**Azure leaning – FIS Internal**

TOPICS

Azure fundamentals

Azure resource manager

Azure monitoring

**Azure fundamentals**

Microsoft Azure is Microsoft's cloud computing platform, providing a wide variety of services you can use without purchasing and provisioning your own hardware.

AZURE is public could providers like AWS and GCP

We do have a private cloud like IBM VMware cisco oracle etc…

**Advantages**

When building or deploying a cloud application, two of the biggest considerations are uptime (or availability) and the ability to handle demand (or scale).

Vertical scaling and Horizontal scaling security pricing

**Cloud services types**

IAS

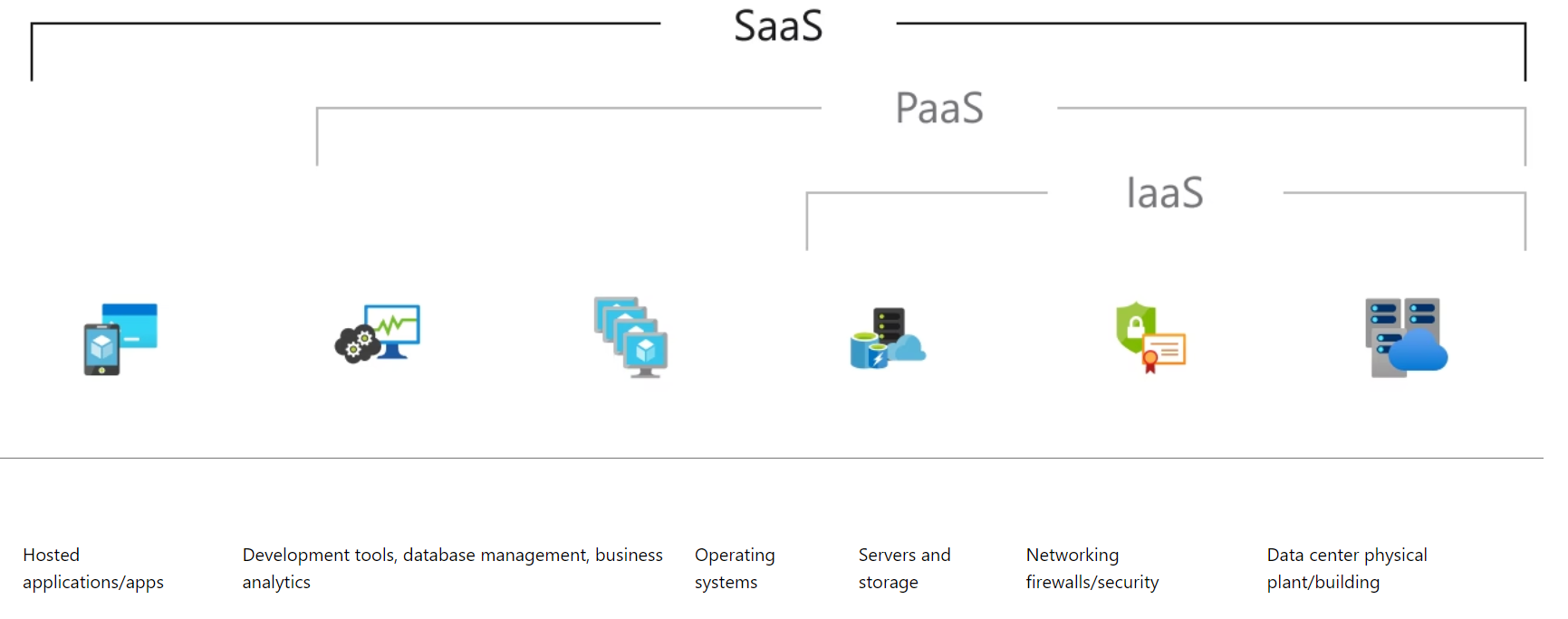
Infrastructure as a service (IaaS) is a cloud computing service offering essential compute, storage, and networking resources on demand, on a pay-as-you-go basis.

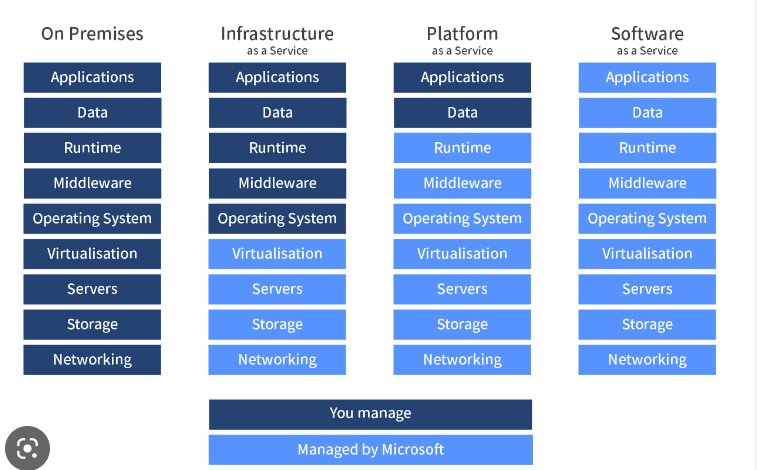
PAS

platform as a service (PaaS) is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications. You purchase the resources you need from a cloud service provider on a pay-as-you-go basis and access them over a secure Internet connection

SAS

SaaS provides a complete software solution that you purchase on a pay-as-you-go basis from a cloud service provider. You rent the use of an app for your organization, and your users connect to it over the Internet, usually with a web browser. All of the underlying infrastructure, middleware, app software, and app data are located in the service provider’s data center. The service provider manages the hardware and software, and with the appropriate service agreement, will ensure the availability and the security of the app and your data as well. SaaS allows your organization to get quickly up and running with an app at minimal upfront cost.

