

v1.0

October 06, 2022

A10 Product Engineering Team

USER MANUAL

Azure ARM A10-vThunder\_vTPS-3NIC-VMSS-GWLB

# PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at: a10-virtual-patent-marking.

# TRADEMARKS

A10 Networks, Inc. trademarks are listed at: a10-trademarks.

# CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced, or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

# DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

# ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

# FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting [www.a10networks.com](http://www.a10networks.com).

Contents

[PATENT PROTECTION 1](#_Toc115967092)

[TRADEMARKS 1](#_Toc115967093)

[CONFIDENTIALITY 1](#_Toc115967094)

[DISCLAIMER 1](#_Toc115967095)

[ENVIRONMENTAL CONSIDERATIONS 2](#_Toc115967096)

[FURTHER INFORMATION 2](#_Toc115967097)

[Introduction to Install vThunder(vTPS) on Microsoft Azure 4](#_Toc115967098)

[Overview of Microsoft Azure 5](#_Toc115967099)

[Azure Terminology 6](#_Toc115967100)

[Pre-requisites [Resource Group, VNet, Service App, vTPS ARM Template] 7](#_Toc115967101)

[QuickStart: Install A10 - vThunder vTPS - Azure portal l ARM 9](#_Toc115967102)

[1. Launch ‘Custom Deployment’ 9](#_Toc115967103)

[2. Launch ‘ARM Template’ 10](#_Toc115967104)

[Annexures 10](#_Toc115967105)

[Annexure 1 – Create Azure Resource Group [RG]. 10](#_Toc115967106)

[Annexure 2 – Create Azure Virtual Network [VNet] & Subnet. 10](#_Toc115967107)

[Annexure 3 – Create Service Application Access Key. 10](#_Toc115967108)

[Annexure 4 – Cloud Resources Information. 10](#_Toc115967109)

[Annexure 5 – Login to vThunder using CLI 10](#_Toc115967110)

[Annexure 6 - Login to vThunder using Console 10](#_Toc115967111)

[Annexure 7 – Verify vTPS DDoS Configuration 10](#_Toc115967112)

[Annexure 8 – Customize Log Analytics Dashboard 12](#_Toc115967113)

[Annexure 9 – Enable Public Traffic to GWLB-vTPS Eco System 12](#_Toc115967114)

[Annexure 10 – Enable vTPS Logs in to Azure Log Analytics Dashboard. 12](#_Toc115967115)

# Introduction to Install vThunder(vTPS) on Microsoft Azure

vThunder for Microsoft Azure is a fully operational, software-only version of the ACOS Series Server Load Balancer (SLB), or Application Delivery Controller (ADC) device, Thread Protecting System (TPS). It is configurable by ACOS CLI, GUI, AXAPI, and Harmony Controller. For more information see Virtual Instances in Harmony Controller.

vThunder is a virtual appliance, yet it retains most of the functionality available on the hard- ware based ACOS appliances. Managing vThunder is the same as managing hardware based ACOS device, and vThunder has the same CLI configurations and GUI presentation.

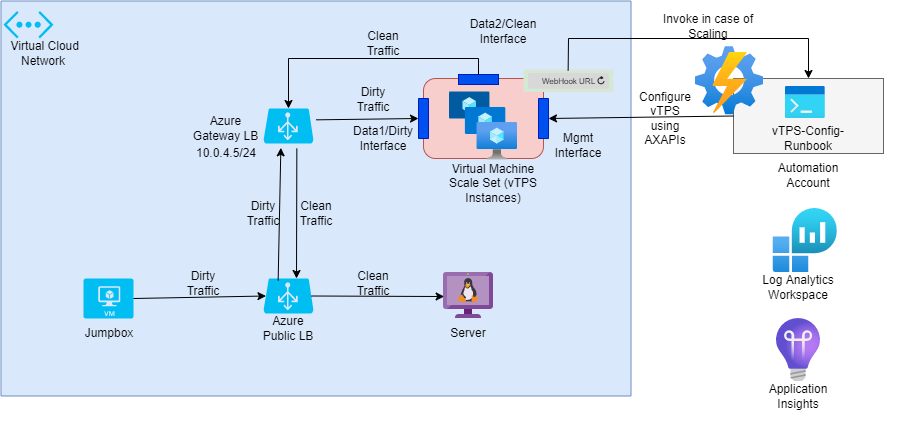
The networking configuration for vThunder is also like hardware based ACOS devices. The maximum throughput of vThunder for Azure is variable and depends on vThunder software license purchase and type instance used to deploy vThunder.

*A10 Networks brings Out-Of-Box template to deploy vThunder(TPS) along with multiple features and functionality with pre-defined format into azure cloud.*

Please refer below section for more details.

* Three Network Card Interface (3NIC).
* Fixed License System (Pay as you go).
* Server Virtual Machine Auto scale set (VMSS).
* vThunder (TPS) Internal Log Monitoring.

Following FIGURE 1-1 : Architecture Blueprint.



# Overview of Microsoft Azure

With the move to the cloud, many teams have adopted agile development methods. These teams iterate quickly. They need to repeatedly deploy their solutions to the cloud, and know their infrastructure is in a reliable state. As infrastructure has become part of the iterative process, the division between operations and development has disappeared. Teams need to manage infrastructure and application code through a unified process.

To implement infrastructure as code for your Azure solutions, use azure resource manager templates. The template is a json native file that defines the infrastructure and configuration for your project. The template uses declarative syntax, which lets you state what you intend to deploy without having to write the sequence of programming commands to create it. In the template, you specify the resources to deploy and the properties for those resources.

**Microsoft Azure** (formerly known as Windows Azure) is Microsoft’s cloud computing platform. Azure is an industry leader for both infrastructure-as-a-service (IaaS) and platform-as-a-ser- vice (PaaS). Azure offers a combination of managed and unmanaged services that lets customers deploy and manage their applications as they see fit.

The Azure cloud computing platform runs on Microsoft data center and is globally dis- tributed across more than a dozen countries. Such global distribution helps ensure customers receive high performance, regardless of where they are located.

Azure is flexible and can support virtually any operating system, from Windows to Linux, any programming language, from Java to C++, and any database, from SQL to Oracle. Azure also offers 99.95% uptime and is the platform that Microsoft uses to run many of its popular ser- vices, such as Bing, Skype, Xbox, and Office 365.

A10 Networks vThunder virtual device can be set up as an instance in Azure’s cloud and can be used to provide a robust thread protecting system.

Microsoft Azure uses the following tools to create and manage resources:

**Azure Portal** - A web console to create and monitor Azure resources. For more information, refer to <https://azure.microsoft.com/en-in/features/azure-portal/>

**Azure PowerShell** - A set of cmdlets used for managing Azure resources from the command line. Launch Azure PowerShell from a browser within the Azure Cloud Shell or install the software on the system to start a local PowerShell session.

For more information, refer to <https://docs.microsoft.com/en-us/powershell/>

**Azure CLI**- Can also be launched from a browser within the Azure Cloud Shell or install the software on the system to start a local CLI session. For more information, refer to <https://docs.microsoft.com/en-us/cli/azure/overview?view=azure-cli-latest>

You **can** launch Cloud Shell from the top navigation bar of the Azure portal.

FIGURE 1-2: Launching Cloud Shell



The following figure shows how vThunder fits into the Microsoft Azure infrastructure.

# Azure Terminology

**Azure account** — The Azure account created has different support plans for different regions. For more information on different Azure regions and availability of types of virtual machines in these regions, refer to

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/overview>

**Resource group** — A resource group is a logical group of all the resources related to an Azure solution. Azure offers flexibility in the allocation of resources to resource groups.

For more information, refer to

[https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group- overview](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-%20overview/)

**Availability set** — An availability set is a logical grouping of Azure VM resources so that each VM resource is isolated from other resources when deployed. This hardware isolation ensures that a minimum number of VMs are impacted during a failure. For more information, refer to

[https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group- overview](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-%20overview/)

**Virtual network** — The Microsoft Azure Virtual Network service enables resources to securely communicate with other resources in an Azure network in the cloud. A virtual network is hence logical isolation of the Azure cloud for an Azure account. You can connect different virtual networks and to on-premises networks. For more information, refer to

[https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-avail- ability-sets](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-avail-%20ability-sets/)

**Network security group (NSG)** — A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure virtual networks (VNet). The NSGs can be associated with subnets or individual NICs attached to the VMs. When an NSG is associated with a subnet, the rules apply to all the resources connected to the subnet.

**Azure Resource Manager (ARM)** — To implement infrastructure as code for your Azure solutions, use Azure Resource Manager templates (ARM templates). The template is a JavaScript Object Notation (JSON) file that defines the infrastructure and configuration for your project. The template uses declarative syntax, which lets you state what you intend to deploy without having to write the sequence of programming commands to create it.

