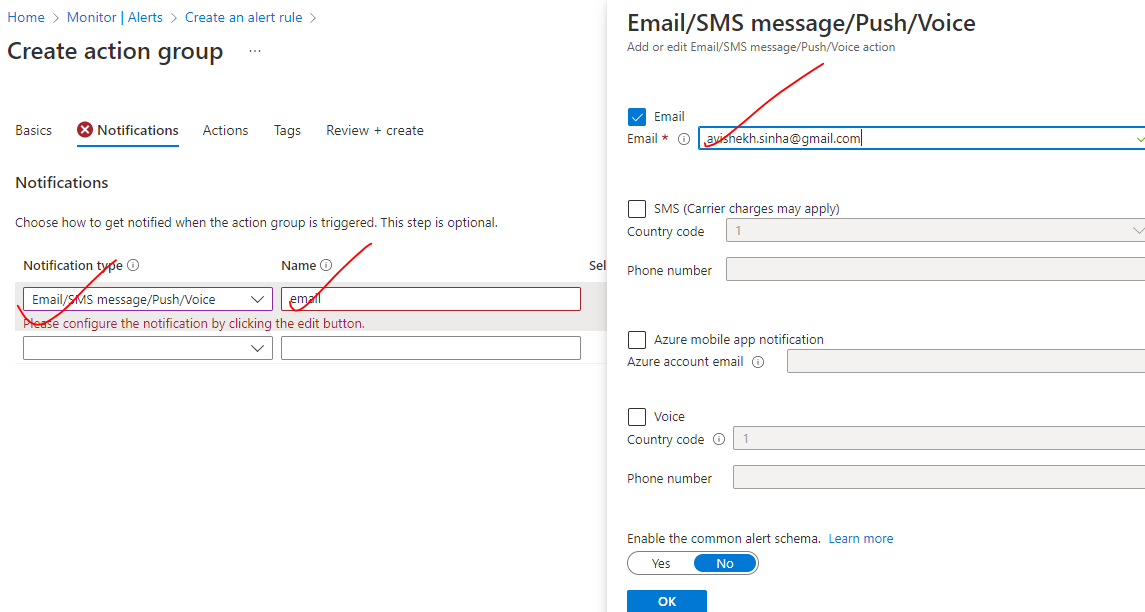


|  |  |
| --- | --- |
| **CHECK EVERY** | Check the CPU utilization metrices every 1 min |
| **LOOPBACK PERIOD** | While checking the metrices – consider the time span of last 5 mins |

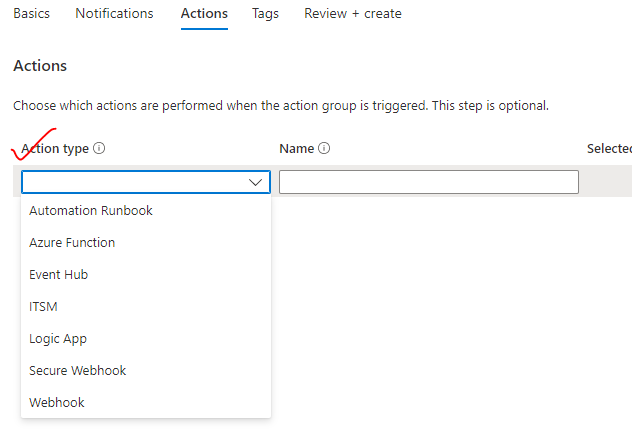
SET UP THE ACTION GROUP

* In Azure Monitoring, an Action Group is a collection of notification preferences and actions that determine how alerts are handled and communicated when specific conditions are met.
* **It allows us to define a set of actions to be taken when an alert is triggered, such as sending emails, SMS messages, making phone calls, or invoking webhooks.**

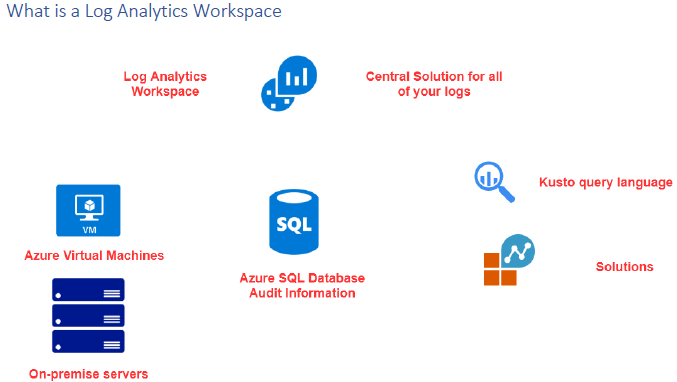




* We can configure an action when the action group is triggered



## LOG ANALYTICS WORKSPACE



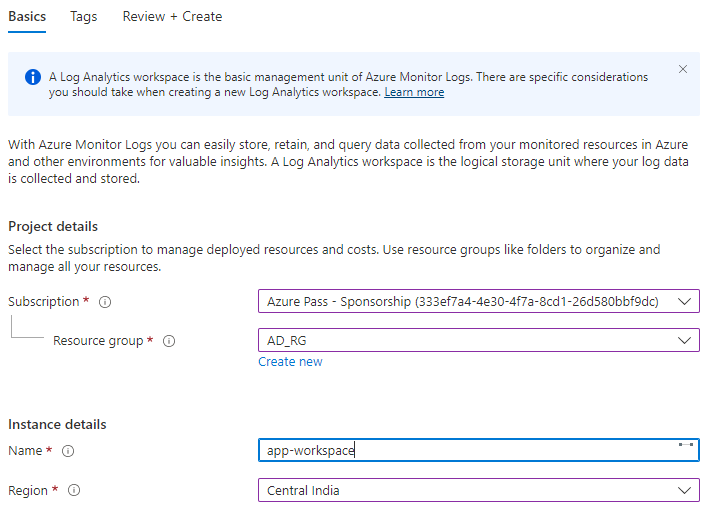
* A Log Analytics workspace is a central repository for storing and analyzing log data collected from various sources, such as Azure resources, virtual machines, on-premises systems, and custom applications.
* It is a key component of Azure Monitor, providing powerful query and analytics capabilities for log data.

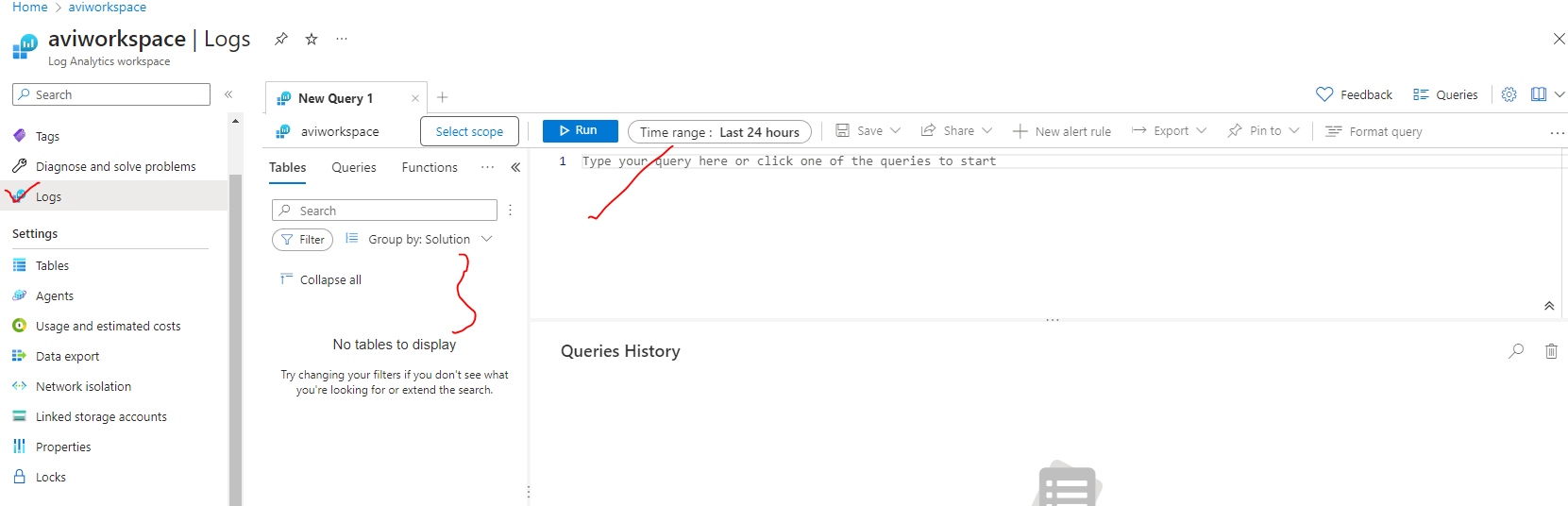
ASPECTS OF LOG ANALYTICS WORKSPACES

* DATA COLLECTION
  1. Log Analytics workspaces collect and ingest log data from various sources. This includes logs generated by Azure resources (such as virtual machines, storage accounts, and Azure Active Directory), as well as logs from on-premises systems and custom applications via agents or connectors.
* LOG DATA STORAGE
  1. Log Analytics workspaces provide a scalable and secure storage environment for log data.
  2. The data is retained for a specified retention period, which can be configured based on requirements.
* QUERY AND ANALYTICS
  1. Log Analytics workspaces offer a powerful **query language called KQL (Kusto Query Language)** that allows us to search, analyze, and visualize log data.
  2. We can perform complex queries, apply filters, join multiple data sources, and create custom visualizations and dashboards.
* ALERTING AND MONITORING
  1. Log Analytics workspaces integrate with Azure Monitor, enabling us to set up alerts based on specific log events or conditions.
  2. We can configure alert rules to trigger notifications or take automated actions when certain log data matches defined criteria.
* INTEGRATION WITH AZURE SERVICES
  1. Log Analytics workspaces seamlessly integrate with other Azure services, such as Azure Monitor, Azure Security Center, and Azure Sentinel. This allows you to leverage log data for monitoring, security, and compliance purposes.

### CREATING A LOG ANALYTICS WORKSPACE

* Search and create “Log Analytics workspace”. Note As it a central logging system - the workspace can be created in any region (independent of the location the resources of which logging will captured) 🡪 Review +Create
* To avoid the cross-region data transfer charges – it always better to create the workspace in the same region.





In the logs section

* On the left-hand side - We ideally see is some tables having log data.
* On the right-hand side, we can write queries against the data that are stored in the tables.