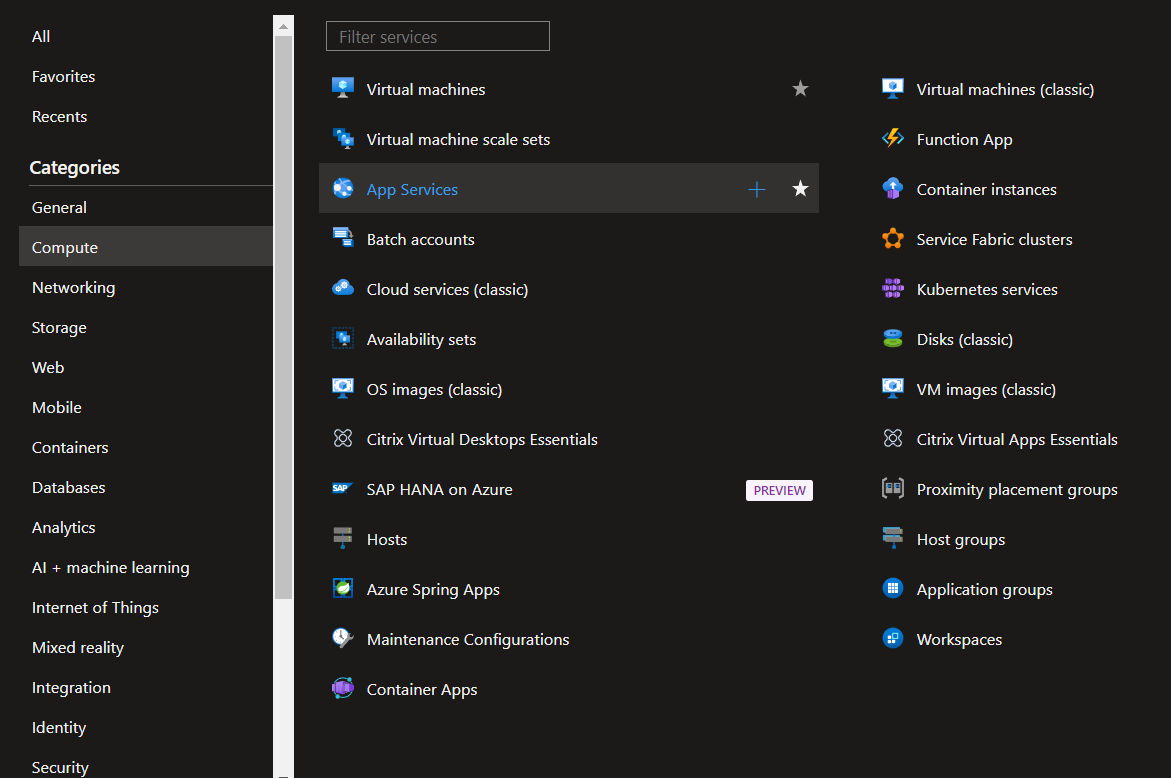




**Azure services**

The Azure cloud platform is more than 200 products and cloud services designed to help you bring new solutions to life

Azure core resources or services are broadly classified into four categories which are computed, networking, storage, and database. Networking is crucial for your cloud deployment to be successful.

****

[**https://datacenters.microsoft.com/globe**](https://datacenters.microsoft.com/globe)

**Describe Azure management infrastructure**

**Regions**

A region is a geographical area on the planet that contains at least one, but potentially multiple datacentres that are nearby and networked together with a low-latency network. Azure intelligently assigns and controls the resources within each region to ensure workloads are appropriately balanced.

When you deploy a resource in Azure, you'll often need to choose the region where you want your resource deployed

**Availability zones**

Availability zones are physically separate data centres within an Azure region. Each availability zone is made up of one or more data centres equipped with independent power, cooling, and networking. An availability zone is set up to be an isolation boundary. If one zone goes down, the other continues working. Availability zones are connected through high-speed, private fiber-optic networks.

**Azure management infrastructure**

The management infrastructure includes Azure resources and resource groups, subscriptions, and accounts. Understanding the hierarchical organization will help you plan your projects and products within Azure.

**Azure resources and resource groups**

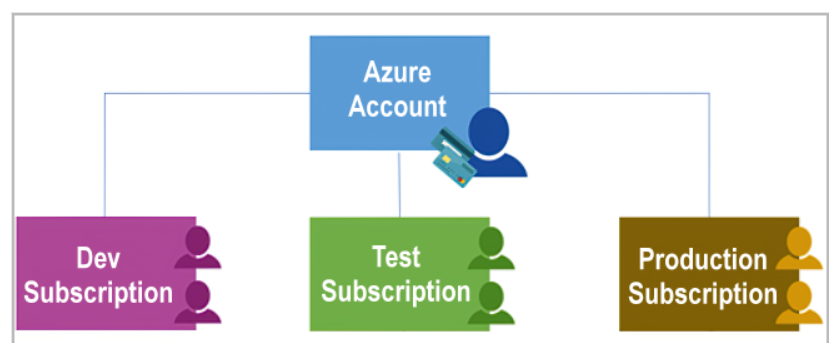
A resource is the basic building block of Azure. Anything you create, provision, deploy, etc. is a resource. Virtual Machines (VMs), virtual networks, databases, cognitive services, etc. are all considered resources within Azure.

Resource groups are simply groupings of resources.

****

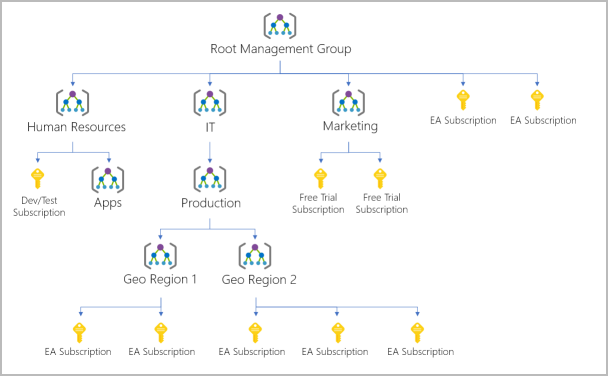
**AZURE Subscription**

In Azure, subscriptions are a unit of management, billing, and scale. Similar to how resource groups are a way to logically organize resources, subscriptions allow you to logically organize your resource groups and facilitate billing.



## Management group, subscriptions, and resource group hierarchy

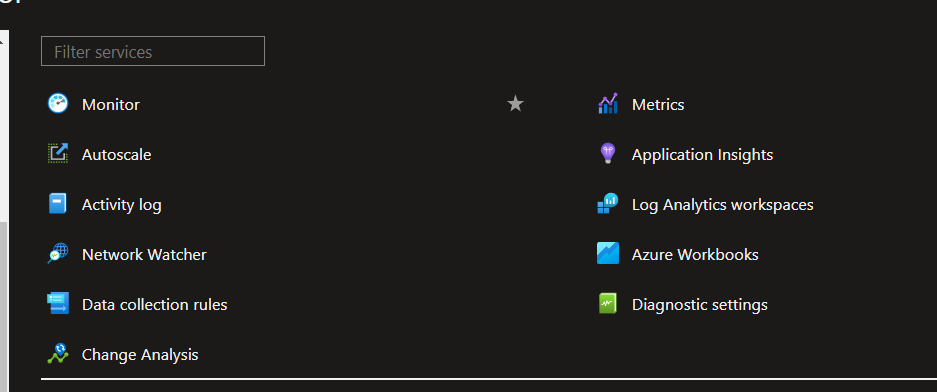
You can build a flexible structure of management groups and subscriptions to organize your resources into a hierarchy for unified policy and access management. The following diagram shows an example of creating a hierarchy for governance by using management groups.