# Pre-requisites [Resource Group, VNet, Service App, vTPS ARM Template]

Please find below detailed pre-requisites to install template using ARM.

1. Azure account and valid subscription.

[Azure Portal](https://azure.microsoft.com/en-in/features/azure-portal/)—A web console to manage azure resources.

1. Azure Resource Group – A resource group container hold all related resources.

In case if you want to use existing resource group that will also work. Just list down and select while executing ARM.

In case you want to create all new then follow below.

Refer [Annexure 1 – Create Azure Resource Group](#_Annexure_1_–_1)

1. Azure Virtual Network – VNet is a virtual network boundary for communication.

In case if you want to use existing vnet that will also work. Just list down Vnet name and four subnet name/range which you want to use and provide while executing ARM.

In case you want to create all new then follow below.

Refer [Annexure 2 - Create Azure Virtual Network [VNet] & Subnet](#_Annexure_2_–)

1. Azure Service Application Access Key – Access key will used to automate scale set creation and configuration. Existing service app will also work.

In case you have existing service app created, and you want to use it just you must add IAM user in Owner section of Service App. List down service app name and provide while executing ARM template.

How to check service app is already available:

Azure Portal -> Menu -> Azure Active Directory -> App Registration -> Check for All applications or Owned applications -> Search or navigate and select anyone.

How to add Owner in existing service app:

Select Service App -> Owners -> Add Owners.

In case you want to create all new then follow below.

Refer [Annexure 3 – Create Service Application Access Key](#_Annexure_1_-)

1. Public Load Balancer IP – Choose Public facing load balancer frontend ip address which will send traffic to private gateway load balancer and private gateway load balancer will send traffic to vTPS instances.

Private GLWB and vTPS will be created by ARM template.

List down public lb ip and provide while executing ARM.

Refer [Public Load Balancer Frontend IP [Public LB]](#_Public_Load_Balancer).

1. ARM Template Artifacts – [Download](https://github.com/dlohia-a10/a10-azure-arm-templates/tree/main)

# [QuickStart: Install A10 - vThunder vTPS - Azure portal l ARM](https://learn.microsoft.com/en-us/azure/virtual-network/quick-create-portal)

Users must keep *Subscription, Resource Group, VNET, Subnet, Client ID, Client Secret, Tenant ID, Public Load Balancer IP, ARM Template File* handy as per [pre-requisites](#_Pre-requisites).

### 1. Launch ‘Custom Deployment’

FIGURE 2-1: Deploy a custom template

Graphical user interface, text, application, email

Description automatically generated

Click ‘Build your own template in editor’

FIGURE 2-2: Select build your own

Graphical user interface, text, application, email

Description automatically generated

### 2. Launch ‘ARM Template’

Click Load File and Select ARM Template file mentioned in [Prerequisite # 5](#_Pre-requisites) download section and save.

File name: A10-vThunder\_vTPS-3NIC-VMSS-GWLB.json

FIGURE 2-3: Load ARM Template

Graphical user interface, text, application

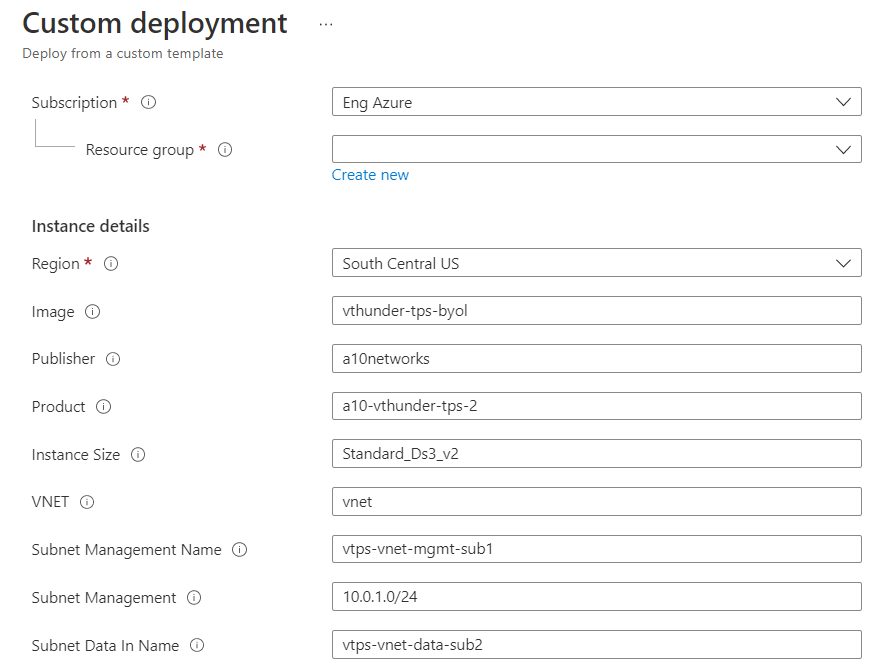
Description automatically generated

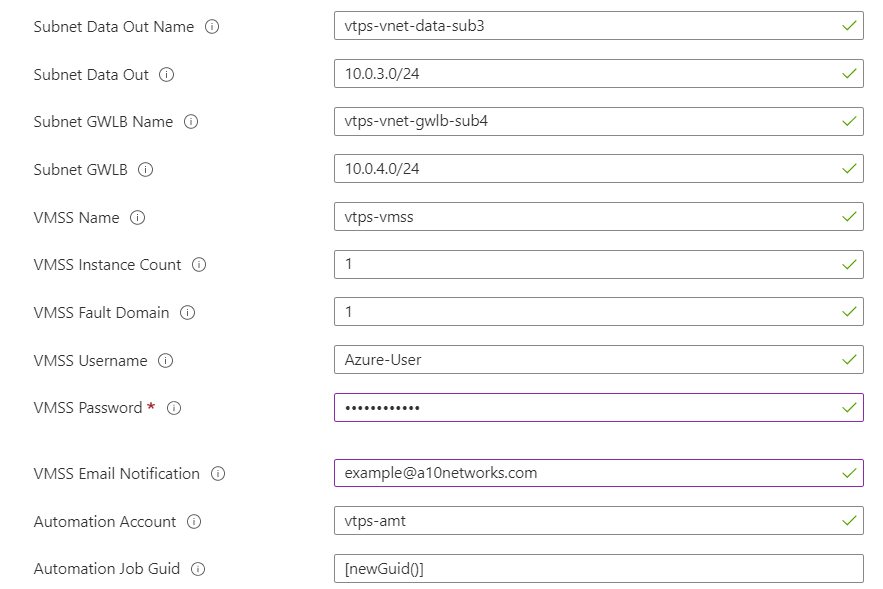
Click Save

New form will be opened. Please enter all details. Most of all are pre-populated and allowed for customization.

Information icon [I] has all necessary information.

FIGURE 2-4: Fill in details and create.





Graphical user interface, text, application, email

Description automatically generated

All Set ! Put your feet up and take it easy. 😊

System may take ~10 to ~20 mins to do end to end installation and setup, depending upon region.

Once installation is done, you can enable public traffic into vTPS ecosystem and enable azure log analytics dashboard and view vTPS logs by default both are disable.

Please refer [Annexure 8 – Enable Public Traffic to GWLB-vTPS Eco System.](#_Annexure_8_–)

Please refer [Annexure 9 – Enable vTPS Logs Monitoring in Azure Log Analytics Dashboard.](#_Annexure_10_–)

Please refer [Annexure 10 – View vTPS Logs in Azure Log Analytics Dashboard.](#_Annexure_10_–_1)

# Annexures

## Annexure 1 – Create Azure Resource Group [RG].

Azure resource group is a container that holds related resources for an azure solution.

Recommended Name : *vtps-rg*

[QuickStart: Create a resource group - Azure portal - Azure Resources Management | Microsoft Learn](https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal)

## Annexure 2 – Create Azure Virtual Network [VNet] & Subnet.

Azure resource group is a container that holds related resources for an azure solution.

One Vnet and four subnets as follows.

Default name: *vnet*

Default address prefix for virtual network is *10.0.0.0/16*

Default management subnet name: *vnet-mgmt-sub1*

Default management subnet range: *10.0.1.0/24*

Default data-in subnet name: *vnet-data-sub2*

Default data-in subnet range: *10.0.2.0/24*

Default data-out subnet name: *vnet-data-sub3*

Default data-out subnet range: *10.0.3.0/24*

Default gwlb subnet name: *vnet-gwlb-sub4*

Default gwlb subnet range: *10.0.4.0/24*

[QuickStart: Create a virtual network - Azure portal - Azure Virtual Network | Microsoft Learn](https://learn.microsoft.com/en-us/azure/virtual-network/quick-create-portal)

## Annexure 3 – Create Service Application Access Key.

Azure access key is required to access resources. To create the Azure access key.

In case you have existing service app created, and you want use it just you must add IAM user in Owner section of Service App.