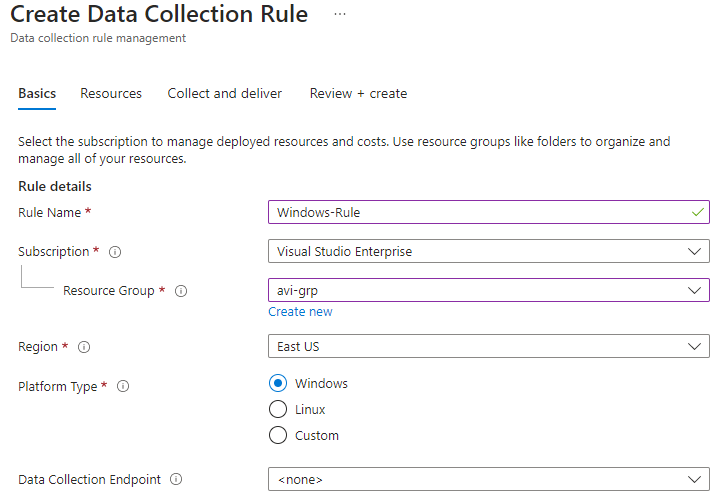
### SENDING DATA TO LOG ANALYTICS



### CREATING DATA COLLECTION

* Go to Azure Monitor Service 🡪 Data Collection Rules 🡪 Create

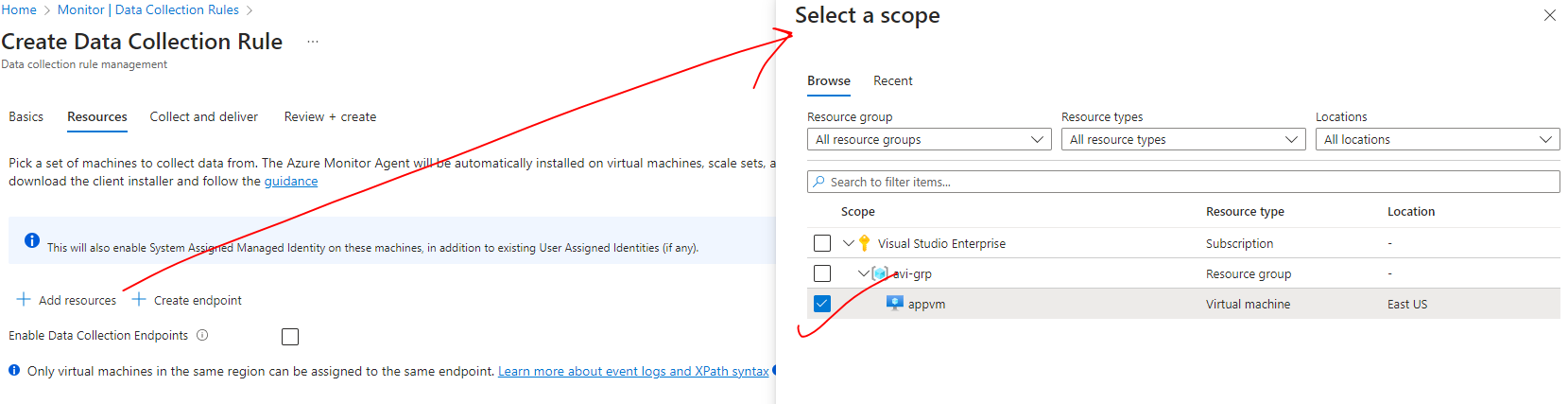
#### STEP 1: CONFIGURE DATA COLLECTION



* **PLATFORM TYPE**: The is the platform of the resource from where we want to collect the data/ logs from.

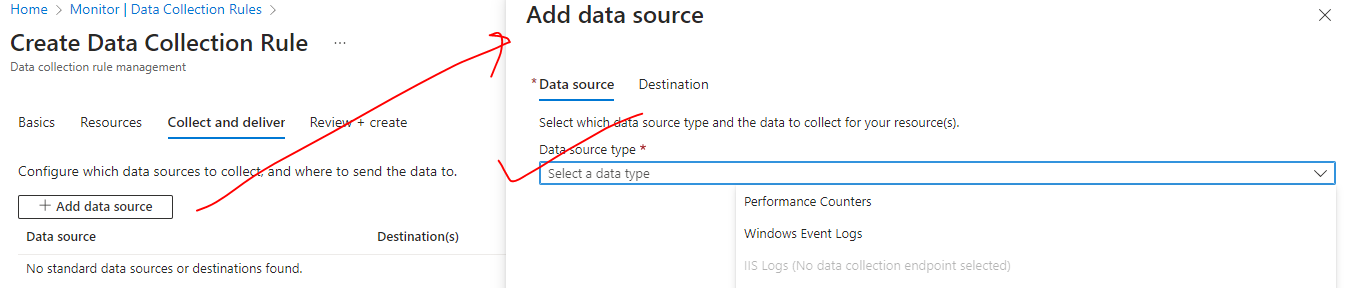
#### STEP 2: ADD THE RESOURCE

* Add the resource added for the data collection rule from where we want to collect the data from



#### STEP 3: ADD THE DATA SOURCE

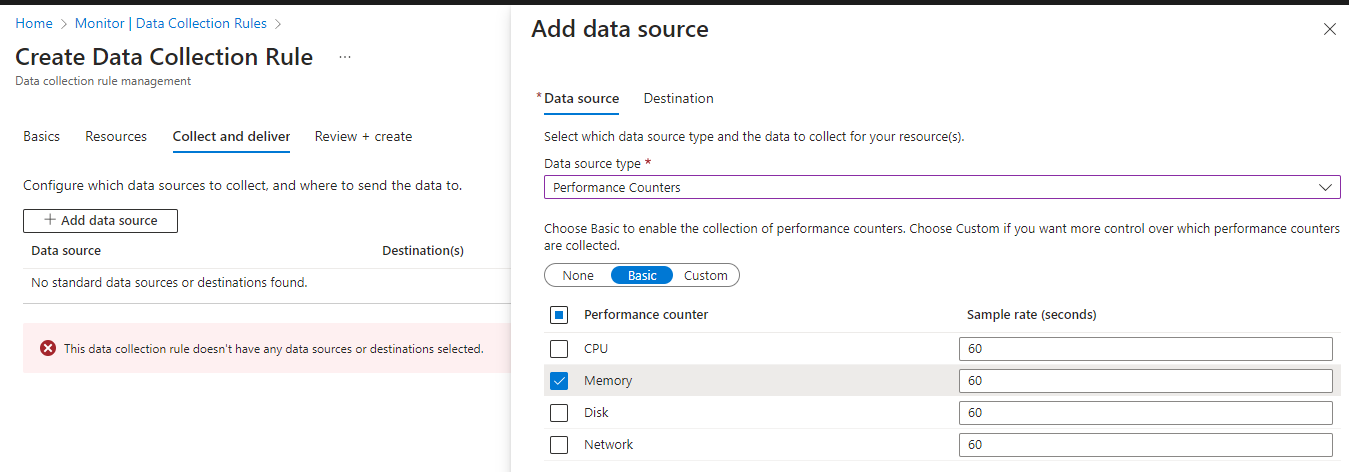
* In this step – we define what type of data we want to capture (Data Source Type)



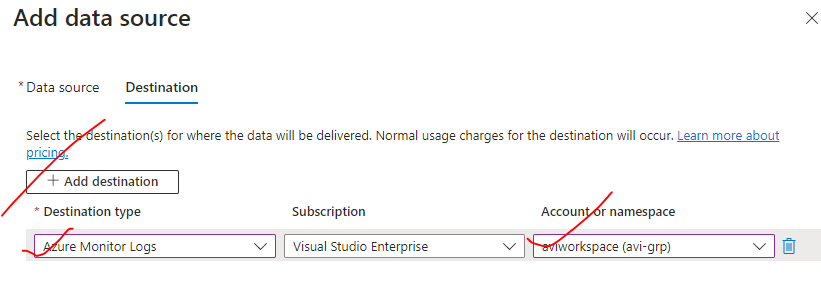
For example, for Windows VM - we have the option of choosing

|  |  |
| --- | --- |
| **PERFORMANCE COUNTERS** | * Performance counters is the performance metrics of the underlying Windows server. |
| **WINDOWS EVENT LOGS** | * Window OS Logs |

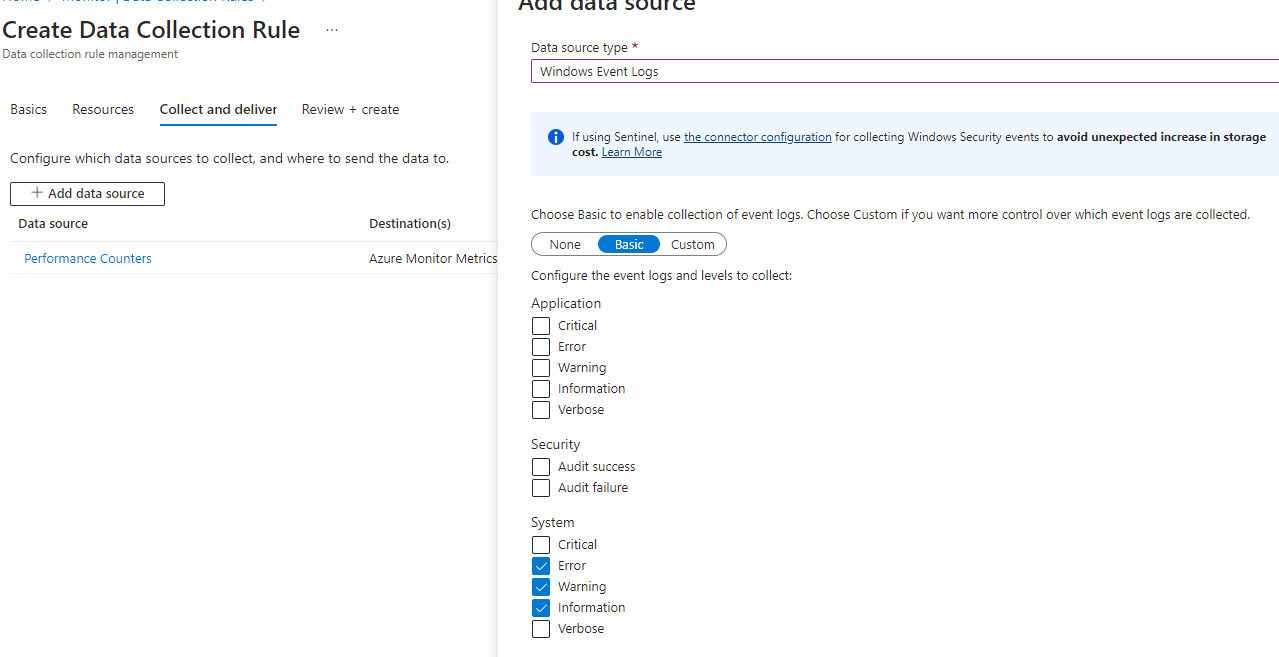
* Let’s select 🡪 Performance Counter. For now, let’s collect the data of Memory In Log Analytics
* Check “Memory” 🡪 Add data source



* Select the destination where want to send the logs to i.e Log Analytics work space 🡪 Save



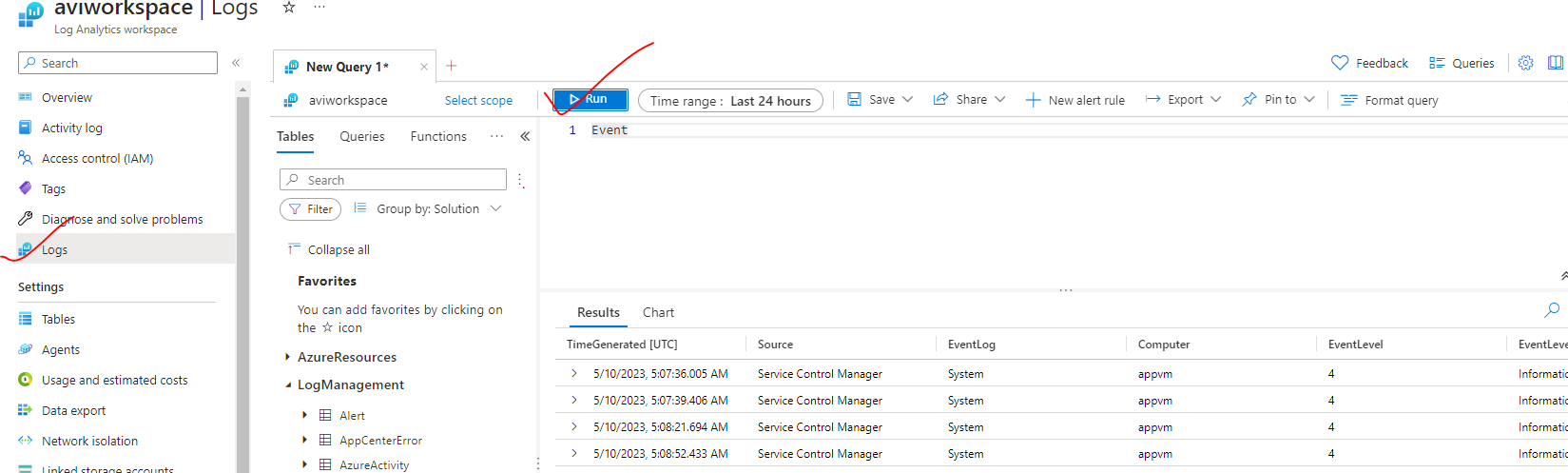
* If we want to collect Window logs data , then “Add Data Source” 🡪 Select the “Data Source type” as “Windows Event Logs” 🡪 select the desired options 🡪 Add Data Source



|  |  |
| --- | --- |
|  | * These are the 2 data source type we want to collect from Windows Based VM * In above use case – We configure the Monitor to collect the data for VM and send that data on to the log analytics workspace |

