DIGITAL SIGNAGE

HARDENING

04/02/2018

Table of Content

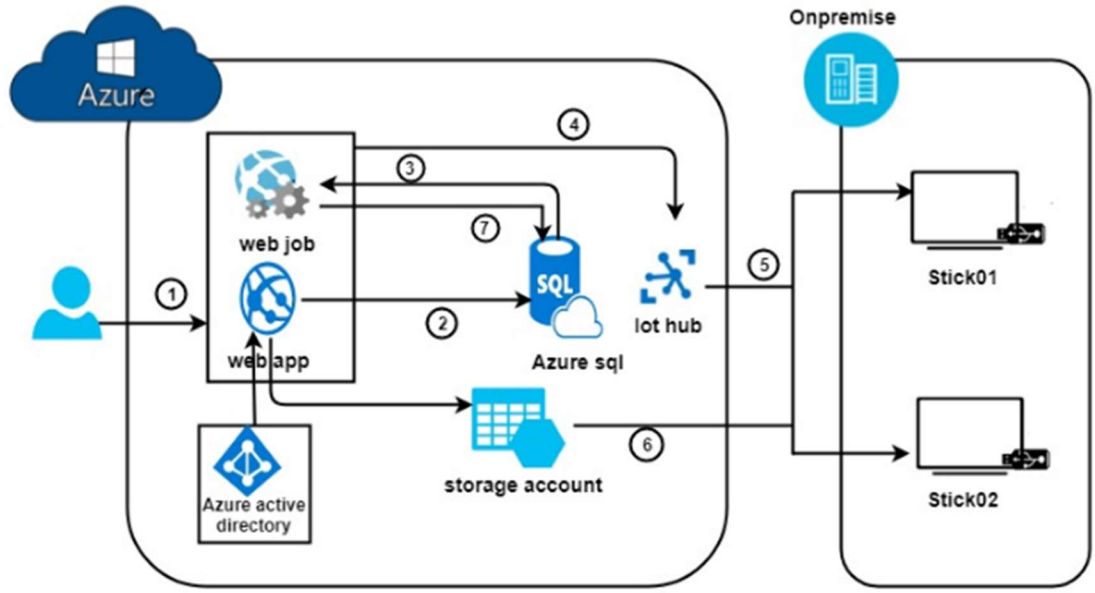
1. About Digital Signage

Digital Signage is a new way to create and display messaging campaigns to customers and employees throughout your organization, also called dynamic signage, you can remotely create, send and display messages to Televisions or other HDMI Capable Displays anywhere in your enterprise Wi-Fi network.

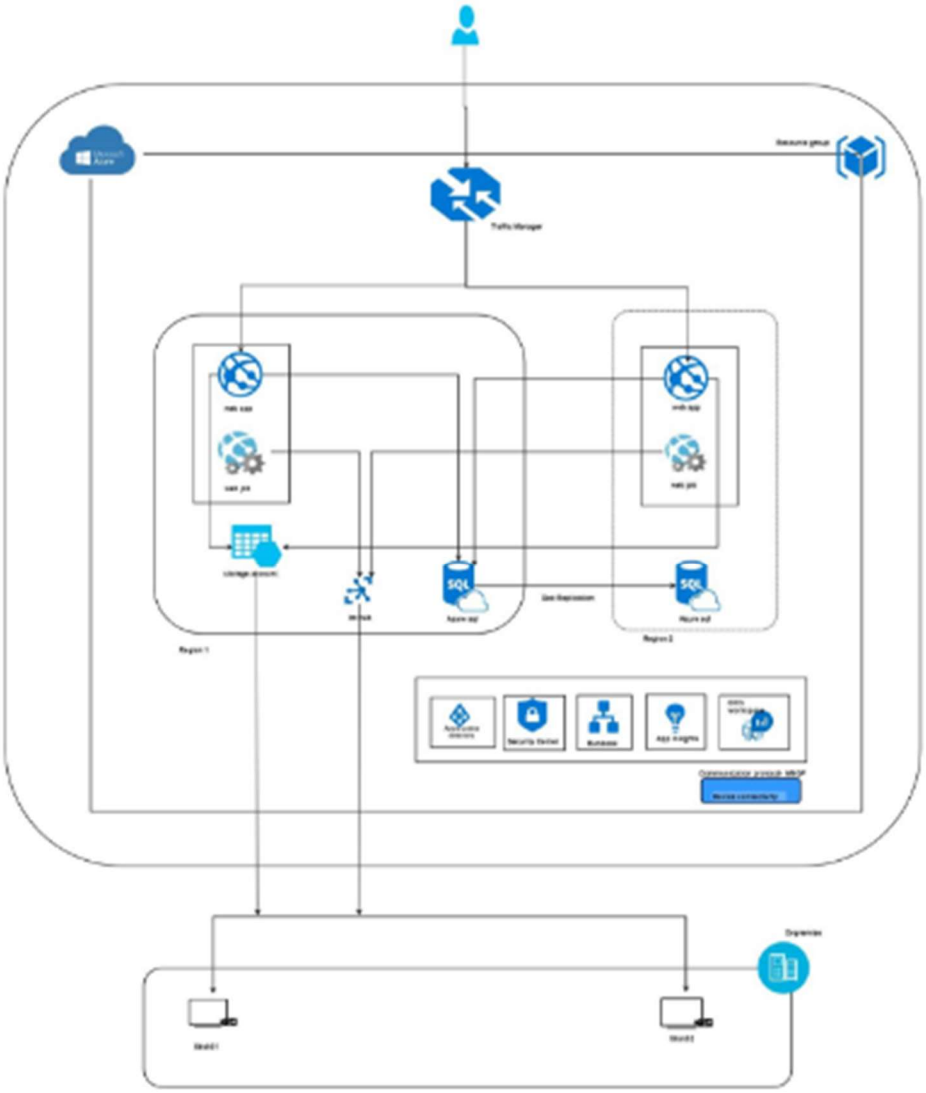
With digital signage, we can get as creative as your imagination allows, and the more innovative your ad, the more attention it's going to draw. Consider the following digital signage campaigns that have really went above and beyond to create a truly innovative customer experience.

2. Architecture Diagram

Architecture Diagram1



Architecture Diagram 2



3. Azure Services

The below described azure services are used for digital signage.

3.1. Azure blob

The word 'Blob' expands to **B**inary **L**arge **Ob**ject. Blobs include images, text files, videos and audios. There are three types of blobs in the service offered by Windows Azure namely block, append and page blobs.

- **Block blobs** are collection of individual blocks with unique block ID. The block blobs allow the users to upload large amount of data.
- **Append blobs** are optimized blocks that helps in making the operations efficient.
- **Page blobs** are compilation of pages. They allow random read and write operations. While creating a blob, if the type is not specified they are set to block type by default.

All the blobs must be inside a container in your storage.

3.2. Azure IoT HUB

Azure IoT HUB is a fully managed service that enables reliable and secure bidirectional communications between millions of IoT devices and a solution back end.

- Provides multiple device-to-cloud and cloud-to-device communication options. These options include one-way messaging, file transfer, and request-reply methods.
- Provides built-in declarative message routing to other Azure services.
- Provides a query able store for device metadata and synchronized state information.
- Enables secure communications and access control using per-device security keys.
- Provides extensive monitoring for device connectivity and device identity management events.
- Includes device libraries for the most popular languages and platforms.

3.3. Azure Web App

Azure Web Apps enables you to build and host web applications in the programming language of your choice without managing infrastructure. It offers auto-scaling and high availability, supports both Windows and Linux, and enables automated deployments from GitHub, Visual Studio Team Services.

3.4. Azure Web Job

Azure Web Job is back-end program you can run inside Azure, without Azure Web Job, you can deploy windows console app or windows service app to your server, then setup scheduler via windows scheduler or other third-party windows scheduler tools.

3.5. Azure SQL DB

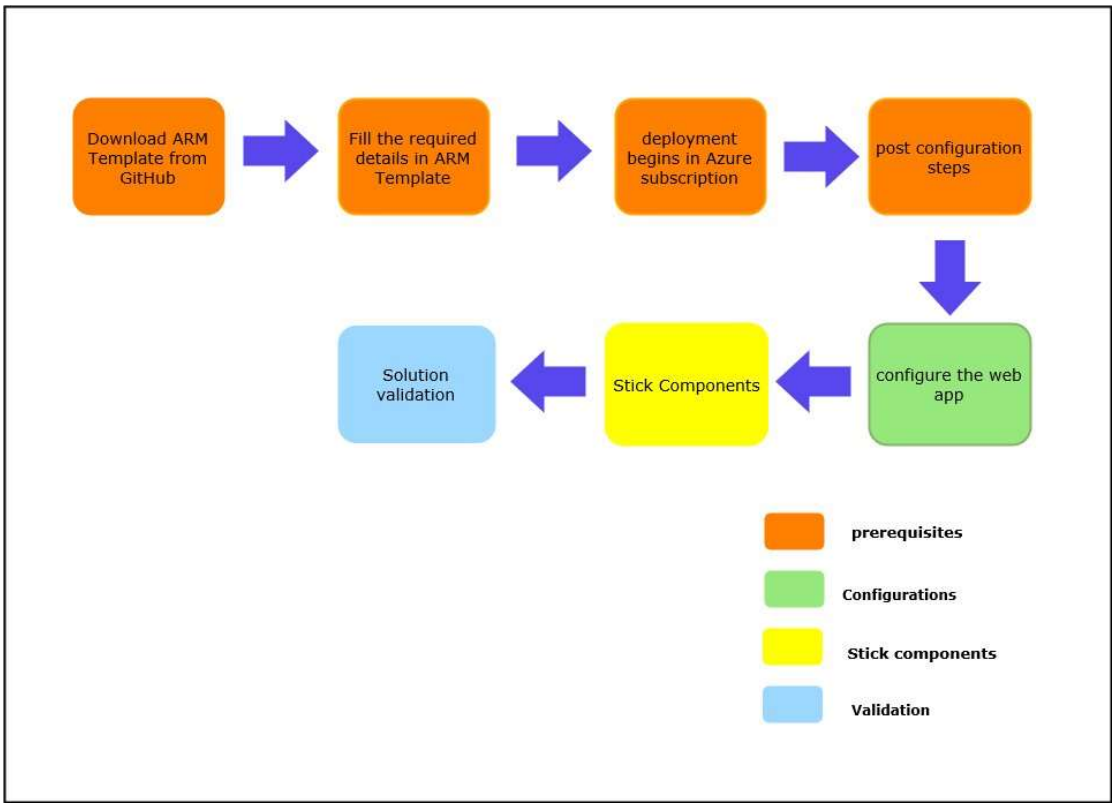
Azure SQL Database is a relational database-as-a service using the Microsoft SQL Server Engine. SQL Database is a high-performance, reliable, and secure database you can use to build data-driven applications and websites in the programming language of your choice, without needing to manage infrastructure.

4. Definitions

Term	Definition
Devices	Devices are HDMI IoT sticks that are plugged into devices, like monitors, projectors or televisions, located at Locations that display contents within a Pl.
Device Group	Device Group is a collection of Devices like group of displays in restaurant or mall.
Locations	A location is like a hotel or restaurant with one or more Devices that display contents within a playlist.
Contents	Contents are your messages, like billboards, that display on Devices located at Locations within a playlist
Playlist	A Playlist is a group of Locations, with one or more Devices at each Location, that display one or more contents on those devices.

5. High Level Deployment Process

Below figure depicts the high-level deployment process architecture.



5.1. ARM Template Definition

The Azure Resource Manager (ARM) is the service used to provision resources in your Azure subscription. It defines the set of resources (for example database server, database, and webapp) needed for a solution. ARM templates also specify deployment parameters that enable a user to configure settings for resources while requesting the resources.

6. Deployment Costs

Below table describes the deployment costs per month for the solution.

Deployment Costs for Type1

Region – US West

Resource Name	Size	Resource Costing model	Azure Cost/Month
Web Application	F1 (Free Tier), Shared Cores, 1 GB RAM, 1GB Storage	PAYG	$0.00
SQL Database	B1 (Standard tier), 5DTU, 2GB included storage per DB	PAYG	$4.90
IoT HUB	F1 (Free Tier), 500 devices, 8000 messages/day	PAYG	$0.00
Log Analytics (Optional)	Free Tier, Daily limit: 500MB Region East US	PAYG	$0.00
Application Insights (Optional)	Basic, 1GB * $2.30 Region: West US2	PAYG	$2.30
Storage Account	Block Blob Storage, General Purpose V1, LRS,100 GB Capacity	PAYG	$2.40
Total Cost			**$7.3**
Total Cost Including Optional Components			**$9.7**

Deployment Costs for Type2

Resource Name	Size	Resource Costing model	Azure Cost/Month
App Service Plan (2 Web Apps + 1 Web Job)	B1 (1 Core, 1.75 GB RAM, 10 GB Storage)	PAYG	$54.75
SQL Database	B1 (Standard tier), 5DTU, 2GB included storage per DB	PAYG	$4.90
IoT Hub	S1, Unlimited devices, 400,000 msgs/day,	PAYG	$50.00
Log Analytics (Optional)	Free Tier, Daily limit: 500MB Region East US	PAYG	$0.00
Application Insights (Optional)	Basic, 1GB * $2.30 Region: West US2	PAYG	$2.30
Storage Account	Block Blob Storage, General Purpose V1, LRS,100 GB Capacity	PAYG	$2.40
Total Cost			**$112.05**
Total Cost Including Optional Components			**$114.35**

Monitoring Status	Delta Price (Model1 ~ Model 2)
With Out Monitoring	104.75
With Monitoring	104.65

Deployment Costs for Type3

Resource Name	Size	Resource Costing model	Azure Cost/Month
App Service Plan (2 Web Apps + 1 Web Job)	B1 (1 Core, 1.75 GB RAM, 10 GB Storage)	PAYG	$54.75
SQL Database	S0 (Standard tier), 10DTU, 250GB Storage	PAYG	$14.72
IoT Hub	S1, Unlimited devices, 400,000 msgs/day,	PAYG	$50.00
Log Analytics (Optional)	Standalone, 1GB * $2.30 * 5 Region East US	PAYG	$11.50
Application Insights (Optional)	Basic, 1GB * $2.30*5 Region: West US2	PAYG	$11.50
Storage Account	Block Blob Storage, General Purpose V1, LRS Redundancy,100 GB Capacity	PAYG	$2.40
Total Cost			**$121.87**
Total Cost Including Optional Components			**$144.87**

Monitoring Status	Delta Price (Model1 ~ Model 3)	Delta Price (Model2 ~ Model 3)
With Out Monitoring	114.57	9.82
With Monitoring	135.17	30.52

Deployment Costs for Type4

Resource Name	Size	Resource Costing model	Azure Cost/Month	Comments
App Service Plan (2 Web Apps + 1 Web Job)	S1 * 2 (1 Core, 1.75 GB RAM, 50 GB Storage)	PAYG	$146.00	One App Service plan in 1 region and another in DR Region
SQL Database	S0 (Standard tier), 10DTU, 250GB Storage	PAYG	$29.44	One SQL Database in 1 region and another in DR Region. Active geo-replication creates up to four online (readable) secondaries in any Azure region. Secondary active geo-replication databases are priced at 100% of primary database prices. The cost of geo-replication traffic between the primary and the online secondary is included in the cost of the online secondary. Active geo-replication is available for all database tiers.
IoT Hub	S1, Unlimited devices, 400,000 msgs/day,	PAYG	$50.00	
Log Analytics (Optional)	Standalone, 1GB * $2.30 * 5 Region East US	PAYG	$11.50	
Application Insights (Optional)	Basic, 1GB * $2.30*5 Region: West US2	PAYG	$11.50	

Resource Name	Size	Resource Costing model	Azure Cost/Month	Comments
Storage Account	Block Blob Storage, General Purpose V1, LRS Redundancy,100 GB Capacity	PAYG	$2.40	
Traffic Manager	N/A * 2	PAYG	$1.44	Required 2 traffic Managers, 1 for Content Manager Web App With 2 End Points and Another for nodeserverapp with 2 End points
Total Cost			**$240.78**	
Total Cost Including Optional Components			**$252.28**	

Monitoring Status	Delta Price (Model1 ~ Model 4)	Delta Price (Model2 ~ Model 4)	Delta Price (Model3 ~ Model 4)
With Out Monitoring	233.48	128.73	118.91
With Monitoring	242.58	137.93	107.41

Deployment Costs for Type5

Resource Name	Size	Resource Costing model	Azure Cost/Month	Comments
App Service Plan (2 Web Apps + 1 Web Job)	S1 * 2 (1 Core, 1.75 GB RAM, 50 GB Storage)	PAYG	$146.00	One App Service plan in 1 region and another in DR Region

SQL Database	S0 (Standard tier), 10DTU, 250GB Storage	PAYG	$14.72	One SQL Database in 1 region and another in DR Region. Active geo-replication creates up to four online (readable) secondary's in any Azure region. Secondary active geo-replication databases are priced at 100% of primary database prices. The cost of geo-replication traffic between the primary and the online secondary is included in the cost of the online secondary. Active geo-replication is available for all database tiers.
IoT Hub	S1, Unlimited devices, 400,000 msgs/day,	PAYG	$50.00	
Log Analytics (Optional)	Standalone, 1GB * $2.30 * 5 Region East US	PAYG	$11.50	
Application Insights (Optional)	Basic, 1GB * $2.30*5 Region: West US2	PAYG	$11.50	
Storage Account	Block Blob Storage, General Purpose V1, LRS Redundancy,100 GB Capacity	PAYG	$2.40	
Traffic Manager	N/A (endpoints * 0.36)	PAYG	$1.44	Required 2 traffic Managers, 1 for Content Manager Web App With 2 End Points and Another for node server app with 2 End points

Azure Security Centre		PAYG	$30.00	
Total Cost			**$256.06**	
Total Cost Including Optional Components			**$267.56**	

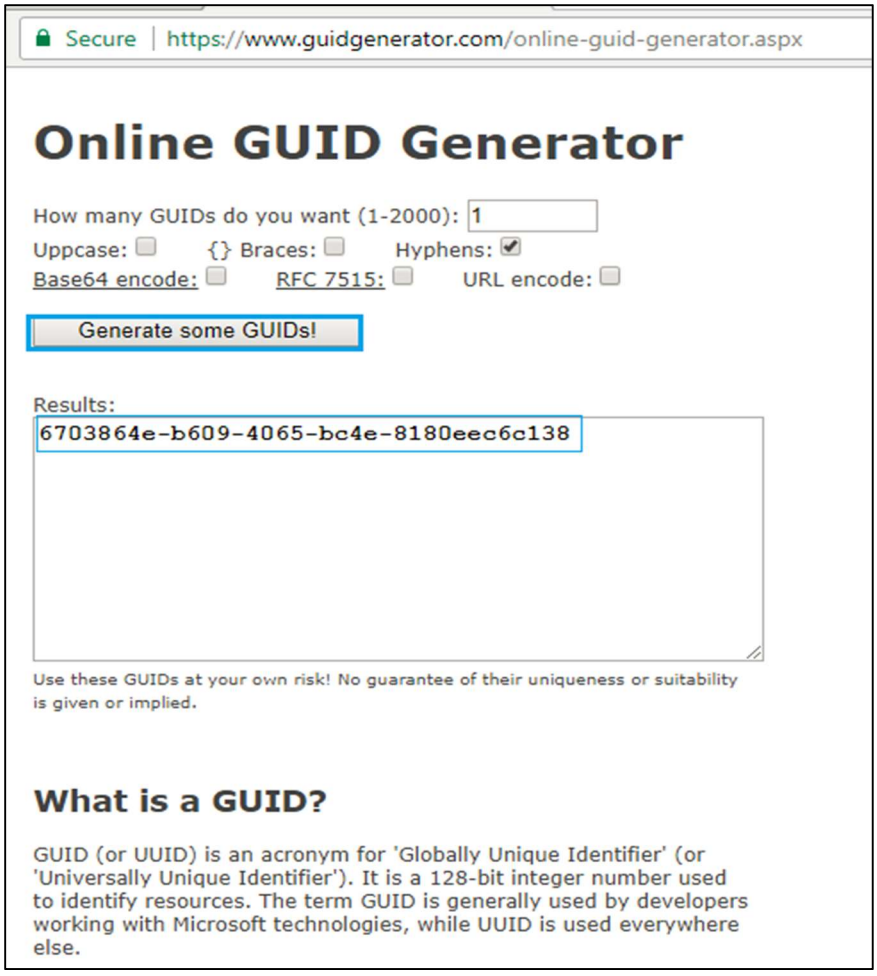
Monitoring Status	Delta Price (Model1 ~ Model 5)	Delta Price (Model2 ~ Model 5)	Delta Price (Model3 ~ Model 5)	Delta Price (Model4 ~ Model 5)
With Out Monitoring	263.48	158.73	148.91	30
With Monitoring	272.58	167.93	137.41	30

7. Pre-requisites

1. GUID Generator
2. Stick devices (physical)

7.1. GUID Generator

The Azure runbook automate job needs a unique GUID as the job ID. We need to generate this GUID as a pre-requisite, please follow the steps to generate the Session Id or Job id, click the link https://www.guidgenerator.com, to open **Online GUID Generator** web page in a browser as shown below:



Click **Generate some GUIDs!** button, the results are displayed in the **Results** box as shown in the above figure.

Copy or note down the GUID value, which will be used during the ARM template deployment.

8. ARM Template Input Parameters

Below is the list of Input parameters, that are to be provided as inputs to the ARM Template.

Parameter name	Description	Allowed values	Default values
sqlAdministratorLogin	provide the user name for the sql server, please make a note of Username this will be used further	Any string	Sqluser
Solution Type	1.solution with monitoring - this will deploy core	solution with monitoring,	

Parameter name	Description	Allowed values	Default values
	digital signage solution & monitoring components. 2. solution without monitoring - this will deploy core digital signage solution	solution without monitoring	
sqlAdministratorLoginPassword	provide the password for the sql server, make a note of the Password this will be used further	Password must be 12 characters and have 3 of the following 1 lower case character, 1 number, and 1 special character	
SessionId	provide the guid prefix for the runbook job to be created		
Costing Model	Costing models have predefined resources sizes. Please refer Costing Model tables	One, Two, Three, Four	
Capacity units	number of desired iot hub units. restricted to 1 unit for F1. Can be set up to maximum number allowed for subscription.	minValue: 1	1
D2c message retention in days period	specify the iot hub messages retention period in days, for device-to-cloud messages	minValue: 1 maxValue: 7	1
D2c partition count	specify the number of desired partitions for device-to-cloud event ingestion. Restricted to 1 unit for F1	1,2, 3, ….. 32	2

Parameter name	Description	Allowed values	Default values
Storage Blob Url	specify the blob url where all your code is present		https://projectiot.blob.core.windows.net/rms-iot/
Sku capacity	describes plan's instance count	1	1
Content Manager AppName	specify the website name for content manager web app	Any String	
Data Retention	specify the oms retention period in days, if you have selected solution type as without monitoring this is optional	minValue: 7, maxValue: 730,	7
App Insights Location	specify the region for application insights, if you have selected solution type as without monitoring this is optional	eastus, northeurope, southcentralus, southeastasia, westeurope, westus2	
Traffic Routing Method	specify the traffic routing method for traffic manager	Performance, Weighted, Geographic Priority	Priority
oms Workspace Region	specify the region for oms workspace, if you have selected solution type as without monitoring this is optional	eastus, westeurope, southeastasia, australiasoutheast	Eastus
d2cPartitionCount	specify the number of desired partitions for device-to-cloud event ingestion. Restricted to 1 unit for F1	2,3,4,5,6,7,8,9,10,11,12,13 14,15,16,17,18,19 20, 21, 22, 23, 24,25, 26,27, 28, 29, 30,31, 32	2

Parameter name	Description	Allowed values	Default values
oms Automation Region	specify the region for oms automation account, if you have selected solution type as without monitoring this is optional	westeurope, southeastasia, eastus2, southcentralus, japaneast, southeastasia, southcentralus, northeurope, canadacentral, australiasoutheast, centralindia, japaneast	eastus2
locationDr	if you select costing model as Four specify the region for web apps and azure sql server disaster recovery it should be different of resource group region otherwise it is optional	Any String	

9. Getting Started

9.1. Setting Azure AD Directory and App registration.

Note:

If either costing model 1, costing model 2 or costing model 3 is the requirement, create an application in active Directory. The Application Name should be Unique.

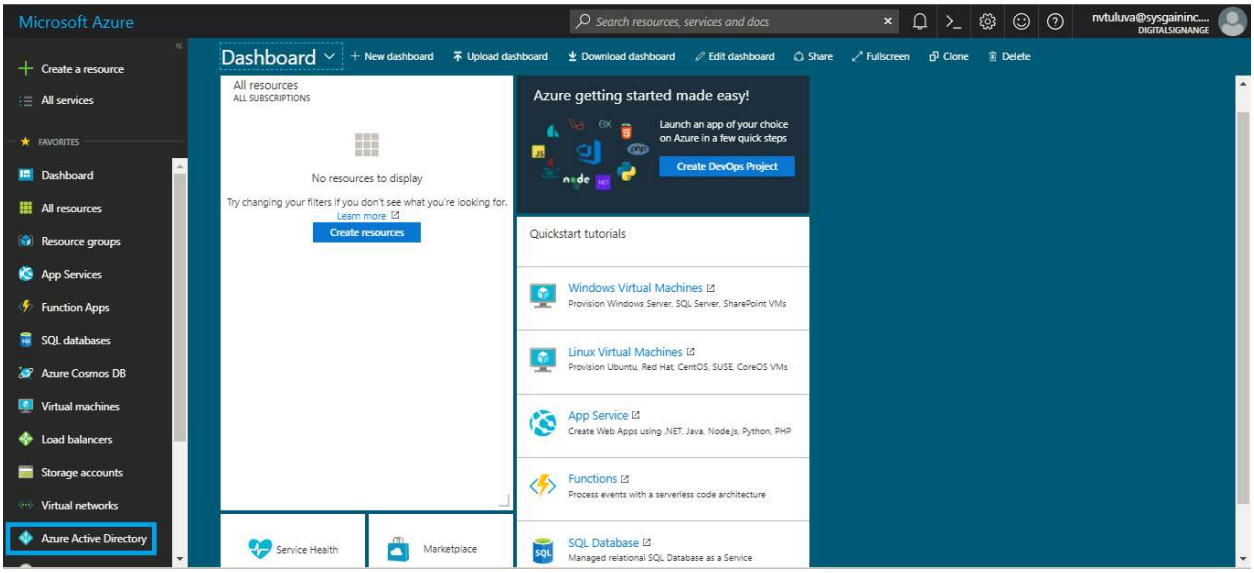
If costing model 4 is the requirement, create two applications with Unique names like contentmanagercostfour and recoverycontentmanagercostfour and Go to properties section and make sure that the values for Home Page ,Logout, Terms of service and Privacy Url are the trafficmanager URL's example, https://contentmanagercostfour.trafficmanager.net/ and click on save button.

Also Go to settings > Reply URLs provide URL https://contentmanagercosfour.trafficmanager.net/ and click on save

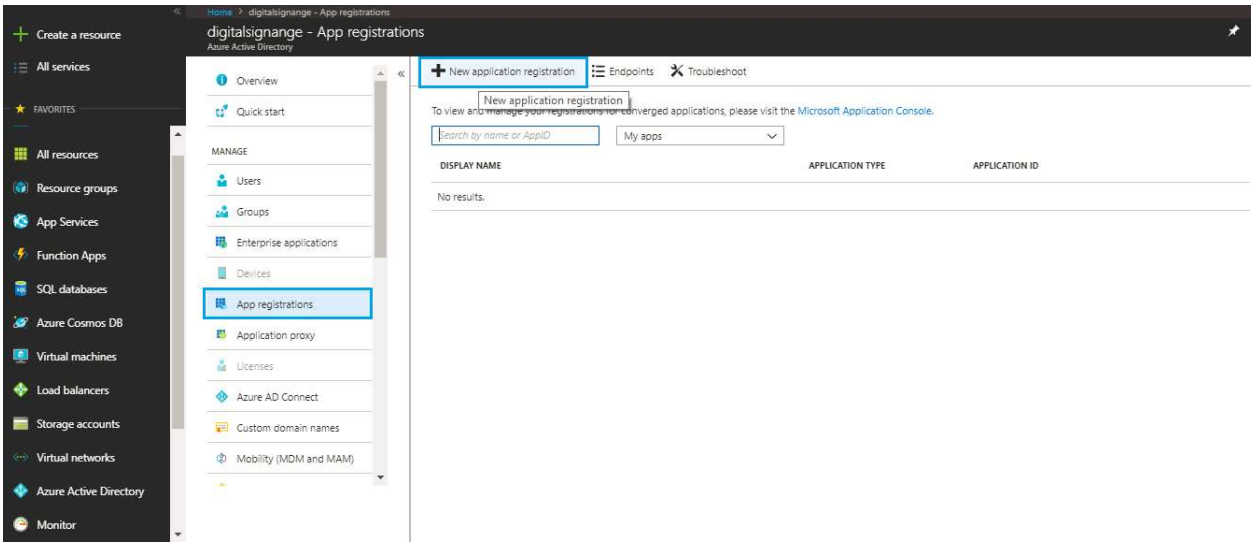
In Costingmodel4 It is important to note that for both the Applications, in the properties sections all the above mentioned URL's should be Trafficmanager URL's

Step 1- To register a new application using the Azure portal

1. Sign in to the Azure portal.
2. If your account gives you access to more than one, click your account in the top right corner, and set your portal session to the desired Azure AD tenant.
3. In the left-hand navigation pane, click the **Azure Active Directory** service



4. click **App registrations**, and click **New application registration**.