Perform the following steps:

1. [Create a Role](#_Create_a_Role)
2. [Register a Service Application](#_Register_a_Service)
3. [Associate Service Application with a Role](#_Associate_Service_Application)
4. [Create Certificate and Secrets](#_Create_Certificate_and)
5. [Collect Azure Access Key](#_Collect_Azure_Access)

#### 1. Create a Role

To create a custom role, perform the following steps:

1. Navigate to the Home > Subscriptions > Registered Subscription Name > Access control (IAM) from left panel.

FIGURE 3-1: Subscriptions - Access control (IAM) window



1. On the Select Access control (IAM) page, select the Roles tab. The Role window is dis- played.

FIGURE 3-2: Access Control - Role Window



1. Click on the +Add tab and select Add custom role option. The Create a custom role window is displayed.

FIGURE 3-3: Add custom role window



1. Enter Customer role name and Description (optional).

FIGURE 3-4: Create a custom role window



1. Click on the **Next** button. The Permission window is displayed.

*FIGURE 3-5: Permission window*



1. Click on the **+Add Permissions** button to create a custom role.
2. Search for the permission to add the custom role.

For example, select **Microsoft Compute** from Add Permissions page.

*FIGURE 3-6: Add permission window*



The Microsoft Compute permission window is displayed.

*FIGURE 3-7: Microsoft Compute permissions window*



1. Select the **Permission** check box(es) and click **Add** button.
2. To add **Microsoft Network** from Add Permissions page, click on the **+Add Permissions**

on Create a custom role page.

*FIGURE 3-8: Create a custom role - Add permissions*



1. Search and select **Microsoft Network** from Add Permissions page.

*FIGURE 3-9: Add permissions - Microsoft Network page*



1. Select the **Permission** check box and click **Add** and **Review + create**.

*FIGURE 3-10: Microsoft Network permissions window*



The **Create a custom role** confirmation window is displayed.



1. Click OK to successfully create the custom role with permissions.

**NOTE:** It may take the system a few minutes to display your role everywhere.

#### 2. Register a Service Application

To register a service application, perform the following steps:

1. Navigate to the Home > Services > Azure Active Directory option.

*FIGURE 3-11: Azure Active Directory page*



1. On the Azure Active Directory page, click on the App registrations menu option from the left panel. The App registration window to register an application is displayed.

*FIGURE 3-12: App registrations window*



1. Click on the **+New Registration** tab. The Register an application window is displayed.

*FIGURE 3-13: Register an application window*



1. Enter the **Name** of the application. For example, acos-sapp.
2. Click on the **Register** button to register the application. The application gets displayed in the list of Azure Active Directory - Apps registrations window.

#### 3. Associate Service Application with a Role

To associate service application with a created role, perform the following steps:

1. Navigate to the **Home** > **Subscriptions** > **Registered Subscription Name** > **Access control (IAM)**.

The Subscription > Access control (IAM) window is displayed.

*FIGURE 3-14: Subscription - Access control (IAM) window*



1. To assign a role to the above scope, click the **+ Add** tab from the main menu options. The Add role assignment window is displayed.

*FIGURE 3-15: Add a role assignment -1*



1. Select a **Role** from the drop-down list. For example, acos-role.
2. Select the **Assign Access to** option from the drop-down list.
3. Enter a string to search and select for a name or email address. For example, acos.
4. Click the **Save** button to save the configuration.

#### 4. Create Certificate and Secrets

To create certificate and secrets for the assigned role, perform the following steps:

1. Navigate to the **Home** > **Services** > **Azure Active Directory** option.

*FIGURE 3-16: Azure Active Directory - Overview page*



1. On the Azure Active Directory - Overview page, click on the App registrations menu option from the left panel. The App registration window with a registered application(s) is displayed.

*FIGURE 3-17: App registrations - Overall applications window*



1. Select a service application from list of applications. The selected service application window is displayed.
2. Select the **Certificates & secrets** option from the left Manage navigation pane. The acos sapp - Certificates & secrets window is displayed.
3. Select the **Start date** and **Expires** date from the date picker.

Or Click the **New client secret** button. The Add a client secret window is displayed.

*FIGURE 3-18: Add a client secret window*



1. Enter the New client secret **Description**, **Expires** value. The entered value is displayed on the acos-Certificates & secrets window.

*FIGURE 3-19: acos-sapp Certificates & secrets window*



NOTE:

Copy the new client secret value, as it is not visible once the page is refreshed.

#### 5. Collect Azure Access Key

To collect Azure access keys, perform the following steps:

1. Navigate to the **Home** > **Azure Active Directory** - **App registrations**.

*FIGURE 3-20: App registrations - Azure Active Directory window*



1. Select service application from the list of applications. The selected service application page is displayed.

*FIGURE 3-21: Selected Service application window*



1. Copy the Client ID, Tenant ID from the service application page. client\_id= 'cc4c86xx-65b3-48xx-a3xx-610cxxxxxxxx’ tenant\_id= '91d27axx-8cxx-41xx-82xx-3d1bxxxxxxxx'
2. Navigate to the **Home** > **Subscriptions** > **Registered Subscription Name**, and copy subscription ID value.

*FIGURE 3-22: Subscriptions window*



1. Create a text file with as subscription, client\_id, client\_secret and tenant\_id as shown below:

subscription='07d34bxx-61xx-47xx-abxx-006bxxxxxxxx'

client\_id='cc4c86xx-65xx-48xx-a3xx-610cxxxxxxxx’ client\_secret='G0x\_hVDzZxxxx-o1Vsw.xxxx.Zxxxx-xx' tenant\_id='91d2xxxx-8xxe-41xx-82xx-3d1bxxxxxxxx’

## Annexure 4 – Cloud Resources Information.

This section will help to understand what all resources will be used in vTPS.

Resource will be created while installation no need to create separately other than resource group and vnet.

#### Azure Resource Group.

Any resource group with any name require to install vTPS. Should be present before installing vTPS.

Default name: *vtps-rg*

#### Virtual Cloud Network. [VNet]

Any VNet with any name should be created prior to install vTPS.

Default address prefix for virtual network is 10.0.0.0/16.

Default name: *vnet*

Subnets.

Total three subnets will be required to install vTPS. Address prefix can be configured in parameter file. Should be present before creating vTPS. User can define own naming strategy.

Default name for management subnet: *vnet-mgmt-sub1*

Default name for data-in subnet: *vnet-data-sub2*

Default name for data-out subnet: *vnet-data-sub3*

Default name for data-out subnet: *vnet-data-sub3*

Default name for data-out subnet: *vnet-gwlb-sub4*

#### Virtual Machine Scale Set. [VMSS]

VMSS will be created with group of VM instances while installation.

Default name: *vtps-vmss-\**

Default host name: *vtps-vmss-\**

Default vmss public ip name: *vtps-vmss-public-ip-\**

**Virtual Machine [VMs] instances**

Instance Name: *vtps-vmss\_\**

Operating system: Linux

Default Size: Standard\_Ds3\_V2 (4 vCPUs, 16 GiB Memory)

Note:

1. Highly recommended to do assessment of your projected traffic before selecting any size. It will cost you.
2. Instances name and size can be customized in parameter file or console.
3. Any instance size will work if it has capacity to create at least 3 NICs.

**Supported VM Sizes**

|  |  |  |
| --- | --- | --- |
| ***Series*** | ***Size*** | ***Qualified Name*** |
| A series | Standard A4\_v2  Standard A4m\_v2  Standard/Basic A4  Standard A8\_v2 | Standard\_A4\_v2  Standard\_A4m\_v2  Standard\_A4  Standard\_A8\_v2 |
| B series | Standard B2\_s  Standard B2ms  Standard B4ms | Standard\_B2\_s  Standard\_B2ms  Standard\_B4ms |
| D series | Standard D3\_v2  Standard DS3\_v2  Standard D5\_v2  Standard Ds8\_V3 | Standard\_D3\_v2  Standard\_DS3\_v2  Standard\_D5\_v2  Standard\_Ds8\_V3 |
| F series | Standard F4s  Standard F8  Standard F16s | Standard\_F4s  Standard\_F8  Standard\_F16s |

Few of sizes are getting retried soon from azure, please refer [Virtual Machine series | Microsoft Azure](https://azure.microsoft.com/en-in/pricing/details/virtual-machines/series/).

For more information, please refer as below.

<https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-> [general](http://sales@a10networks.com/)

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes>.

#### Network Interface Card. [NIC]

All below network interface will be created while installation. No need to create separately.

Default name for management interface: *vtps-vmss-nic1-mgmt*

Default name for data interface (Data In): *vth-vmss-nic2-data*

Default name for data interface (Data In): *vth-vmss-nic3-data*

#### Network Security Group. [NSG]

Default all interfaces are associated with security group and all will be created while installation.