**Azure monitoring**

**It is a SAS service**

Azure monitoring is a one-stop solution.

****

The data pull logs or information from many resources VM, Applications, Networks, containers, storage, custom endpoints, etc.

Two stores namely Metrics and logs

we can use these for various operations Like

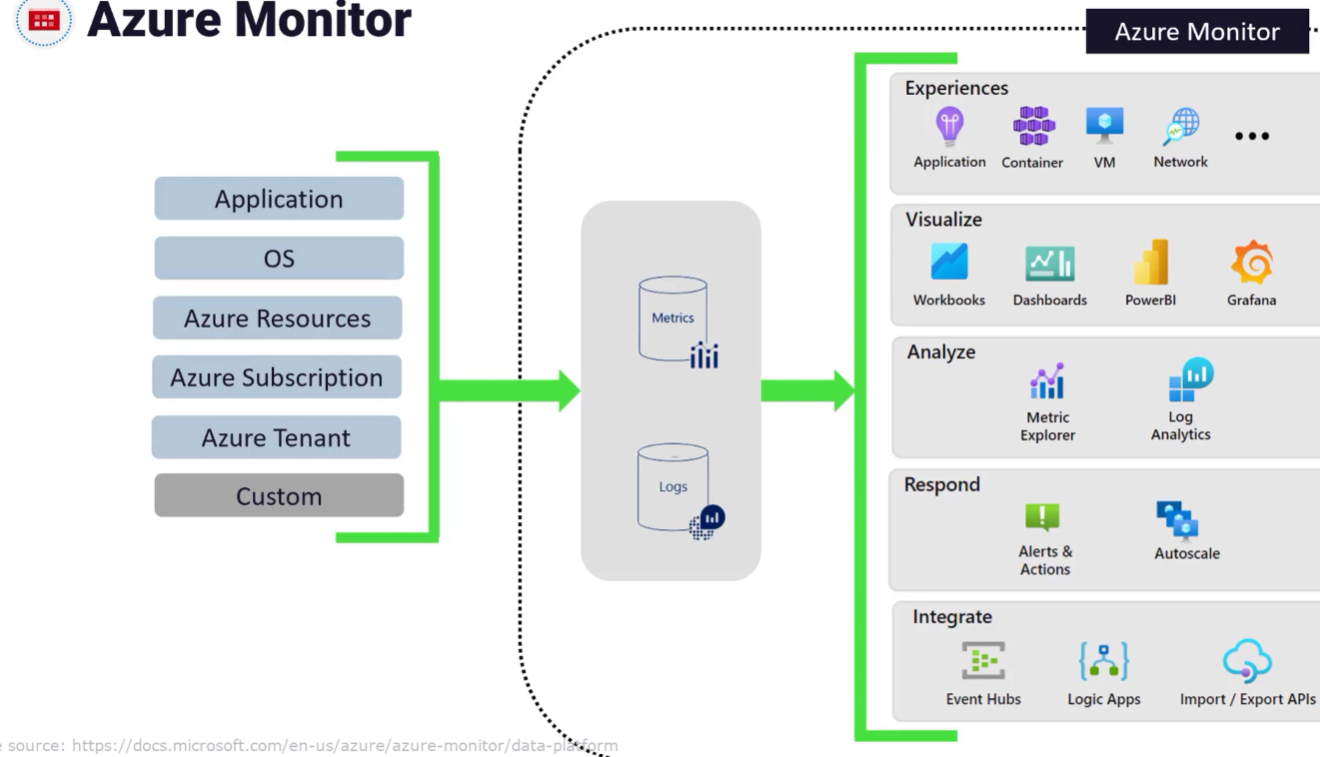
Experiences - View the insight of application vm network etc

Visualize - Dashboard workbooks PowerBI and etc

Analyse - Metrics exposure and Log Analytics workspace

Respond -Alerts and Actions and Autoscaling

Integrate - EventHub, snow, Netcool etc

****

**Metrics and Logs**

**Metrics** - zero configuration, Metrics are collected from Azure without any additional configuration.

* Real-time data represent the state of a system.
* Time series metrics plotted time axis to represent the state of the system at a point in time

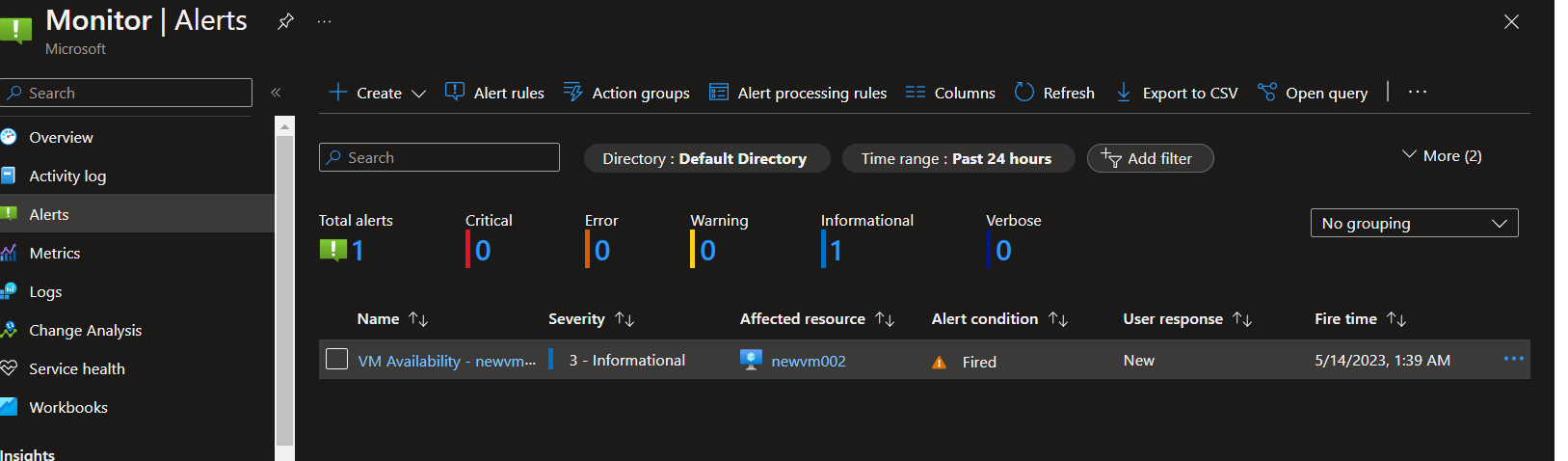
Ex- Memory utilization, CPU, Network

**Logs** – we need to configure Log analytical workspace. We need to deploy the agent inside the virtual machine

It KQL (KUSTO QUERY LANGUAGE) you can perform joins, aggregations, etc

**EX -Event viewer in windows**

**CREATE AN ALERT RULE**



Azure Monitor alerts - We can see a list of alerts

Creating alert rule: situation creation in SCAPM

Create an alert rule to identify and address issues when important conditions are found in your monitoring data. Learn more

Scope: VM, Storage, application, etc

Condition: Signals - It is Like a formula in SCAPM

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Action group: An action group is a set of actions that can be applied to an alert rule. Learn more

**Alert rule details:**

Severity - warning, information critical

Alert rule name: situation name Example: subid\_lob\_win\_cpu\_warning

Alert rule description: what is this alert for?