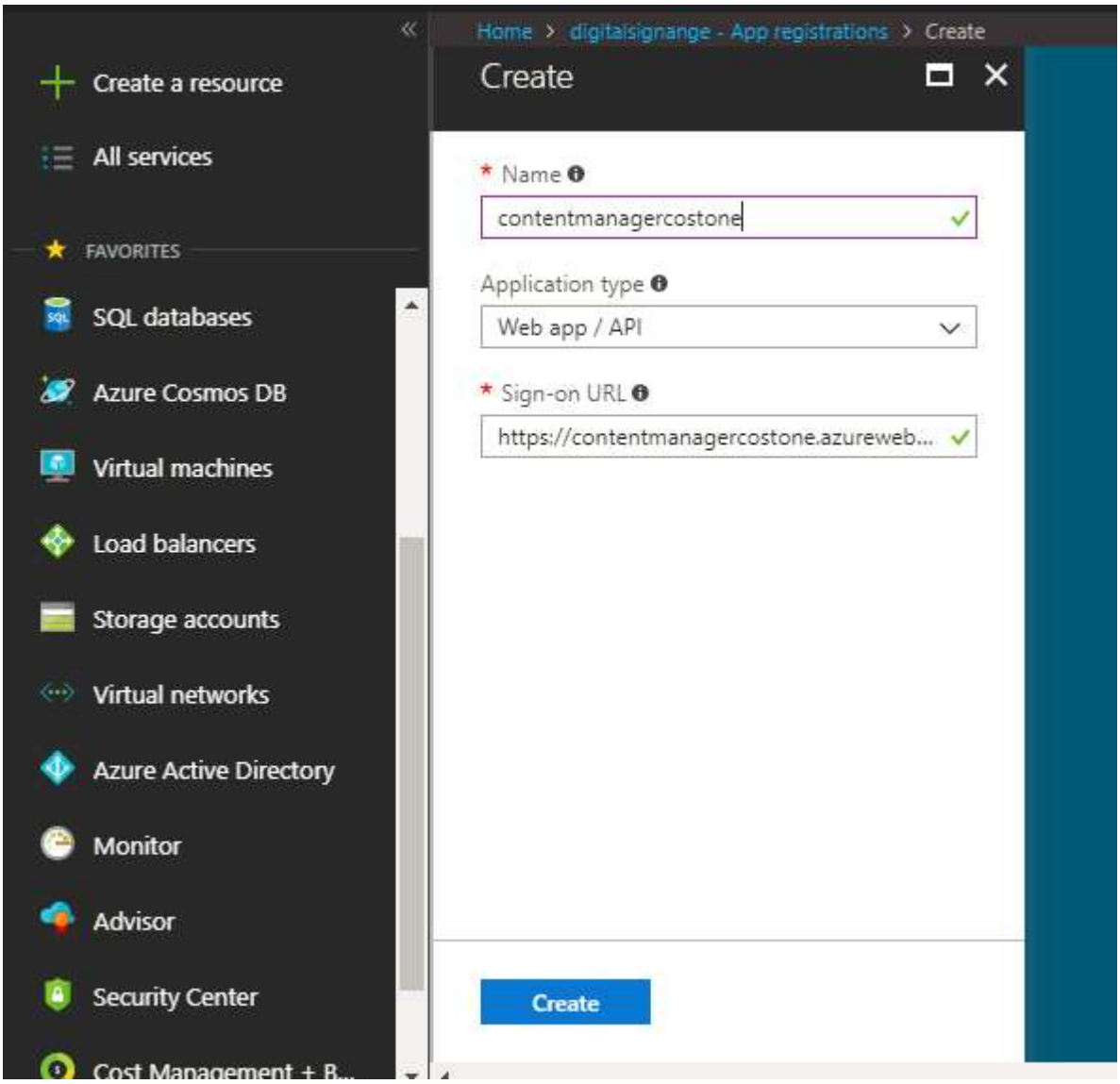


5. In the **Create** page, enter your application's registration information:

   - **Name:** Enter a meaningful application name
   - **Application type:**
     - Select "Web app / API" for client applications and resource/API applications that are installed on a secure server. This setting is used for OAuth confidential web clients and public user-agent-based clients. The same application can also expose both a client and resource/API.
   - **Sign-On URL:** For "Web app / API" applications, provide the base URL of your app. For example, https://contentmanagercostone.azurewebsites.net/ might be the URL for a web

app running on your local machine. Users would use this URL to sign in to a web client application.

- **Redirect URI:** For "Native" applications, provide the URI used by Azure AD to return token responses. Enter a value specific to your application, for example https://contentmanagercostone.azurewebsites.net/
- **Setting Url in Properties –** Enter values for Home Page, Logout, Terms of service and Privacy Url. example, http://localhost:31544 might be the URL for a web app running on your local and for deployed application it will be, for example http://MyFirstAADApp



Name: contentmanagercostone

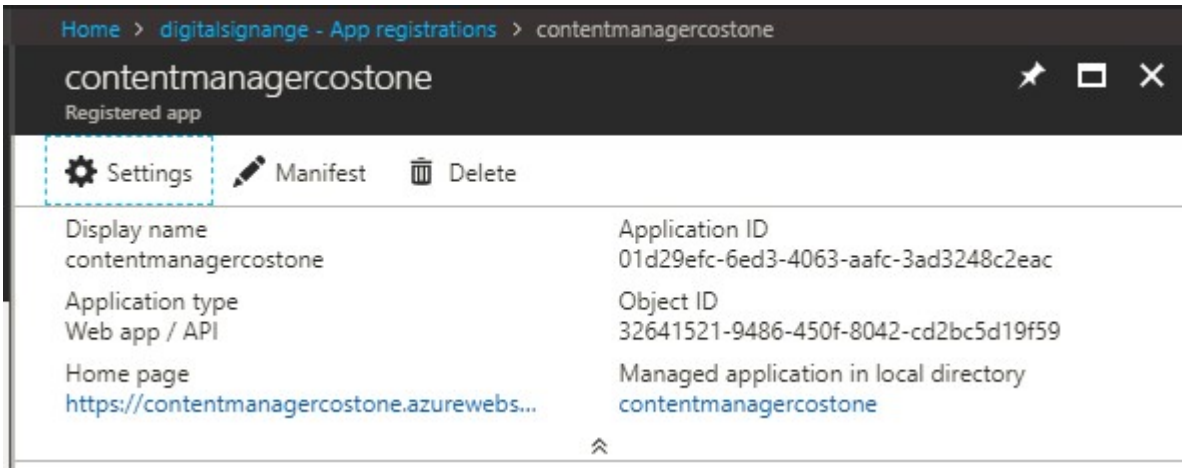
Application type: Web app / API

Sign-on URL: https://contentmanagercostone.azurewebsites.net/

Provide the above details & click **Create**. The following page is displayed.

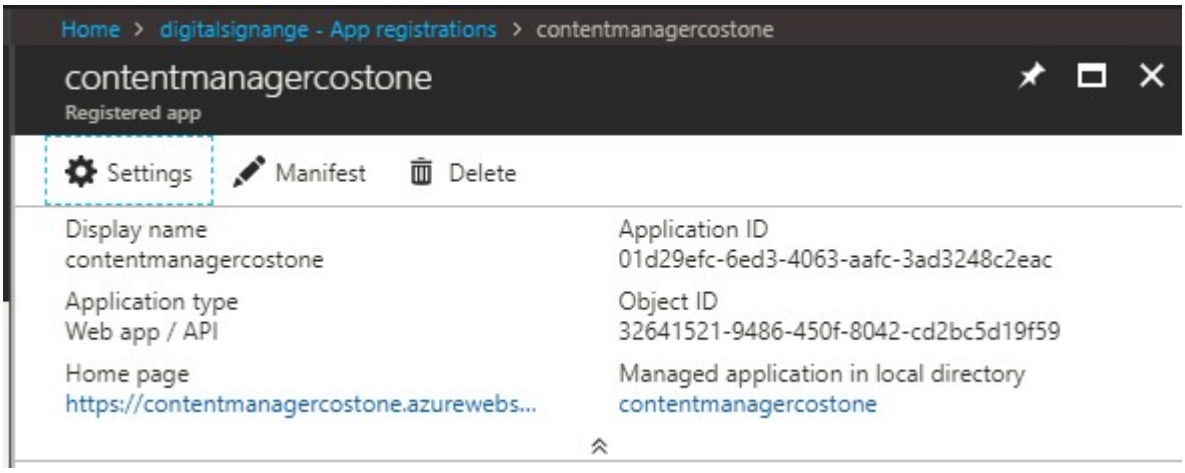
For **Costing Model 4**, the URL should be like

https://contentmanagercostfour.trafficmanager.net



Note down the **Display name**, **Application ID** and **Home page URL** which will be used as input parameters in the ARM template deployment in the next steps.

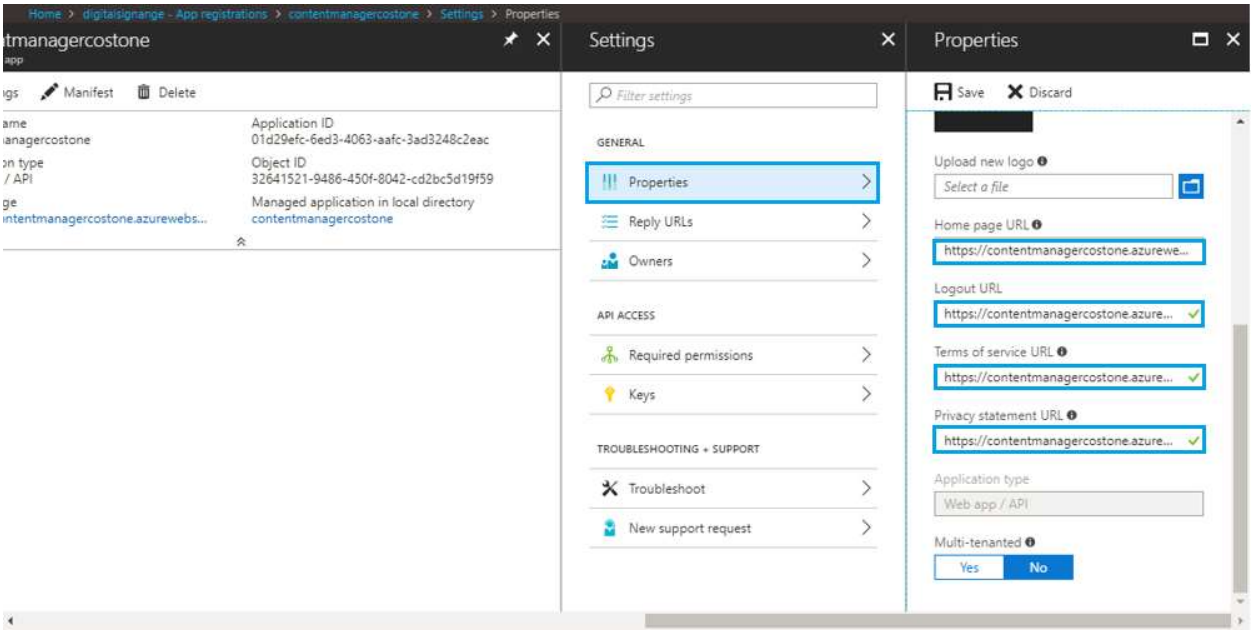
6. Click **Settings** as shown in the following figure.



7. Go to **Properties** section and Enter values in **Home Page URL**, Logout **URL**, **Terms of service URL** and **Privacy Statement Url** fields respectively. For example, https://contentmanagercostone.azurewebsites.net/ and click **Save**.

For **Costing Model 4**, the URL should be like

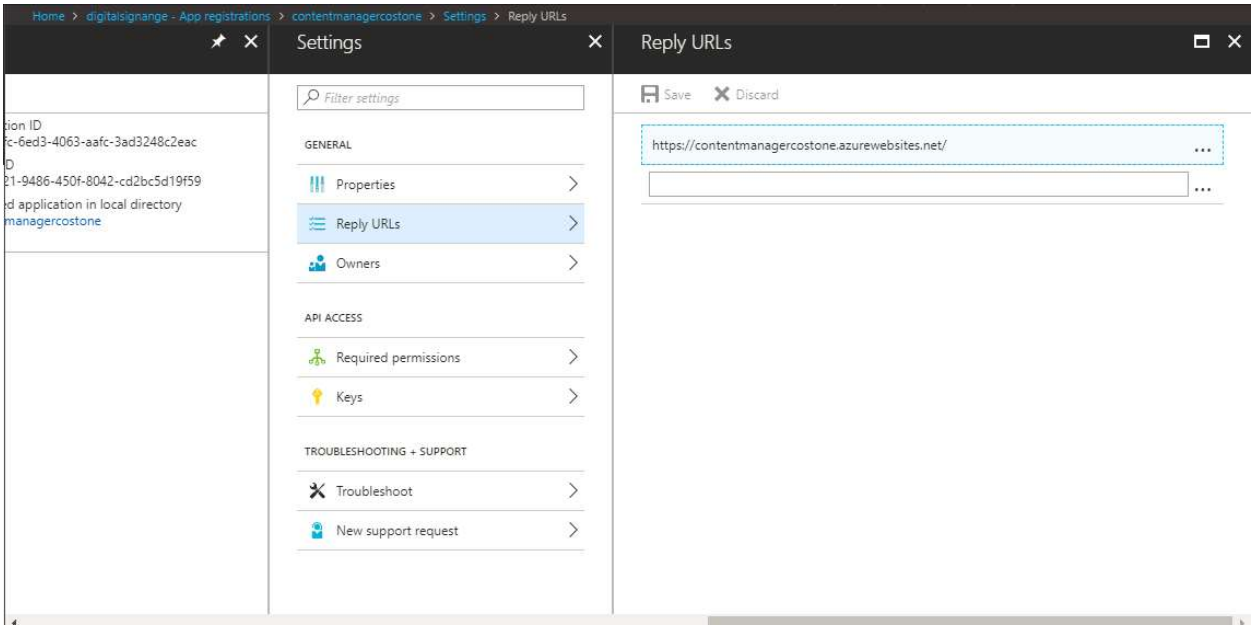
https://contentmanagercostfour.trafficmanager.net



8. Go to **Settings** > **Reply URLs** and provide URL https://contentmanagercostone.azurewebsites.net and click **Save**.

For **Costing Model 4**, the URL should be like

https://contentmanagercostfour.trafficmanager.net



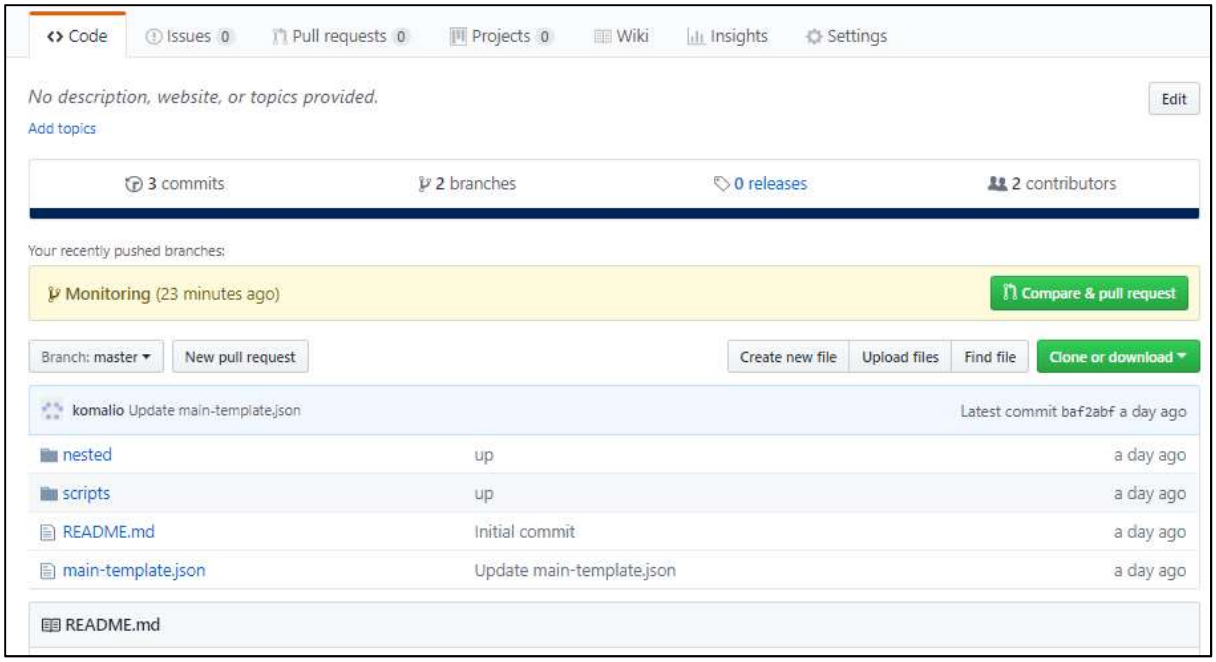
Now you have successfully created **contentmanagercostone** application in your tenant. Note down the **Application ID**, **App Display Name** and **URL**.

Note: For costing model1, costing model2 and costing model3 create only one application.

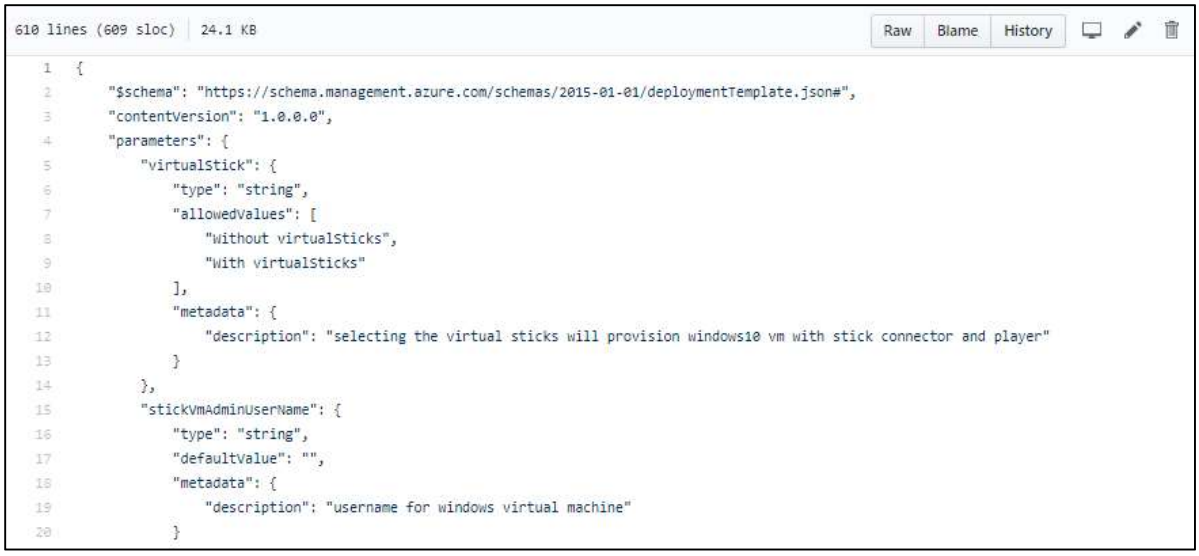
But for costing model 4 create two applications like contentmanagercostfour and recoverycontentmanagercostfour need to be created.