Default name for management : *vtps-vmss-nsg-mgmt*

Default name for data : *vtps-vmss-nsg-data*

Default Security Rules:

#### Public Load Balancer Frontend IP [Public LB]

This public load balancer is main door and existing load balancer from where all traffic will be routed for any system. This public lb will send all traffic to gwlb and then gwlb will sends to vTPS.

ARM will not create public load balancer.

This is required while executing arm template. User should have handy.

It cannot be wild card [0.0.0.0]. In case it is not created yet, you can choose any dummy ip[72.0.0.1] while arm execution. Later it can be changed from vTPS CLI.

Once the arm template execution completes, public lb should be updated with gwlb. Please refer [configure public lb](#_Annexure_9_–).

Once configuration is done then only traffic will be routed to vtps.

#### Gateway Load Balancer [GWLB].

Gwlb will created while installation.

Default gwlb frontend private ip name: *vtps-gwlb-frontend-ip-\**

Default GWLB Name: *vtps-gwlb-*\*

#### Azure Automation Account

One automation account will be created while installation. No need to create separately.

Default name: *vtps-amt-\**

Azure runbook with webhook will be created within automation account.

Default name: *vtps-config*

Webhook Default name: *vtps-config-webhook*

#### Monitoring Services

Below resources will be created while installation.

Default name for Log Analytic Workspace: *vtps-log-analytics-workspace-\**

Default name for App Insights: *vtps-app-insights-\**

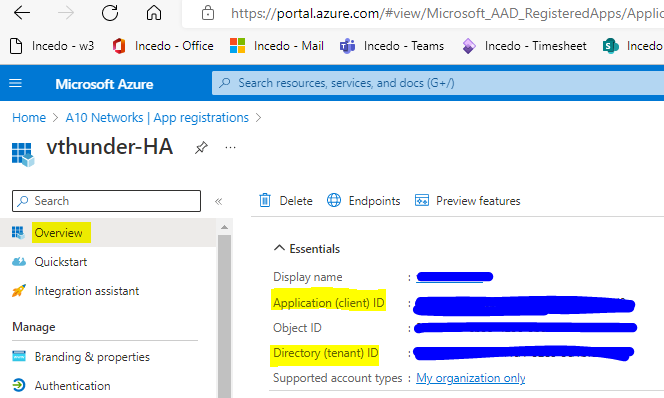
#### Service App Account & Credentials

Application client id and tenant id can be found in service application resource and with this access key vtps can be configured dynamically in scale-set.

In case service application key is not created, please follow [Annexure 1 - Generate Service Application Access Key](#_Annexure_1_-)

Below steps shows how to read client id, tenant id.

Go to Azure Portal -> Azure Active Directory -> Service App -> Overview ->



Below steps shows how to read client secret.

Go to Azure Portal -> Azure Active Directory -> Service App -> Certificates & Secrets -> Value = Client Secret

Graphical user interface, text, application, email

Description automatically generated

## Annexure 5 – Login to vThunder using CLI

SSH to vThunder Instance:

Open putty and connect.

IP: Get vThunder Public IP

User Id [Default]: admin

Password [Default]: a10

After login.

Execute Command -> enable

Password -> <just press enter>

Text

Description automatically generated

## Annexure 6 - Login to vThunder using Console

GUI: Check below vThunder GUI

To enable GUI, enable few ports.

Web URL: http://IP

<https://ip/gui/auth/login/>

User Id [Default]: admin

Password [Default]: a10

## Annexure 7 – Verify vTPS DDoS Configuration

login into vThunder.

Check all configurations. Run command ‘show running-config’:

Confirm all below parms.

Text

Description automatically generated

Text

Description automatically generated

## Annexure 8 – Enable Public Traffic to GWLB-vTPS Eco System

This section will enable traffic routing from public load balancer to gateway load balancer created by vTPS. Gateway load balancer will then send all traffic to vTPS.

Please follow below steps.

Azure Portal -> Load Balancer -> Search Public Load Balancer -> Frontend IP Configuration -> Select IP -> Select Gateway Load Balancer [vtps-gwlb-frontend-ip-\*] -> Save.

## Annexure 9 – Enable vTPS Logs in to Azure Log Analytics Dashboard.

This section will enable traffic routing from vtps system to azure log analytics rest api using internet. All logs will be published to azure log analytics workspace via nat gateway.

Please follow below steps.

Azure Portal -> Nat Gateways -> Select [vtps-nat-gateway-\*] -> Subnets -> Select Virtual Network [provided while arm execution] -> Management Subnet [provided while arm execution] -> Save

## Annexure 10 – View vTPS Logs in Azure Log Analytics Dashboard

This section will enable log dashboard and provide platform to query logs. All logs coming from vtps will be shown and can be filter as per queries.

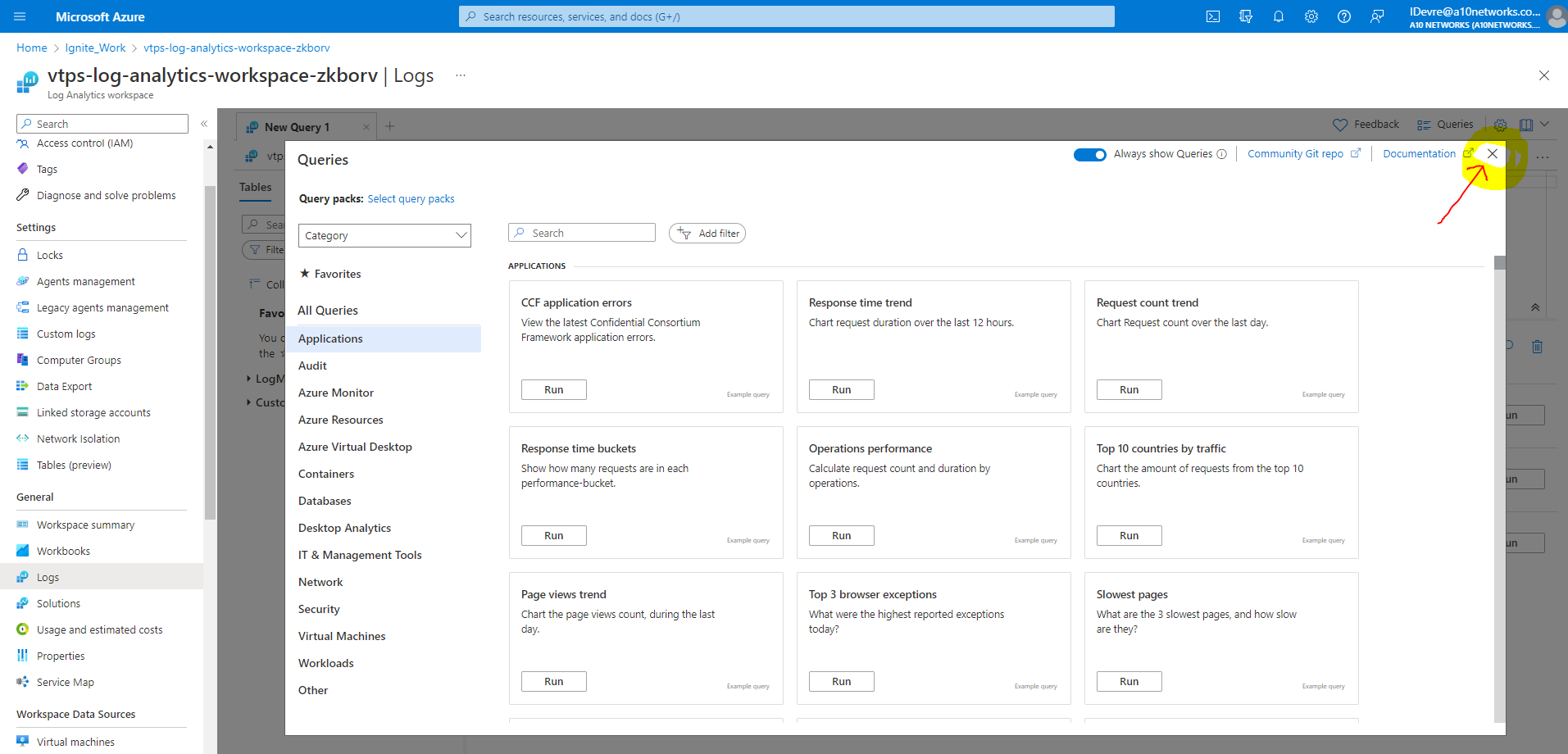
1. Azure Portal -> Log Analytics Workspaces -> Search & Select Log Analytics Workspace ID [provided while arm execution] -> Logs.

Graphical user interface, text, email

Description automatically generated



1. Please close any popup. [Query pack section please close it].





1. Click on the custom log table section.

Table “VMSS\_TPS\_DDOS\_DDET\_LOGS” will be populated under custom logs section. (After first logs get publish it may take 3 to 5 min to get displayed).

Graphical user interface, text, application, email

Description automatically generated



1. Execute following query

Query 1: Query to fetch all records from the table.