Region: location only that region this condition will apply.

Creating situations and assigning to the servers which are available and required in that region

Action Group –

Notification – EMAIL Azure resource manager Role, contributor etc.

EMAIL / PUSH -Email to the TEAM

Actions –

Action type: Event hub, ITSM

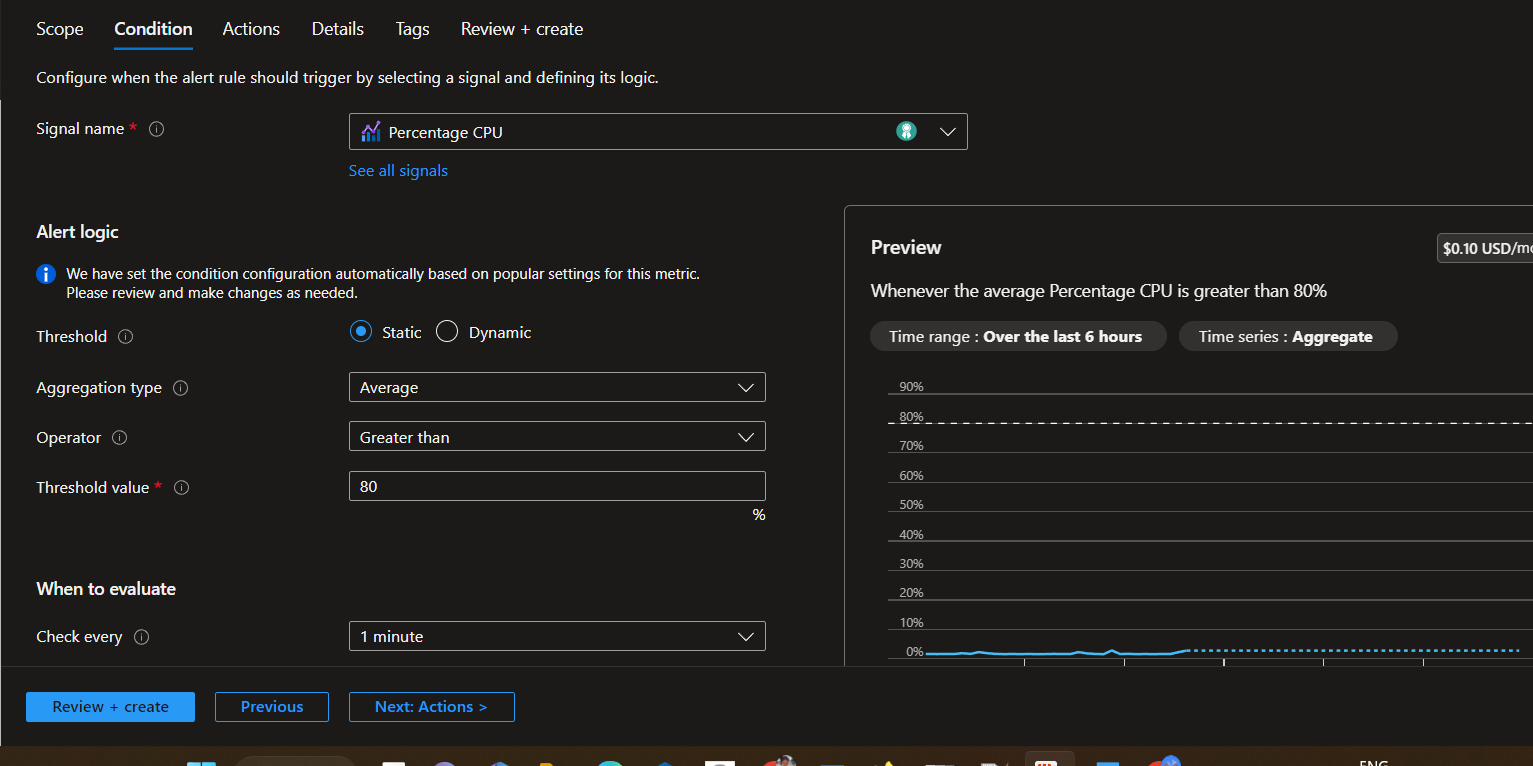
CEEEEE AN ALERT DIRECTLY ON VM OR GO TO THE ALERT ICON AND

We can create an alert rule directly on the VM or form a monitoring console create and assign it to the VM

Create assign n in the scope (select the server – situation creation on source or situation editor creation situation and assign to the sources)

Scope, condition, Action, and Details

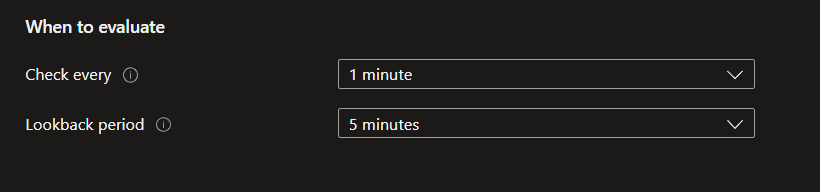
Signal name – the attribute in scamp. disk. network, process