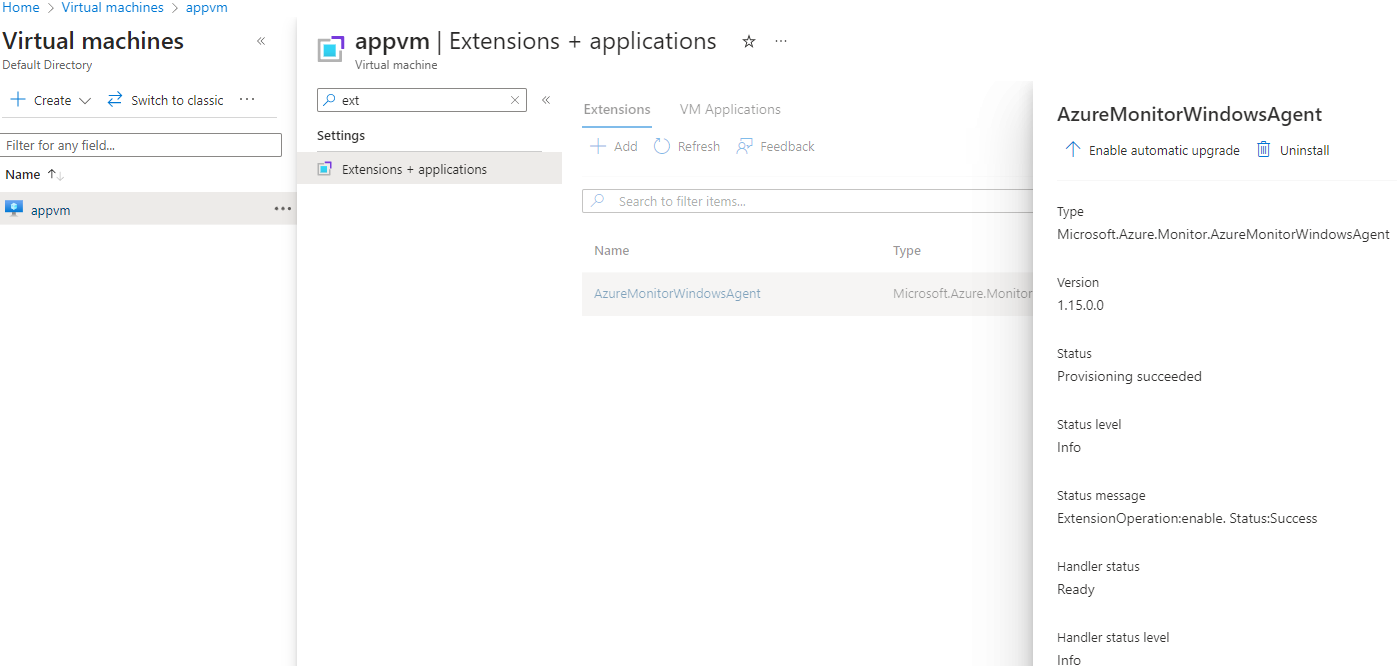
#### STEP 4: RUN QUERY TO FETCH THE LOGS

Go to Log Analytics Workspace 🡪 Logs



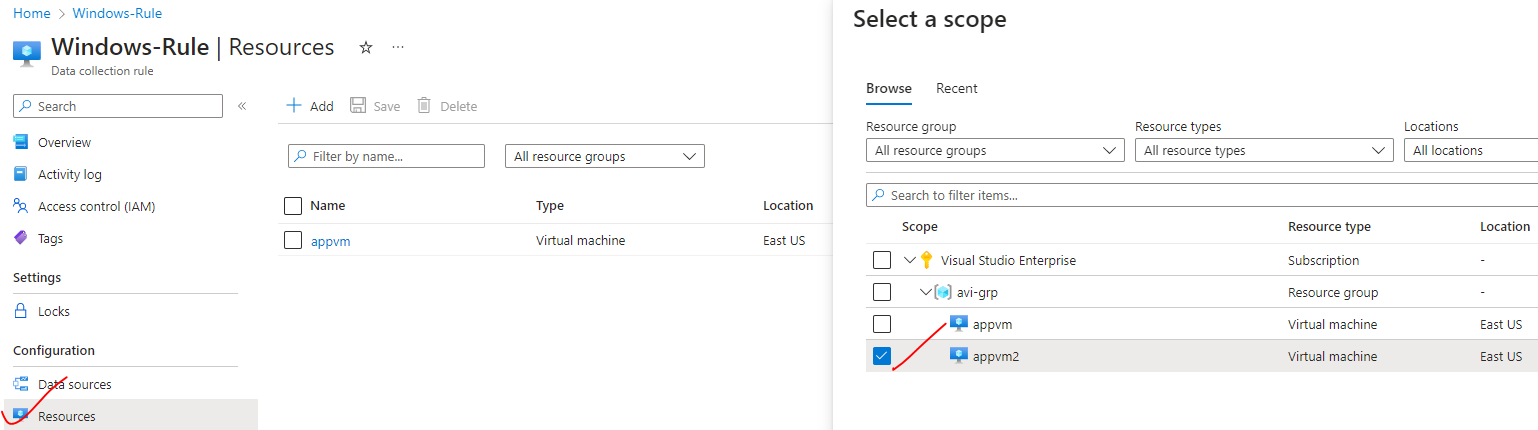
### CONNECTING A VM TO LOG ANALYTICS WORKSPACE

|  |  |
| --- | --- |
|  | * When you enable that feature of the data collection rule of sending data on to the log analytics workspace, there is a Windows agent that gets installed. * To view the installed extension 🡪 Go to VM 🡪 Extension+ application |



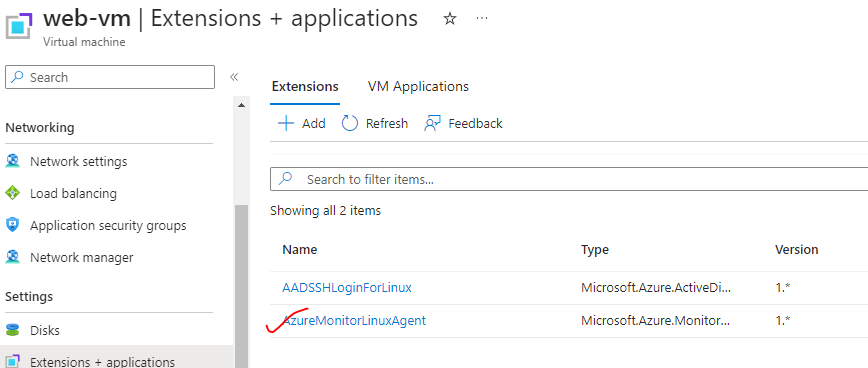
#### ATTACHING A NEWLY CREATED VM WITH LOG ANALYTICS WORKSPACE

* We can attach a newly created VM(**appvm2**) to the log analytics workspace🡪 Go to the “Data Collection rule”
* Go to the Resource 🡪 Select the new VM to be added🡪 Apply



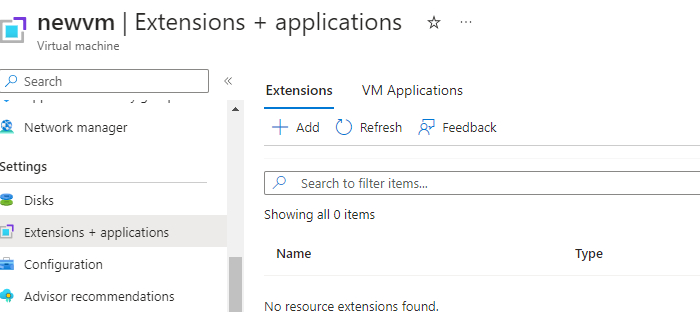
### CONNECTING ANOTHER VMs TO LOG ANALYTICS WORKSPACE

* When the VM is connected to Log Analytics workspace – it will install an extension to the VM based of type of VM

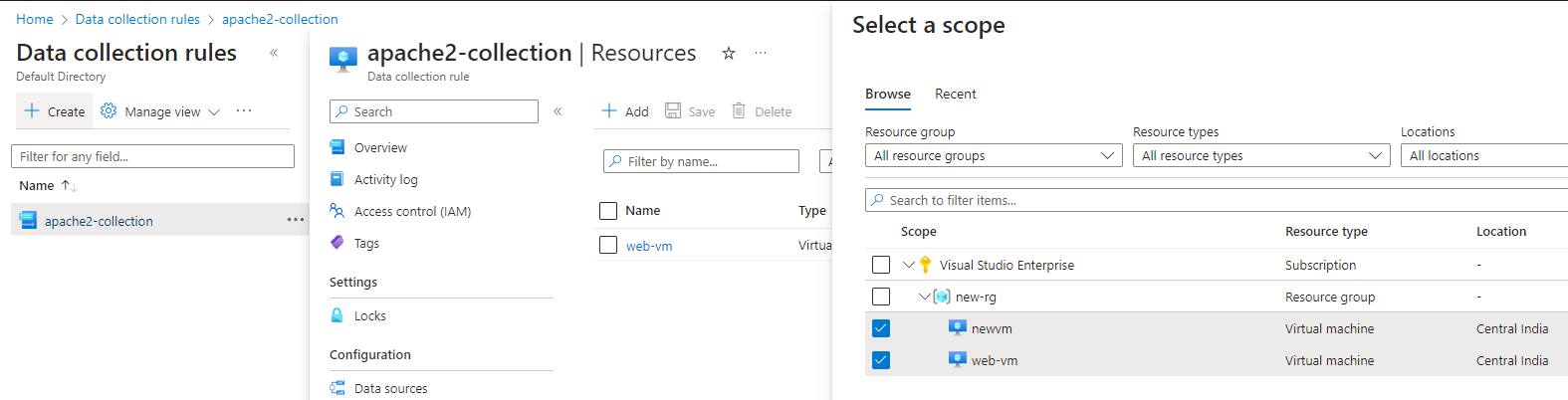


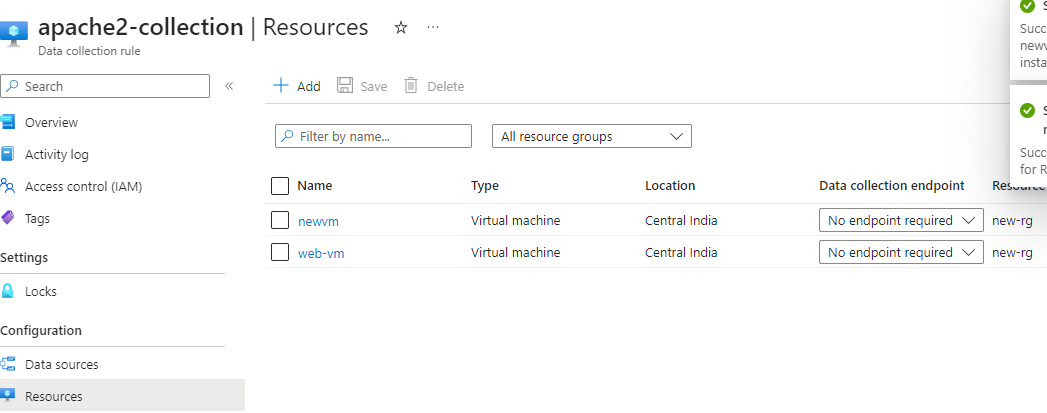
Now If want to add a new VM to the log analytics work space