Copy table name [VMSS\_TPS\_DDOS\_DDET\_LOGS] into query box. And click Run.

It will result entire contents.

Graphical user interface, text, application, email

Description automatically generated



Query 2: Query all records which are “anomaly detected”.

let FindString = "anomaly detected";

VMSS\_TPS\_DDOS\_DDET\_LOGS\_CL

| where log\_data\_s has FindString

Graphical user interface, text, application, email

Description automatically generated

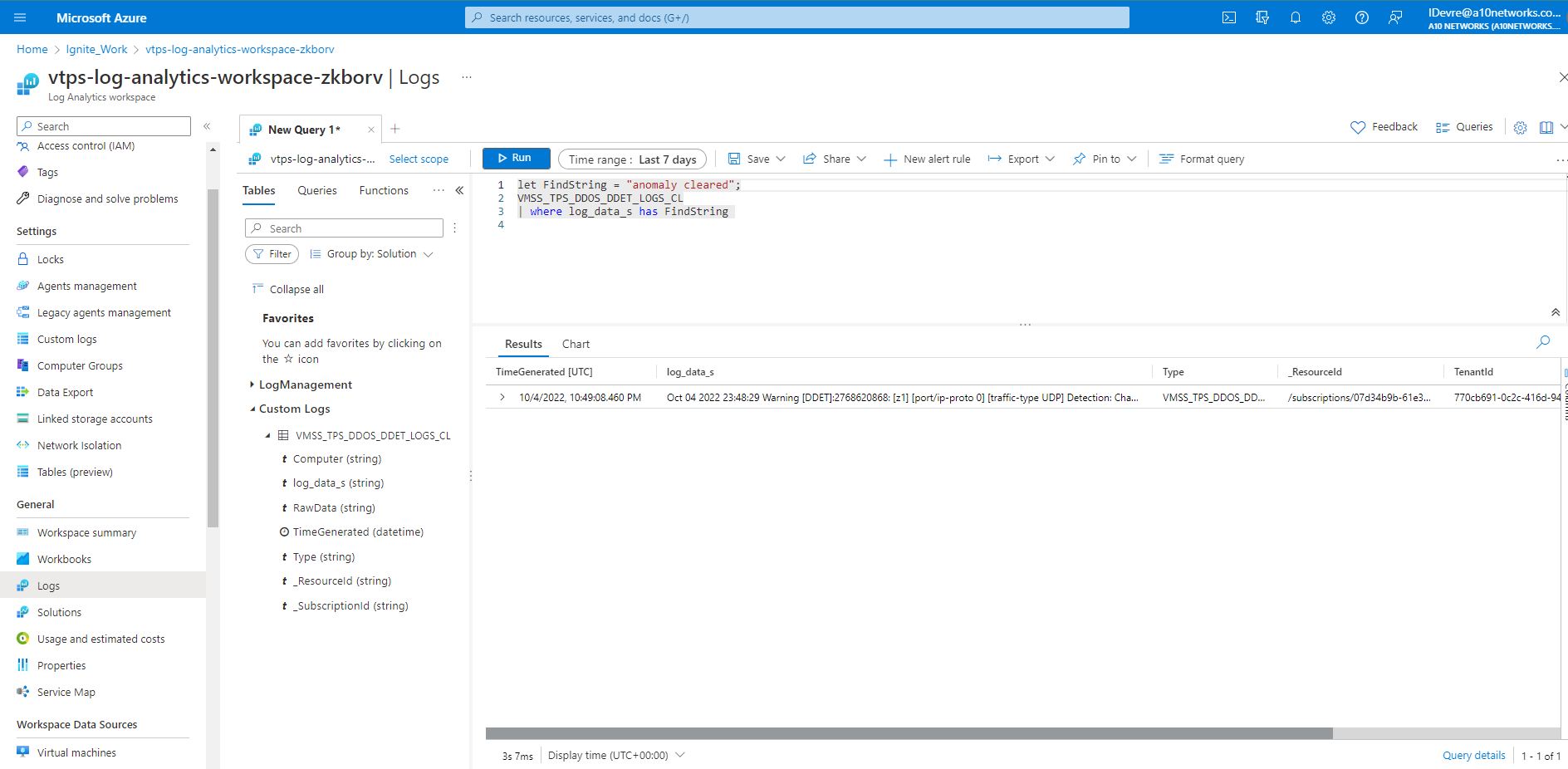


Example 2: Query all records which are “anomaly cleared”.

let FindString = "anomaly cleared";