9.2. ARM template deployment

1. Login to git hub, navigate to your Digital Signage project repo, Select **main-template. json**



2. Select **Raw** from the top right corner.



3. Copy the raw template and paste in your azure portal for template deployment.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "virtualStick": {
            "type": "string",
            "allowedValues": [
                "Without virtualSticks",
                "With virtualSticks"
            ],
            "metadata": {
                "description": "selecting the virtual sticks will provision windows10 vm with stick connector and player"
            }
        },
        "stickVmAdminUserName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "username for windows virtual machine"
            }
        },
        "stickVmAdminPassword": {
            "type": "securestring",
            "defaultValue": "",
            "metadata": {
                "description": "password for windows virtual machine"
            }
        },
        "sqlAdministratorLogin": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The SQL authentication admin user of the SQL Server, make a note of Username this will be used further"
            }
        },
        "sqlAdministratorLoginPassword": {
            "type": "securestring",
            "defaultValue": "",
```

9.3. Deployment Scenario

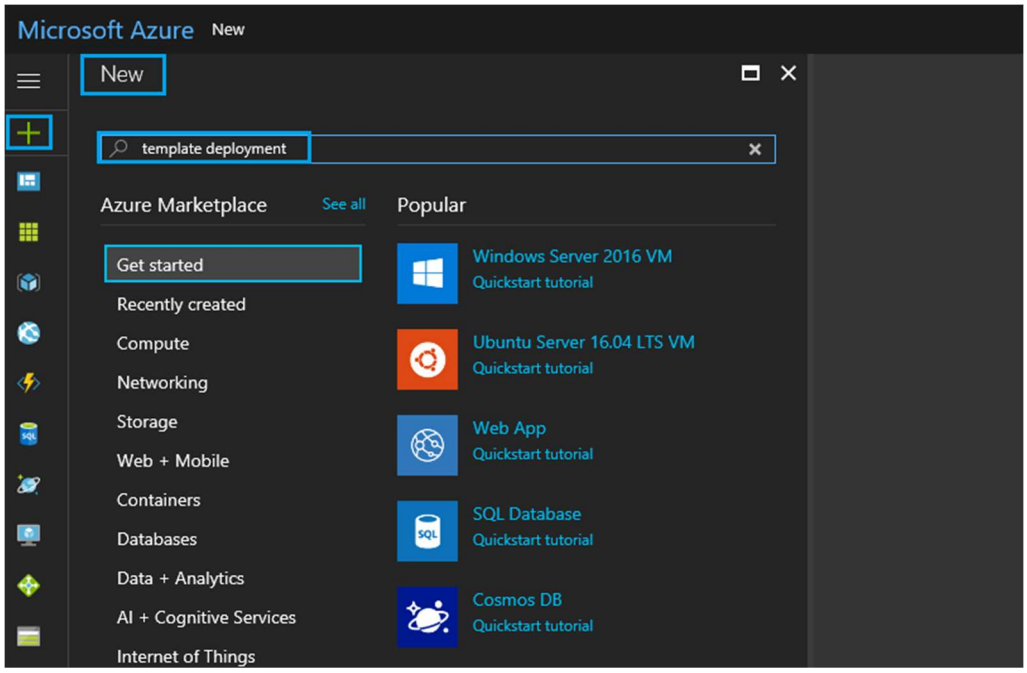
The following sections describes the various scenarios of deployment.

9.3.1. Deploy ARM Templates using Azure portal

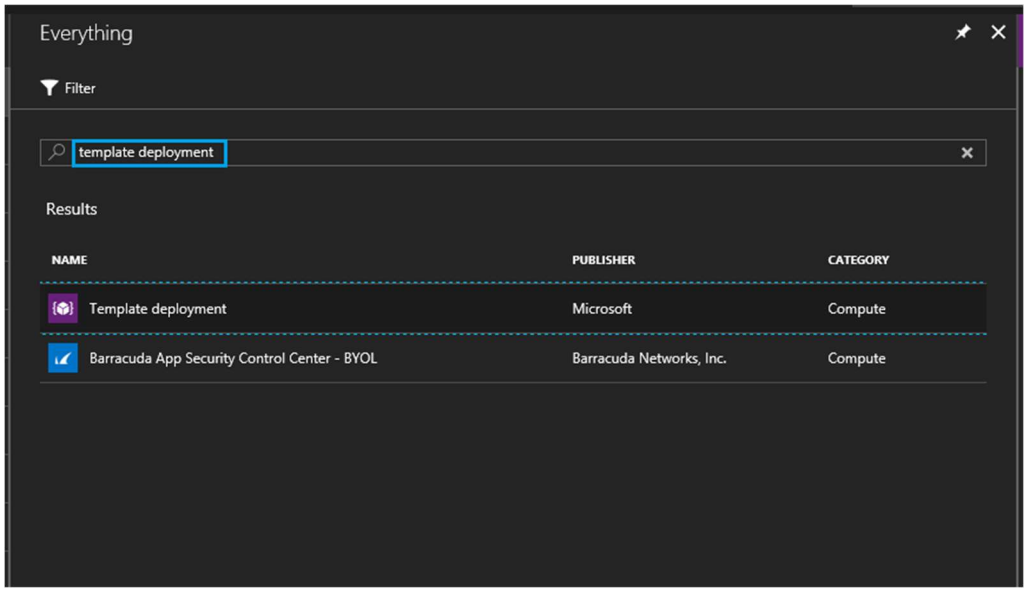
The Resource Manager template you deploy can either be a local file on your machine, or an external file that is in a repository like GitHub.

To deploy a template for Azure Resource Manager, follow the below steps.

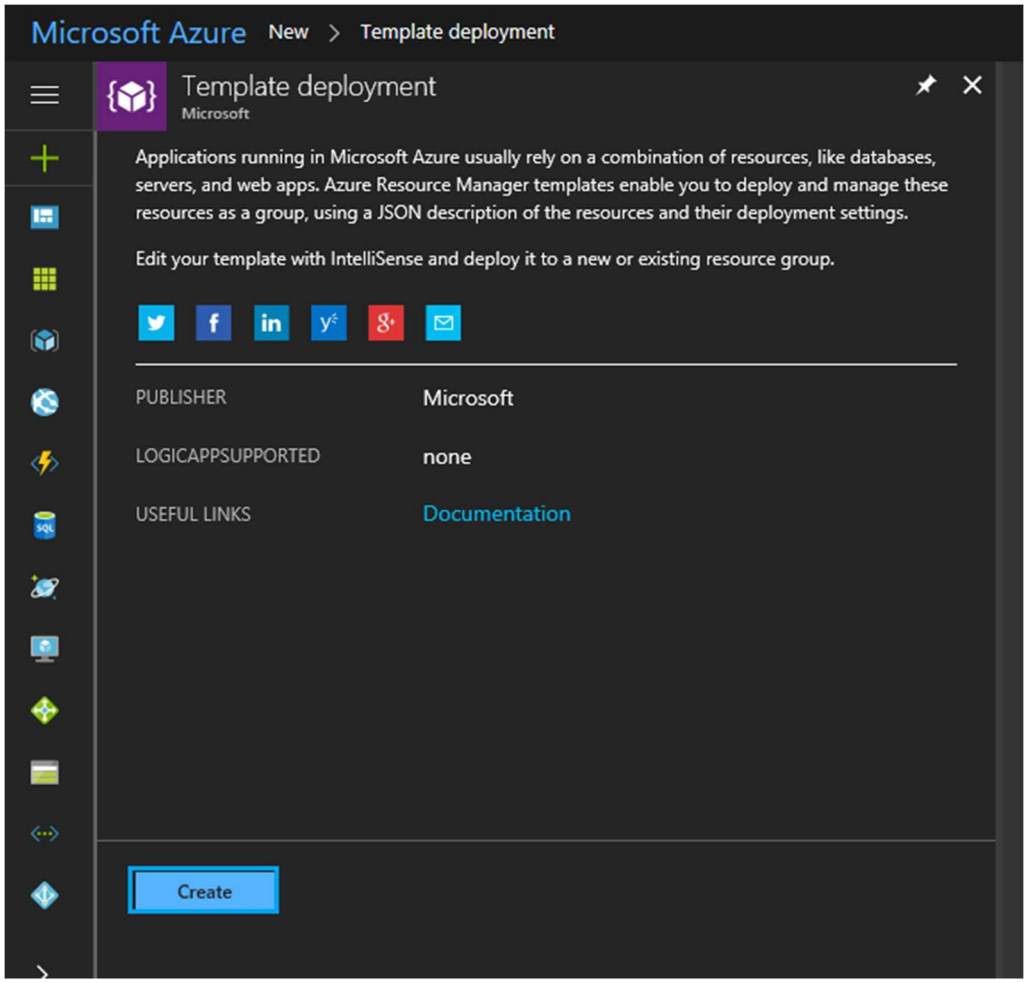
1. Open **Azure portal**, Navigate to **New (+)**, search for the key word **Template deployment**.



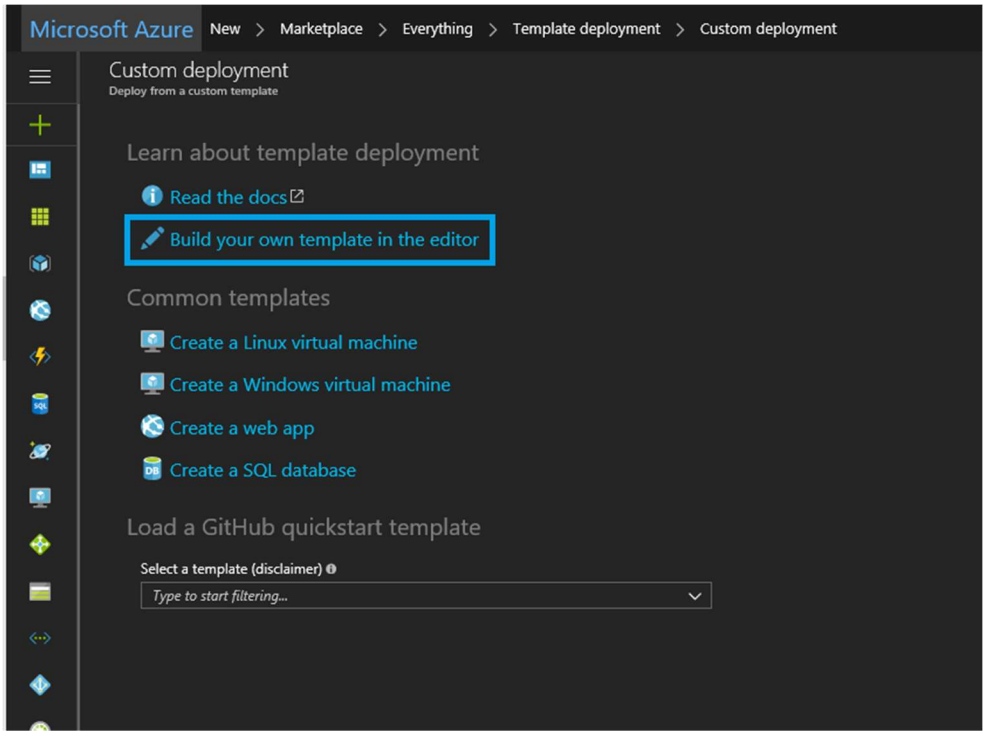
2. The search results are displayed as shown in the following figure, Select **Template deployment.**



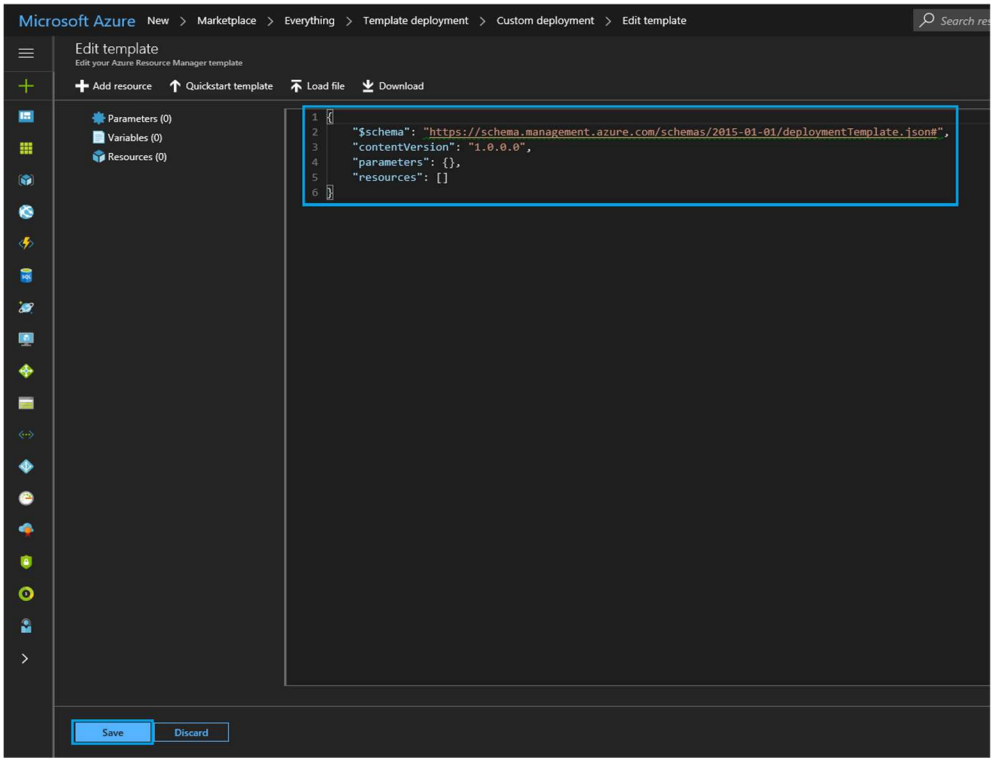
3. Click **Create** button as shown in the following figure.



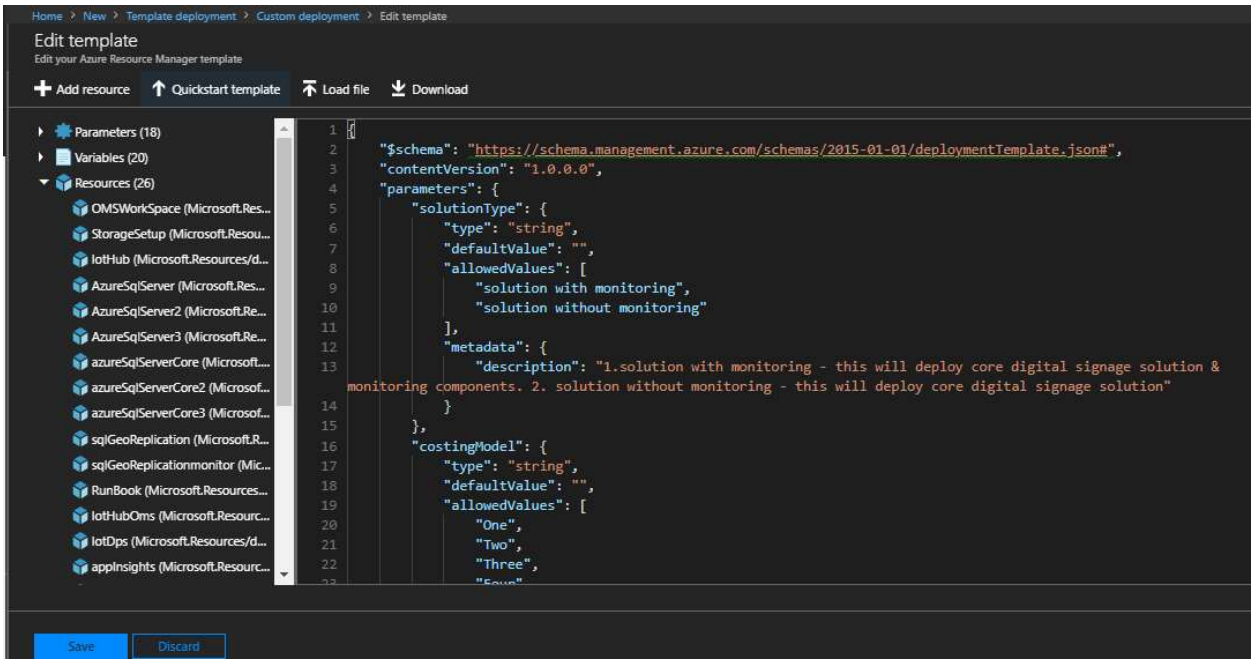
4. Click **Build your own Template in the editor** link as shown in the following figure.



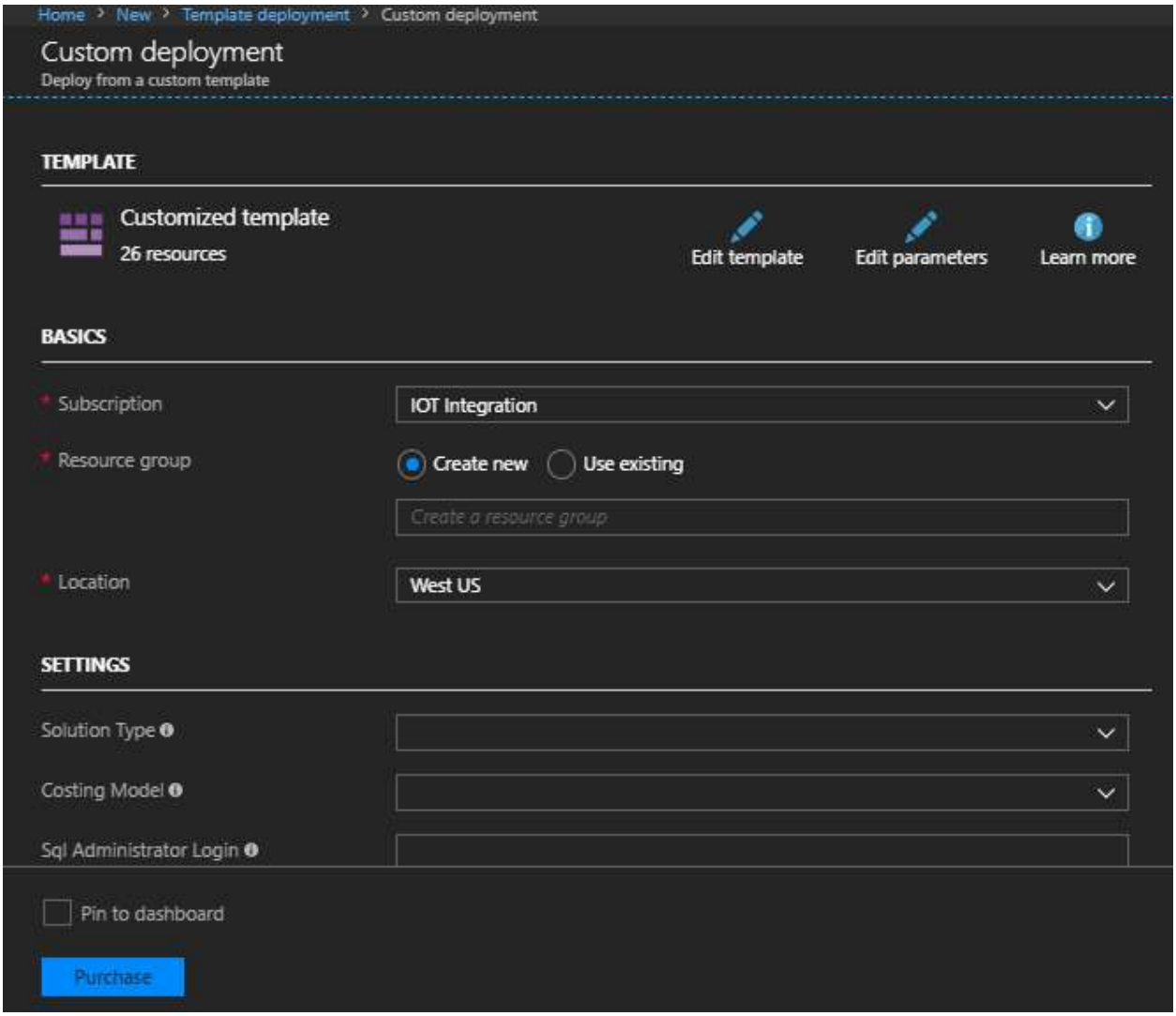
5. The **Edit template** page is displayed as shown in the following figure.

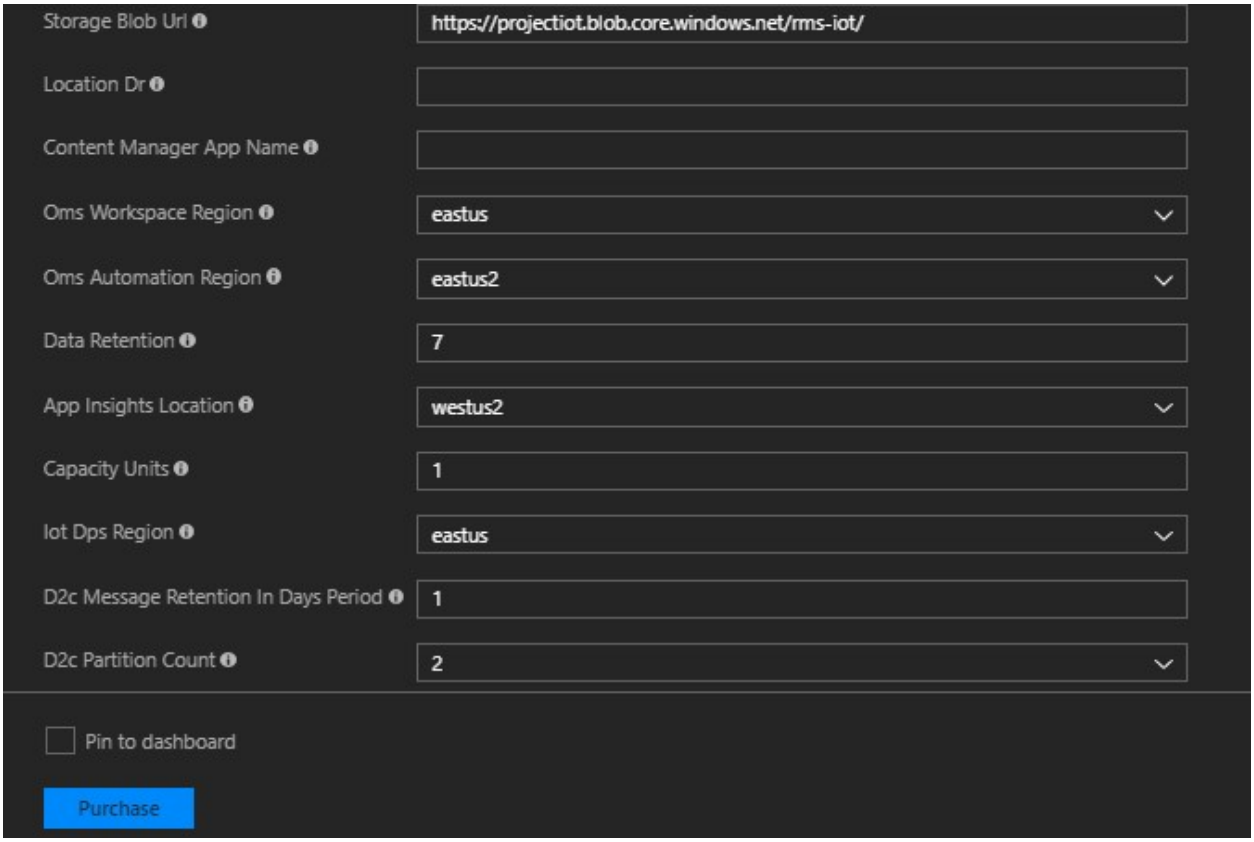


6. Replace / paste the template and click **Save** button.

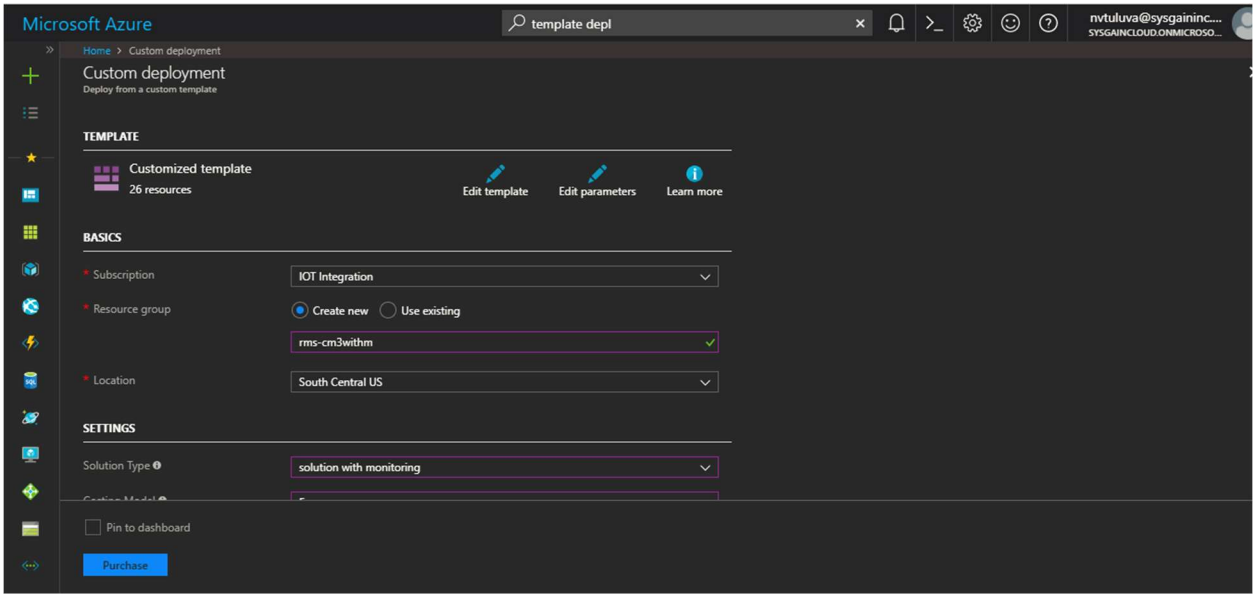


7. The **Custom deployment** page is displayed as shown in the following figure.

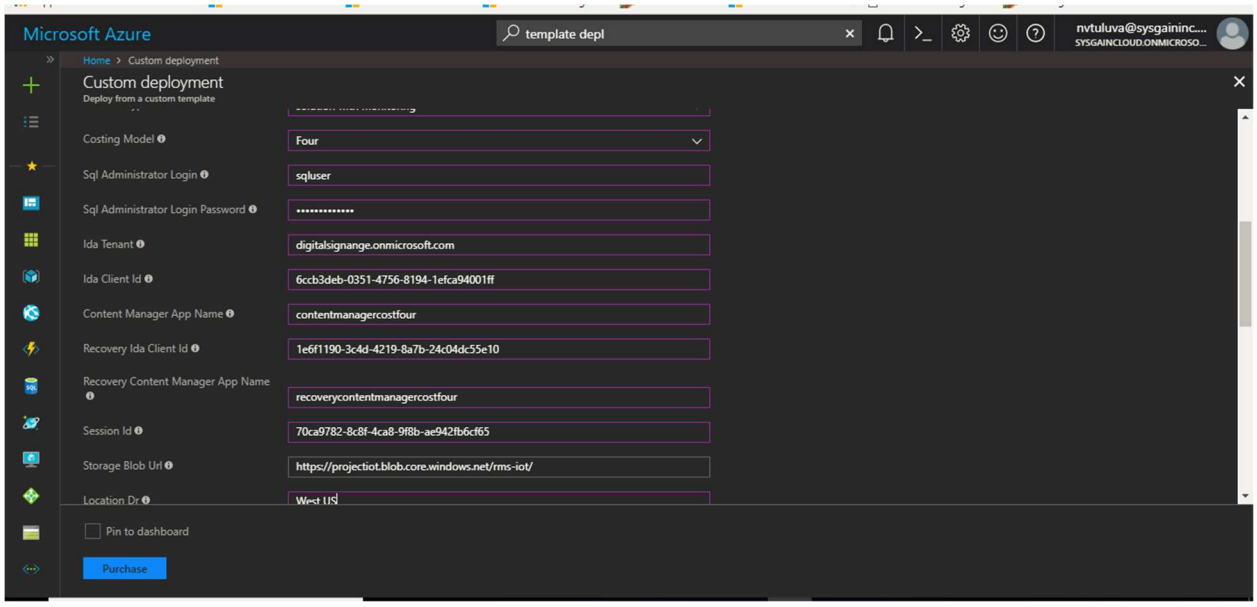

Home > New > Template deployment > Custom deployment
Custom deployment
Deploy from a custom template
TEMPLATE
Customized template
26 resources
Edit template
Edit parameters
Learn more
BASICS
* Subscription
IOT Integration
* Resource group
Create new
Use existing
Create a resource group
* Location
West US
SETTINGS
Solution Type
Costing Model
Sql Administrator Login
Pin to dashboard
Purchase

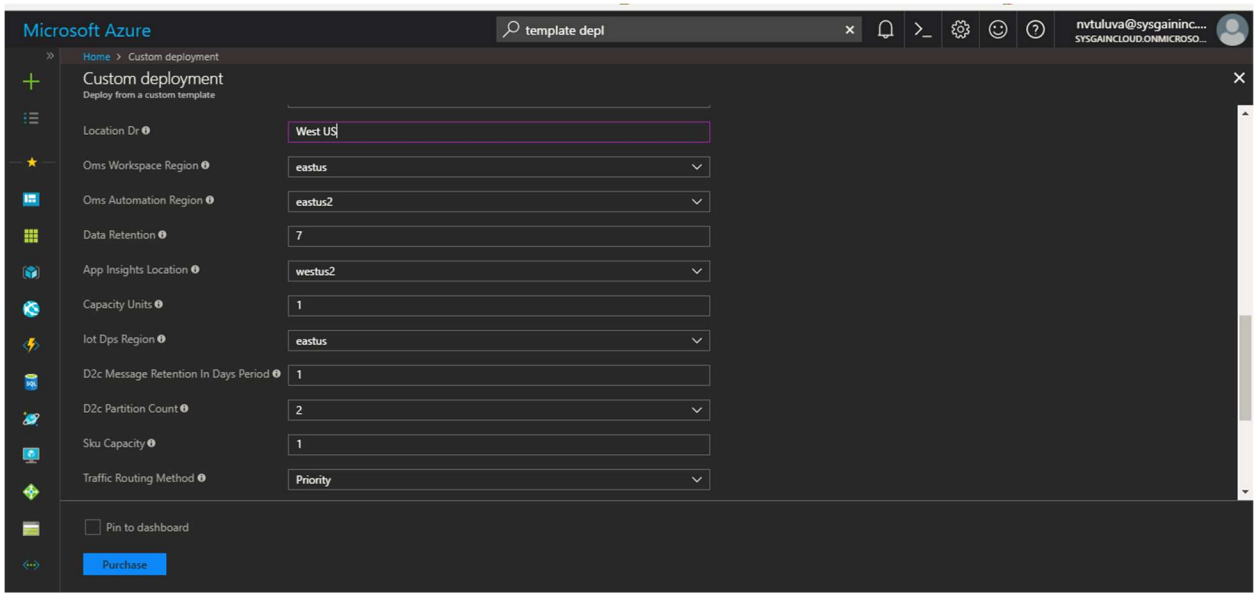


8. From **Azure Portal**, deploy the template by providing the parameters in custom deployment settings as shown in the following figure.

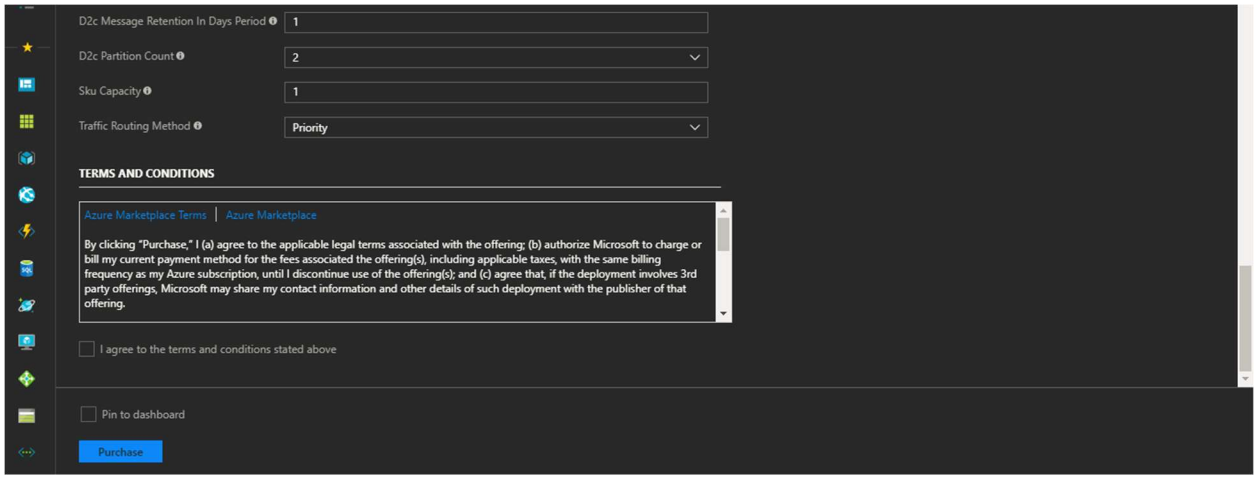


9. Paste the noted / copied **session id** field in **Settings** section of the **Custom deployment** page as shown in following figure. Also fill the **tenant** and **Client** details of your registered app as shown in the figure below





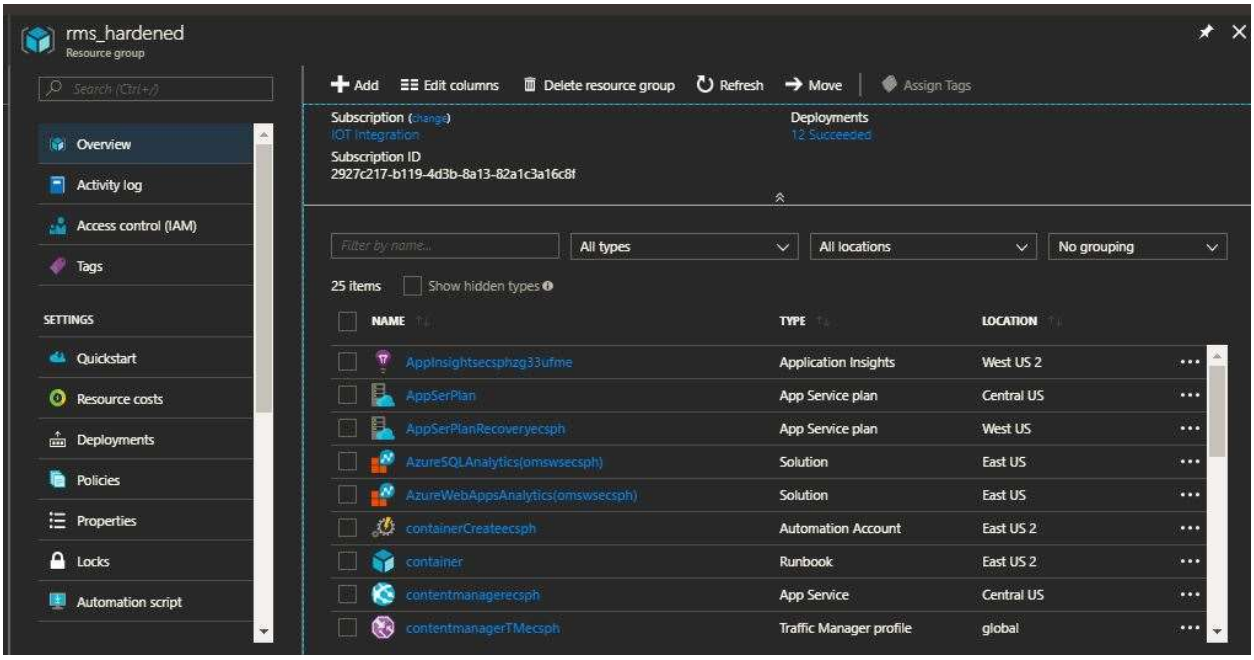
10. Once all the details are entered, select the **I agree to the terms and conditions** check box and click the **Purchase** button.

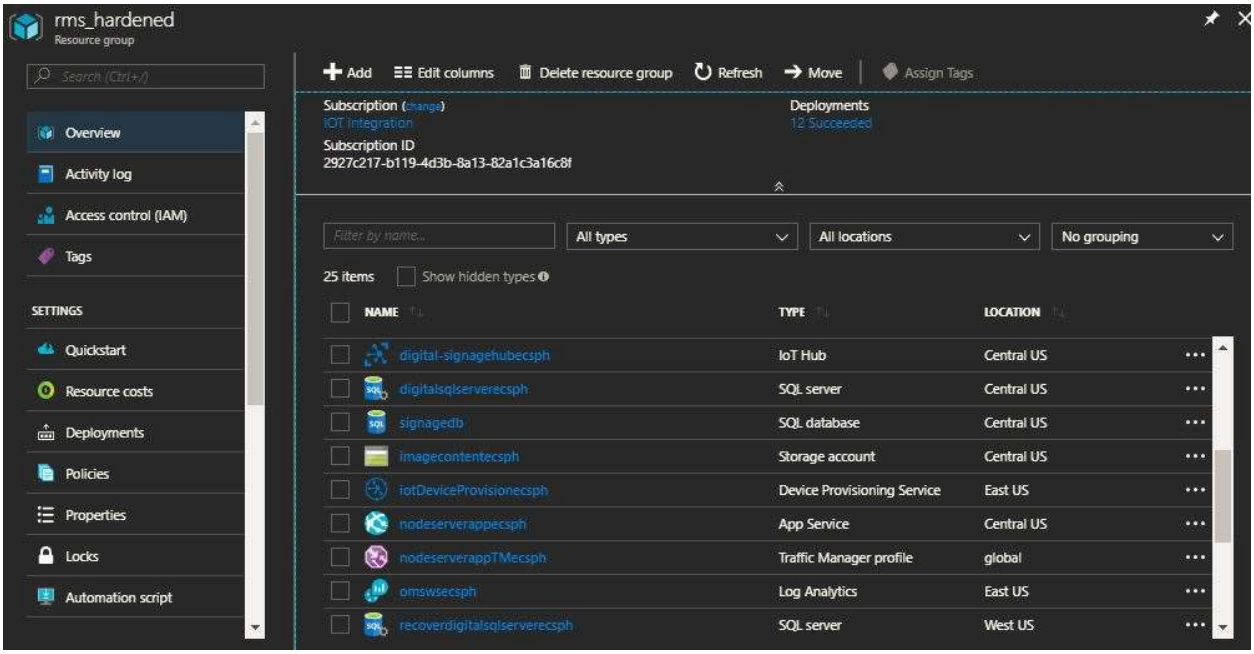


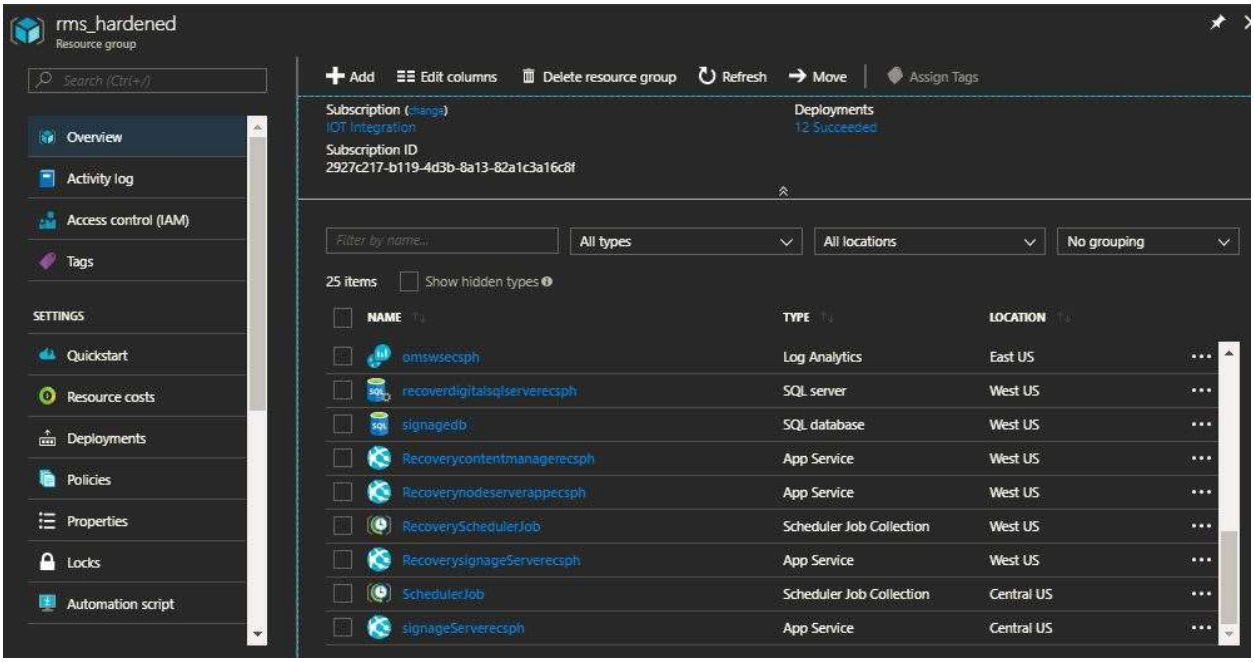
11. After the successful deployment of the ARM template, the following **resources** are created in a **Resource Group**.

    - 2 App Service plan
    - Automation Account
    - Runbook
    - 6 App Services
    - Storage account
    - IoT HUB
    - IoT Device provisioning service
    - 2 SQL server
    - 2 SQL database
    - Storage account
    - 2 Scheduler Job Collection
    - 2 Traffic manager account
    - 1 campaign expire webjob

12. Once the solution is deployed successfully navigate to the resource group, select the created resource group to view the list of resources that are created in the **Resource Group** as shown in the following figure.


rms_hardened
Resource group
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
SETTINGS
Quickstart
Resource costs
Deployments
Policies
Properties
Locks
Automation script
Add
Edit columns
Delete resource group
Refresh
Move
Assign Tags
Subscription (change)
IOT Integration