* **Step 1: SET UP A NEW VM**
* **Step 2: The New VM will have no Agent extension installed.**

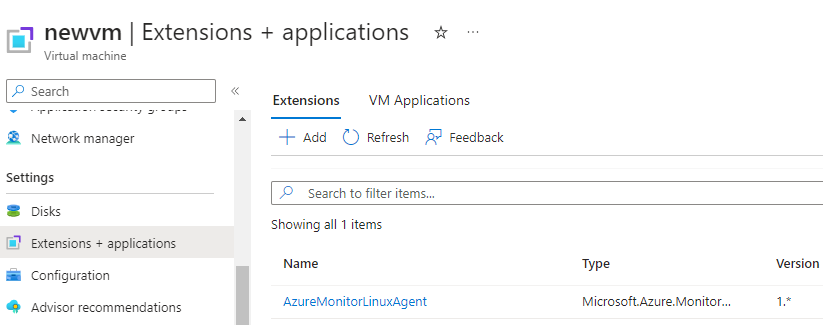
-

* **Step 3: Add the new VM in the data collection rules**





* **Step 4 : New Extension has been installed in the newVm**



### LOG ANALYTICS QUERIES

### CUSTOM LOGS

* Custom logs refer to logs that are not automatically collected by default log sources, such as Azure services or infrastructure components.
* Custom logs are logs that we can configure and send to Log Analytics from our own applications, services, or virtual machines.
* Custom logs allow us to collect and analyze specific logs that are important for our application or environment. This could include application logs, system logs, security logs, or any other type of log data that is relevant to your monitoring and analysis needs.
* By configuring a custom data source in Azure Log Analytics, we can define the log files or log patterns that we want to collect and send to the Log Analytics workspace. This enables us to centralize and analyze all the+ log data in a single location, along with other logs from Azure services and infrastructure components.

#### SETTING UP CUSTOM LOGS

Lets say we need to set up the custom logs in the log analytics workspace for nginx or apache2 installed on a Linux VM. Below are the steps we need to follow for the same

##### STEP 1: SET-UP A LINUX VM

* **Install Apache 2**

|  |  |
| --- | --- |
| COMMAND TO INSTALL APACHE2 WEBSERVER | sudo apt update  sudo apt install apache2 |

##### STEP 2: DOWNLOAD THE SAMPLE LOGS (E.G ACCESS.LOG) FOR APACHE2

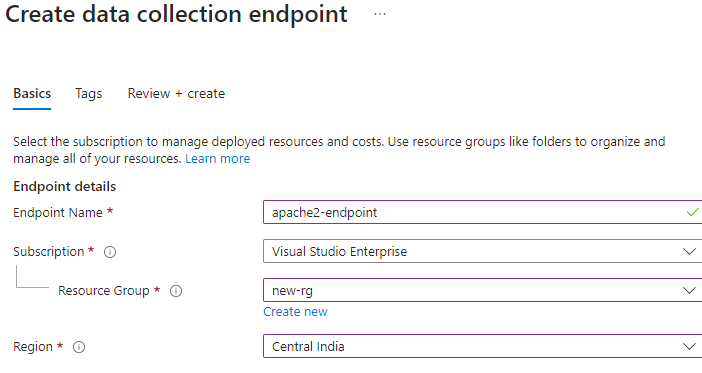
* + We need to download (using winscp)the sample logs to send across to the log analytics workspace so it can create a table accordingly. Why??
  + For Windows event logs, Microsoft already understands the structure and what type of data is being sent or is present in the Windows event logs. That's why it already has these inbuilt tables that can consume or can store that log information.
  + But for custom logs, apache2 has its own structure when it comes to storing logs that it needs to be stored in a different table. So a new table needs to be in place for this.

SAMPLE ACCESS LOGS(APACHE2 WEBSERVER)

|  |
| --- |
| 34.145.227.243 - - [06/Jan/2024:10:54:53 +0000] "GET / HTTP/1.1" 200 11229 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome  /120.0.0.0 Safari/537.36"  198.203.181.181 - - [06/Jan/2024:10:54:54 +0000] "GET / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome  /120.0.0.0 Safari/537.36"  34.145.165.227 - - [06/Jan/2024:10:54:55 +0000] "GET /favicon.ico HTTP/1.1" 404 493 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck  34.145.227.243 - - [06/Jan/2024:10:54:53 +0000] "GET / HTTP/1.1" 200 11229 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome  /120.0.0.0 Safari/537.36" |

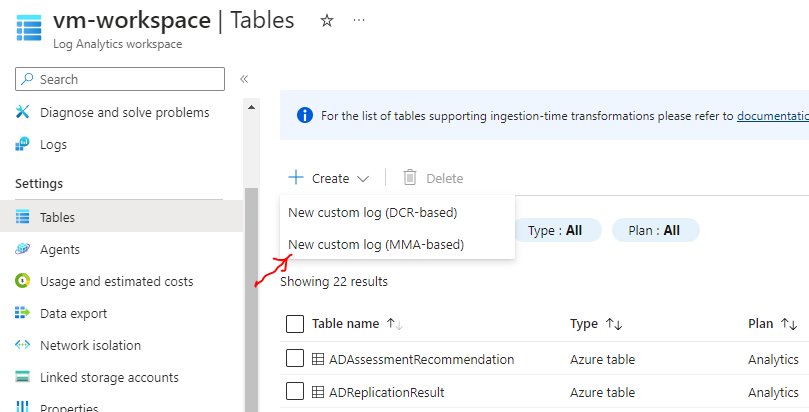
##### STEP 3: CREATE A DATA COLLECTION ENDPOINT

* To send data to Log analytics workspace we need to set up a data collection endpoint

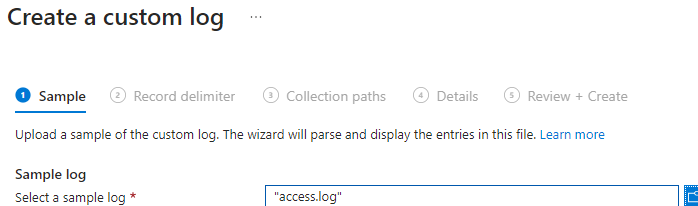


##### STEP 4: CREATE TABLE IN LOG ANALYTICS WORKSPACE

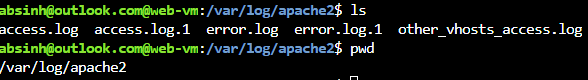
* **Navigate to Log Analytics workspace 🡪 Table**
* **Create MMA based custom logs.**



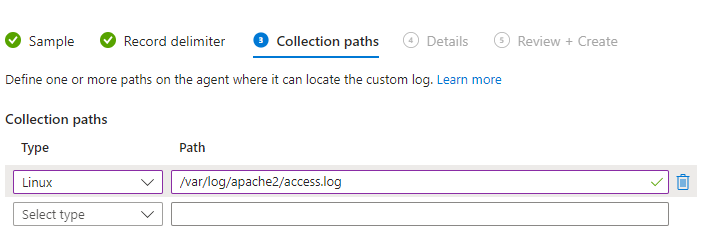
* **Upload the sample logs(e.g access.log)**



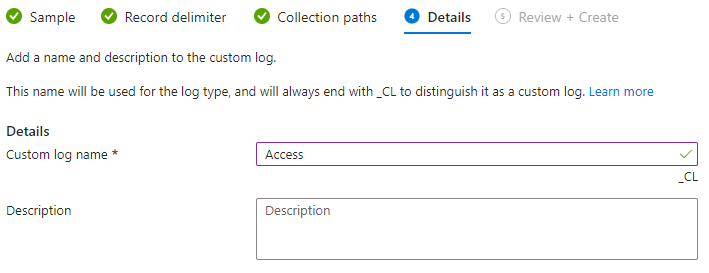
* **Give the path of the log where it has to tracked . For example, access.log**

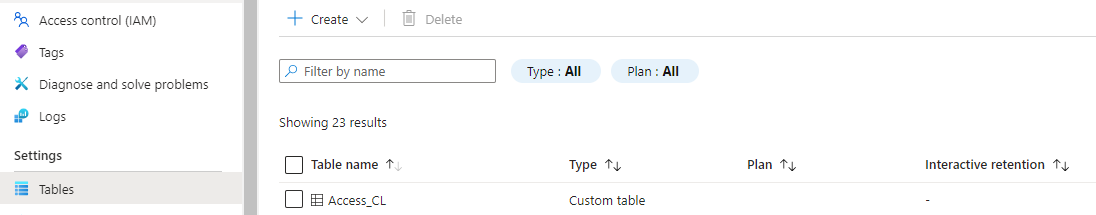


* **This is the path where the access logs are built**

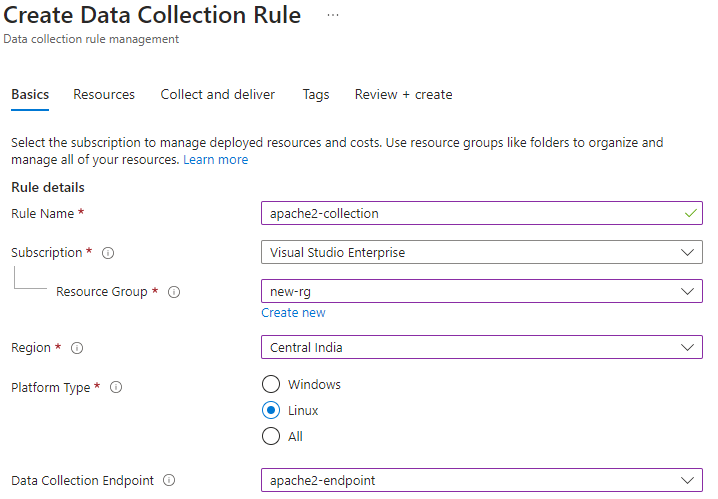


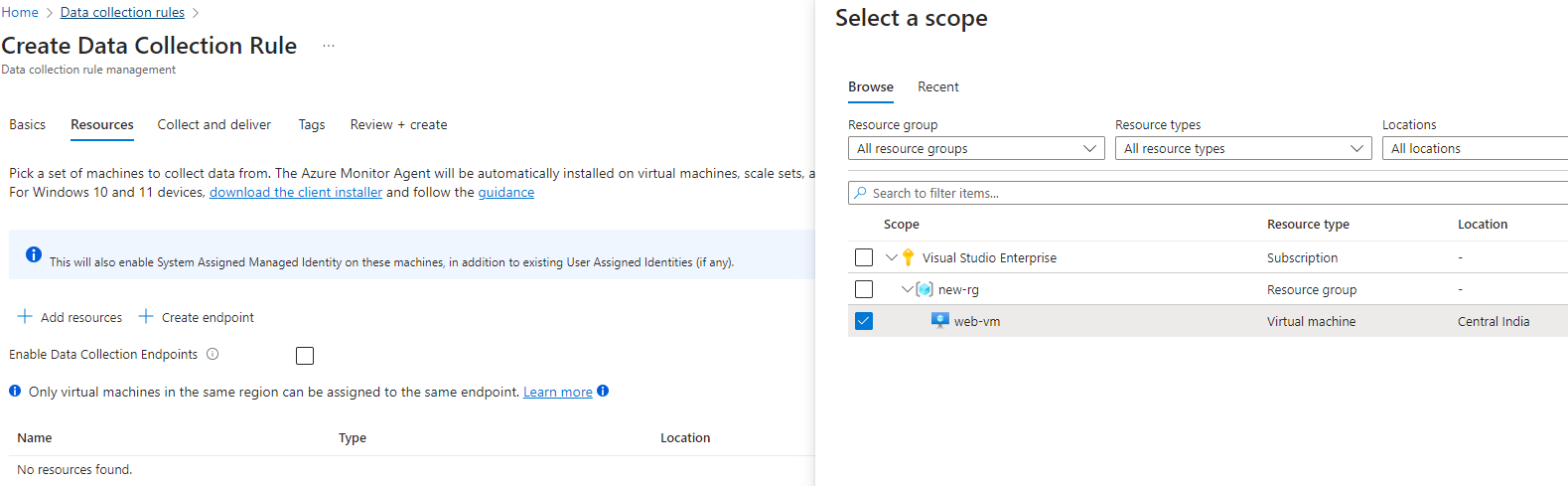
* **GIVE THE NAME OF THE TABLE TO BE CREATED IN LOGS ANALYTICS WORKSPACE**
  + - The table names are appended by **“\_CL**”. **For example – Access\_CL**