**Time interval**

Check every: Checking time of the rule. Like the Sampling interval in SCAPM

Lookback period: Consecutive sampling same like SCAPM



Alert rule details

Severity

Name –

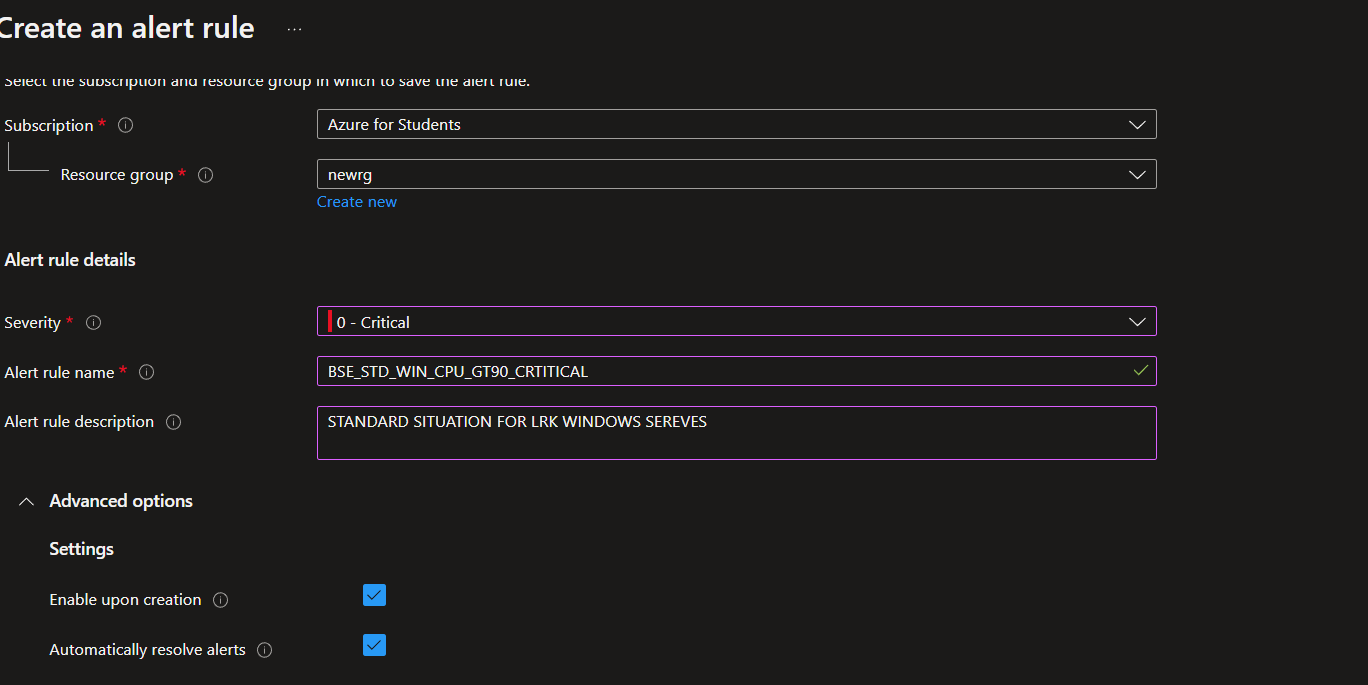
Description

**\*\*\* Advanced options \*\*\***

Setting

Enabled upon creation - Enabling the situation (like starting)

Automatically resolve alerts – if the issue resolve CPU hikes process missing



Log Analytics workspace - Like TDW (History viewing and setting up monitoring )

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

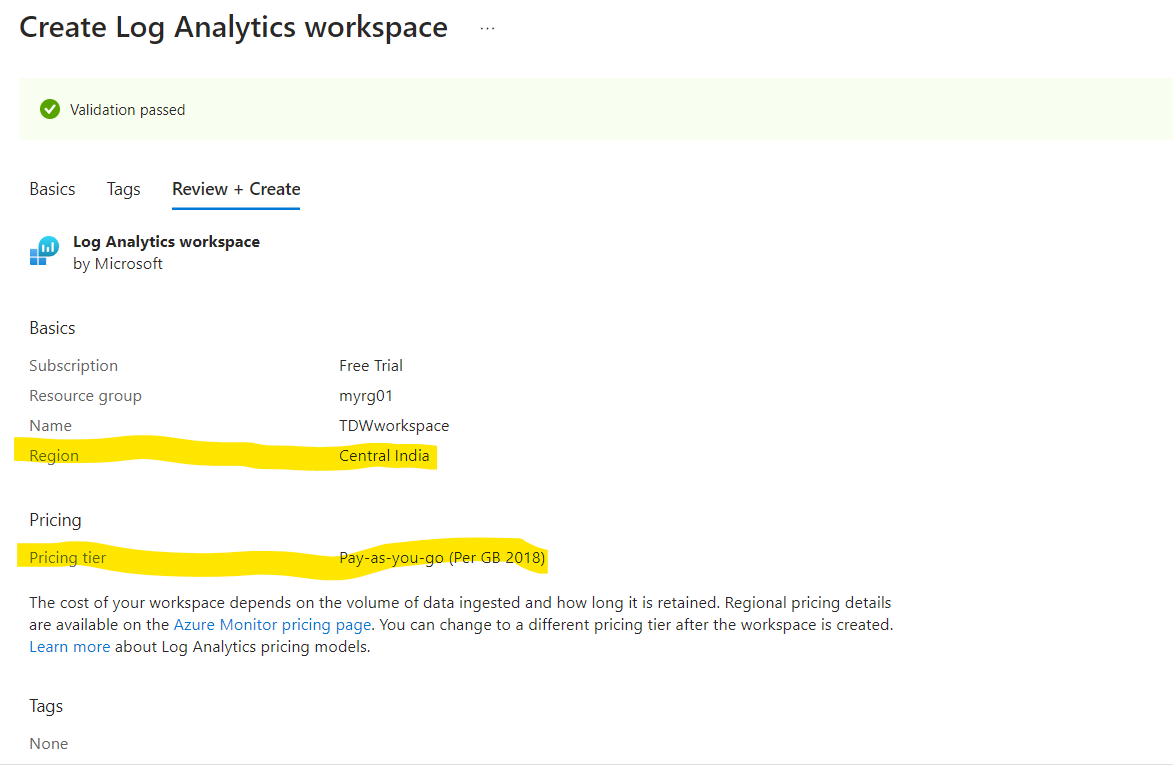
Separate COST 30 Days free. (SBU needs to be corrected need to check the pricing calculator)