Subscription ID
2927c217-b119-4d3b-8a13-82a1c3a16c8f
Deployments
12 Succeeded
Filter by name...
All types
All locations
No grouping
25 items
Show hidden types
NAME
TYPE
LOCATION
AppInsightsecsphzg33ufme
Application Insights
West US 2
AppSerPlan
App Service plan
Central US
AppSerPlanRecoveryecsph
App Service plan
West US
AzureSQLAnalytics(omswsecsph)
Solution
East US
AzureWebAppsAnalytics(omswsecsph)
Solution
East US
containerCreateecsph
Automation Account
East US 2
container
Runbook
East US 2
contentmanagerecsph
App Service
Central US
contentmanagerTMecsph
Traffic Manager profile
global


rms_hardened
Resource group
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
SETTINGS
Quickstart
Resource costs
Deployments
Policies
Properties
Locks
Automation script
Add
Edit columns
Delete resource group
Refresh
Move
Assign Tags
Subscription (change)
IOT Integration
Subscription ID
2927c217-b119-4d3b-8a13-82a1c3a16c8f
Deployments
12 Succeeded
Filter by name...
All types
All locations
No grouping
25 items
Show hidden types
NAME
TYPE
LOCATION
digital-signagehubecsph
IoT Hub
Central US
digitalsqlserverecsph
SQL server
Central US
signagedb
SQL database
Central US
imagecontentecsph
Storage account
Central US
iotDeviceProvisionecsph
Device Provisioning Service
East US
nodeserverappecsph
App Service
Central US
nodeserverappTMecsph
Traffic Manager profile
global
omswsecsph
Log Analytics
East US
recoverdigitalsqlserverecsph
SQL server
West US



9.3.2. Deploy ARM Templates using Azure CLI

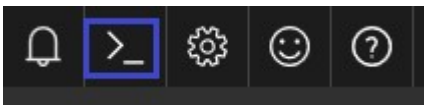
Azure CLI is used to deploy your resources to Azure. The Resource Manager template you deploy, can either be a local file on your machine, or an external file that is in a repository like GitHub.

Azure Cloud Shell is an interactive, browser-accessible shell for managing Azure resources. Cloud Shell enables access to a browser-based command-line experience built with Azure management tasks in mind.

Deployment can proceed within the Azure Portal via Azure Cloud Shell.

9.3.3. Customize main-template.parameters.json file

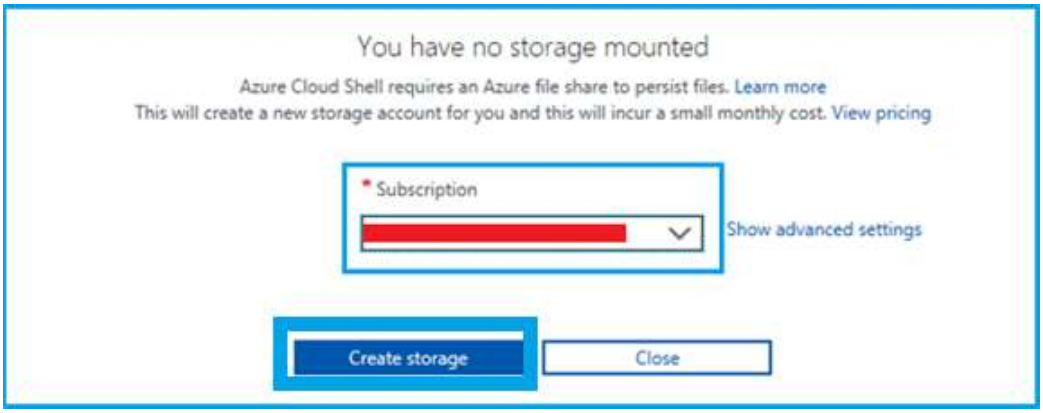
1. Log in to Azure portal.
2. Open the prompt.



3. Select **Bash (Linux)** environment as shown in the following figure.

4. Select your preferred **Subscription** from the dropdown list.

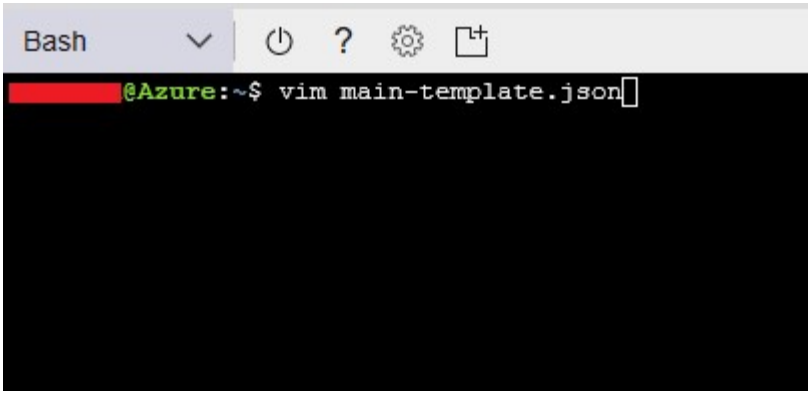
5. Click **Create Storage** button as shown in the following figure.



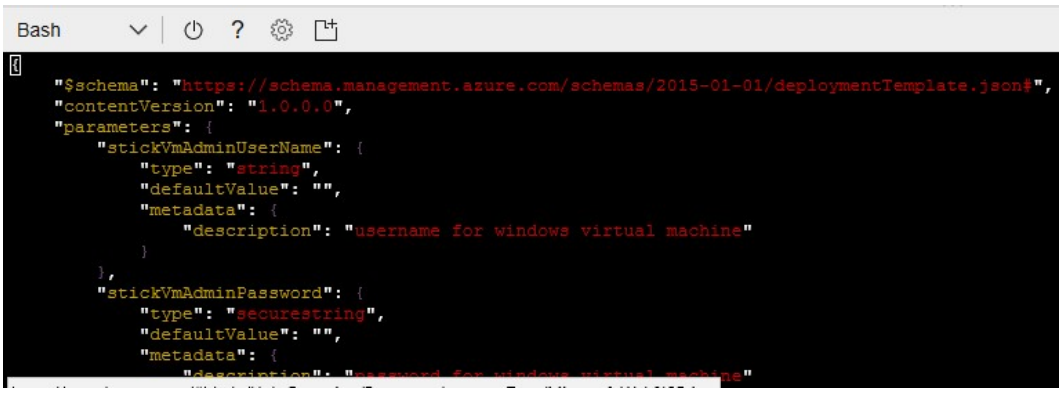
6. Copy **main-template.json** and **main-template.parameters.json** to your Cloud Shell before updating the parameters.

7. Create **main-template.json** using the following command.

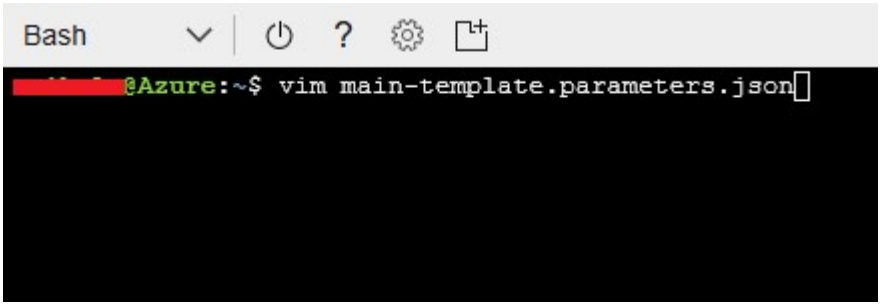
```
vim main-template.json
```



8. Paste your **main-template.json** in editor as shown below and save the file.



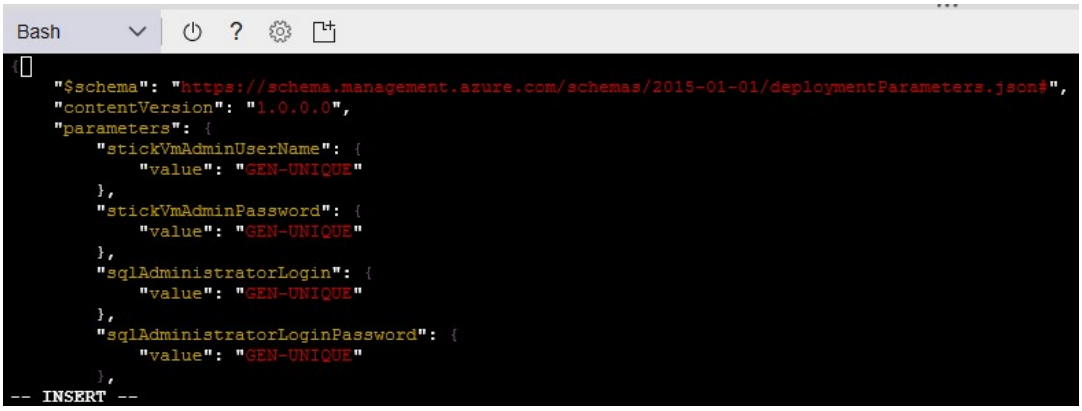
9. Create **main-template.parameters.json.**



10. Paste your **main-template.parameters.json** in editor.

11. Update the following parameters in main-template.json file

    a. **sqlAdministratorLogin**
    b. **sqlAdminstratorLoginPassword**
    c. **sessionId,storageBlobUrl**
    d. **omsWorkspaceRegion**
    e. **omsAutomationRegion**
    f. **dataRetention**
    g. **omsLogAnalyticSku**
    h. **appInsightsLocation**
    i. **stickVMSize**
    j. **iotHubSkuName**
    k. **capacityUnits**
    l. **d2cMessageRetentionInDaysPeriod**
    m. **d2cPartitionCount**
    n. **skuName**
    o. **skuCapacity**



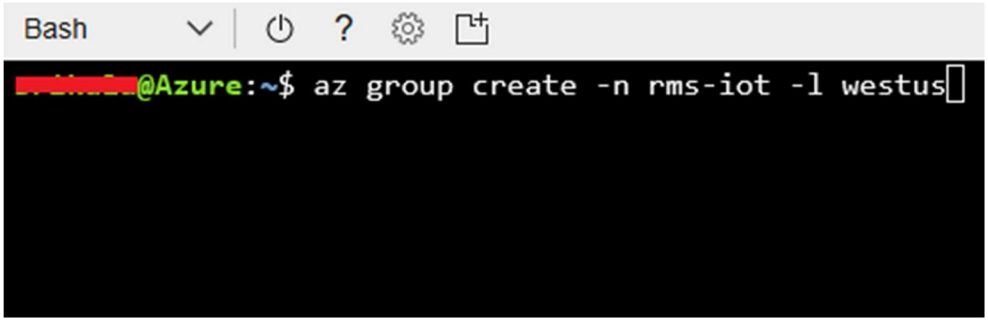
9.3.4. Create Resource Group for Digital Signage solution

Use the **az group create** command to create a **Resource Group** in your region, e.g.:

Description: To create a resource group, use **az group create** command,
It uses the name parameter to specify the name for resource group (-n) and location parameter to specify the location (-l).

Syntax: `az group create -n <resource group name> -l <location>`

`az group create -n <****> -l <***>`



9.3.5. Execute the template deployment

Use the **az group deployment create** command to deploy the ARM template

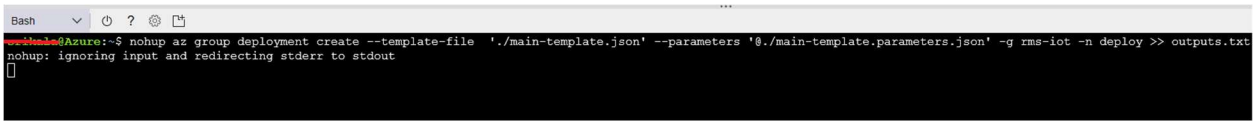
Description: To deploy the ARM Template, you require two files:

1. **main-template.json** – contains the resource & its dependency resources to be provisioned from the ARM template

2. **main-template.parameters.json** –contains the input values that are required to provision respective SKU & Others details, for more details on the input parameter values navigate to Section 7 of this document.

Syntax: `az group deployment create --template-file './<main-template.json filename>' --parameters '@./<main-template.parameters.json filename>' -g <` provide resource group name that created in the **section 9.3.4** `> -n deploy >> <provide the outputs filename>`