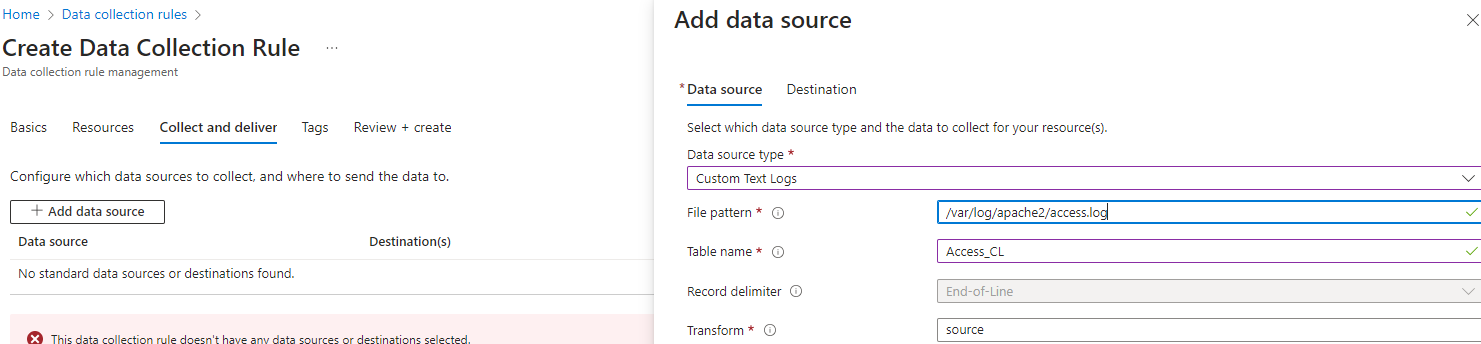


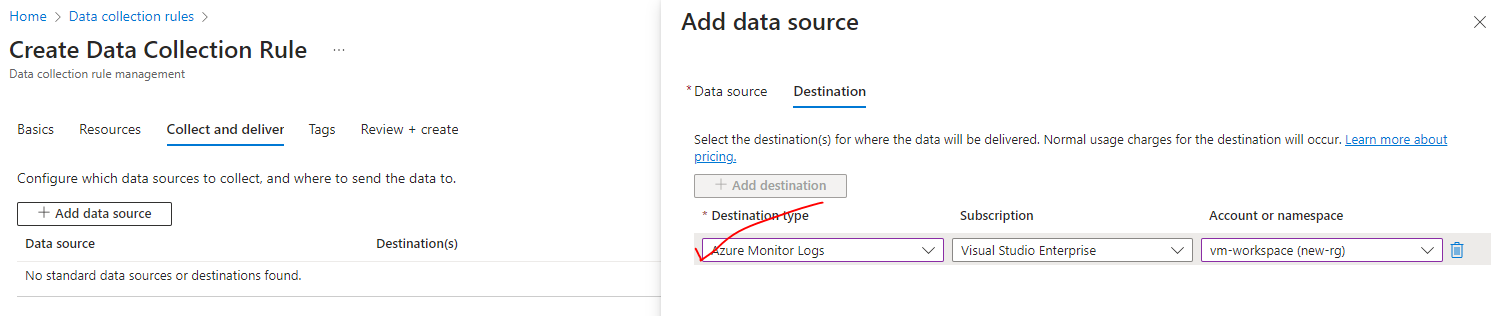
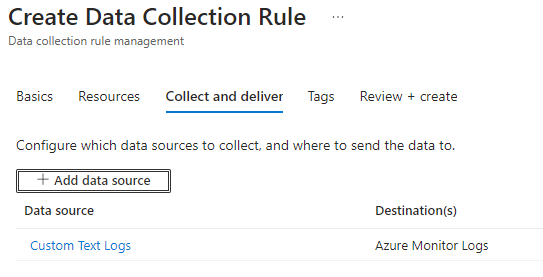
* **CUSTOM TABLE CREATED**
* 

##### STEP 5: CREATE A DATA COLLECTION RULE



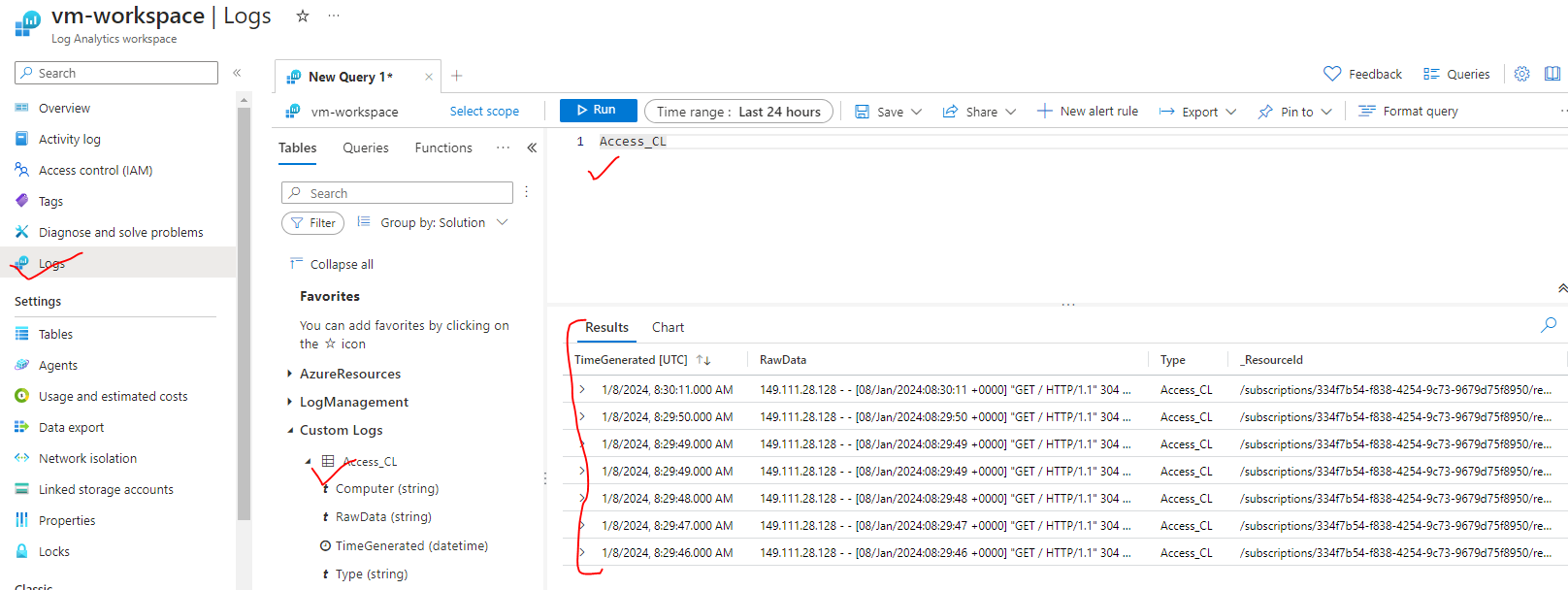




##### STEP 6: NAVIGATE TO THE TABLE IN THE LOG ANALYTICS WORKSPACE

* Log Analytics workspace 🡪 Logs
* Write the query to fetch the access log of the apache2 webserver

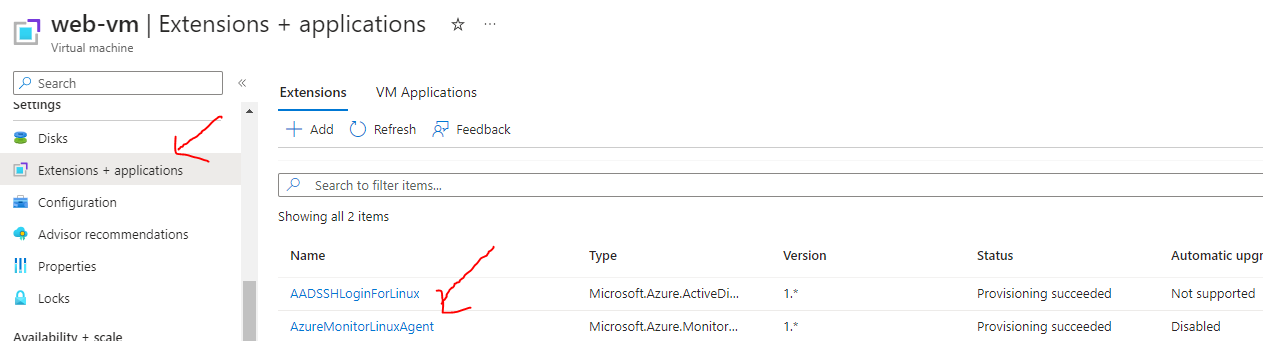


## AZURE BACKUP

* In Azure Backup service - The backup data gets written into Recovery Services vault.
* **The Recovery Services vault needs to be in the same Region when we are using the Azure Backup service for Azure Virtual Machines.**