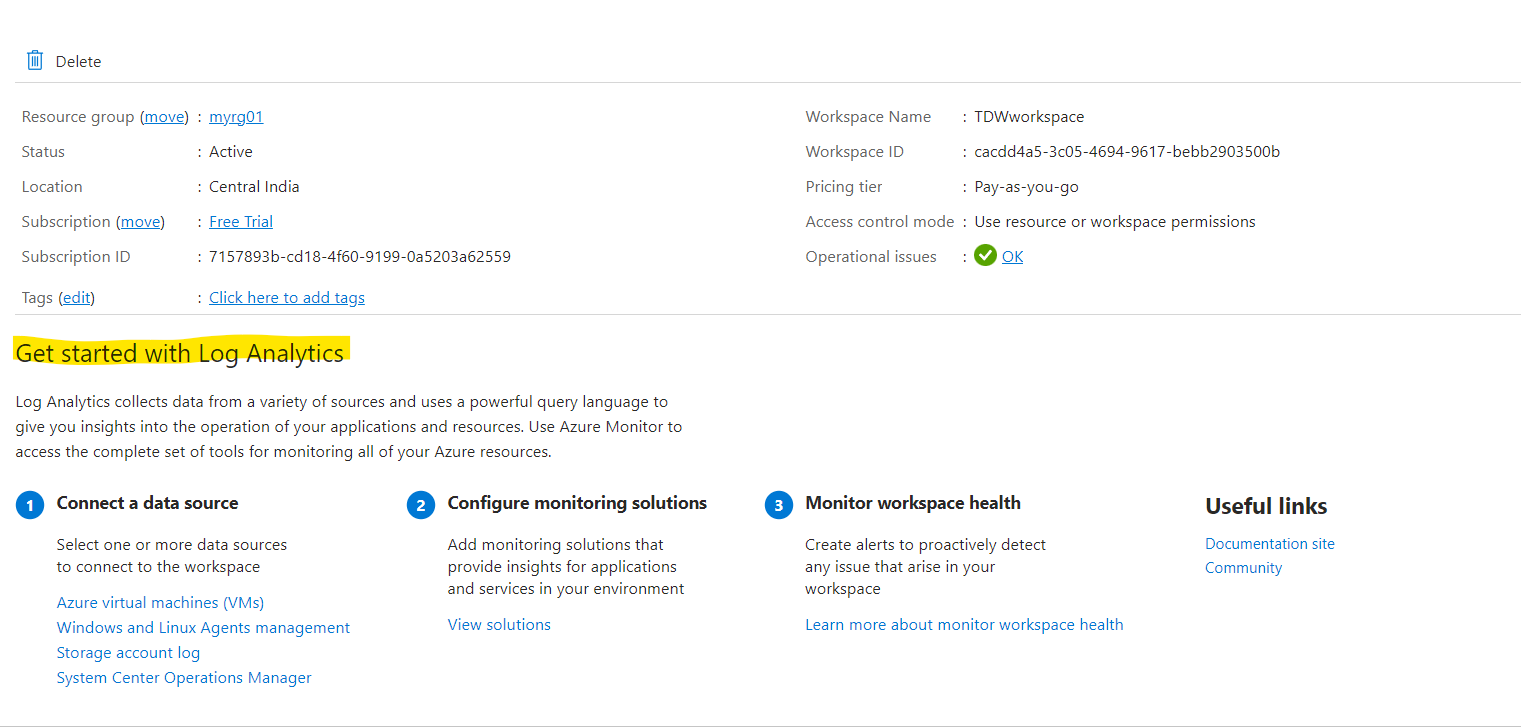
Azure Monitor collects data from metrics (its default) and logs source

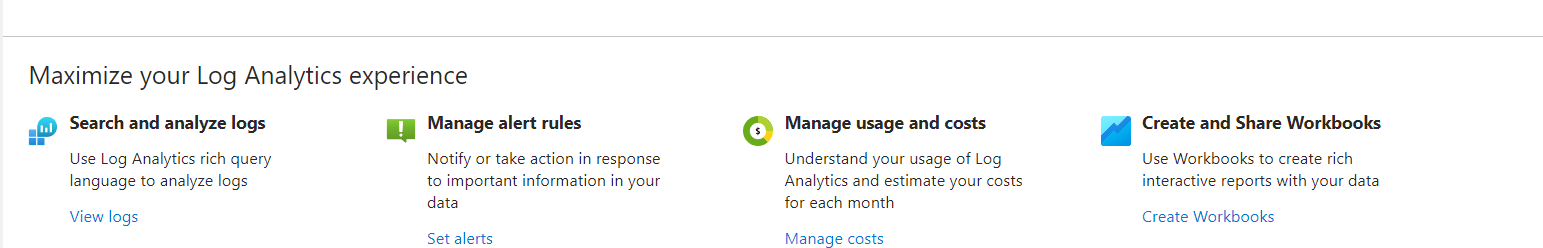
Data collection – data generated from resources in the cloud and on-premises