```
az group deployment create --template-file './main-template.json' --parameters '@./main-template.parameters.json' -g rms-iot -n deploy >> outputs.txt
```



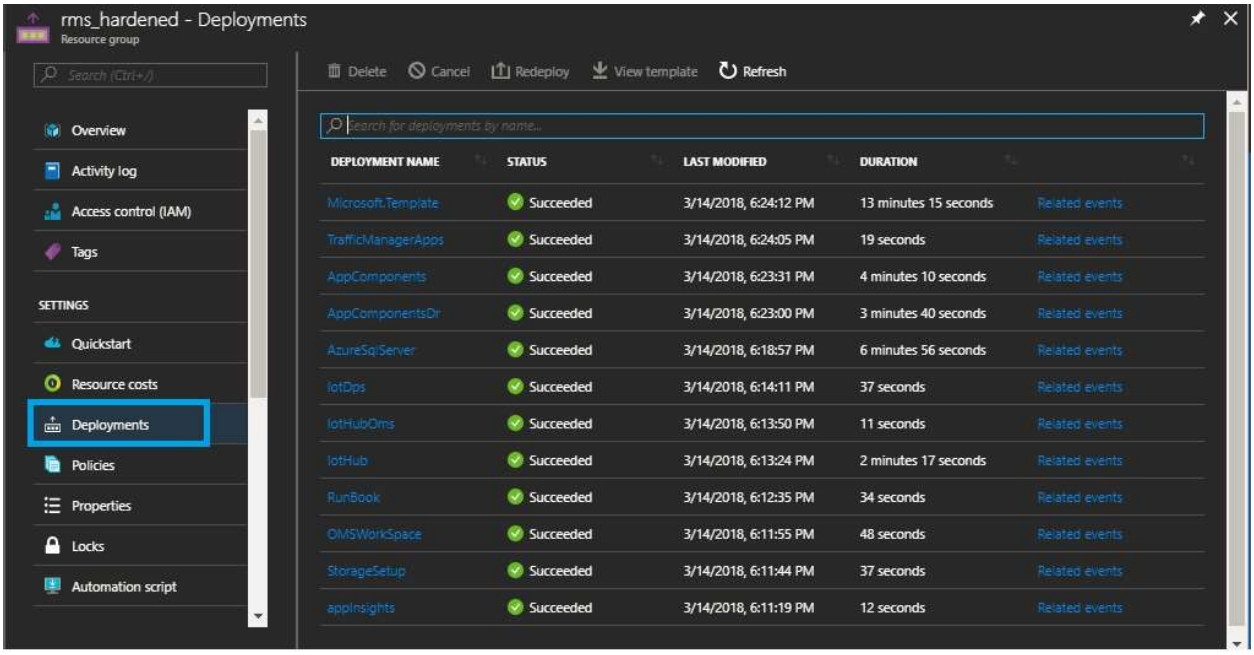
Deployment may take between 15-20 minutes depending on deployment size.

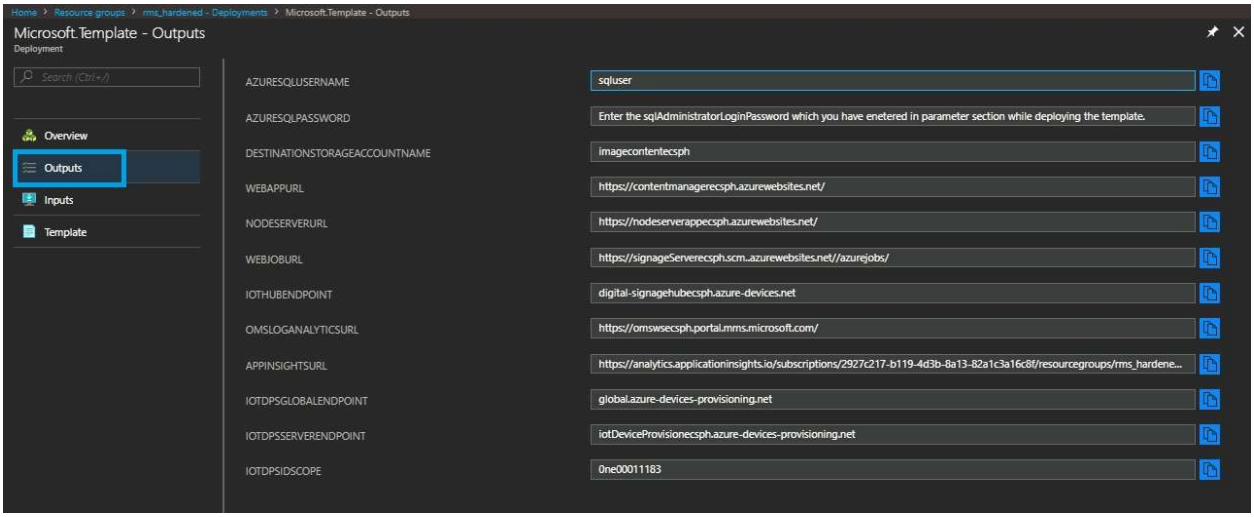
After successful deployment you can see the values in the output section of ARM template for

a. **azureSQLEndpoint**
b. **azureSQLsignageDBName**
c. **azureSQLUsername**
d. **azureSqlPassword**
e. **stcikVMFQDN**
f. **stcikVmadminUsername**
g. **stcikVmAdminPassword**
h. **destinationStorageAccountName**
i. **webJobUrl**
j. **IoTHubEndPoint**
k. **webAppUrl**
l. **nodeServerUrl**
m. **omsLogAnalyticsUrl**
n. **appInsightsUrl**
o. **iotDpsGlobalEndPoint**
p. **iotDpsServerEndPoint**
q. **iotDpsIdScope**

10. Post Deployment

1. After successful Arm Template deployment using **azure portal**, the output value can be obtained from **Deployments > Microsoft.Template** as shown in the following figure.



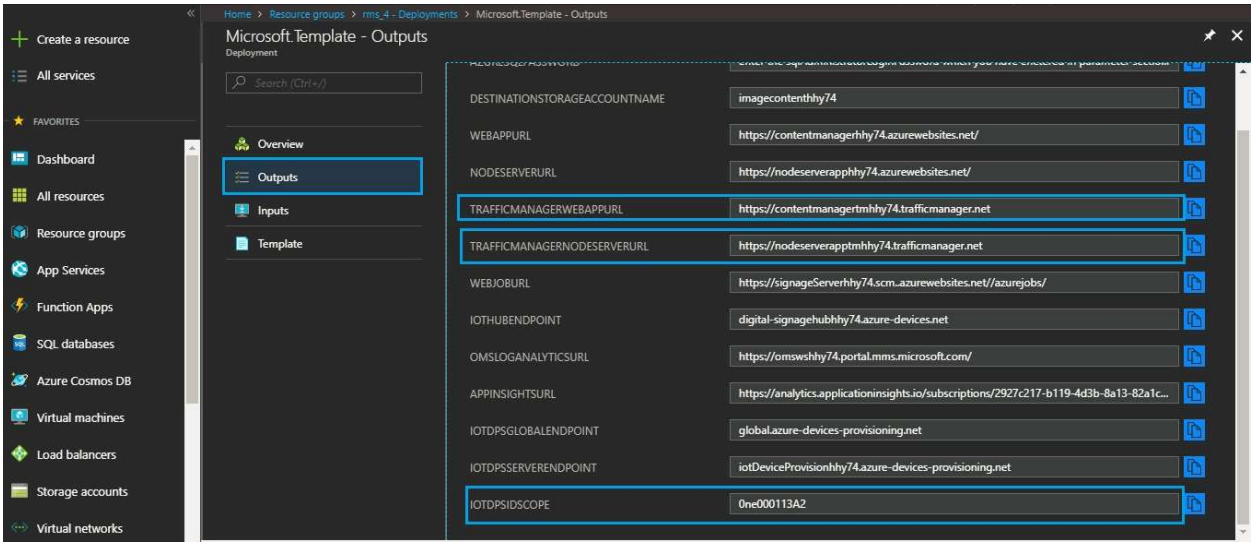


2. Copy or note down the following which will be used in the next steps.

TRAFFICMANAGERWEBAPPURL

TRAFFICMANAGERNODESERVERURL

IOTDPSIDSCOPE


Create a resource
All services
FAVORITES
Dashboard
All resources
Resource groups
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Home > Resource groups > rms_4 - Deployments > Microsoft.Template - Outputs
Microsoft.Template - Outputs
Deployment
Search (Ctrl+/)
Overview
Outputs
Inputs
Template
DESTINATIONSTORAGEACCOUNTNAME
imagecontenthhy74
WEBAPPURL
https://contentmanagerhhy74.azurewebsites.net/
NODESERVERURL
https://nodeserverapphhy74.azurewebsites.net/
TRAFFICMANAGERWEBAPPURL
https://contentmanagertmhhy74.trafficmanager.net
TRAFFICMANAGERNODESERVERURL
https://nodeserverapptmhhy74.trafficmanager.net
WEBJOBURL
https://signageServerhhy74.scm..azurewebsites.net//azurejobs/
IOTHUBENDPOINT
digital-signagehubhhy74.azure-devices.net
OMSLOGANALYTICSURL
https://omswshhy74.portal.mms.microsoft.com/
APPINSIGHTSURL
https://analytics.applicationinsights.io/subscriptions/2927c217-b119-4d3b-8a13-82a1c...
IOTDPSGLOBALENDPOINT
global.azure-devices-provisioning.net
IOTDPSSERVERENDPOINT
iotDeviceProvisionhhy74.azure-devices-provisioning.net
IOTDPSIDSCOPE
0ne000113A2

11. Digital Signage DPS Player

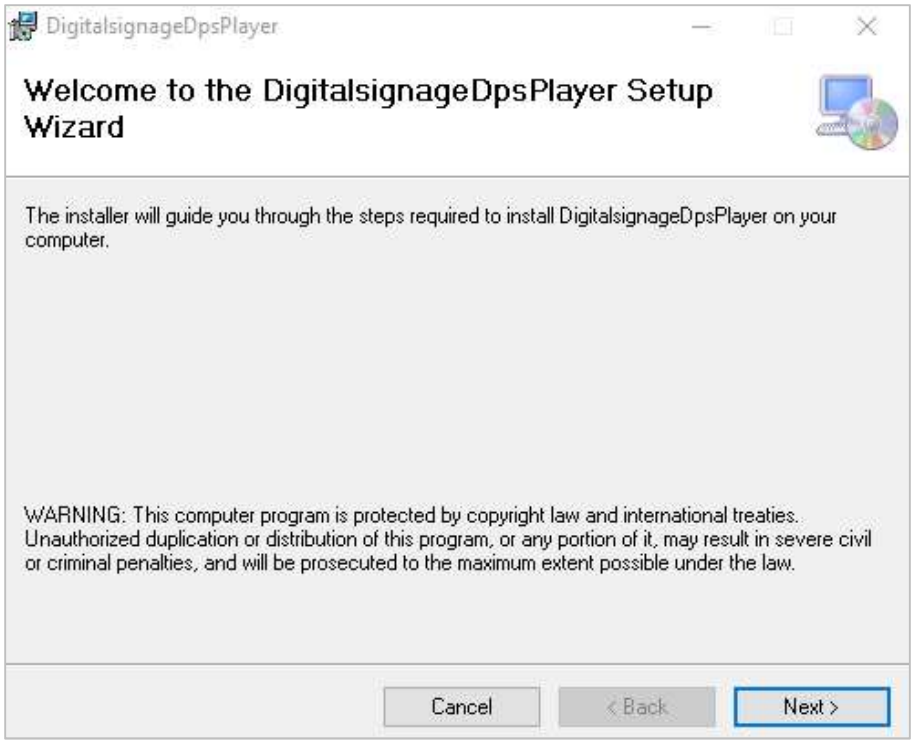
11.1. Installation of Stick Player software on a Virtual machine

1. Download the Digital signage DPS player setup file from the below link.

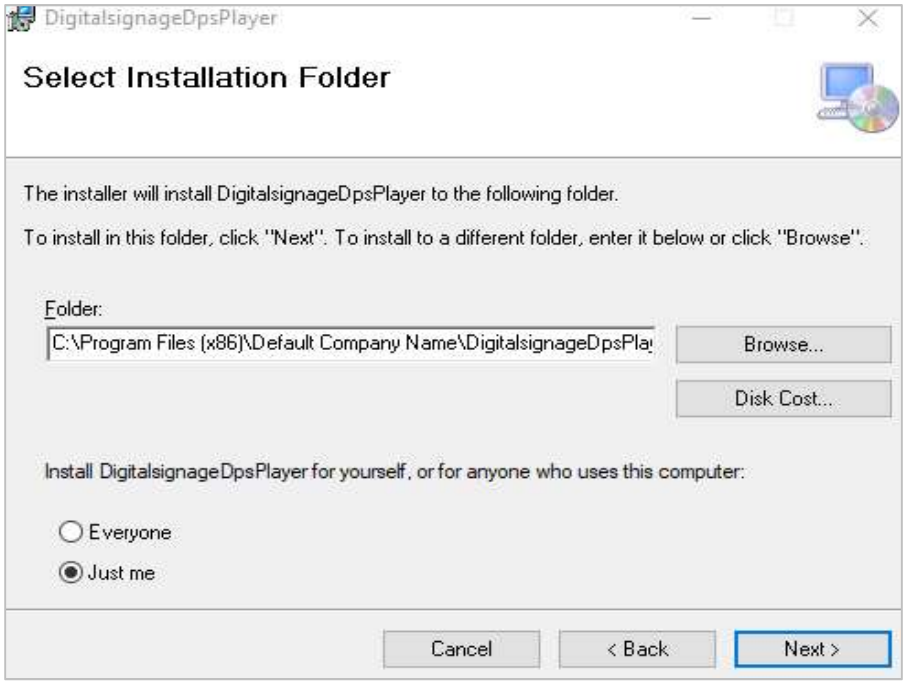
https://projectiot.blob.core.windows.net/rms-iot/DigitalSignageDpsPlayer.msi

2. Click **More Info**, and select **Run anyway** option.

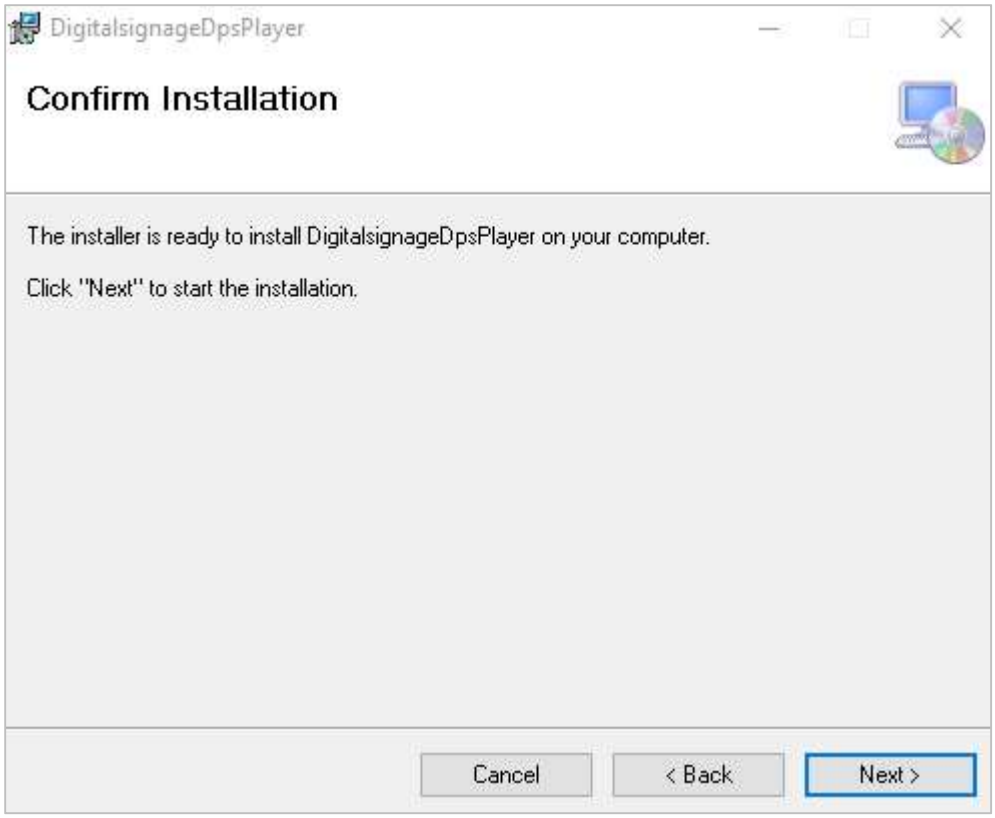
3. Click **Next** button.



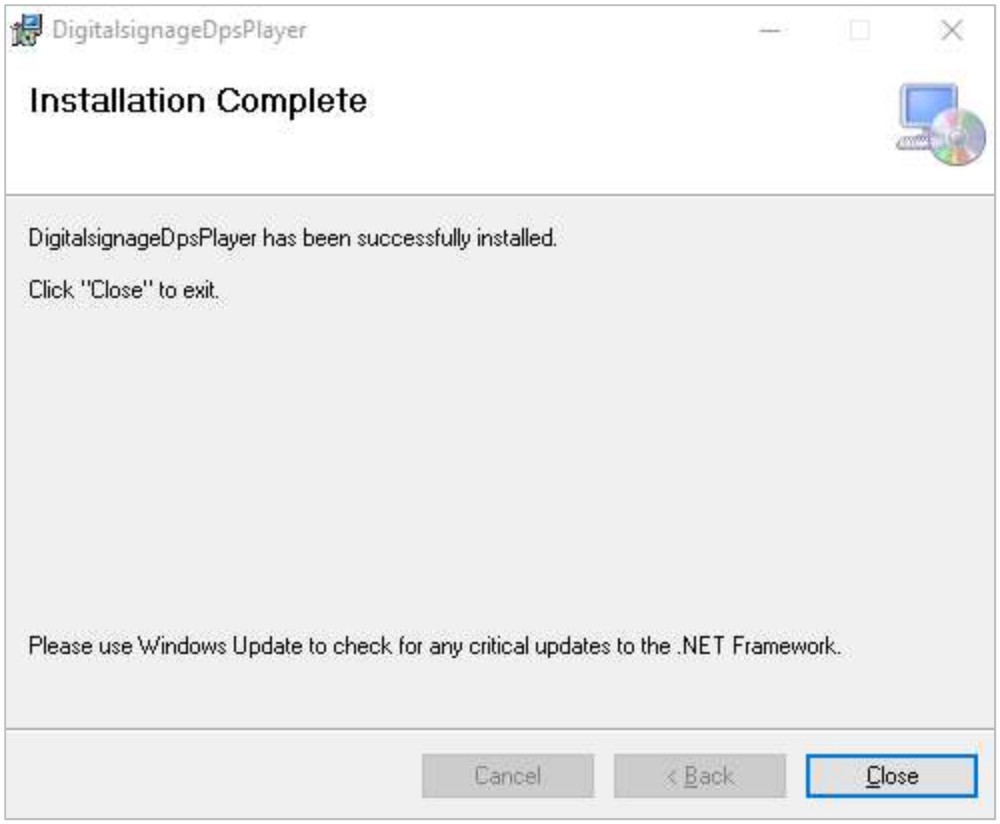
4. Click **Next** button.



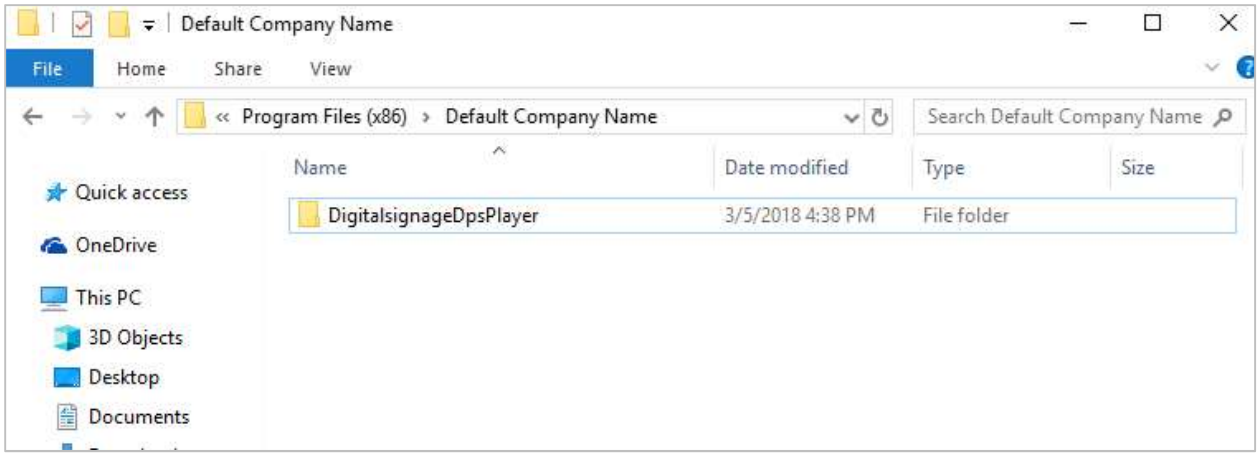
5. Click **Next** button.



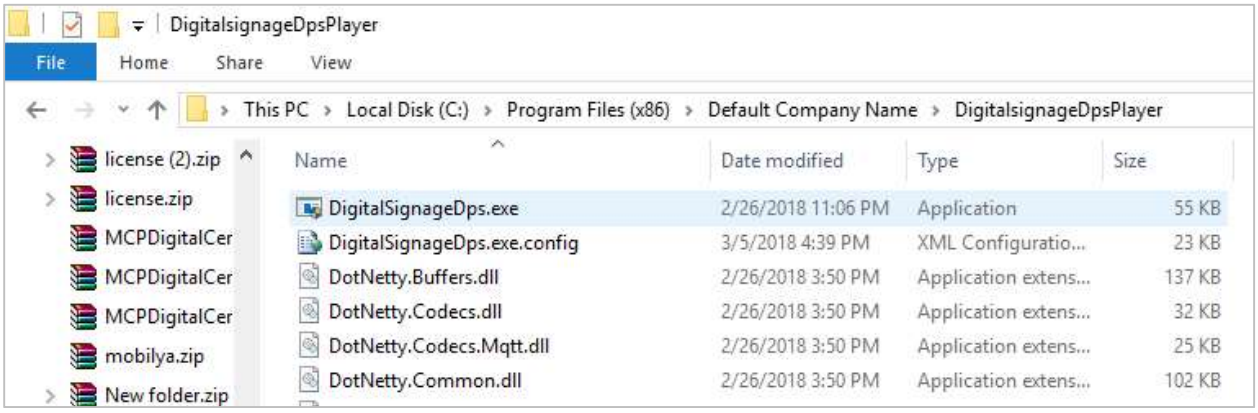
6. Click **YES** in the dialogue box.
7. Click **Close** button.



8. Once installation is finished, navigate to path **Local Disk (C:) > Program Files (x86) > Default Company Name > DigitalsignageDpsPlayer**

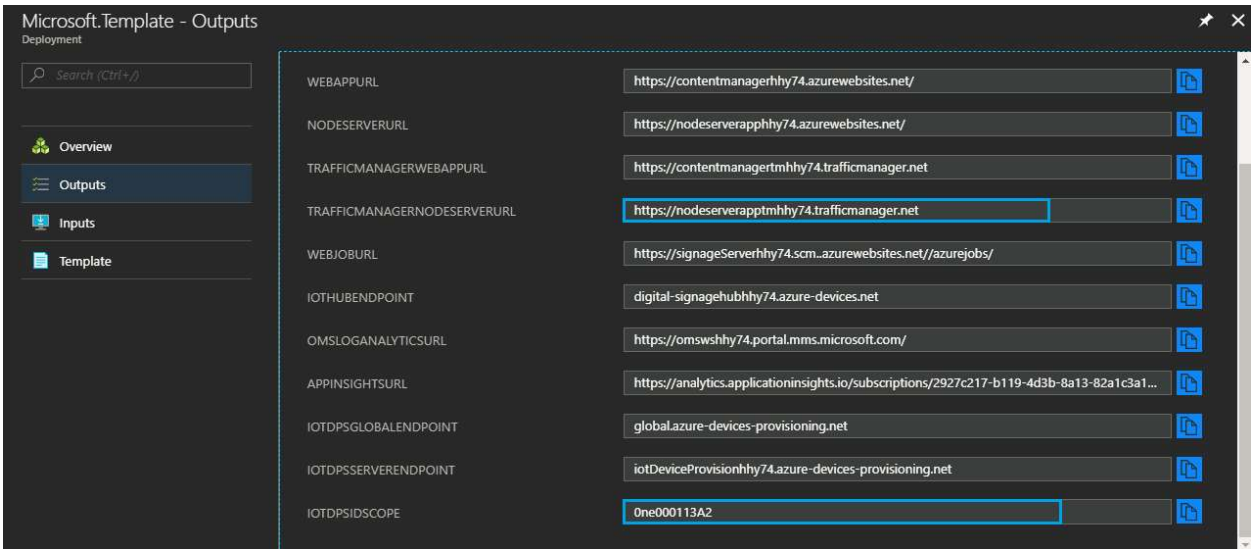


9. Right click on **DigitalSignageDps.exe.config** file folder and open with **notepad++**



10. Paste the copied **ID Scope** near DeviceProvisioningScopeId and **URI** near WebApiAddress, and save the file.

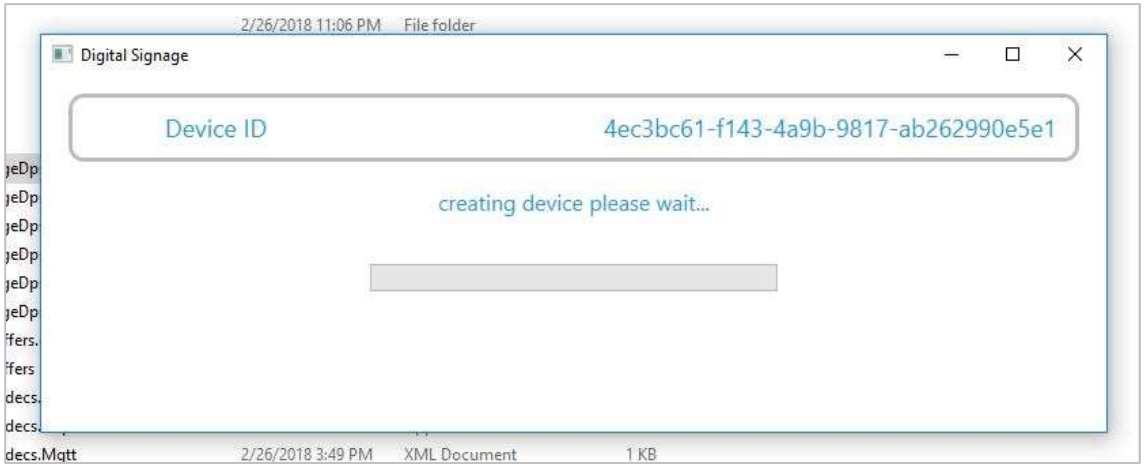
11. Go to **resource group** > **Deployments** > **Microsoft Template** > **Outputs**. Copy **TRAFFICMANAGERNODESREVER URL** & **IOTDPSIDSCOPE.**



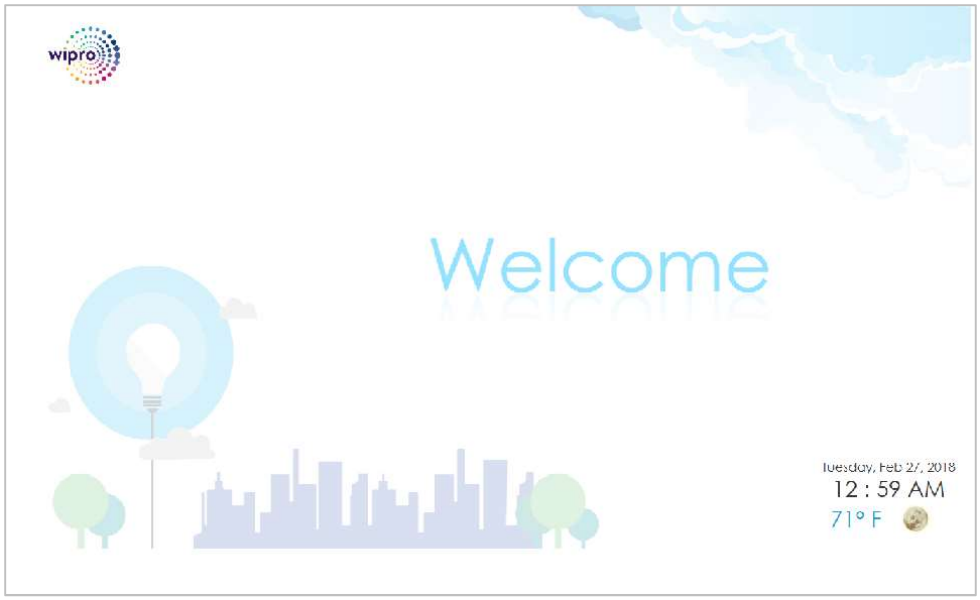
12. Paste the copied **ID Scope** near DeviceProvisioningScopeId and **TRAFFICMANAGERWEBAPPURL** near WebApiAddress, and save the file.