### BACKUP PROCESS

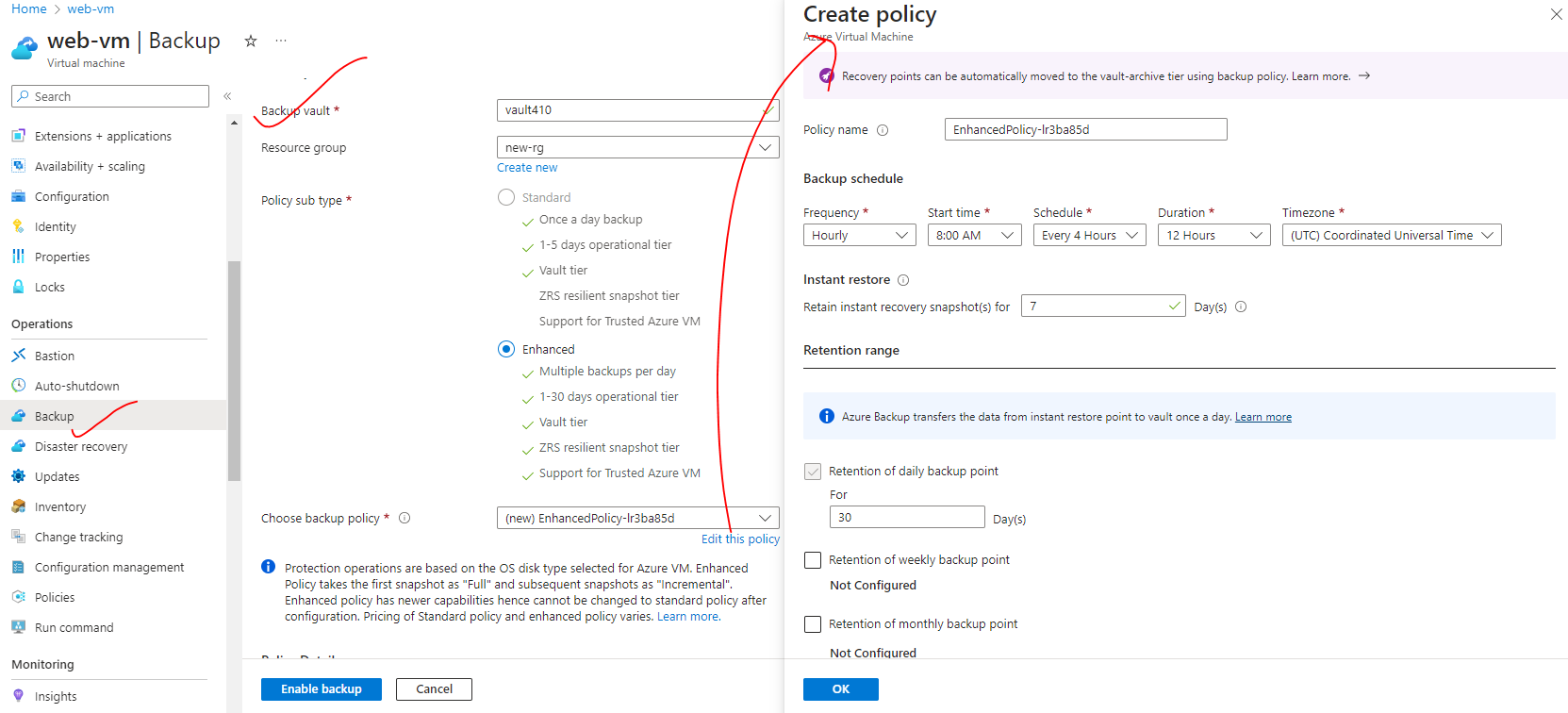
1. An extension is installed on the VM – Supported for both Windows and Linux VM
2. The backup tool first takes a snapshot of the data and stores it in the local machine.
3. The snapshot of data is then copied to Recovery Service Vault



#### SETTING UP BACKUP FOR VIRTUAL MACHINE

##### ENABLE THE BACKUP FOR THE VM – RECOVERY SERVICE VAULT

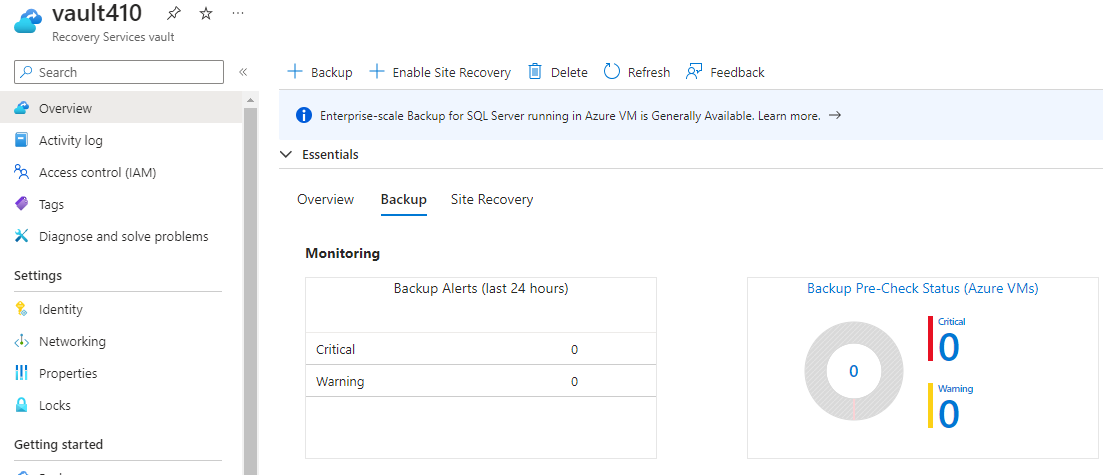
* Go to VM 🡪 Backup



* The Recovery Service Vault has a Policy associated with it. Policy in the Backup Vault service refers to the backup policy that defines the **backup schedule, retention period, and other settings for the data protection of resources** within the Azure environment.
* The Backup Recovery Service Vault allow us to create and manage these policies to ensure your data is protected and recoverable.
  + BACKUP SCHEDULE
    - We can define the frequency at which backups are taken for the resources. This can be daily, weekly, or customized to meet specific requirements.
  + INSTANT RESTORE: In the backup process
    - It first takes a snapshot of the entire VM and the data on the VM.
    - The snapshot is stored locally on the VM itself - based on the snapshot itself, and then after some time that snapshot will be stored in the recovery services vault.
    - If the Instant Restore = 7 – Then we can retain the snapshot on the VM for 7 days
  + RETENTION RANGE
    - The policy allows us to specify how long the backup data should be retained.
    - We can set the retention period in terms of days, weeks, months, or years.

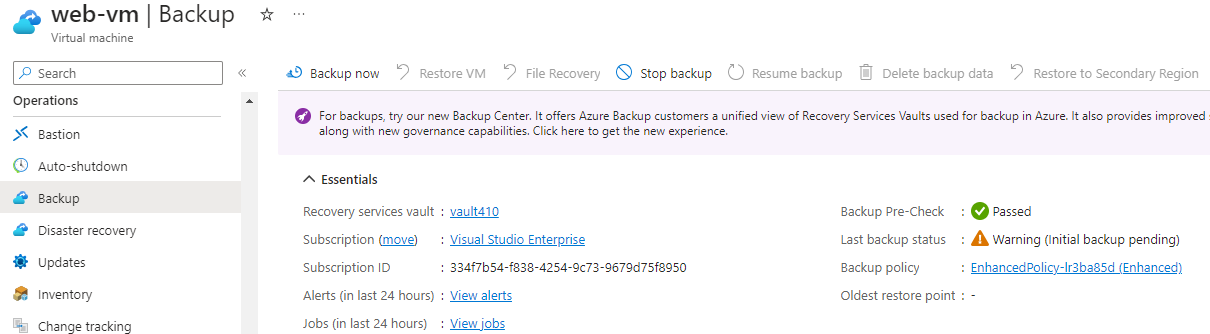
##### RECOVERY SERVICE VAULT

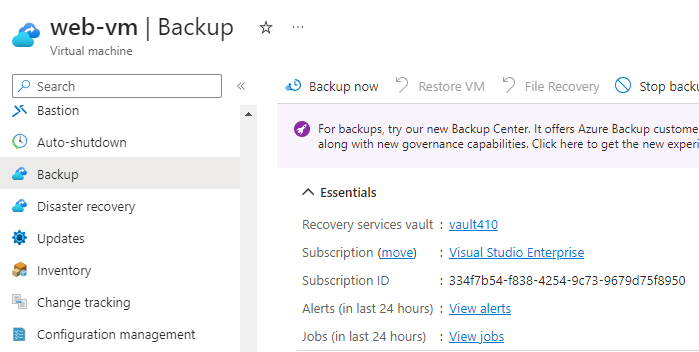
* When we enable the backup for the VM – it will create a separate resource called “Recovery Service Vault”

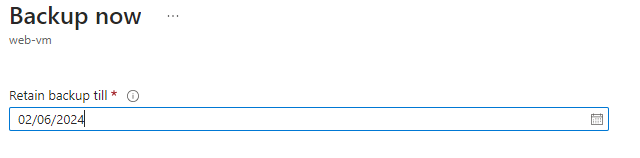


##### TRIGGERING THE BACKUP - MANUALLY

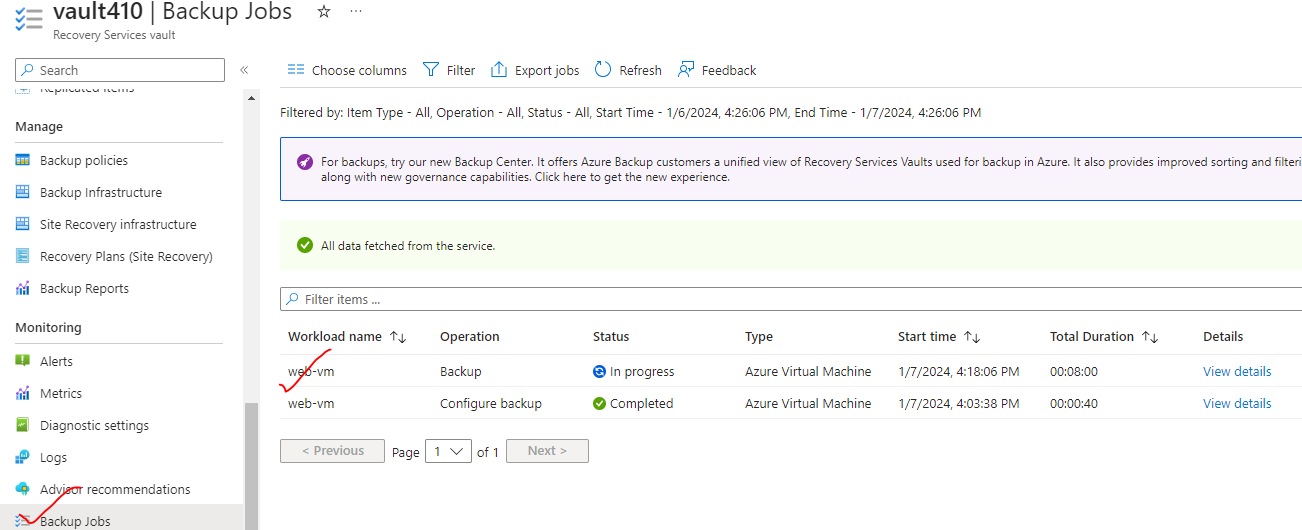
* Once the backup is enabled – the backup will happen based on the defined policy. But the backup can be triggered manually as well using “Backup now”