Can be collected to Azure log analytics workspace

Reporting and visualization – Use KQL for report and visualization

****

****

****

**Agents (AMA, LOG ANALYTICS AGENT )**

**Zero configuration.**

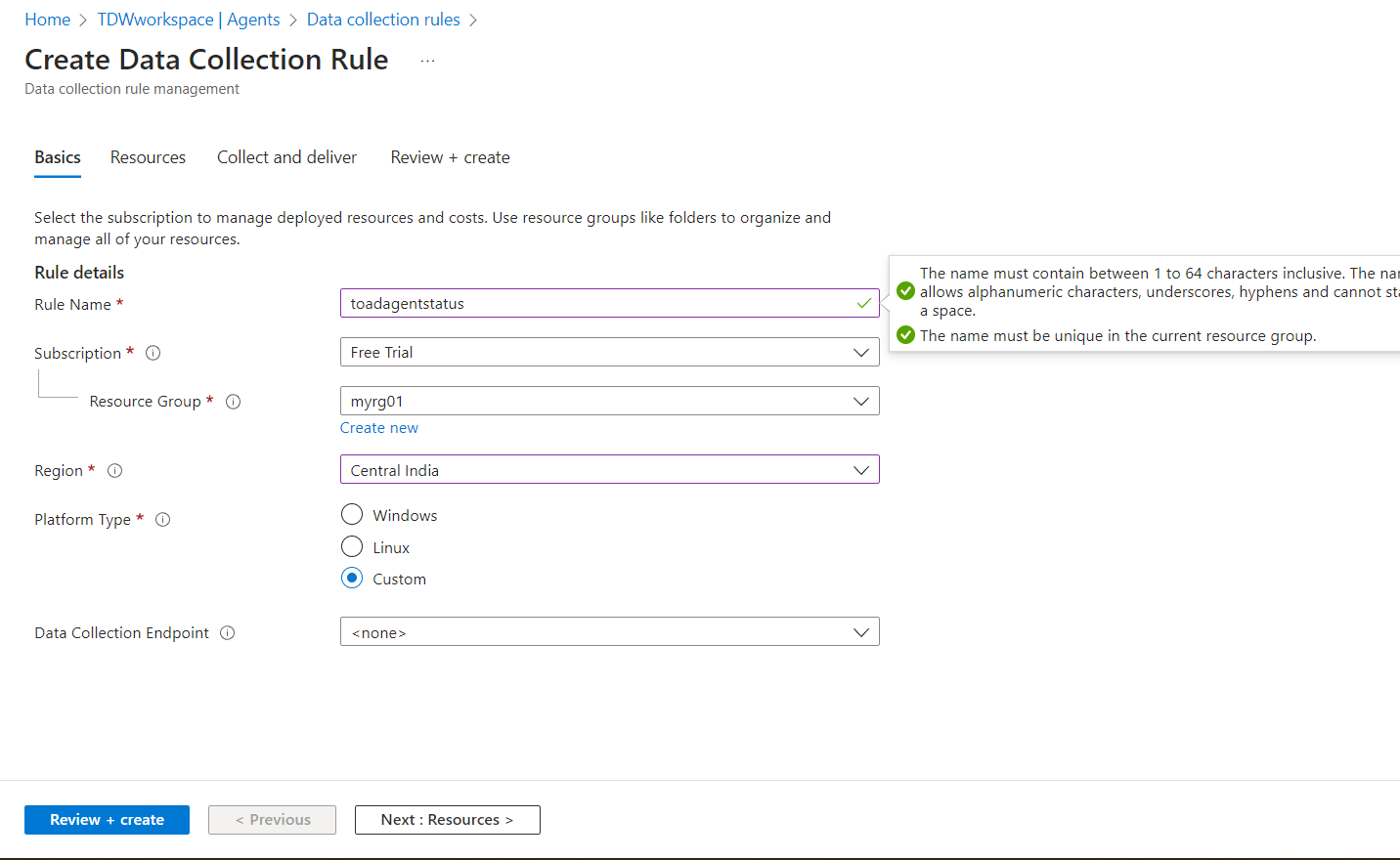
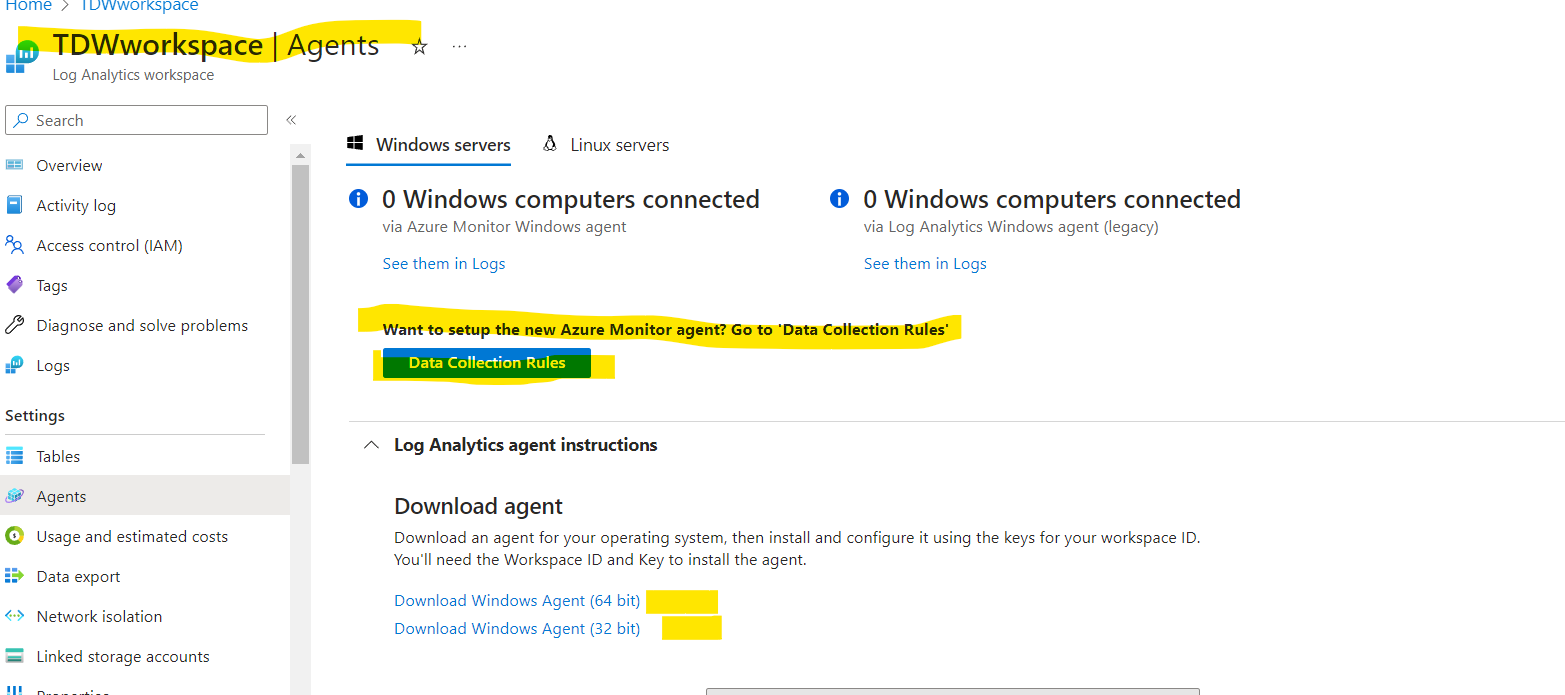
[**https://learn.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview**](https://learn.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview)