```
      <conversionPattern value="%date [%username] - %message%newline" />
    </layout>
  </appender>
  <logger name="Player">
    <level value="DEBUG" />
    <appender-ref ref="PlayerLogger" />
  </logger>
  <logger name="FaceRecognition">
    <level value="DEBUG" />
    <appender-ref ref="FaceRecognitionLogger" />
  </logger>
  <logger name="Connector">
    <level value="DEBUG" />
    <appender-ref ref="ConnectorLogger" />
  </logger>
</log4net>
<appSettings>
  <add key="WebApiAddress" value="http://nodeserverapptmecsph.trafficmanager.net" />
  <add key="ScopeId" value="One00011183" />
  <add key="ClientSettingsProvider.ServiceUri" value="" />
</appSettings>
<startup>
  <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6.1" />
</startup>
<runtime>
  <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
    <dependentAssembly>
      <assemblyIdentity name="System.Runtime" culture="neutral" publicKeyToken="b03f5f7f11d50a3a" />
      <bindingRedirect oldVersion="0.0.0.0-4.1.2.0" newVersion="4.1.2.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="System.Net.Http" culture="neutral" publicKeyToken="b03f5f7f11d50a3a" />
```

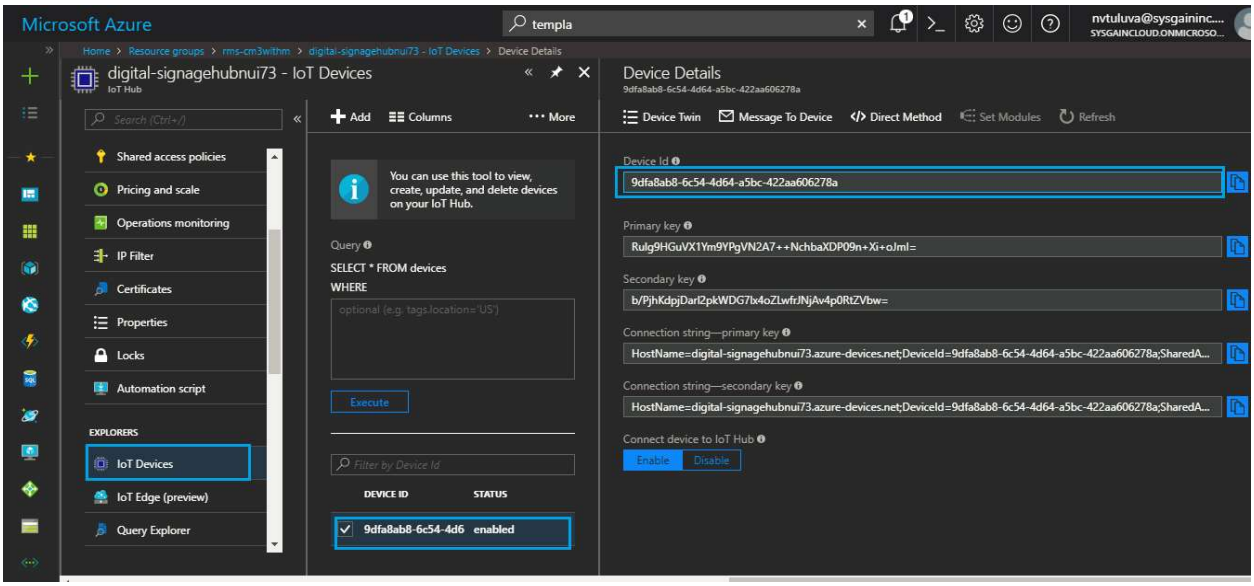
13. Navigate to path **Local Disk (C:) > Program Files (x86) > Default Company Name > DigitalsignageDpsPlayer,** right click **DigitalSignageDps.exe** file and select **run as Administrator**, you can view **Device ID** as shown in the following figure.



14. The Digital Signage app displays the device id and a **Welcome** page is displayed as shown in the following figure.

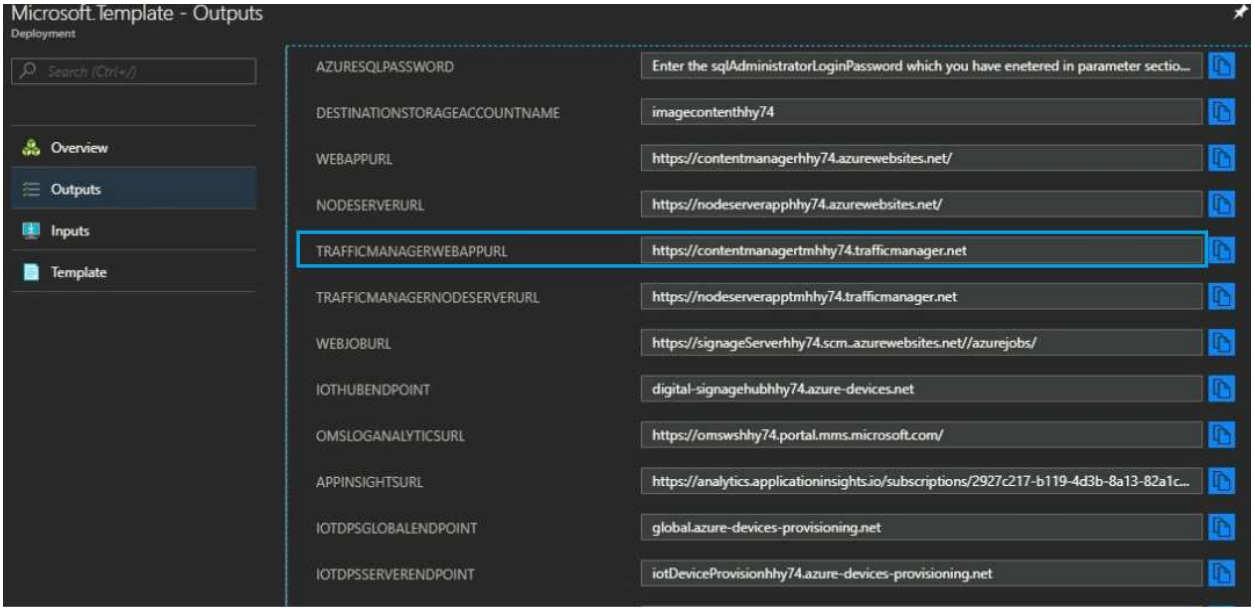


15. The **Digital Signage** app would create the device in **Azure IoT HUB** with its device id as shown in the following figure.

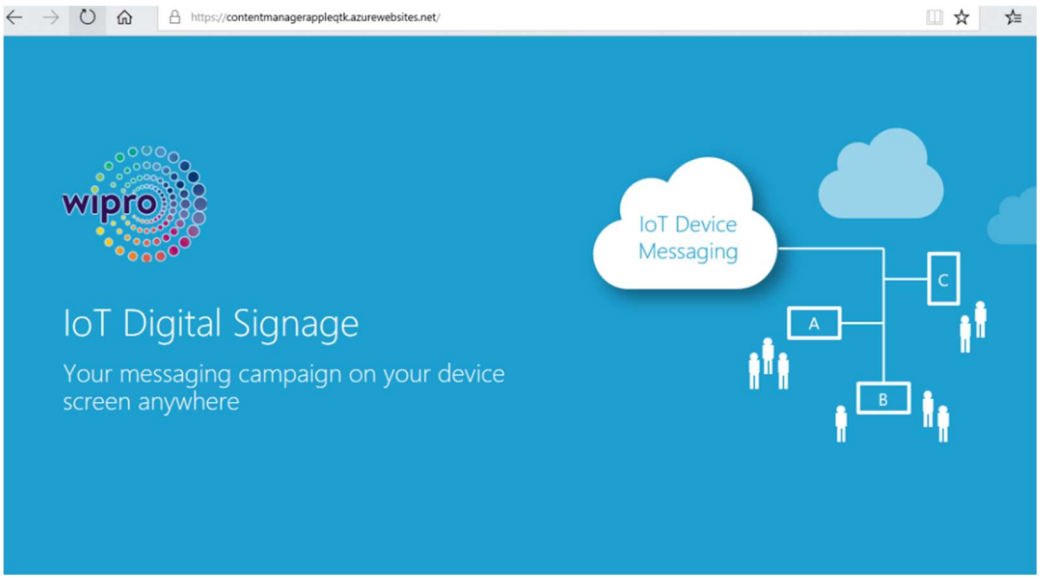


12. Signup to Digital signage UI

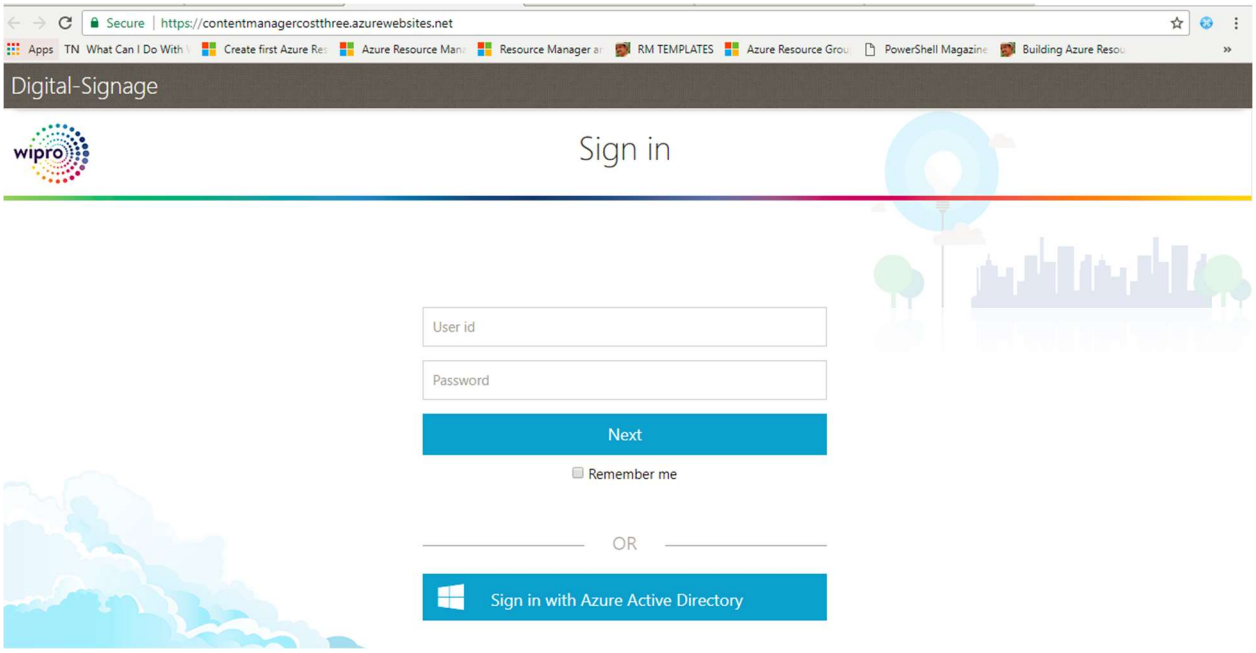
1. Copy and paste the traffic manager web app url from the output section in a browser.
2. Go to **resourcegroup** > **deployments** > **Microsoft Template** > **outputs**
3. Copy the **TRAFFICMANAGERWEBAPPURL** and paste it in a browser.



4. Copy and paste the following web App URL from the output section in a browser, the following page is displayed.



5. In the **Sign in** page, click **Sign in with Azure Active Directory** as shown in the following figure.

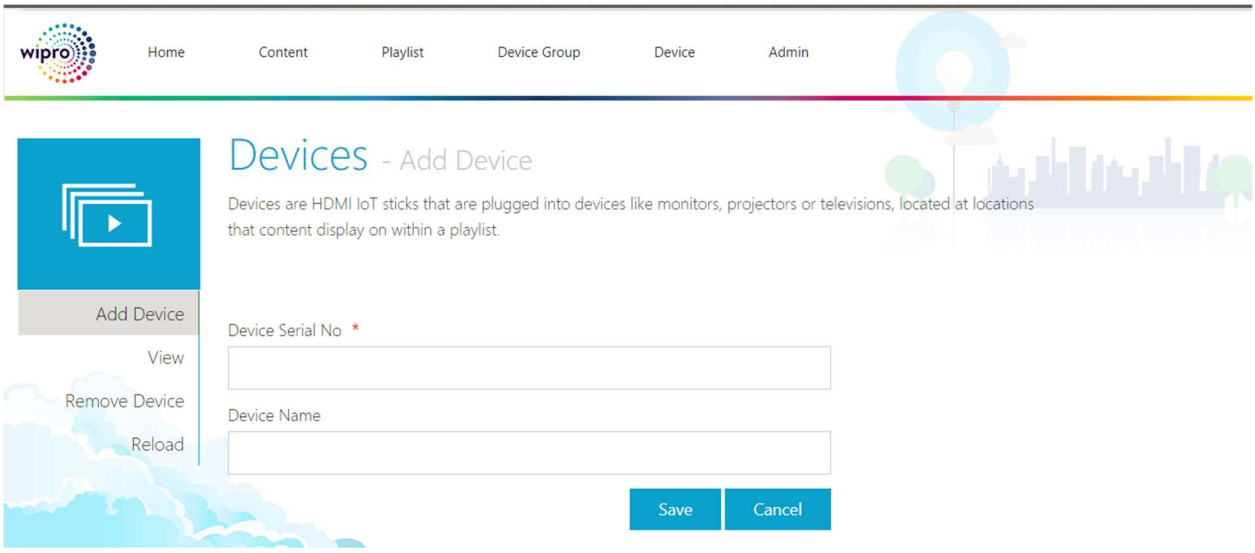


6. Once you login the **Home** page is displayed as shown in the following figure.

12.1. Add Device

To add device, follow the below steps,

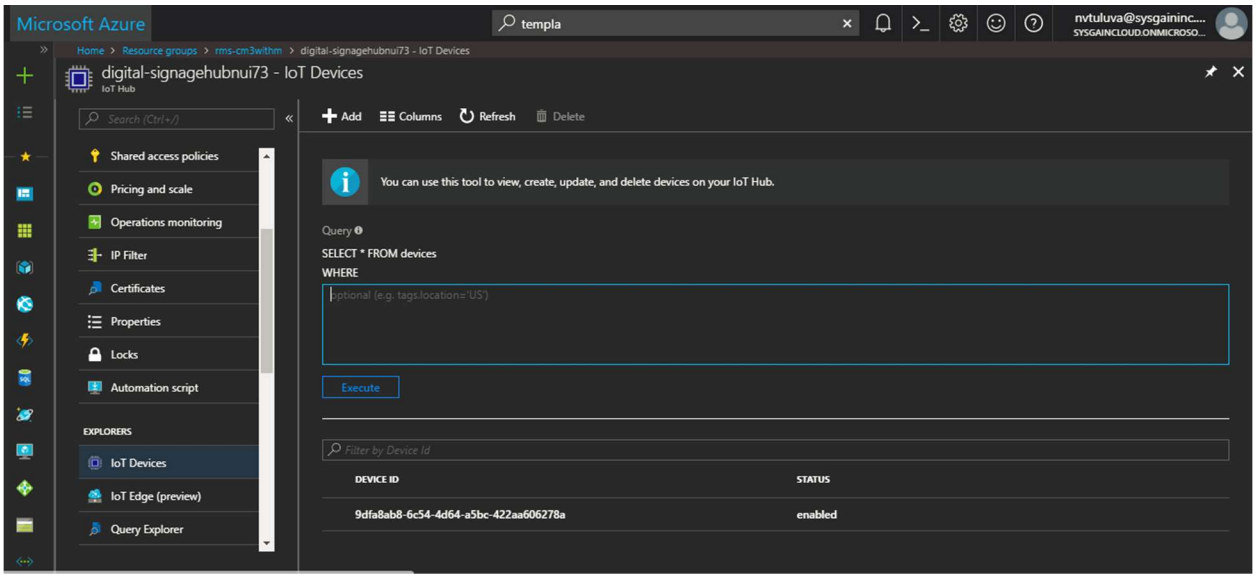
1. Click "**Device**" from top of menu **Devices** page is displayed as shown in the following figure.



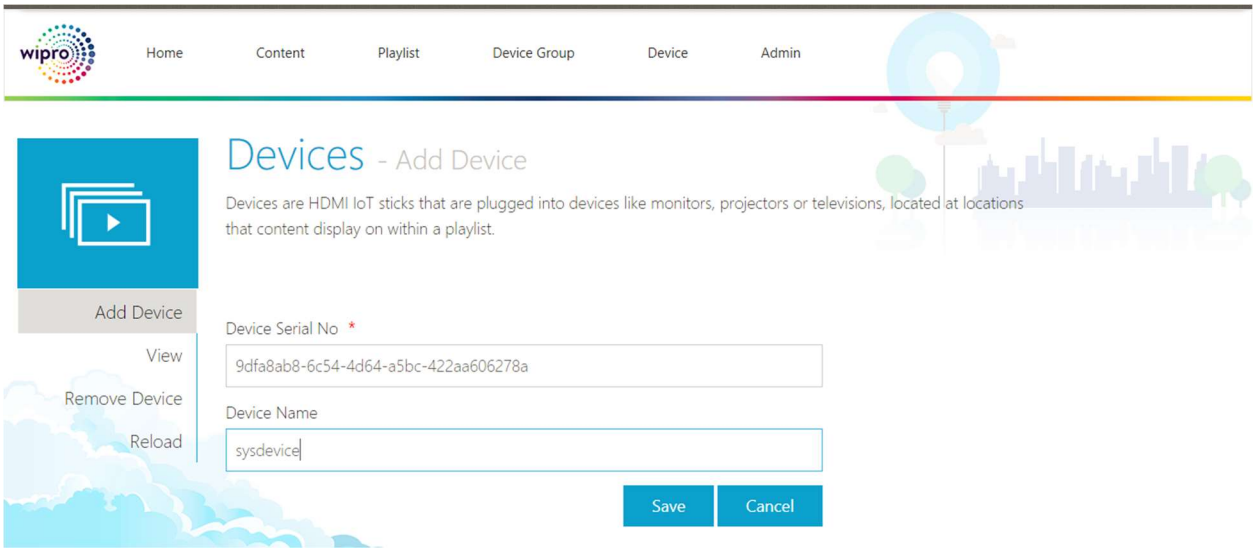
2. Select **Add Device** option from the left menu.

3. Enter Device **Serial Number**

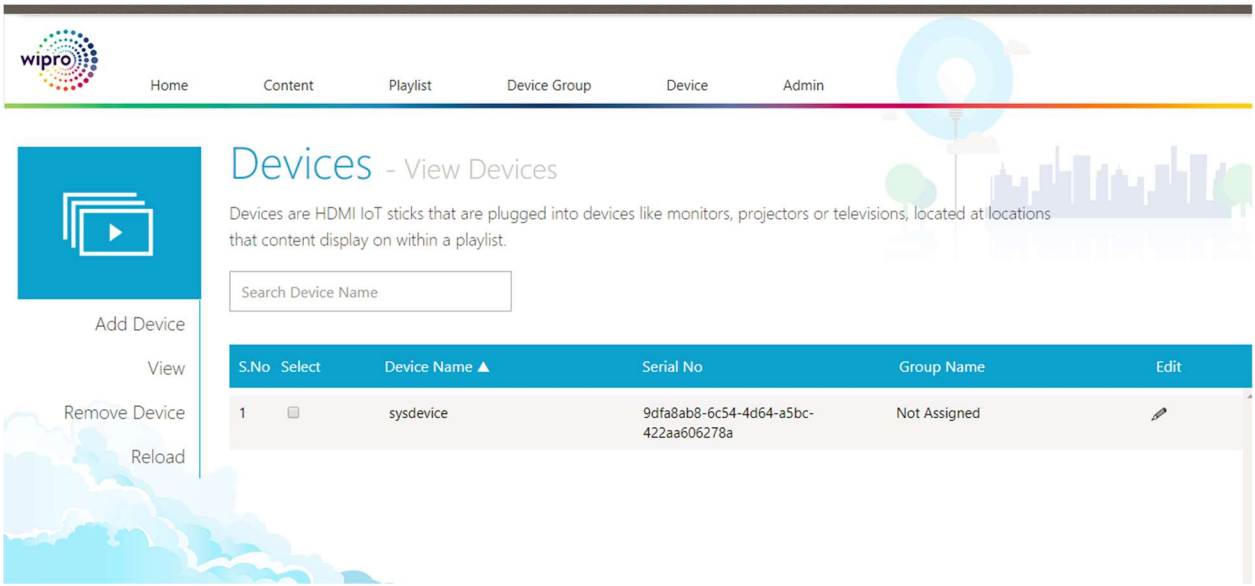
You must provide the **Serial Number** created by the **DPS** device. You can copy the serial number navigating to **resource groups > IoT HUB > IoT Devices** from left side of panel **> copy the Device Id** as shown in the following figure.