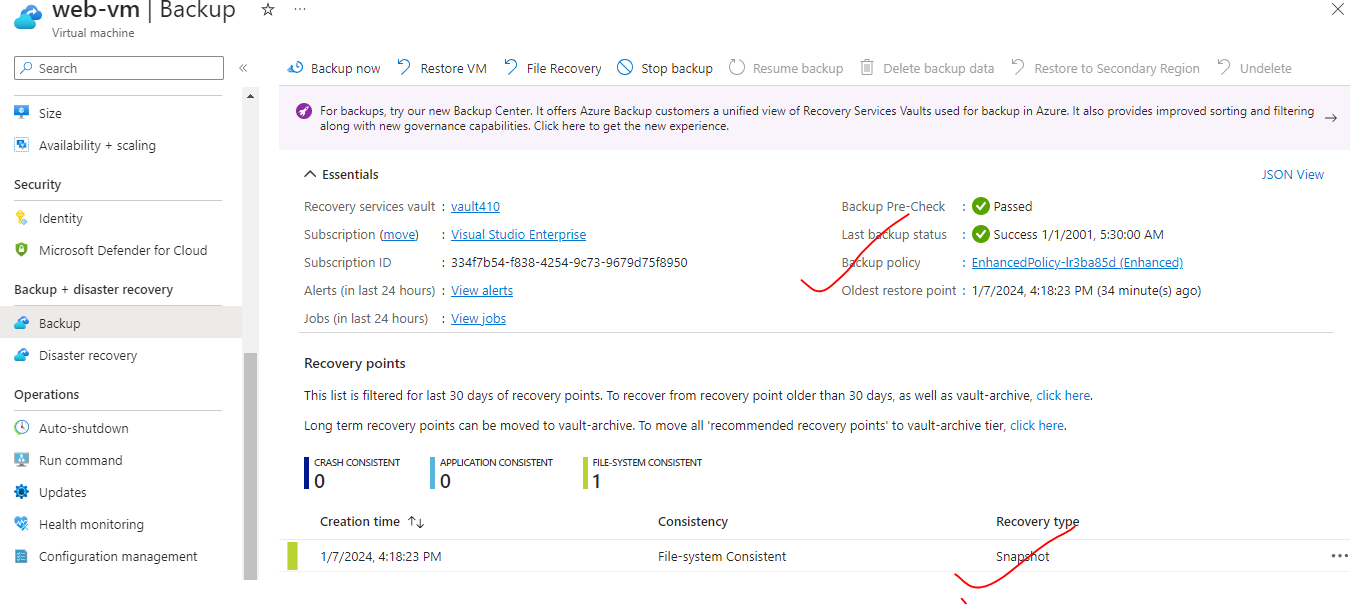
##### CHECK THE STATUS OF BACKUP



WORKFLOW FLOW FOR BACKUP IN RECOVERY SERVICE VAULT

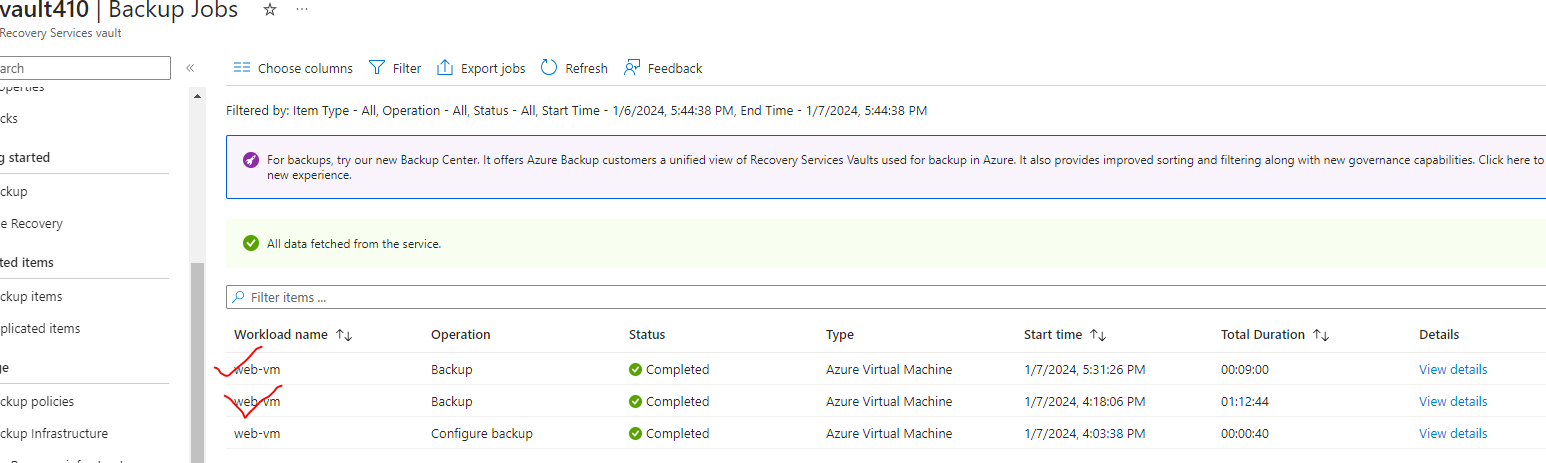


##### SNAPSHOT CREATED

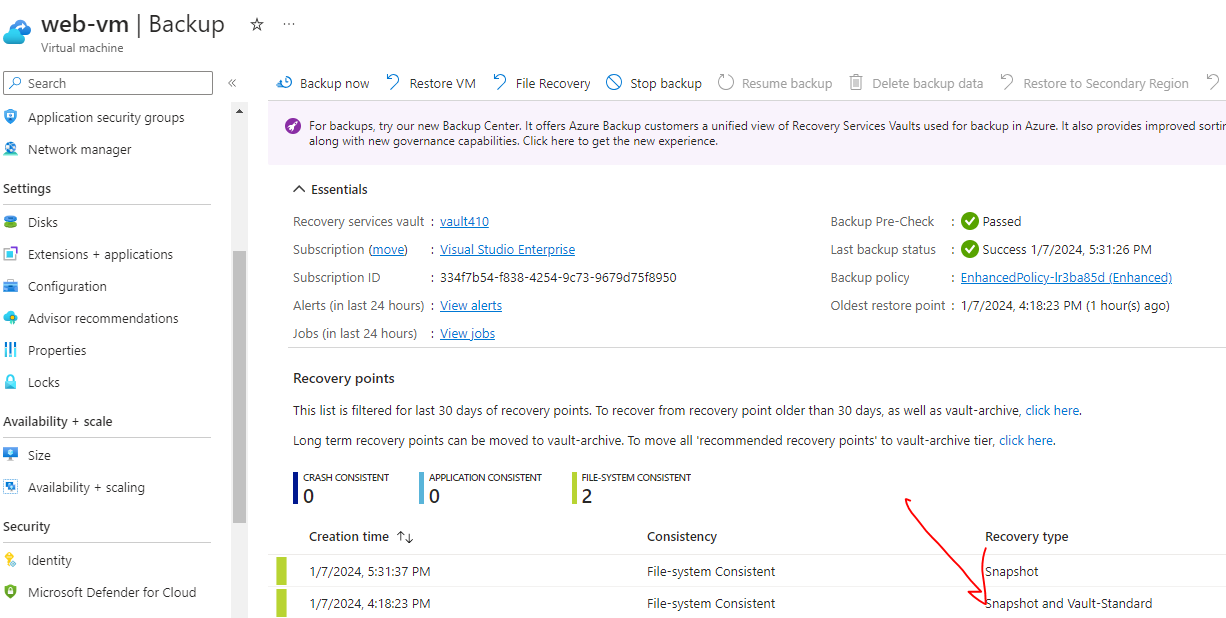


##### BACKUP COMPLETED

* The backup has been completed – this will create a snapshot in the VM itself and copy the snapshot in the Recovery Vault Service



* Go the VM 🡪 Backup : The “Recovery type” of “SnapShot and Vault Standand” shows that snapshot has been copied to Recovery Service Vault.



#### FILE RESTORE / RECOVERY

#### VM RESTORE / RECOVERY

* To restore a VM from the backup -we have 2 options

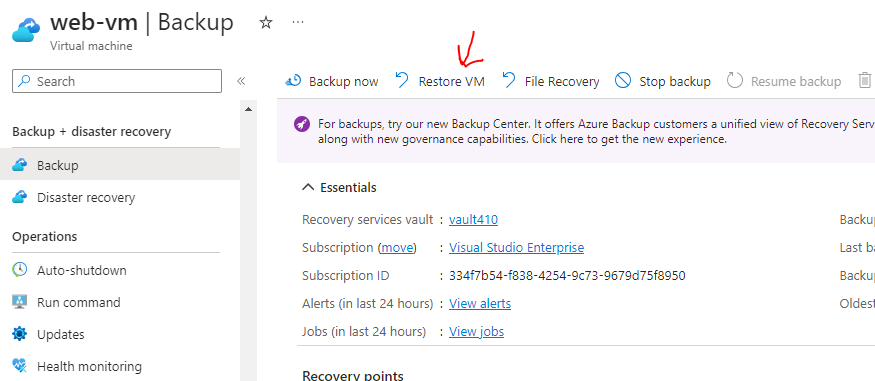
1. **CREATE A NEW VM FROM THE BACK UP**
2. **REPLACE THE EXISTING VM FROM THE BACK UP**

* The backup process needs a storage account as a staging location

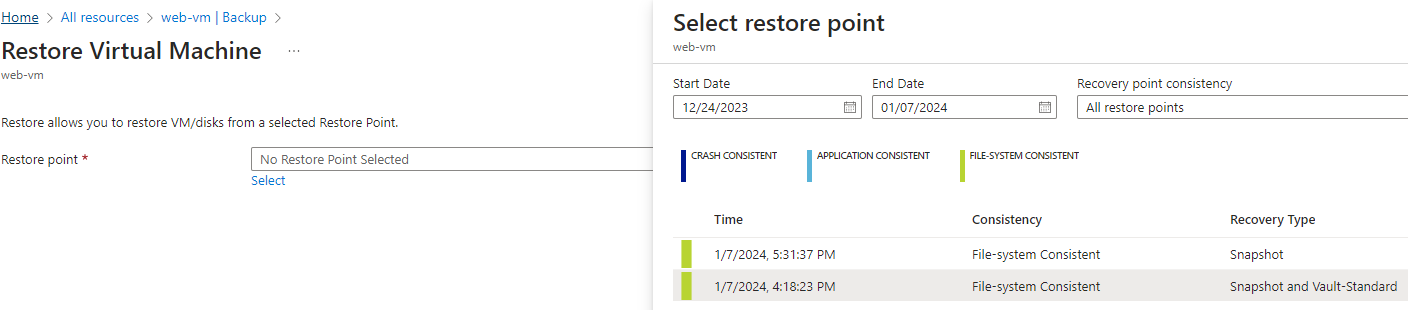
|  |
| --- |
| **TEST**   * **The VM which we are recovering is a linux VM which has apache installed** * **When the Vm is recovered (by creating a new VM) – The new VM should have apache installed as well** * **OLD VM** |

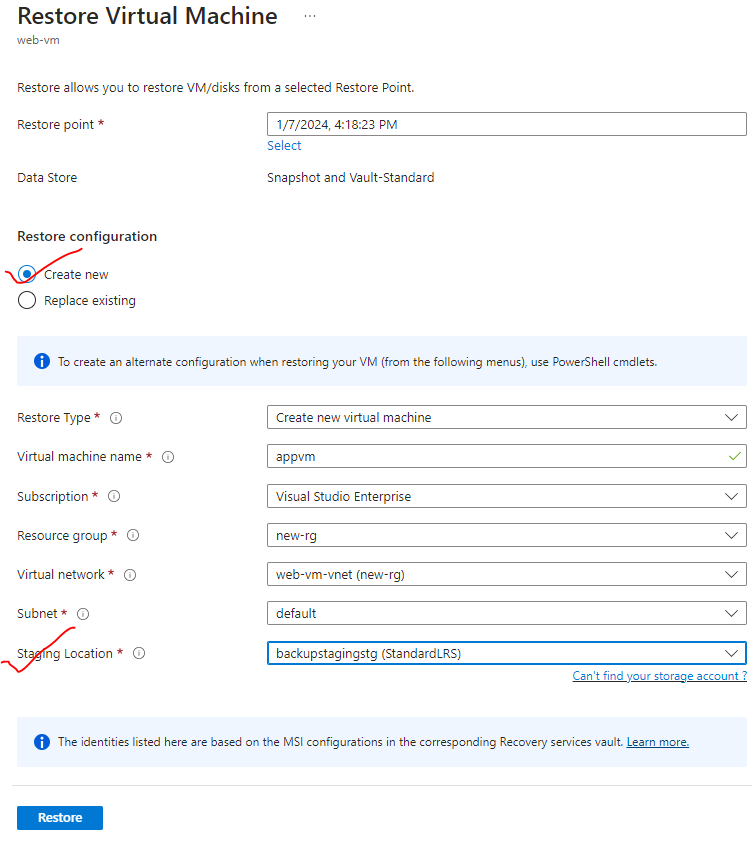
**In below example – we will create a new VM from the backup**