VMSS\_TPS\_DDOS\_DDET\_LOGS

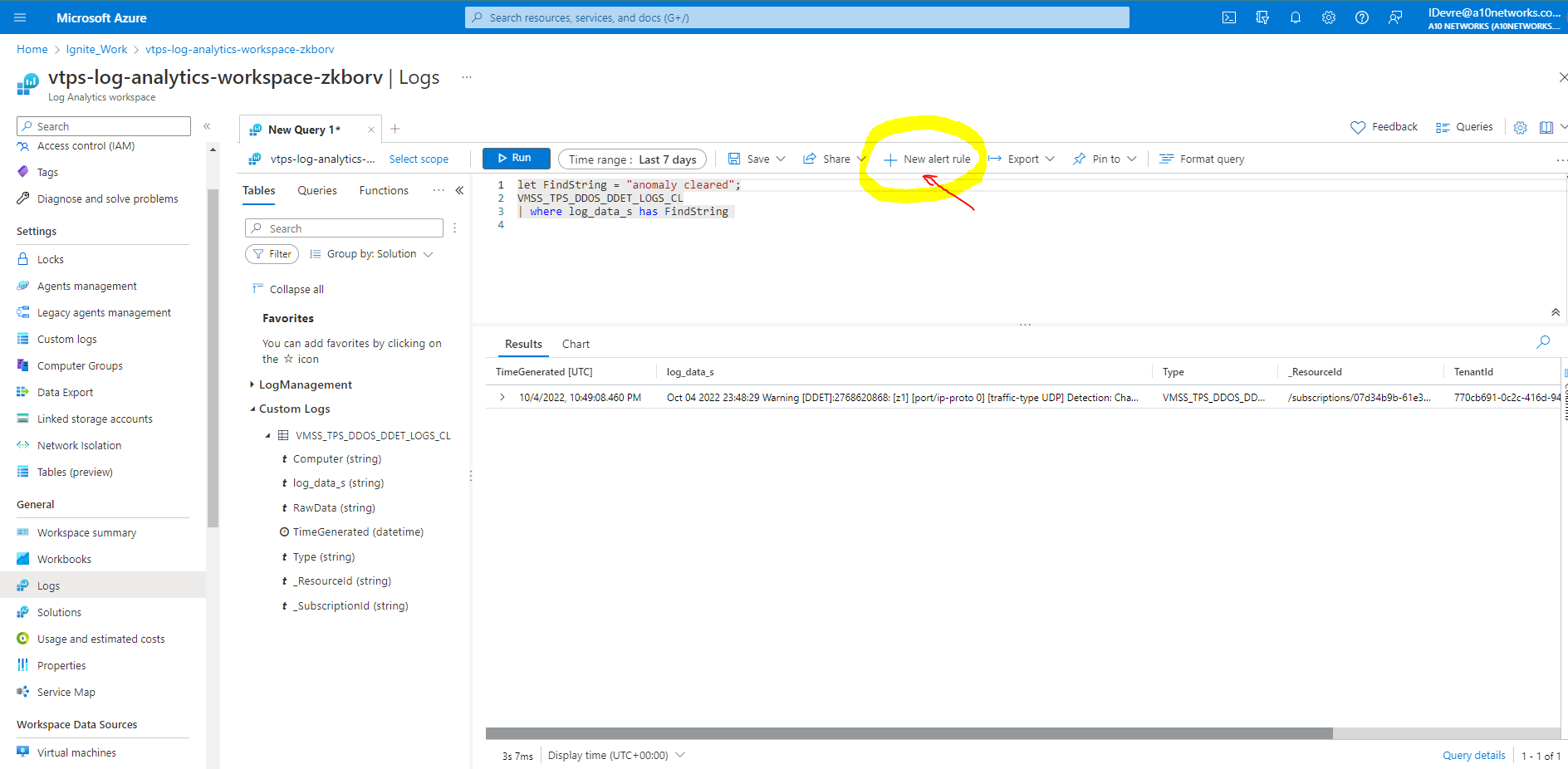
| where LogEntry has FindString





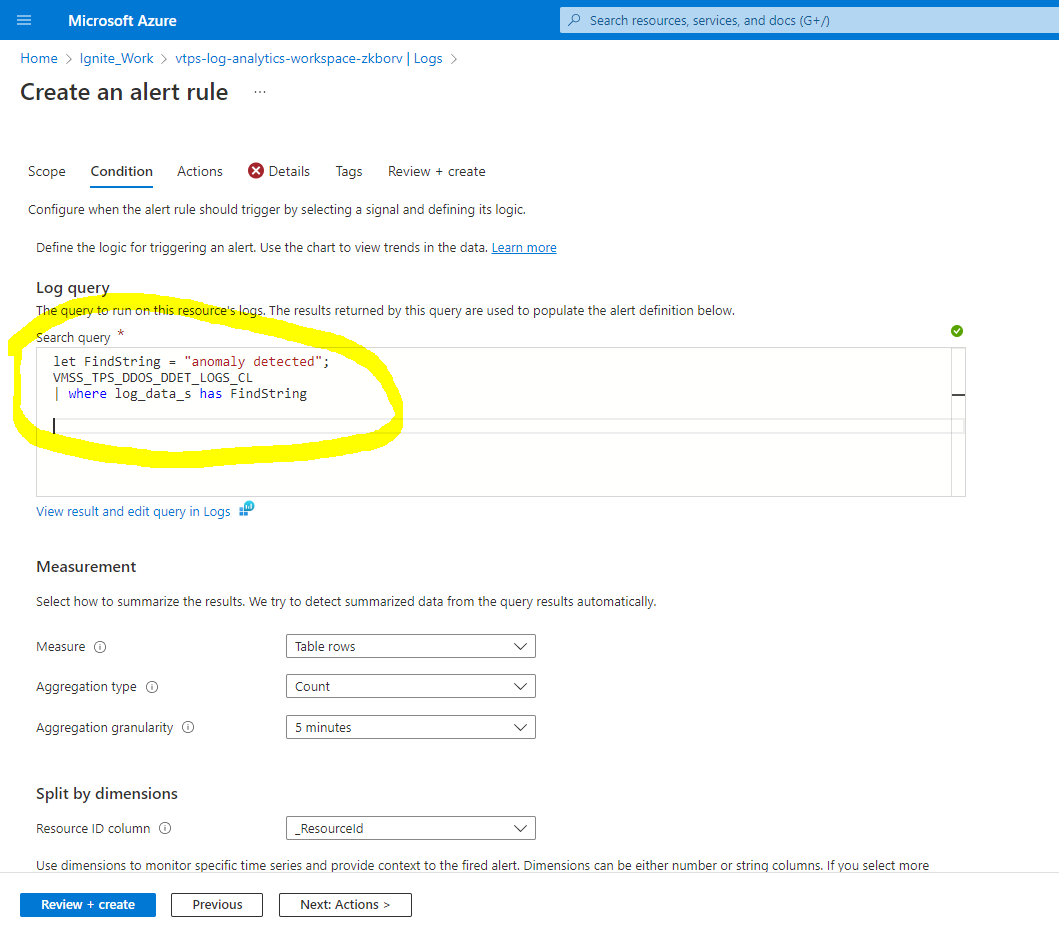
1. Create Alert Rule and Action Group.

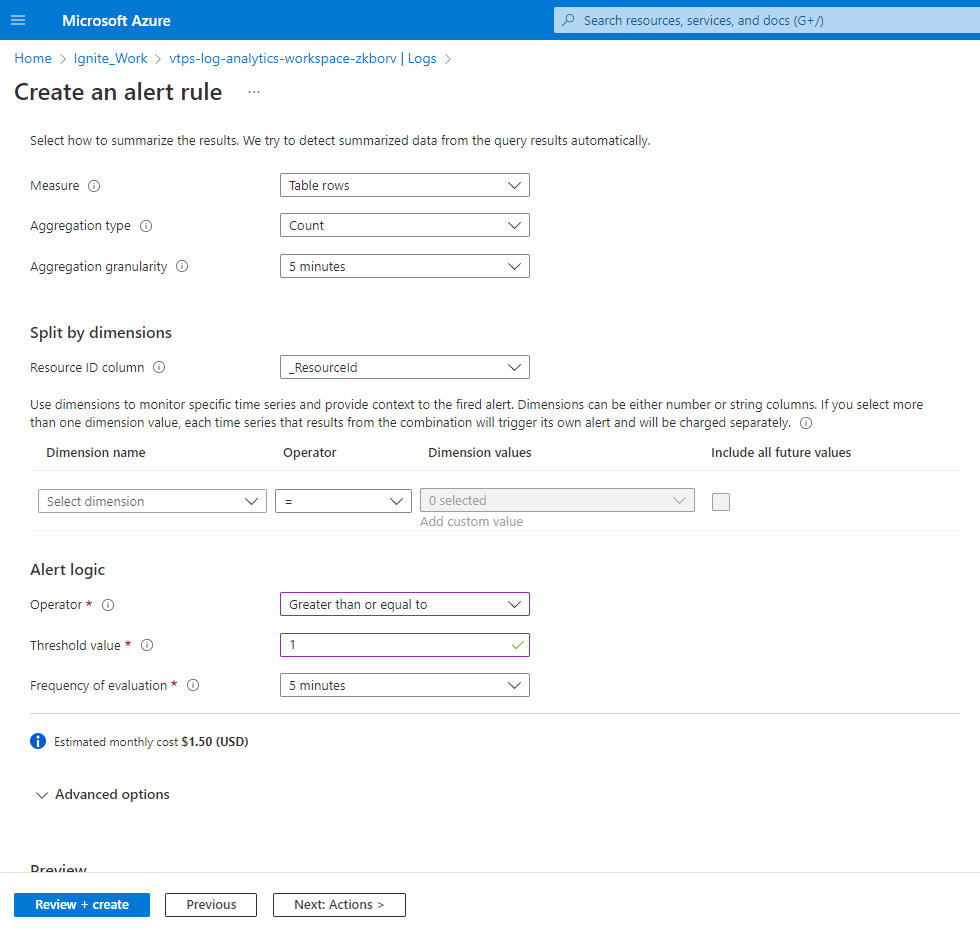
For example: Send email alert notification for all anomaly detected records in last 5 mins aggregated for all instances with threshold equal or greater than 1.

* + 1. Click on “New alert rule” as shown in following snap.



* + 1. You will see the same query in search query box on which you want to trigger the alert. You can also put your own query.

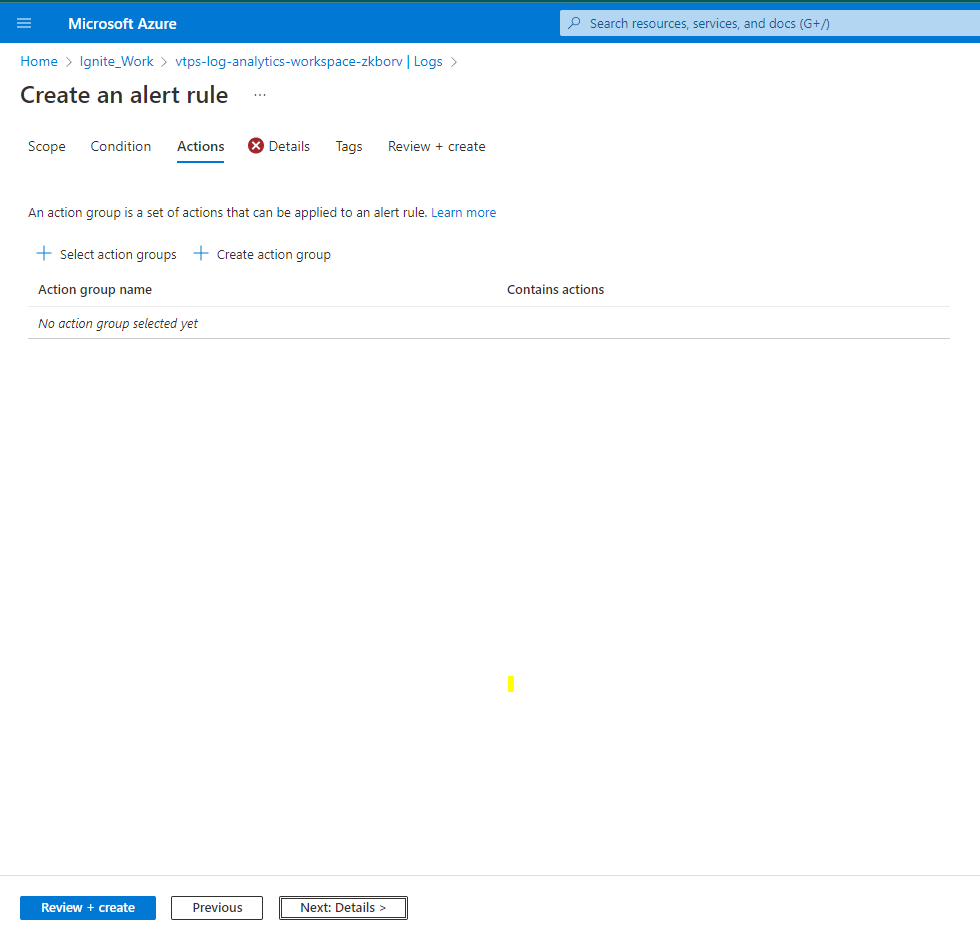




aggregation granularity will aggregate last 5 min records.