4. Paste the copied Device id in **Device serial No** field and enter the name in the **Device Name field** respectively.



5. Click **Save** button, the **device** is added.



Note: In this scenario the **Serial Number** is Device Id that was created in IoT HUB

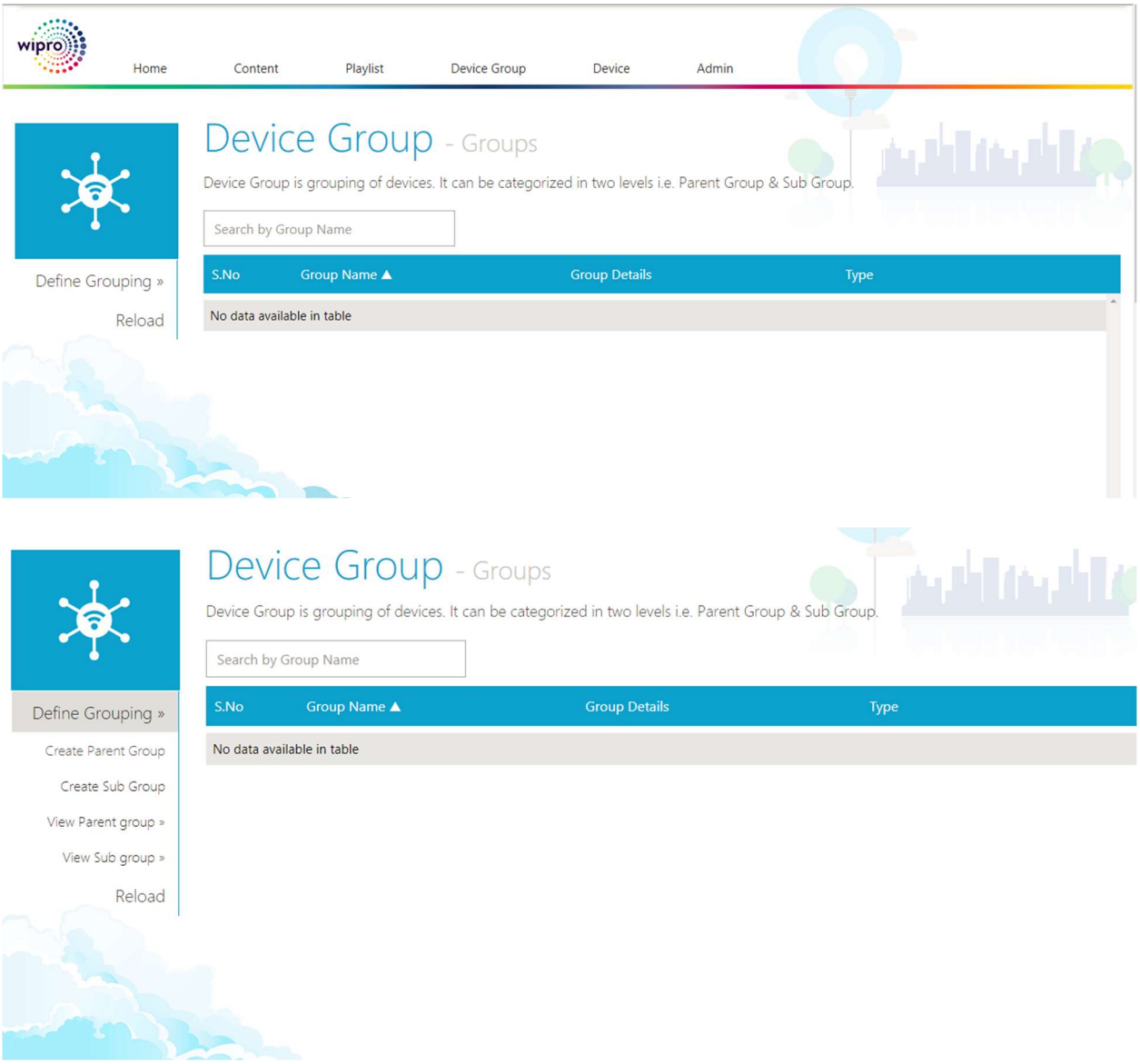
example: "**digitalsignageiothubid**" which was saved in earlier step.

12.2. Device Group

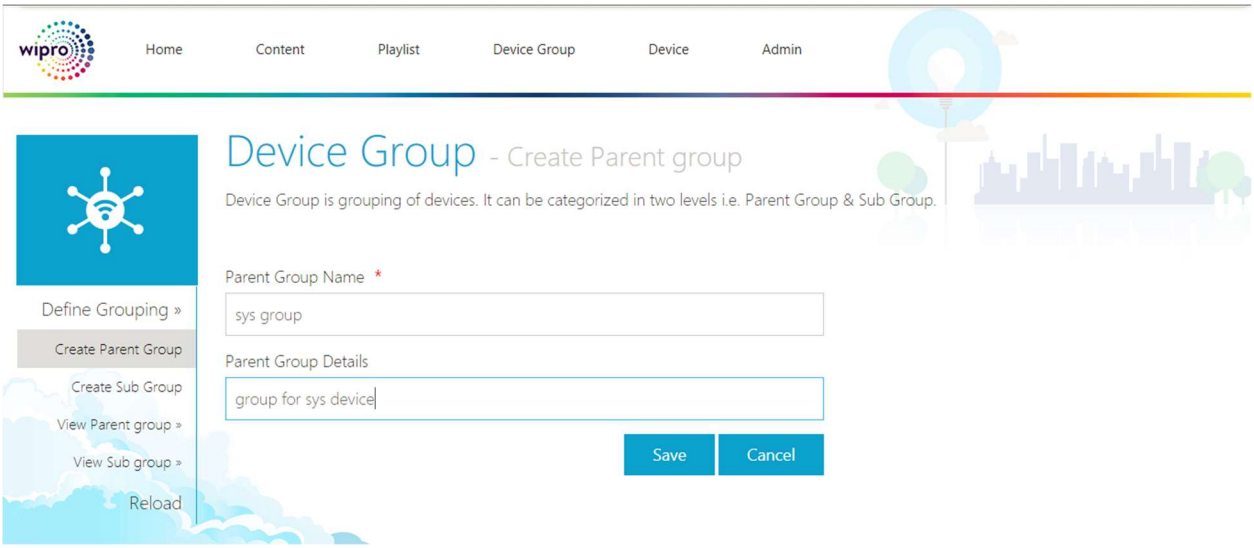
1. Select "**Device Group**" from the top menu

12.2.1. Create Device Group

2. To create a device group, select **Device Groups** from the **Device** top menu, the device group page is displayed as shown in the following figure.

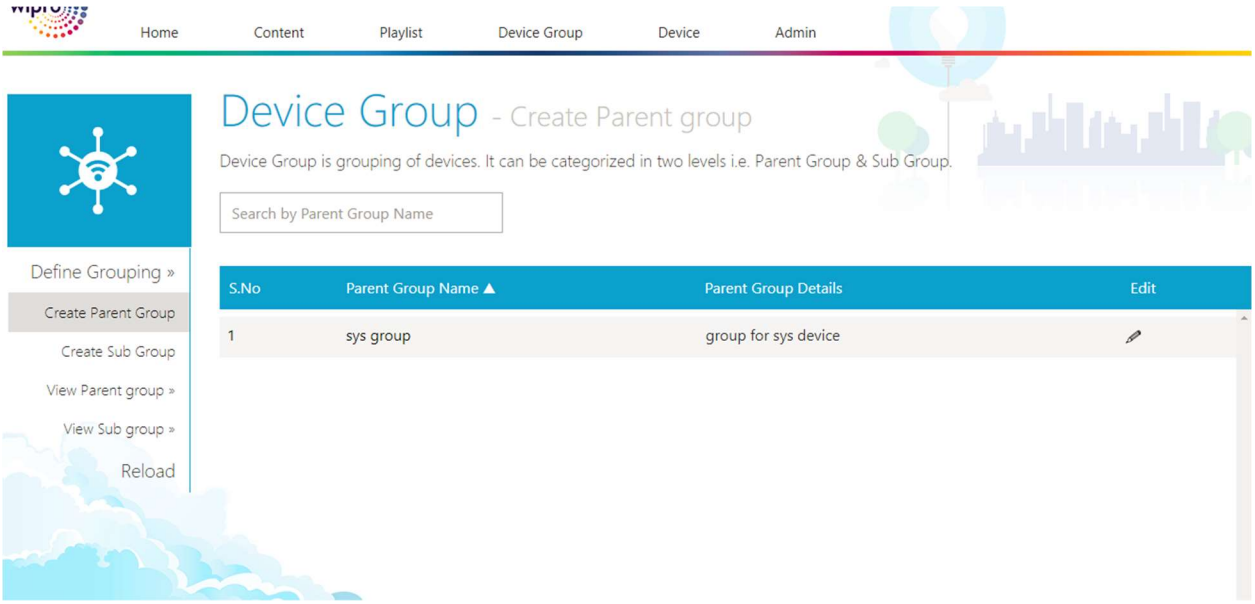


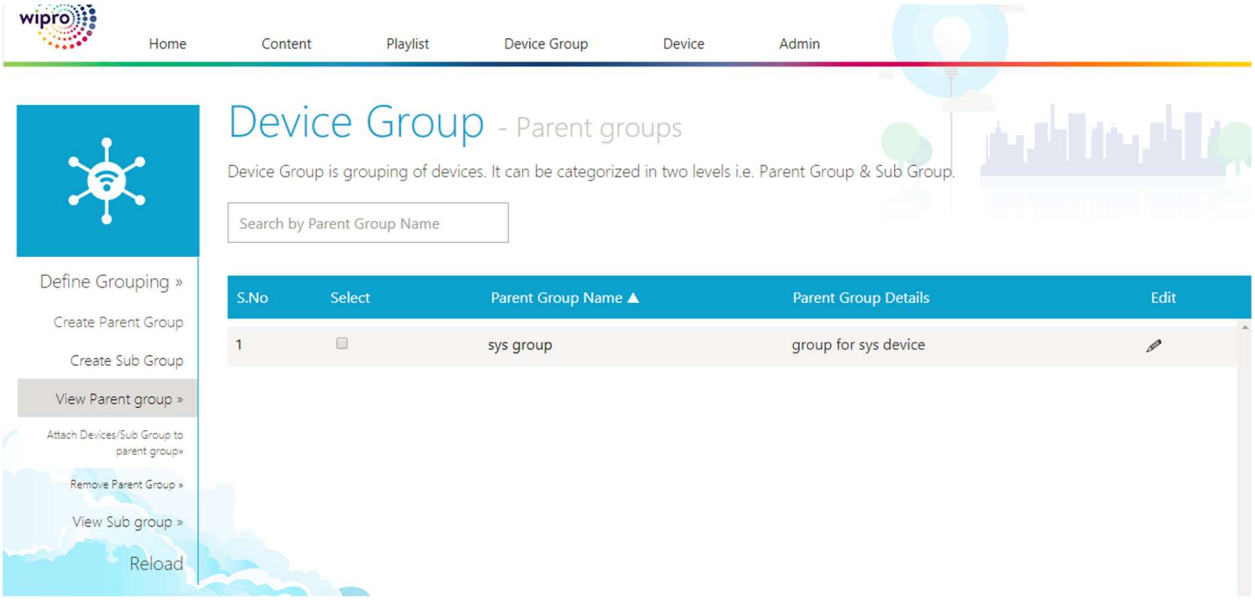
3. Select "**Create Parent Group**" from the left menu give the details of the ParentGroup i.e. Name and Details and click **Save** button.



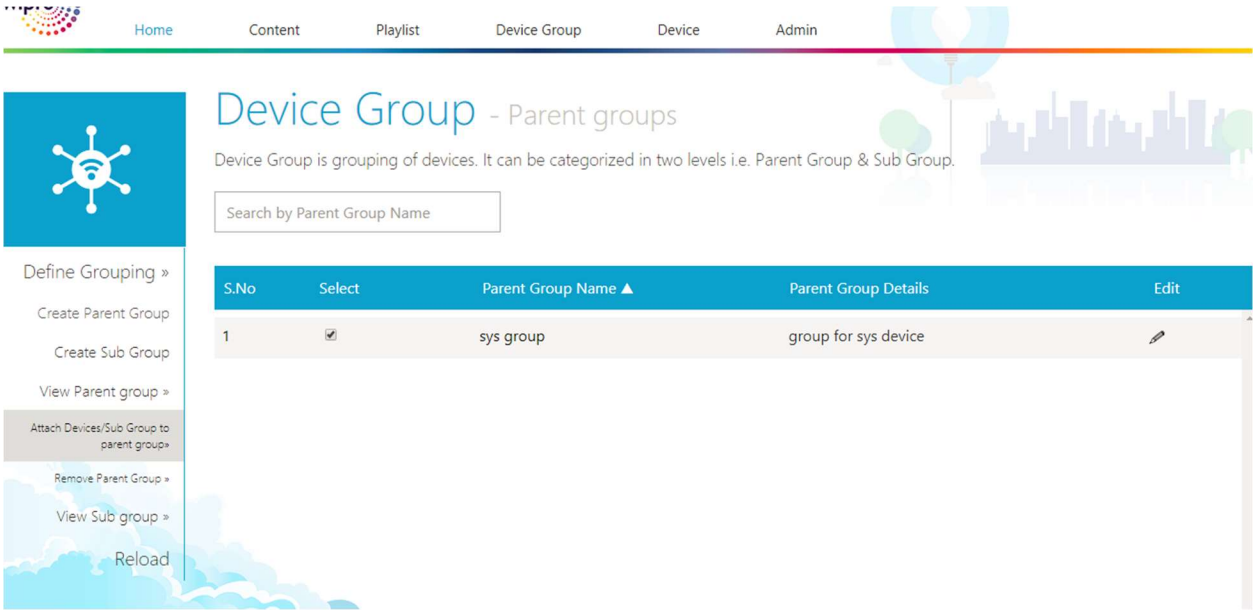
12.2.2. Assign a device to the device group

4. Click **View Parent Group** from the left menu and Select **Attach Devices/Sub group to the Parent Group.**

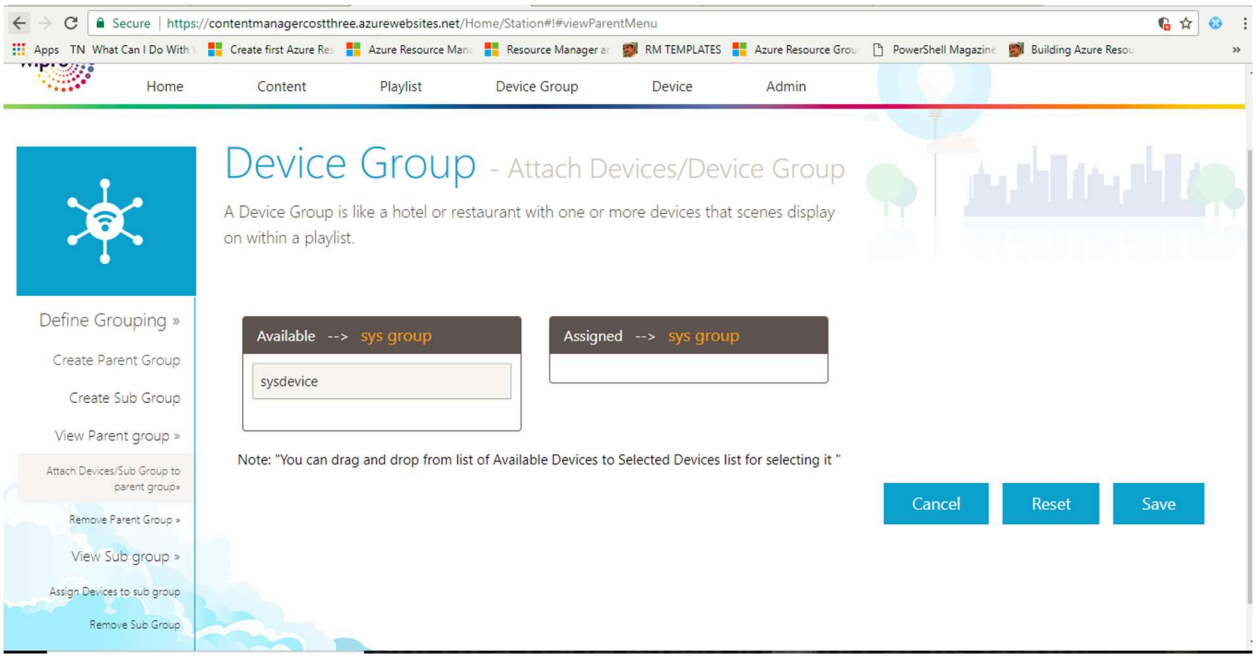




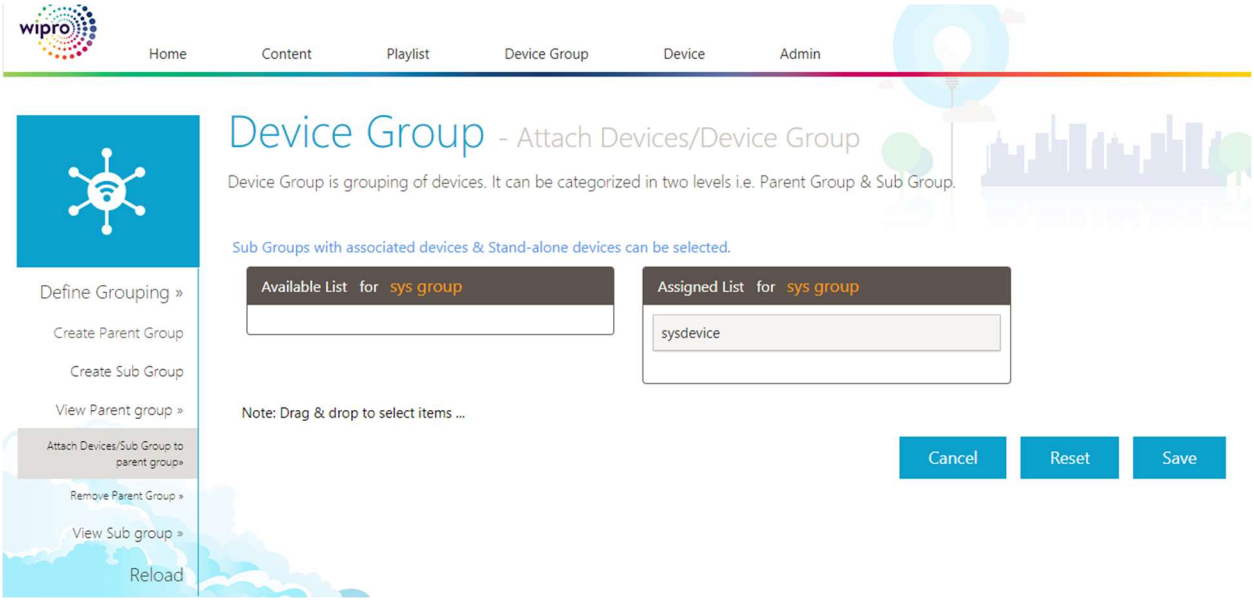
5. Once the **Group name** check box is selected the following page is displayed as shown in the following figure.



6. Select **Device(s)** and Move the devices by Drag-and-drop operation from the "**List Available**" to the "**List Assigned**".

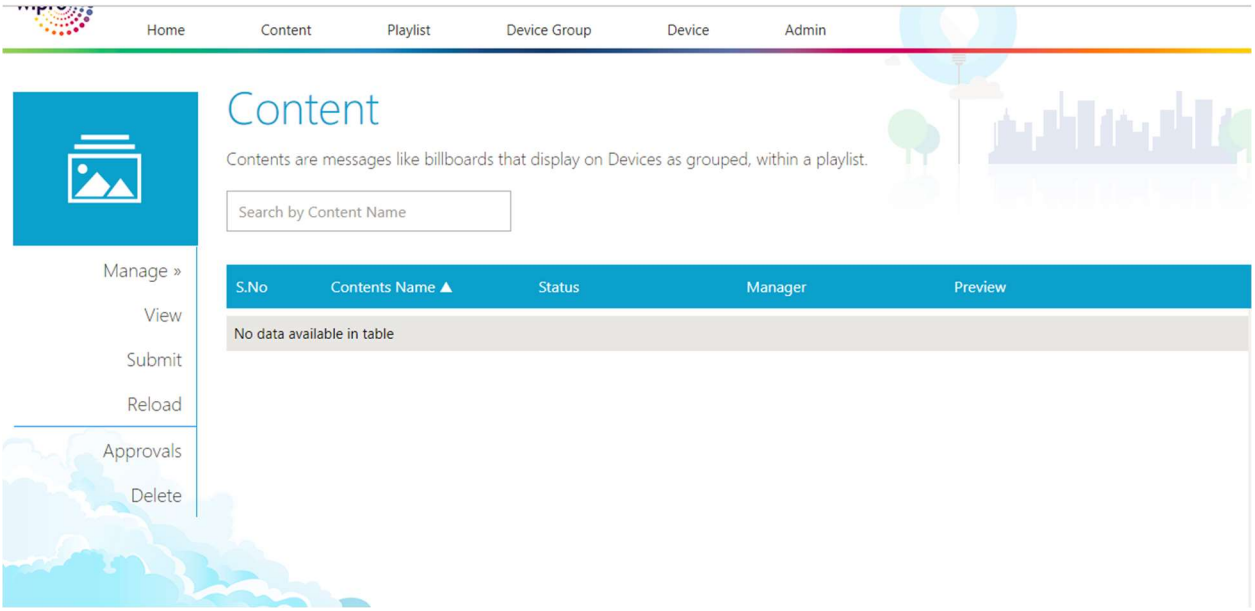


7. Click **Save** button, the selected device is added to the group.



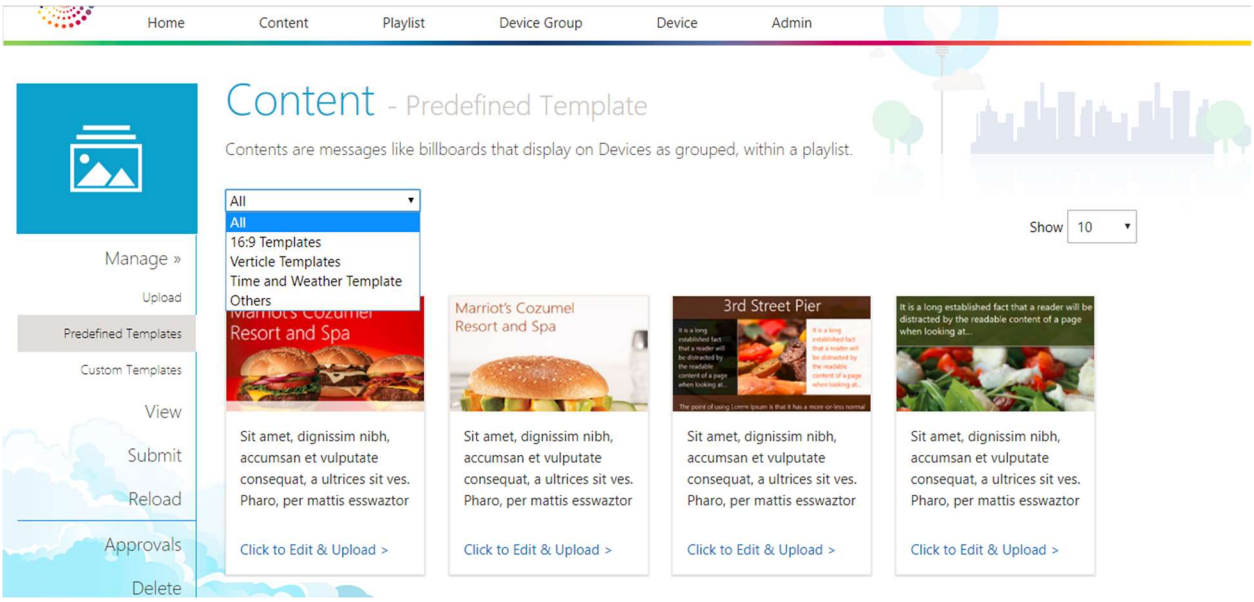
12.3. Content

Select "**Content**" from the top menu. You can upload your own content, usually an image with text you have created, or you can select a Template and create your Content with the Template tool.



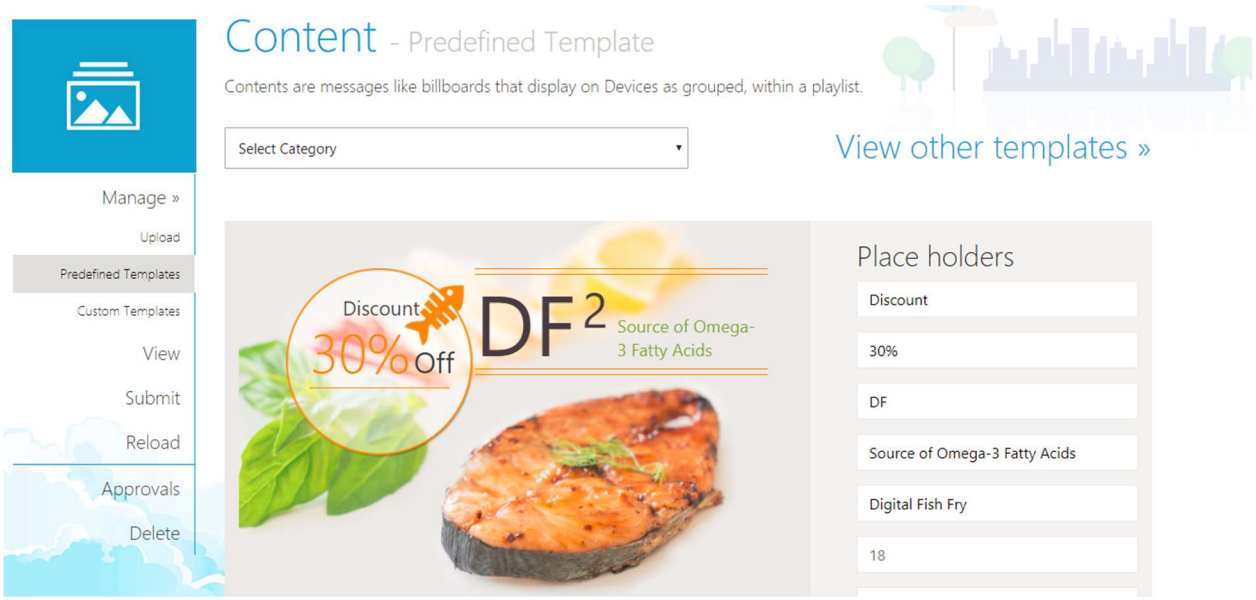
12.3.1. Add Content – Predefined Template

1. Select **"Manage > Predefined Template"** from the left menu. This is the message composed of images and text that will appear on devices at your Content within your playlist.

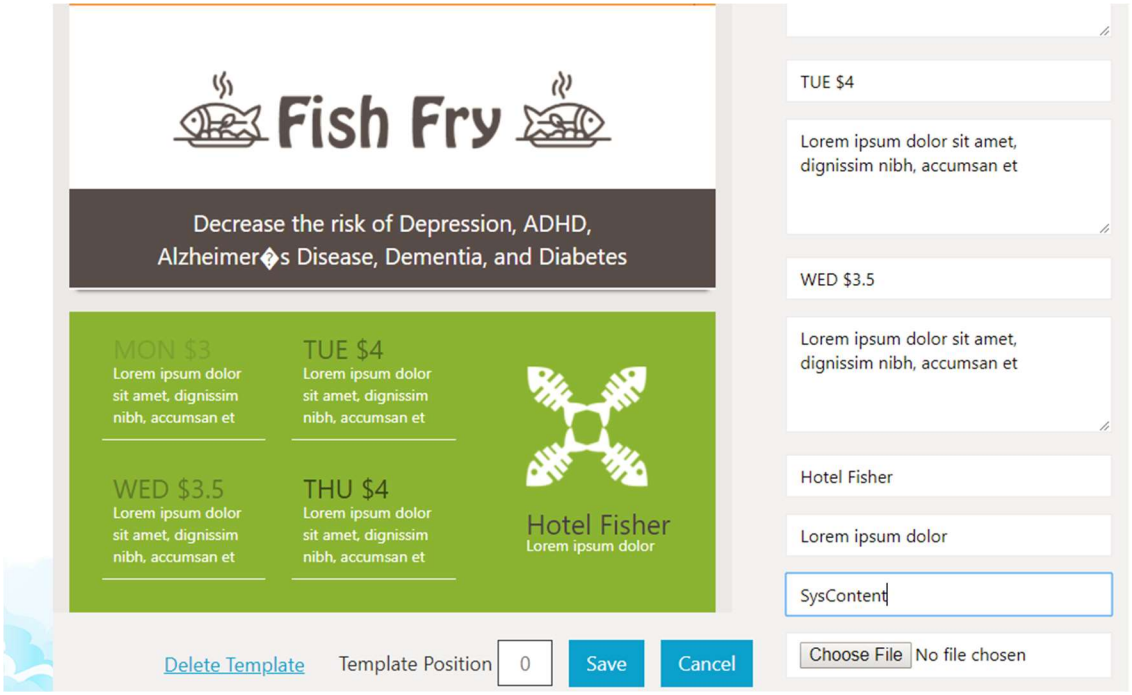


2. Choose a Template and select **"Click to Edit and Upload."** As shown in the following figure. Choose a static template to Customize with your images and text.

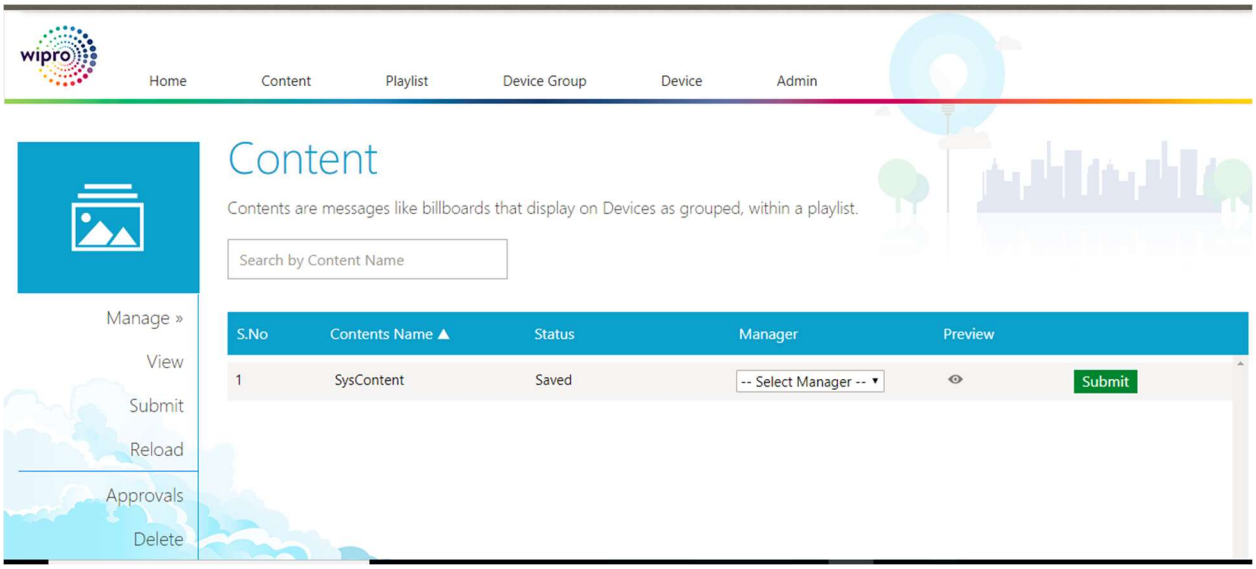
3. Select the category from the dropdown list as shown in the above figure.

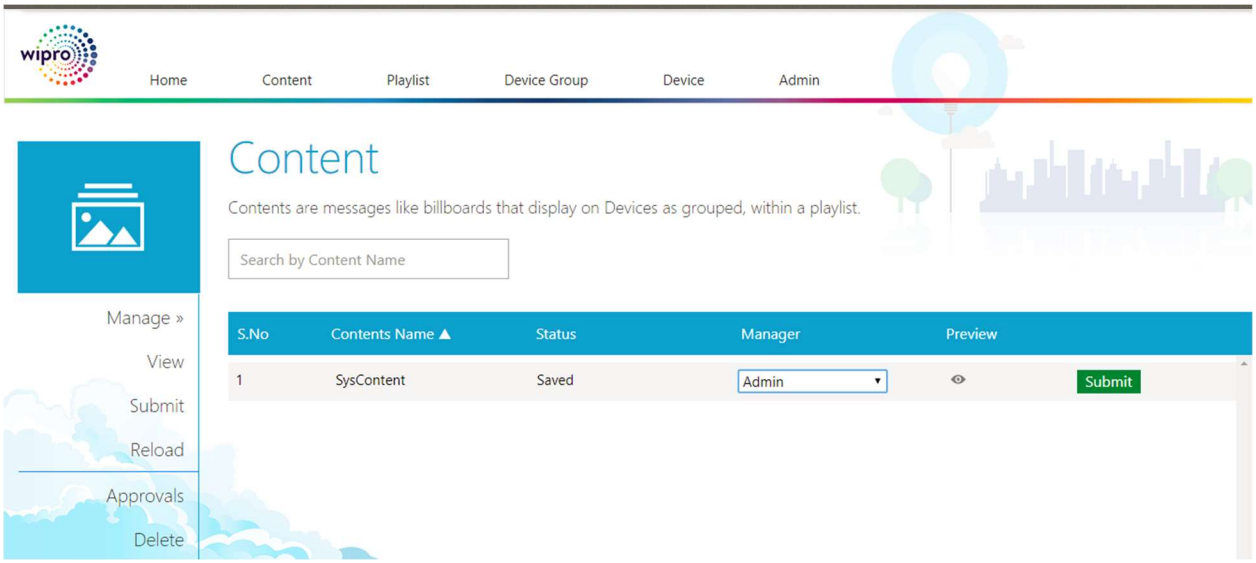


4. In the **Place holders** section, Enter the **Template Name** in the field and click **Save** button.



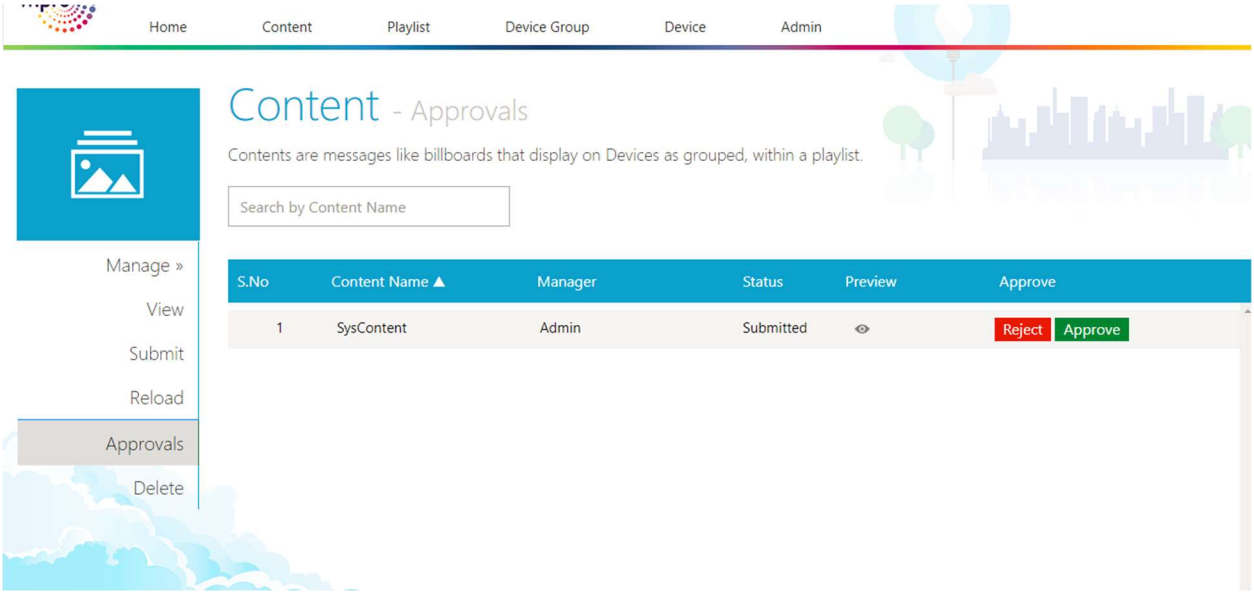
5. Click **Submit** button, the **Content** page is displayed as shown in the following figure. Select the manager as Admin





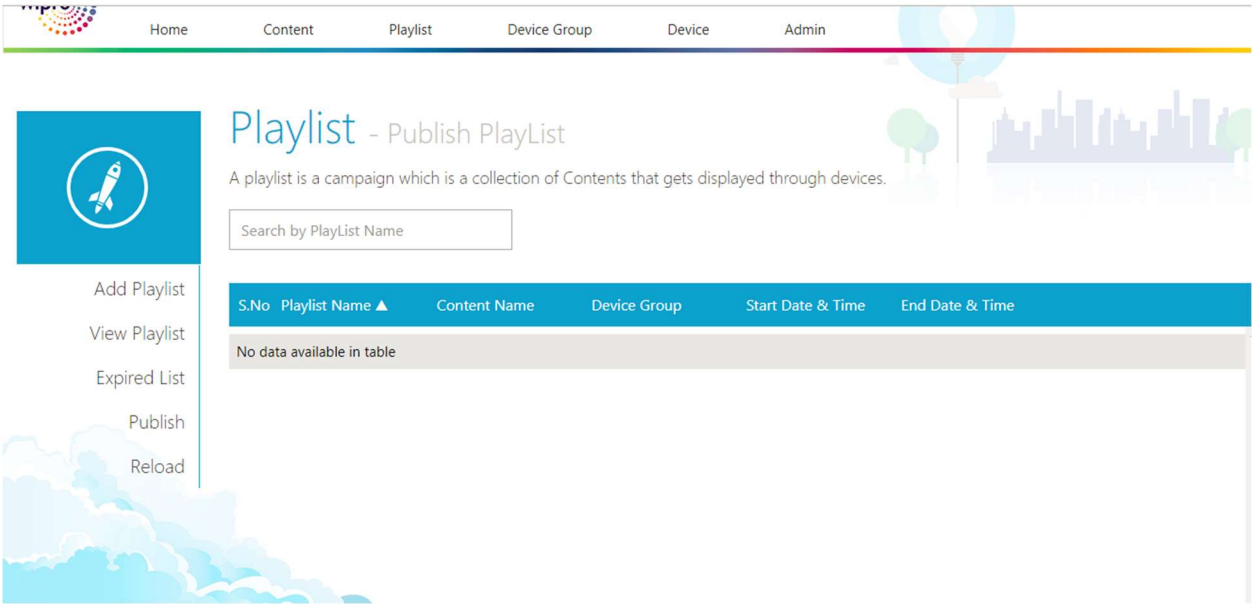
6. Select **View** from the left menu to display the list of contents that are added earlier.

7. Click **Approvals** to check the contents which are pending for Approval by the Admin.



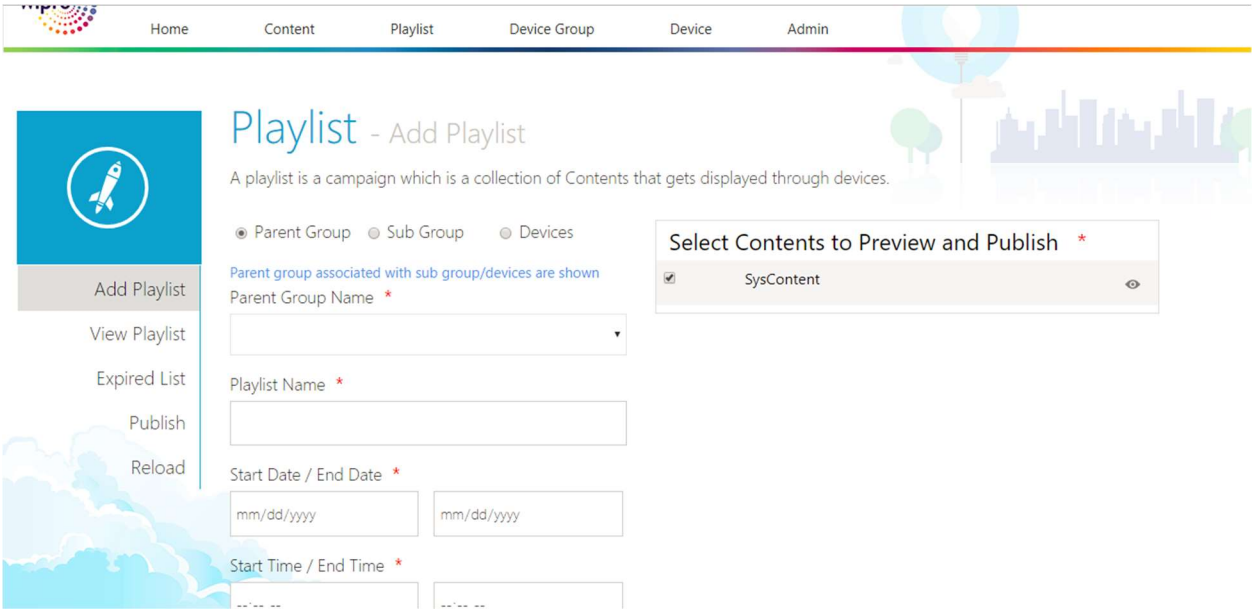
12.4. Playlist

Select "**Playlist**" from the top menu, the publish playlist page is displayed as shown in the following figure.