1. Go to the VM 🡪 Back Up 🡪 Restore VM



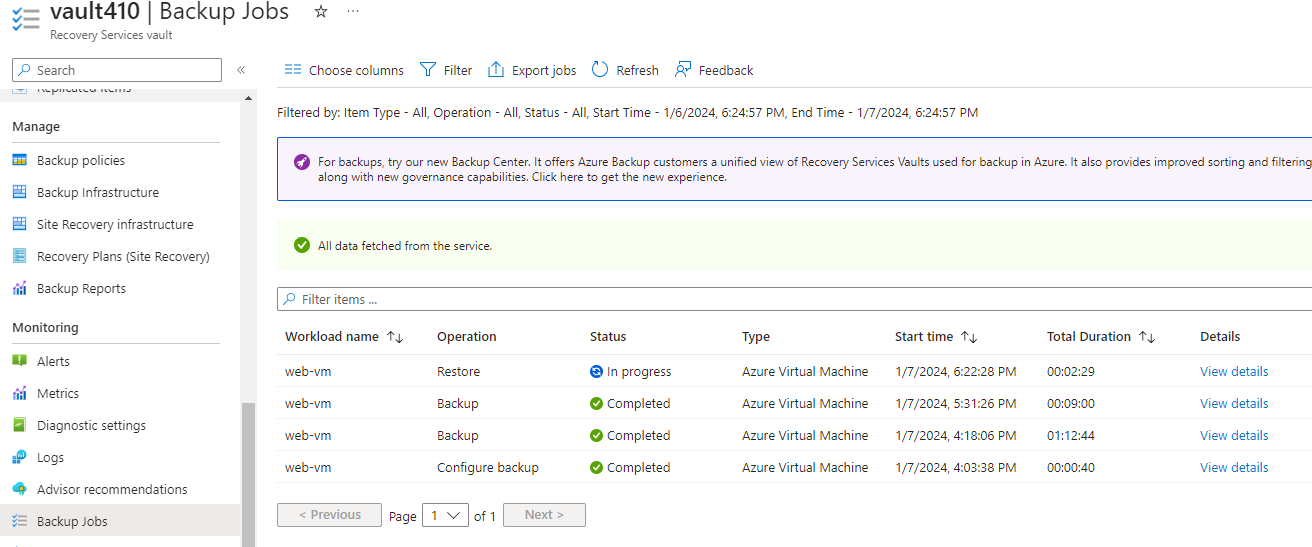
SELECT THE RESTORE POINT



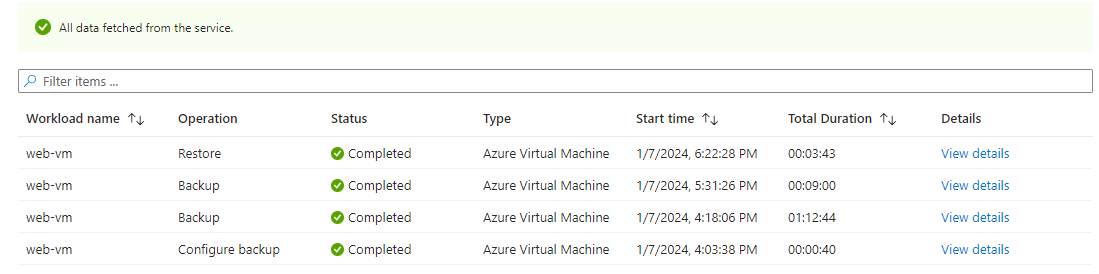


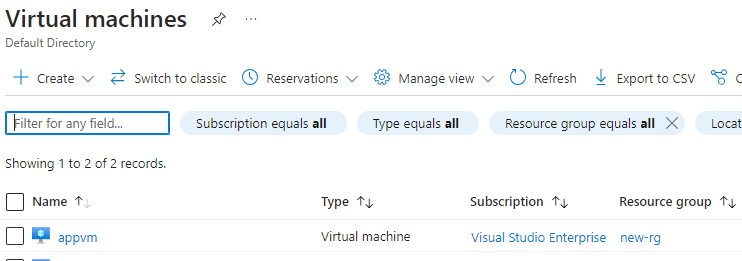
STATUS OF BACKUP

* Go to Recovery Service Vault 🡪 Backup Jobs to get the status of the Backup job

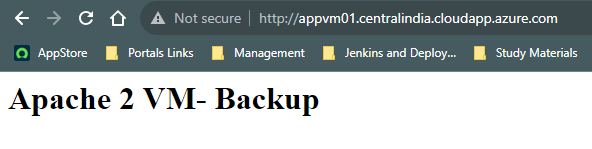


* Once the backup job is completed. We can see the “new VM” created for the Backup





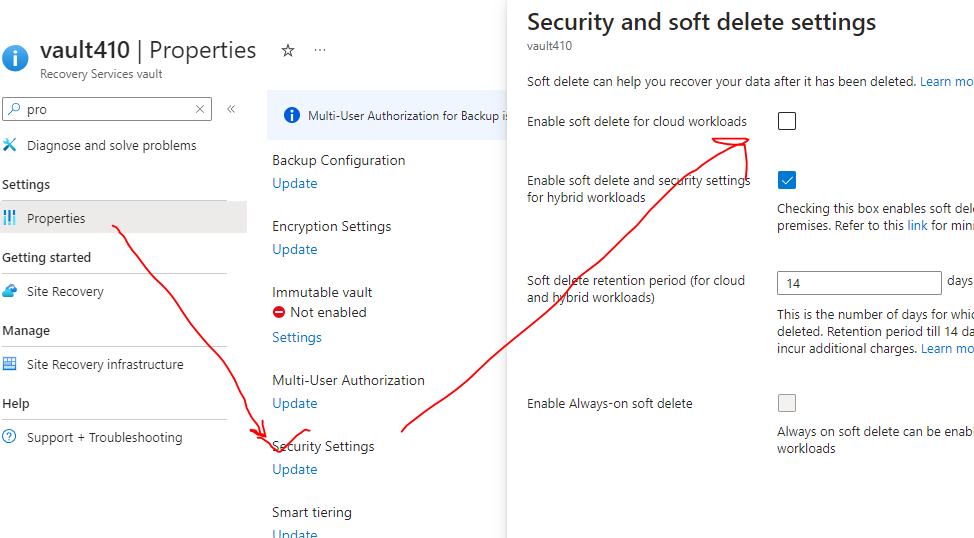
RESTORED VM – appvm



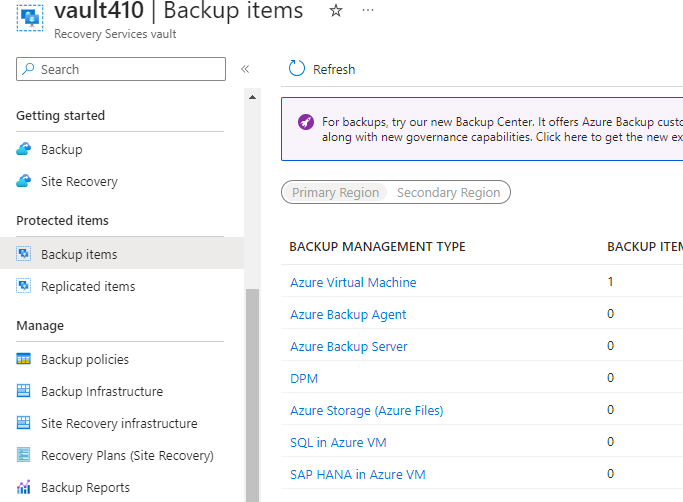
#### DELETING THE RECOVERY SERVICE VAULT

To delete the Recovery Service Vault we have to undergo certain steps

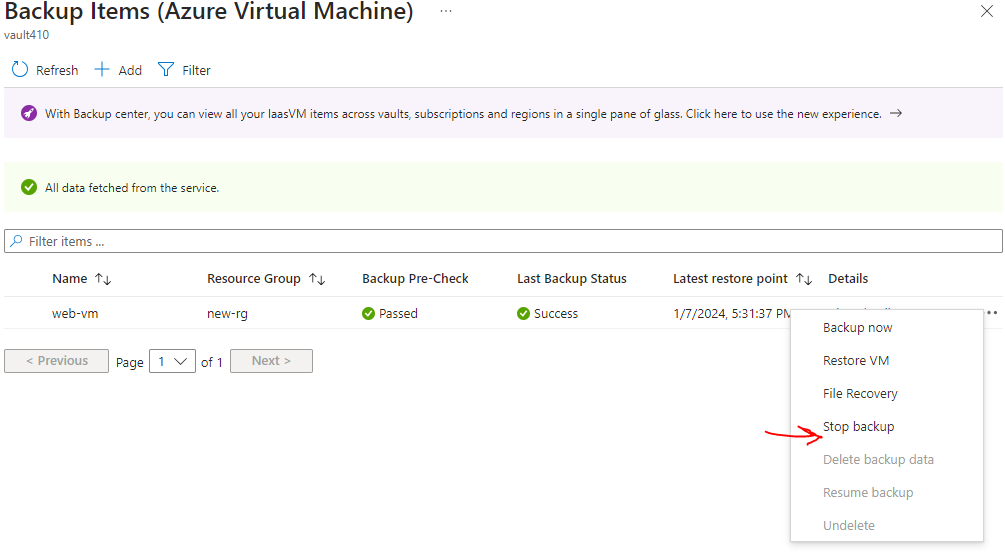
* **STEP 1: DISABLE “enable soft delete for cloud workloads”** 
  1. GO to Recovery Services Vault 🡪 Properties 🡪 Security Settings

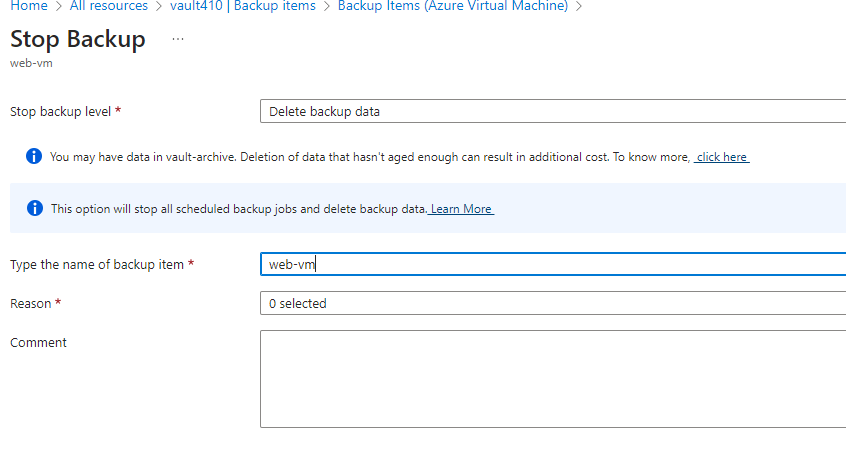


STEP 2: STOP THE BACKUP



* Go to Backup items 🡪 Select the service of which we want to stop the backup
* Go the context menu 🡪 Stop Back-up





## AZURE SITE RECOVERY