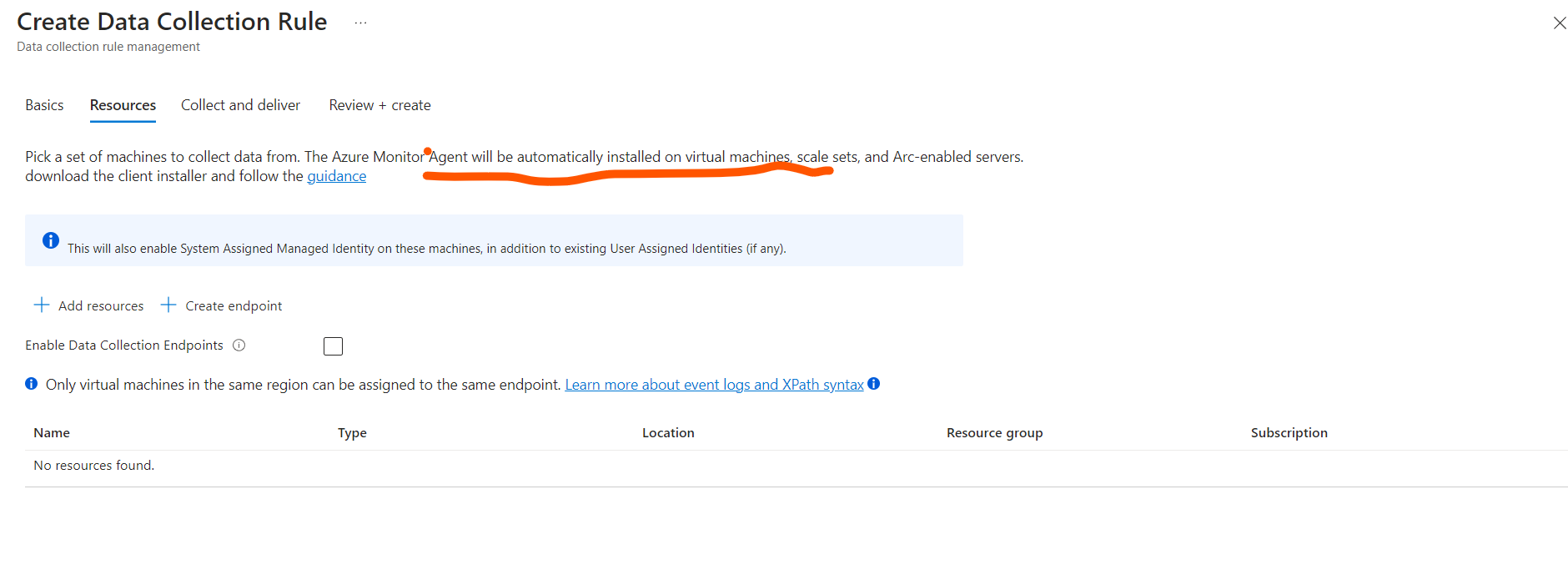
Azure Monitor Agent (AMA) collects monitoring data from the guest operating system of Azure and hybrid virtual machines and delivers it to Azure Monitor for use by features, insights, and other services, such as [Microsoft Sentinel](https://learn.microsoft.com/en-us/azure/sentinel/overview) and [Microsoft Defender for Cloud](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction). Azure Monitor Agent replaces all of Azure Monitor's legacy monitoring agents. This article provides an overview of Azure Monitor Agent's capabilities and supported use cases.

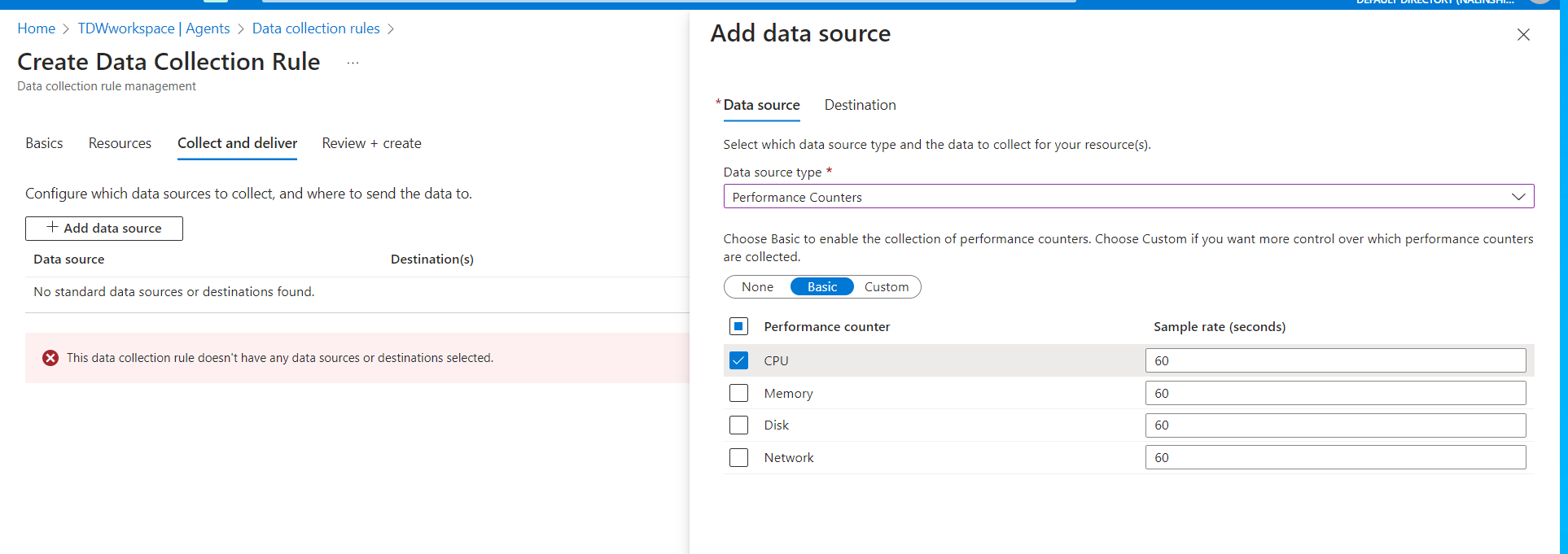
**Azure monitoring agent - (AMA) Microsoft monitoring agent)**

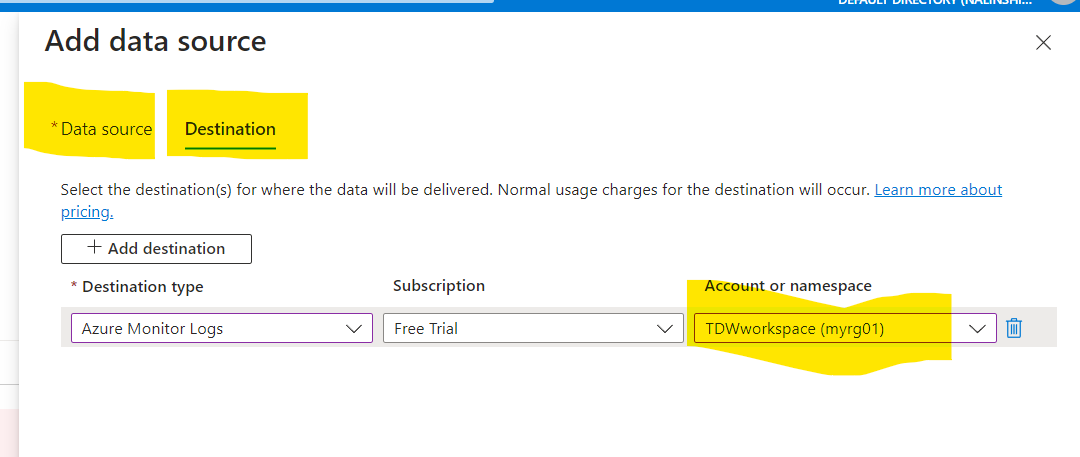
**AMA will pump the data to the log analytics workspace via data rules**

**Log analytics workspace – agents -data collection rules**

****

****

****

****

Once the date source and destination added you can start creating alert rule and bulk assign to the VM’s.