Above rule is also applied on options “frequency of evaluation” in Alert logic section.

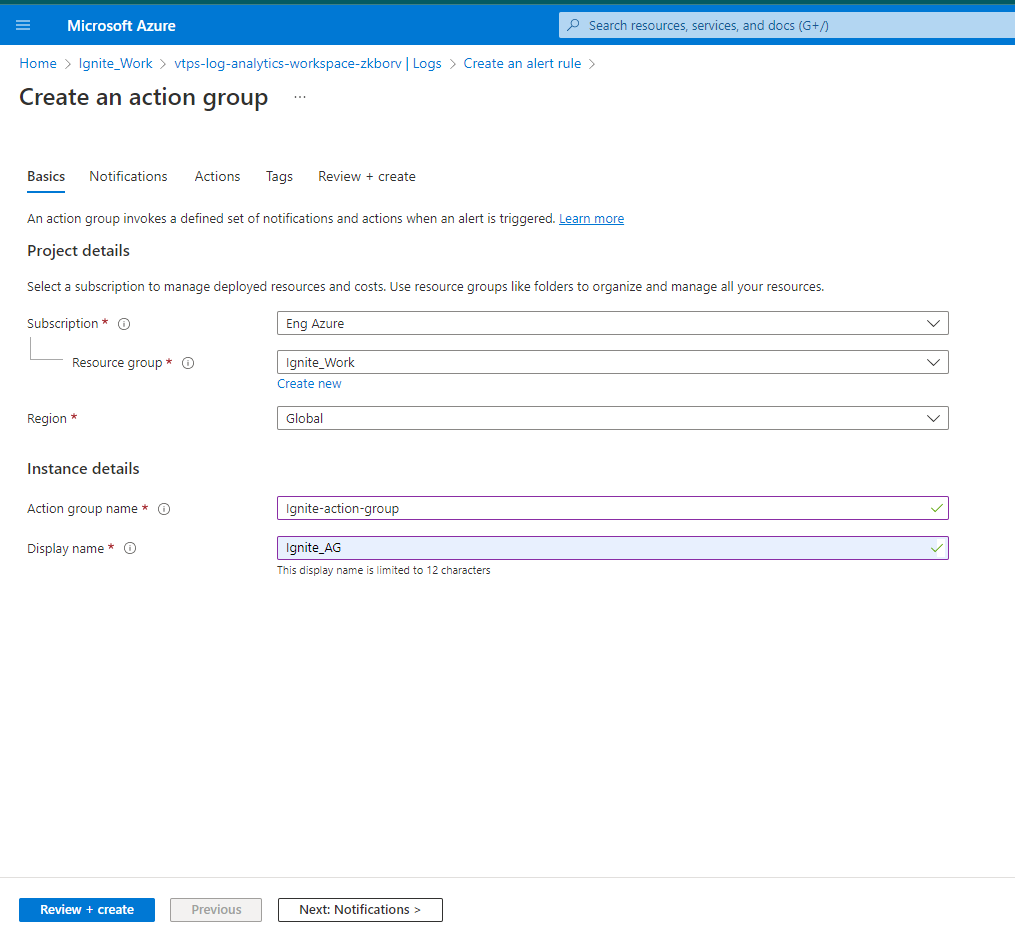
* + 1. Click on “Next: Actions”. To create action group.
    2. Click on “Create action group”.



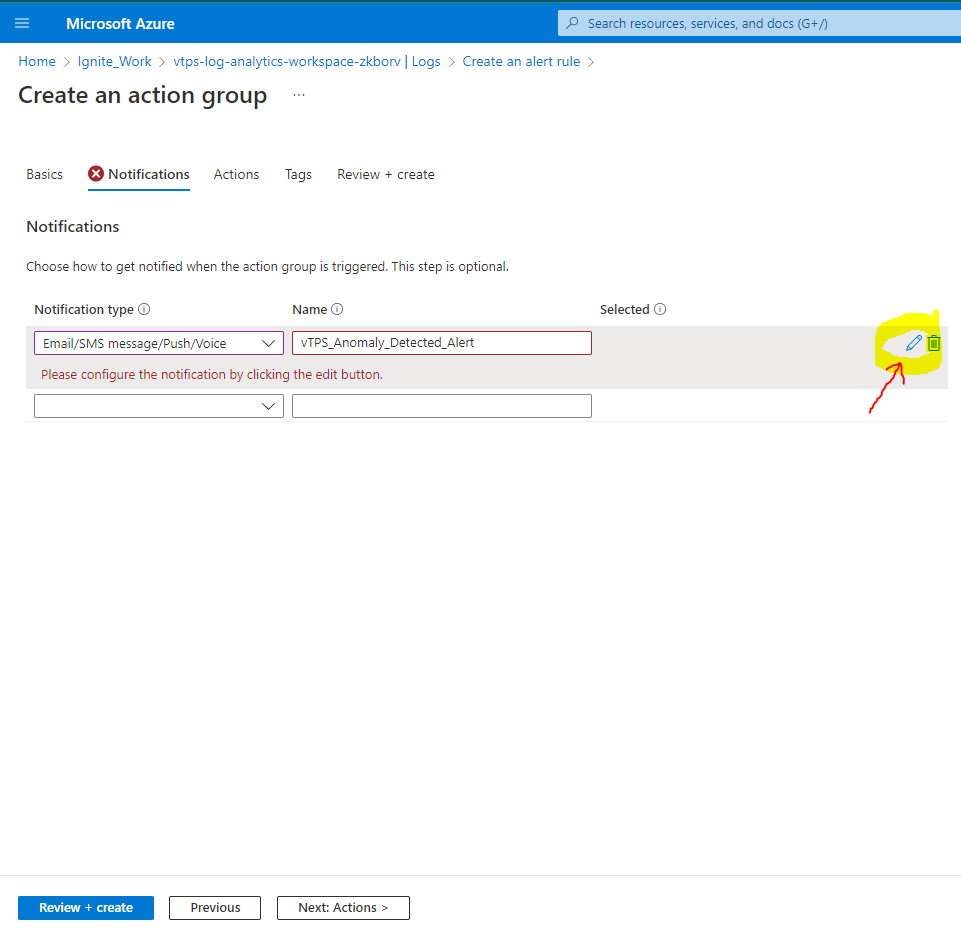


* + 1. Fill the action group name and display name





* + 1. Click on “Next: Notifications”.
    2. On create notification page, select notification type “Email/SMS message/PUSH/Voice”.
    3. Enter Name of the Alert Notification. Ex. vTPS\_Anomaly\_Detected\_Alert\_Notification.
    4. Click on Edit button as shown in following snap.



* + 1. Edit page will pop-up. Choose how you want to get alert notifications.

1. If you want Email notifications, Click on Email checkbox and provide your Email id.
2. If you want SMS/Voice Call, click on SMS/Voice Call checkbox, and provide Phone No.
3. If you want Azure mobile app notification, click on Azure mobile App checkbox and Provide Email id. Download Azure Mobile App. Login with the same Email id as you provided earlier.



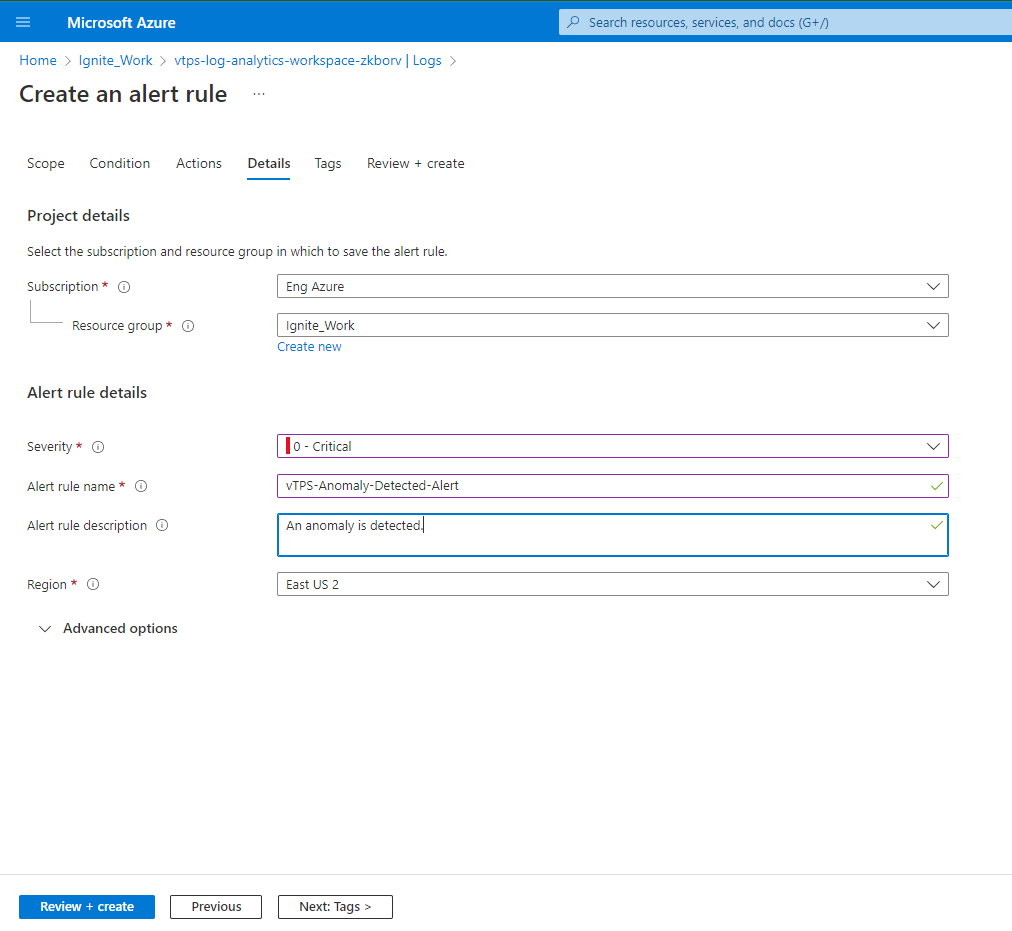


* + 1. Click on “OK”
    2. Click on “Next: Action”
    3. Choose which actions are performed when the action group is triggered. This step is optional. Keep it blank. Do not change anything.
    4. Click on “Next: Tags”. Tags are name and value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Put some related and informative string in tags. Tag does not affect another config.
    5. Click on “Review + Create”. Review the details and click on create.
    6. Action group will be created and create alert rule page will be opened.

Graphical user interface, text, application, email

Description automatically generated

* + 1. Recently created action group will be added in action group list.
    2. Click on “Next: Details”.
    3. Create an alert rule and Project details page will open.



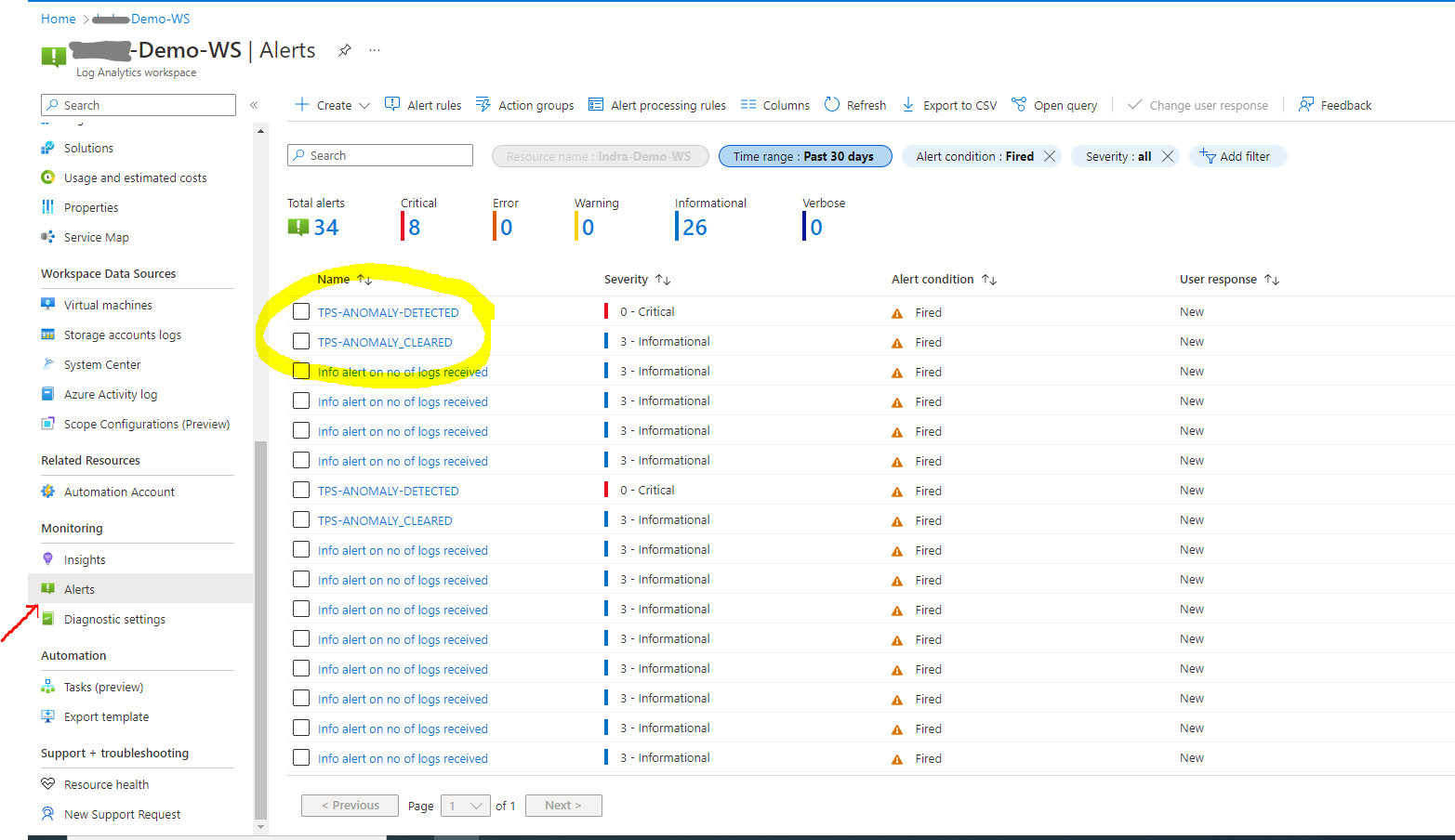
* + 1. Select severity, fill something informative in alert rule name and description box. This information will be added into notification email.
    2. Click on “Next: Tags”. Tags are name and value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Put some related and informative string in tags. Tag does not affect another config.
    3. Click on “Create + review”.
    4. Review carefully, the pricing details, condition to trigger the alert and action group. Click on Create. Alert will be created.

1. How Alert will be notified?

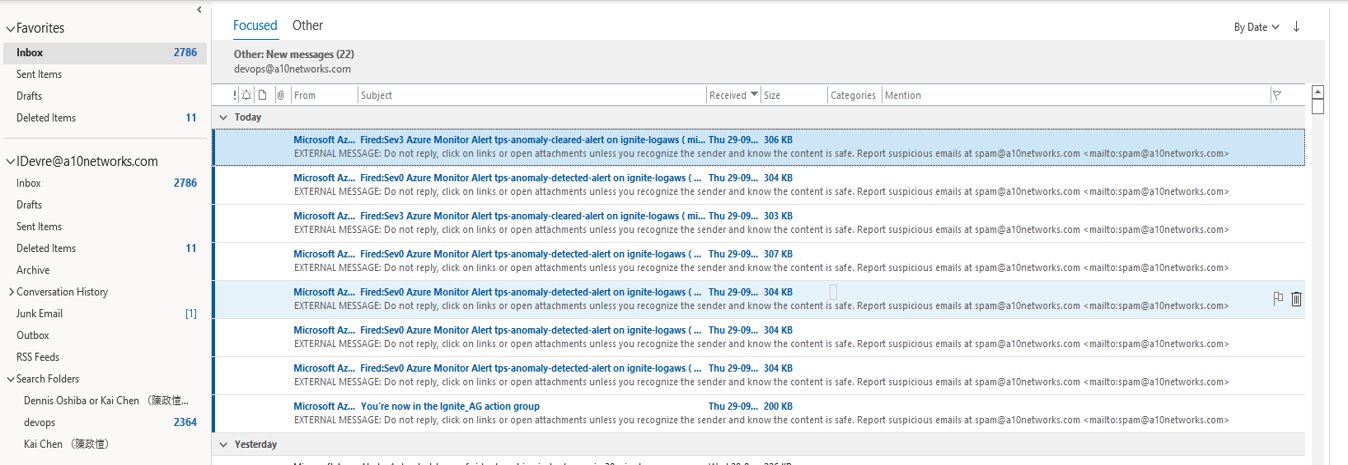
Once user start getting logs in log analytics workspace. Provided query will be evaluated in time interval provided in frequency of evaluation.

If query result satisfies alert triggered condition (alert logic). Alert will be triggered, and action group will be activated to send notifications.

1. How to check alerts on Azure portal
   * 1. Open log analytics workspace.
     2. Click on Alerts



1. How alert notifications will look like?
   * 1. Email Notifications





* + 1. Azure Mobile App Notifications

Graphical user interface, application

Description automatically generated