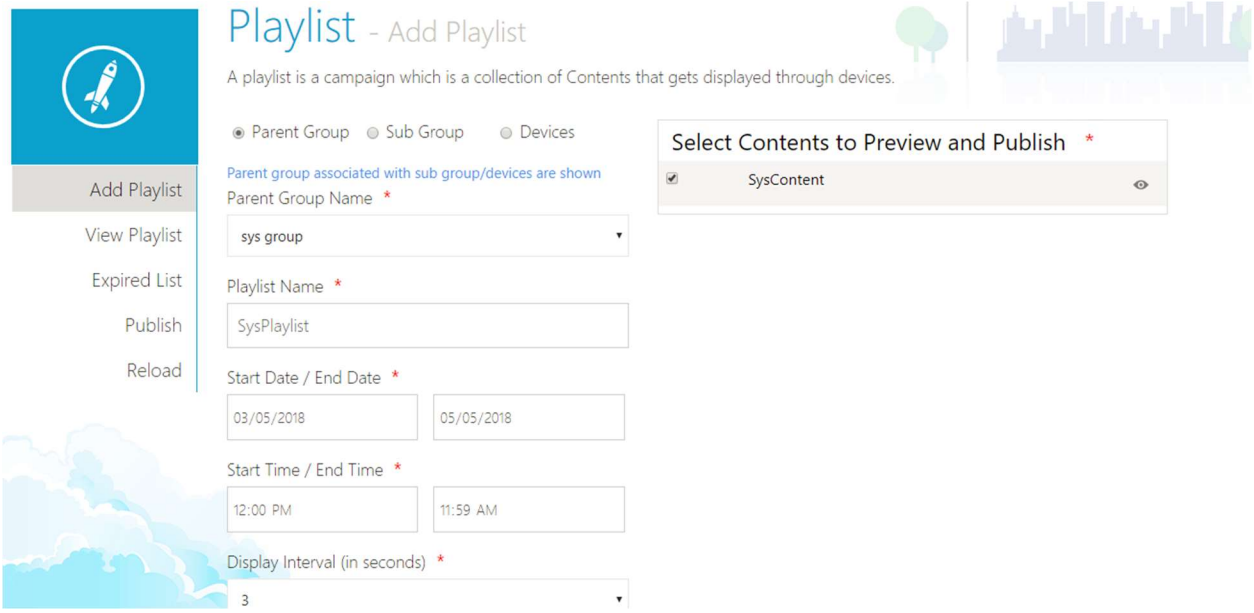
12.4.1. To Add a Playlist

1. Select "**Add Playlist**" from the left menu, the **Add Playlist** page is displayed as shown in the following figure.

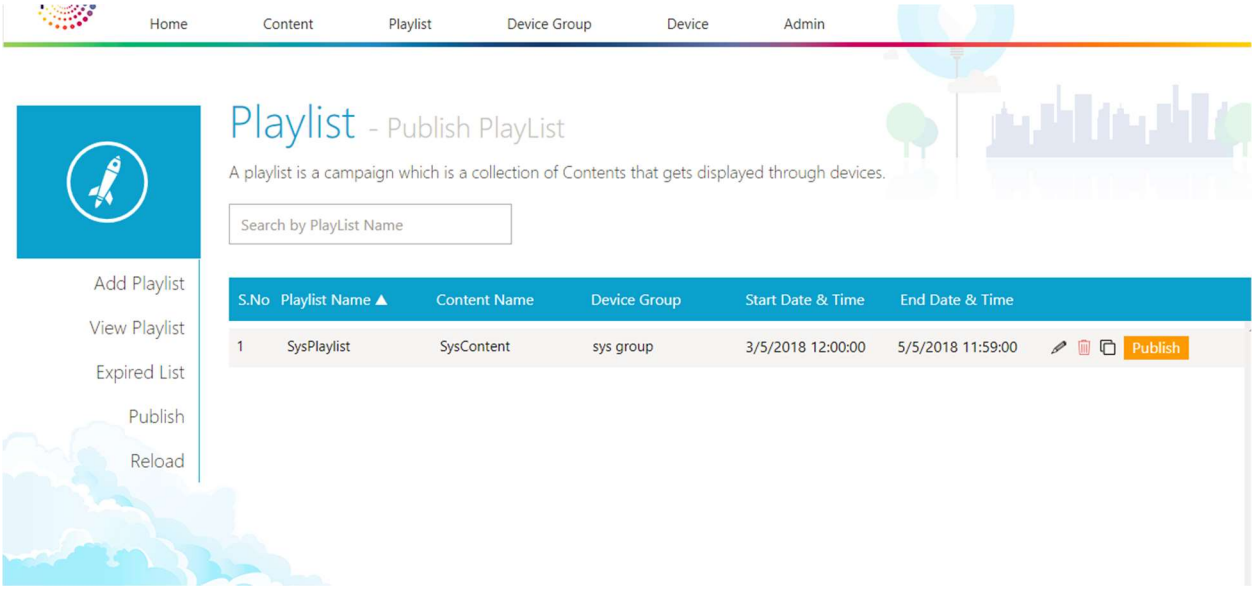


12.4.1.1. Define the settings for the playlist

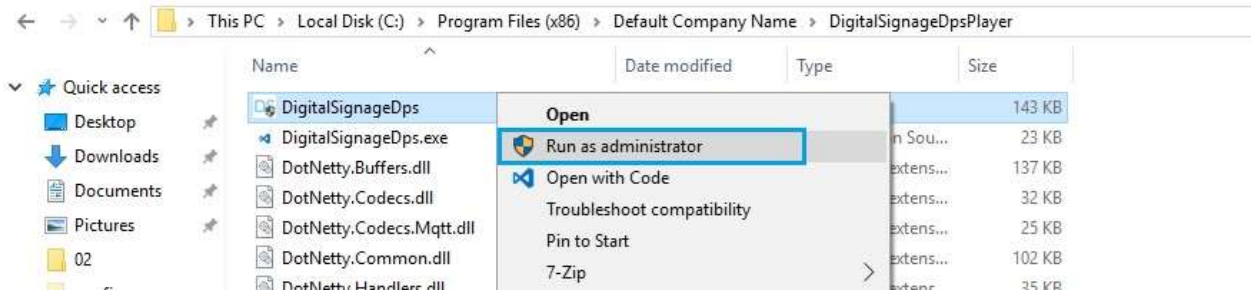
1. In the **Select Contents to Preview and Publish** section, Select one or more check boxes of the content for your Playlist as shown in the following figure.



2. Enter the **Playlist Name** in the respective field.
3. Enter the **Start/End Date** and **Start/End Time** in their respective fields.
4. Set the **Display Interval (In seconds) and Frequency** from the dropdown list.
5. Click **Save** button to save the Playlist is added,
6. Click **Publish** button, a message "**Playlist Published Successfully**" is displayed.



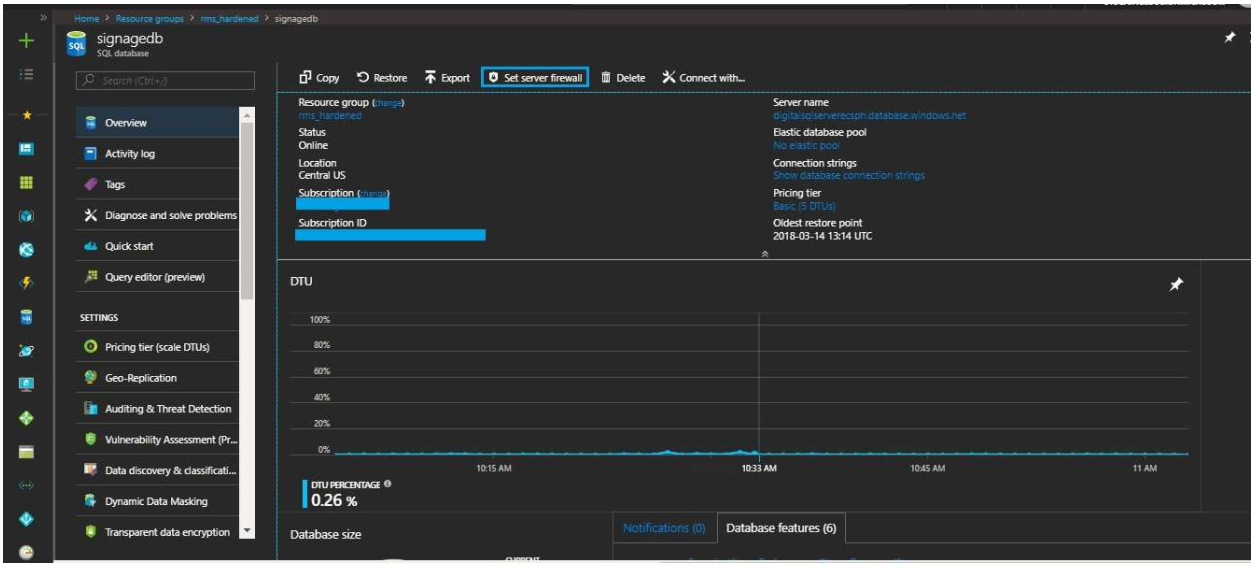
7. Run Digital signage player, Marriot image will appear.



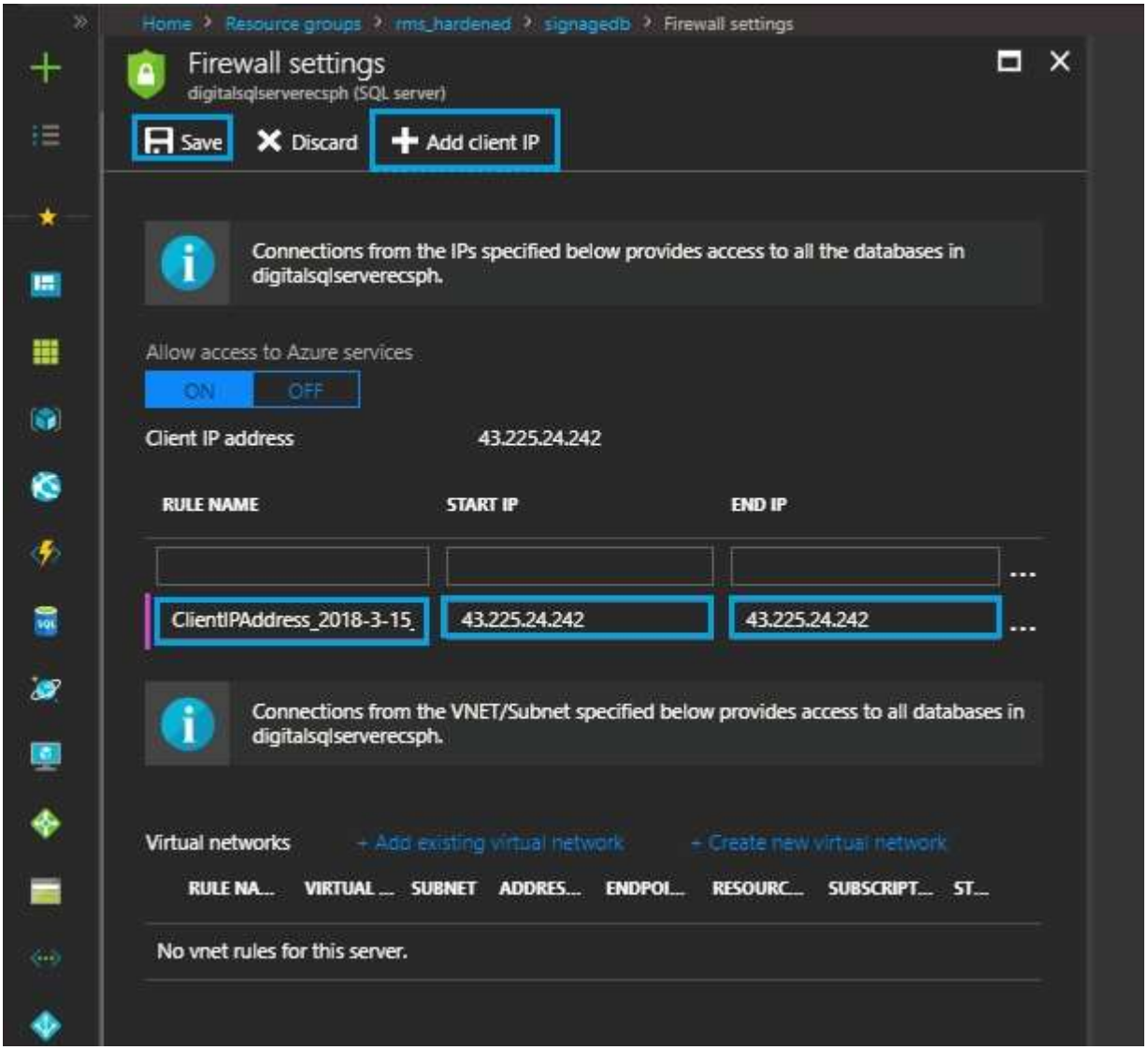
13. Validation

13.1. SQL Server verification

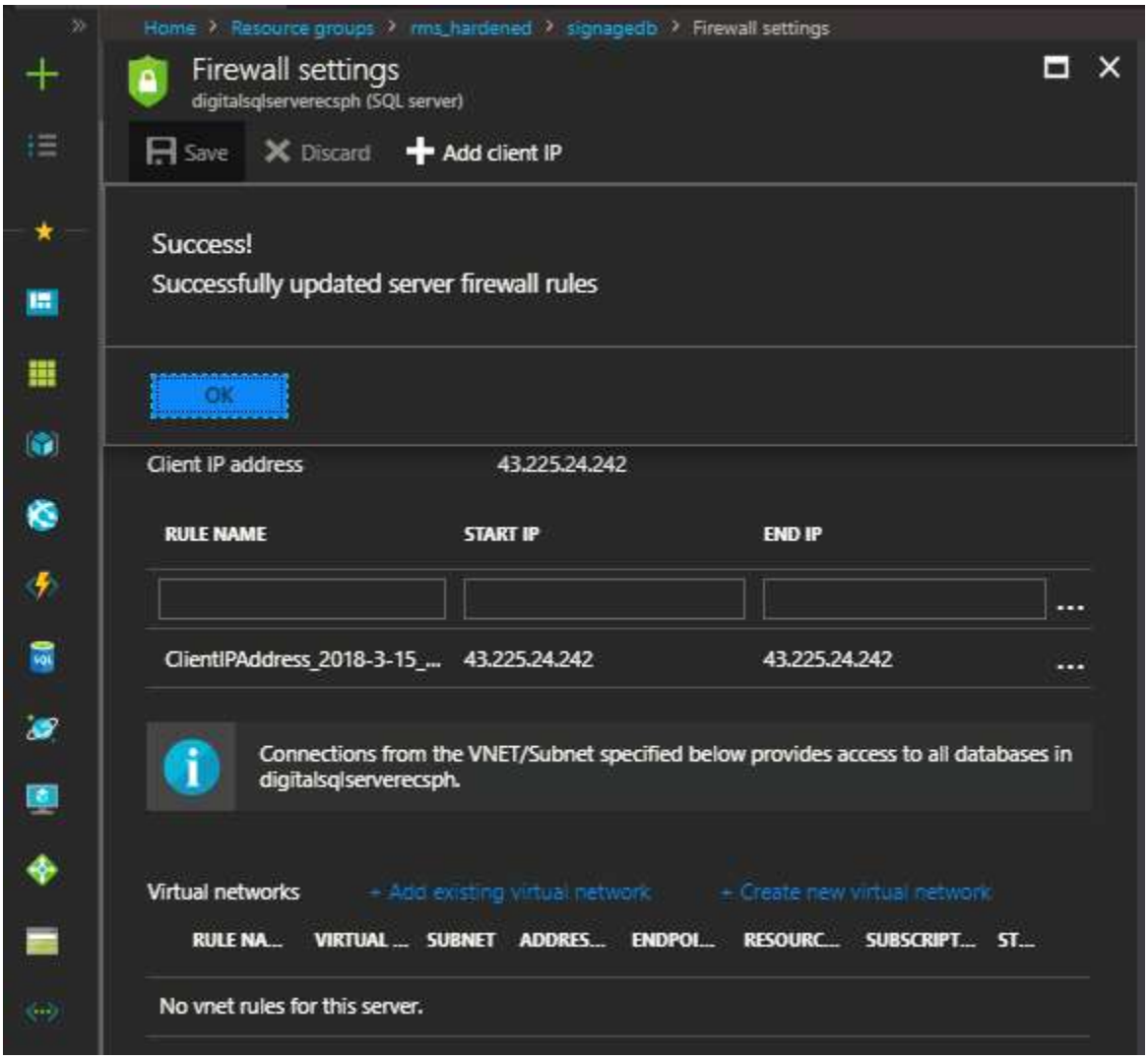
1. Go to the **Azure portal > Resource group** and click **set server firewall**.

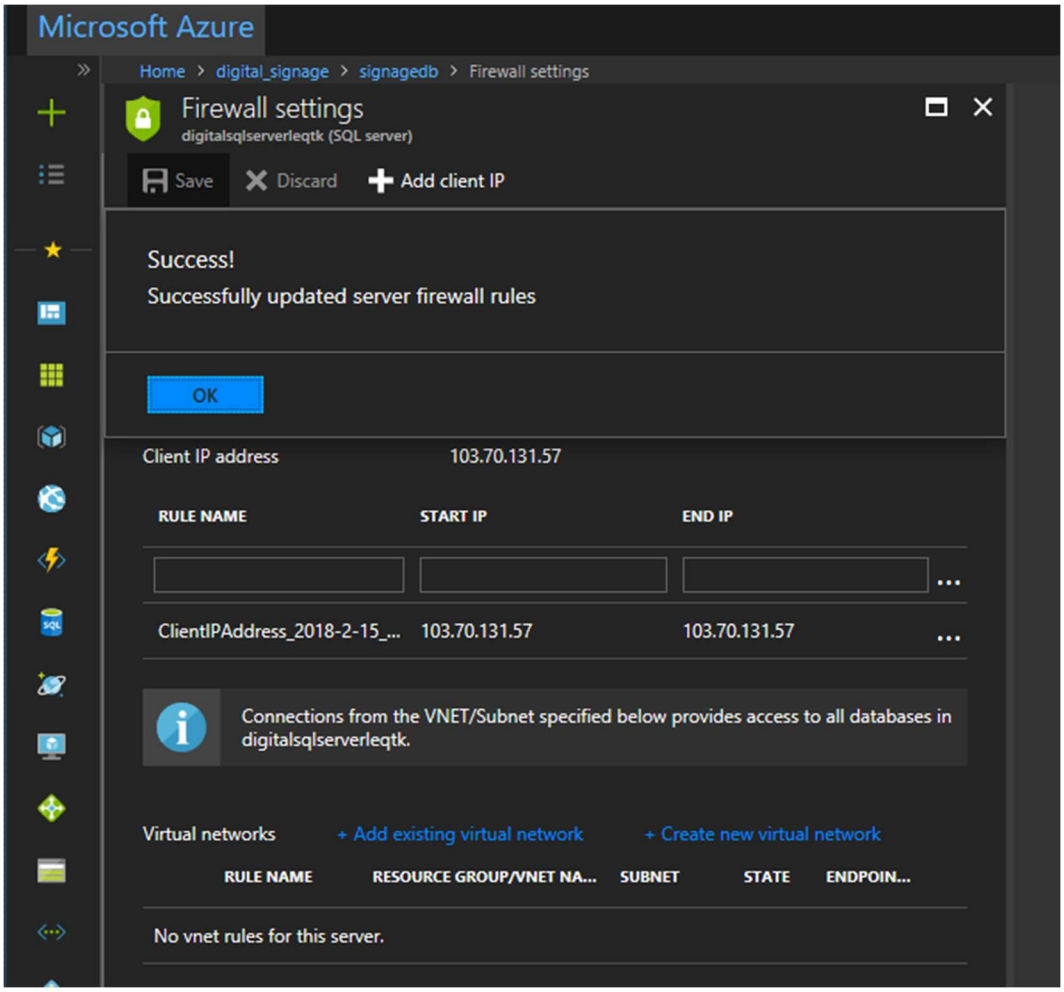


2. Go to **Firewall settings > + Add client IP**, update the firewall rules and click **Ok** button.

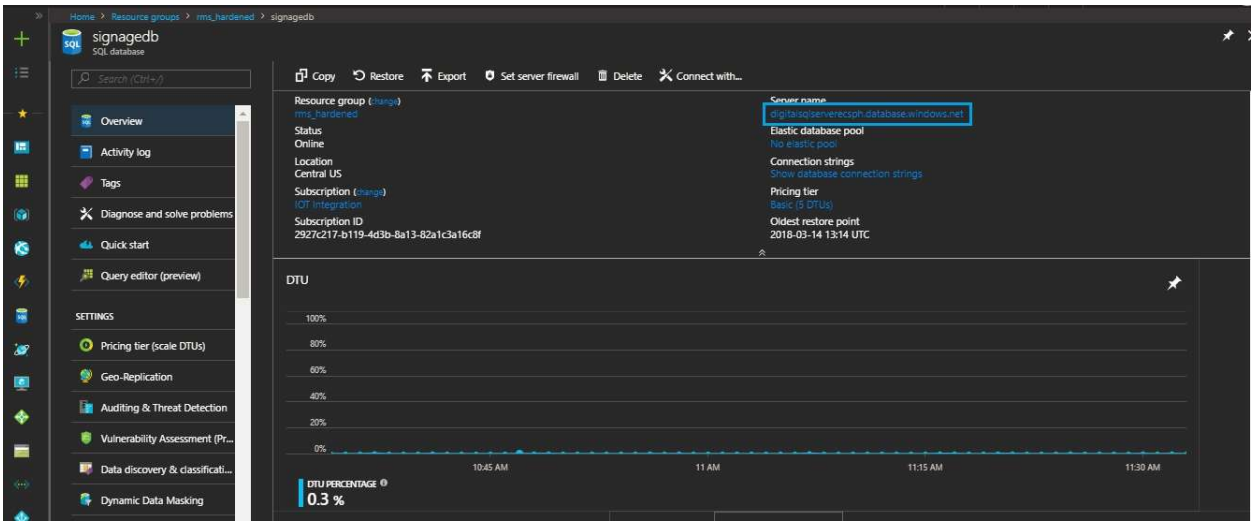


3. Click **Ok** button a message "***Success***!" is displayed as shown in the following figure.


Home > Resource groups > rms_hardened > signagedb > Firewall settings
Firewall settings
digitalsqlserverecsph (SQL server)
Save
Discard
Add client IP
Success!
Successfully updated server firewall rules
OK
Client IP address 43.225.24.242
RULE NAME
START IP
END IP
ClientIPAddress_2018-3-15_... 43.225.24.242 43.225.24.242
Connections from the VNET/Subnet specified below provides access to all databases in digitalsqlserverecsph.
Virtual networks
+ Add existing virtual network
+ Create new virtual network
RULE NA... VIRTUAL ... SUBNET ADDRES... ENDPOI... RESOURC... SUBSCRIPT... ST...
No vnet rules for this server.

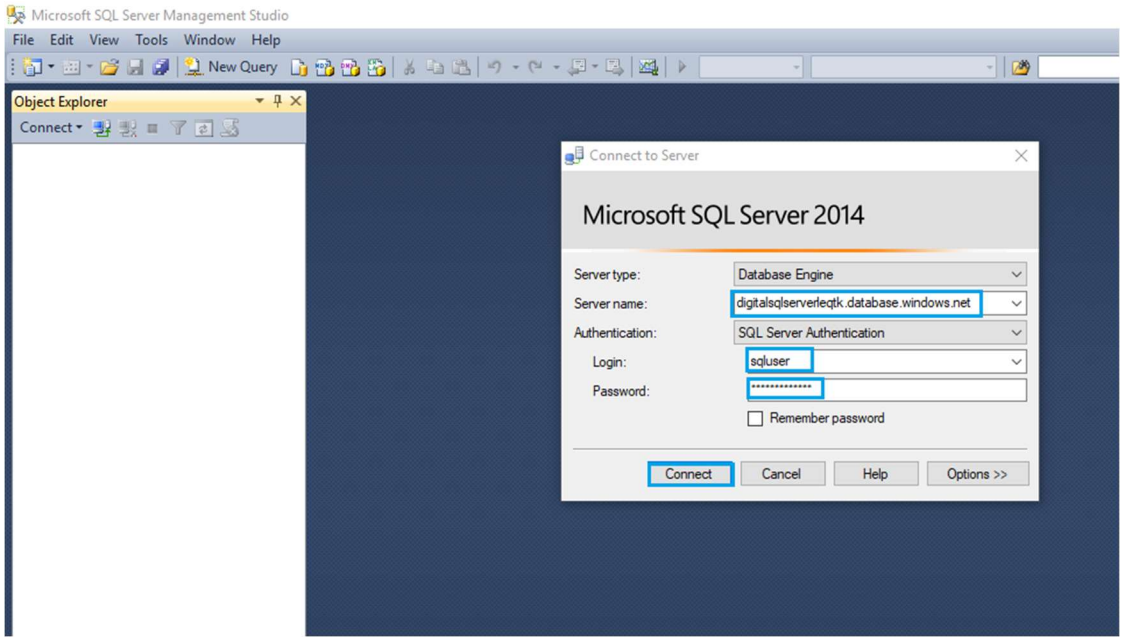


4. Open **Azure portal** and copy the server name.

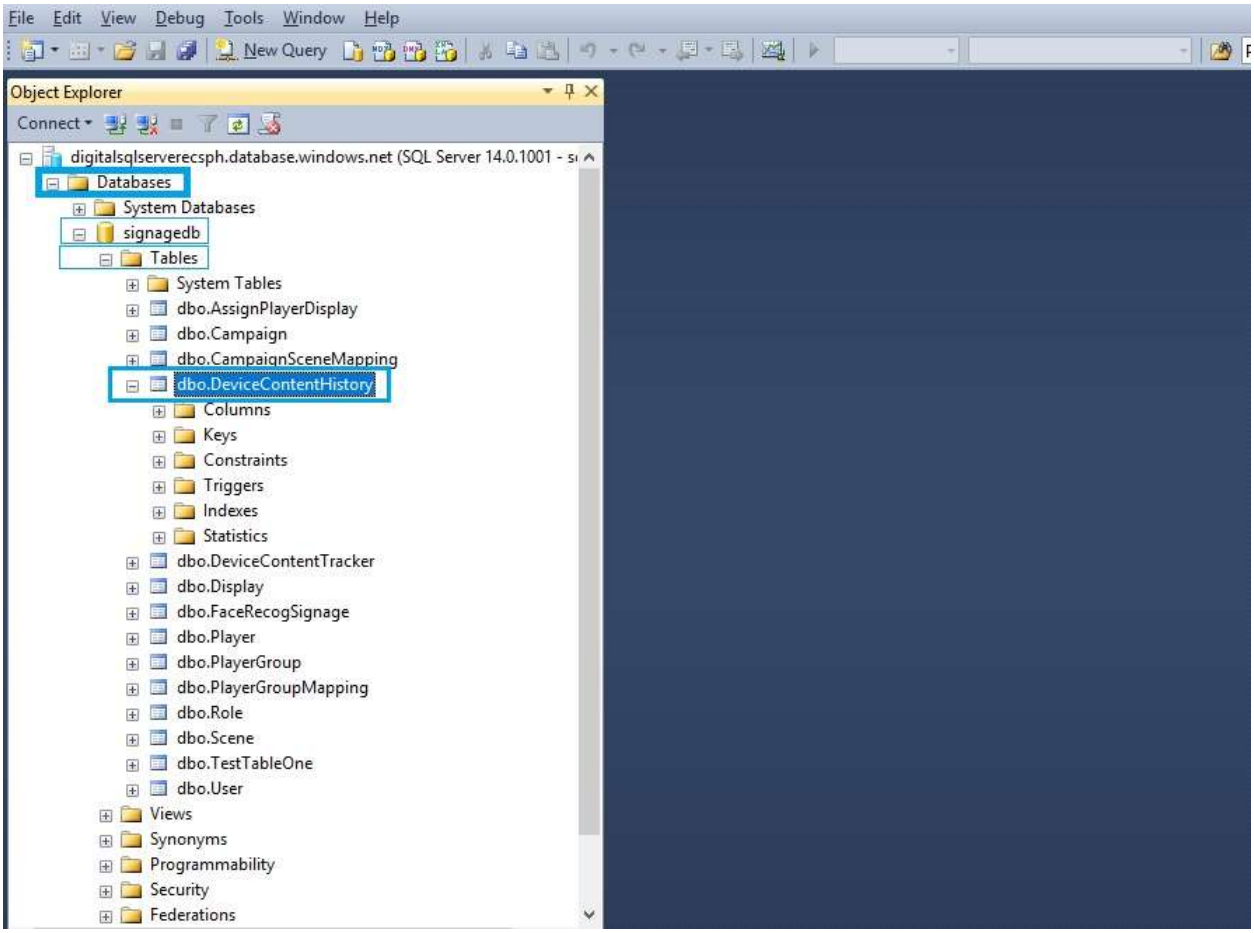


5. Open **SQL management server** and paste the copied **Server name** in the respective field.

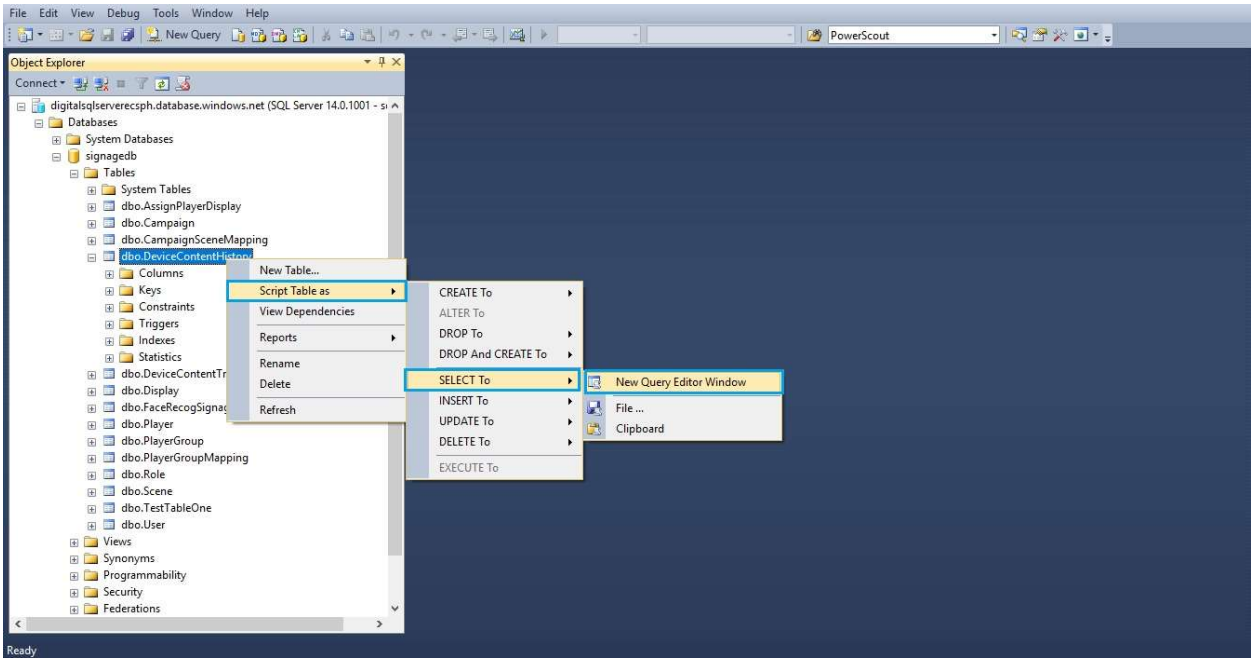
6. Enter the Login and password which are provided for SQL at the time of template deployment and click **Connect** button.



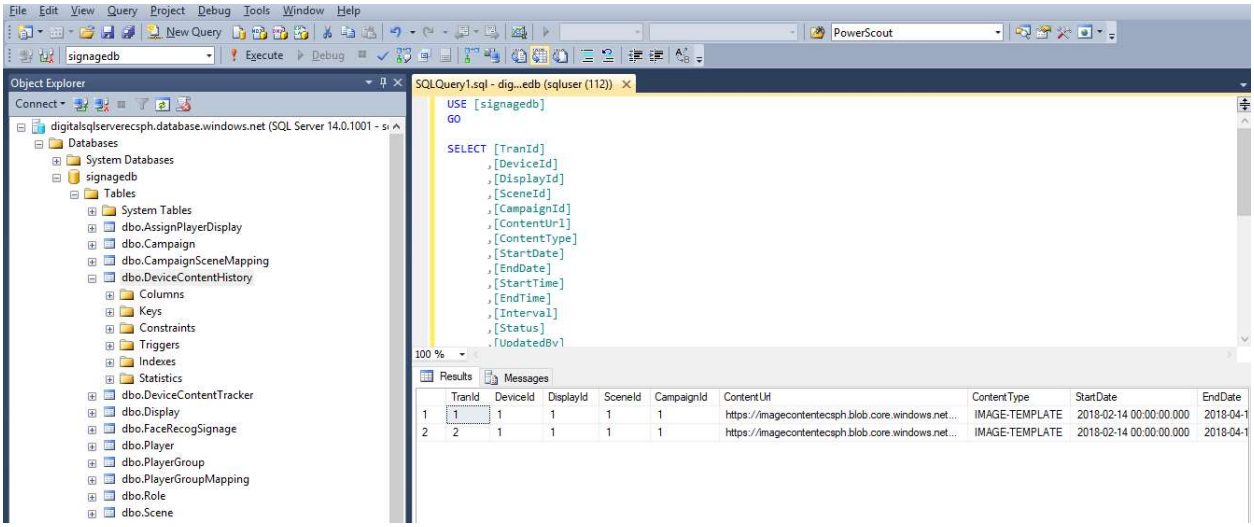
7. Navigate to **Databases > System Databases > Tables** and select the table as shown in the following figure.



8. Right click on **dbo.devicecontent.tracker** table and click **Select top 1000 rows** option.

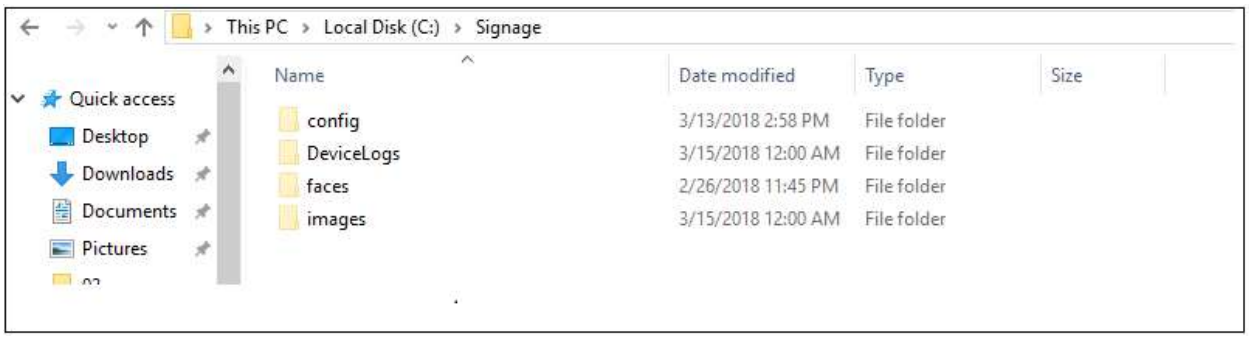


9. The table is displayed as shown in the following figure.

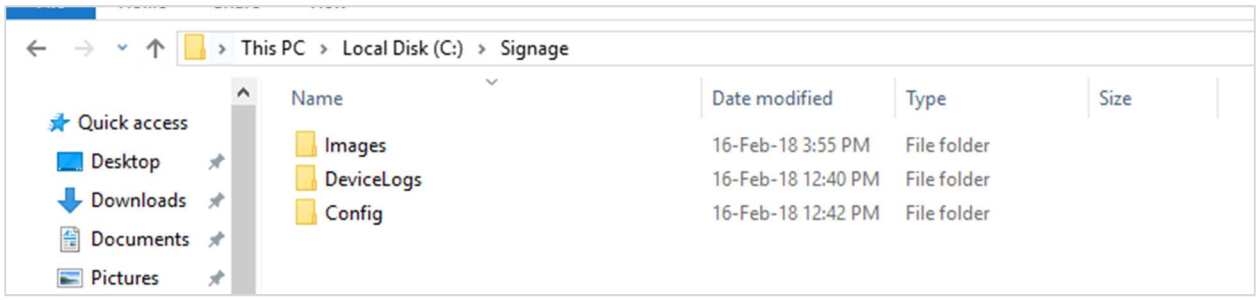


13.2. Stick VM Cache Verification

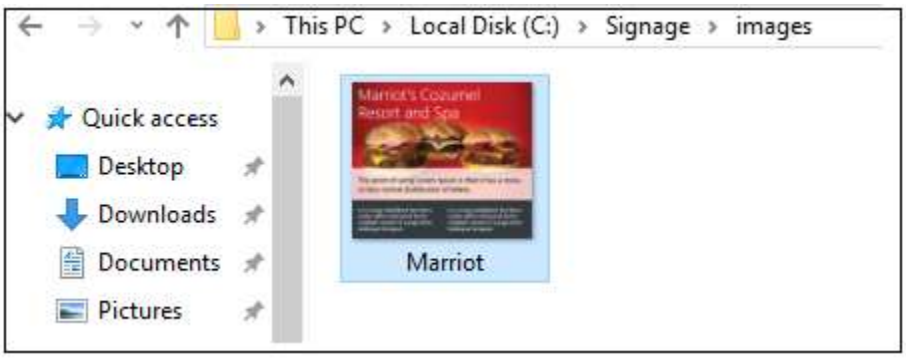
1. Go to **Local disk (C:)** > **Device** to verify deviceconfig.xml



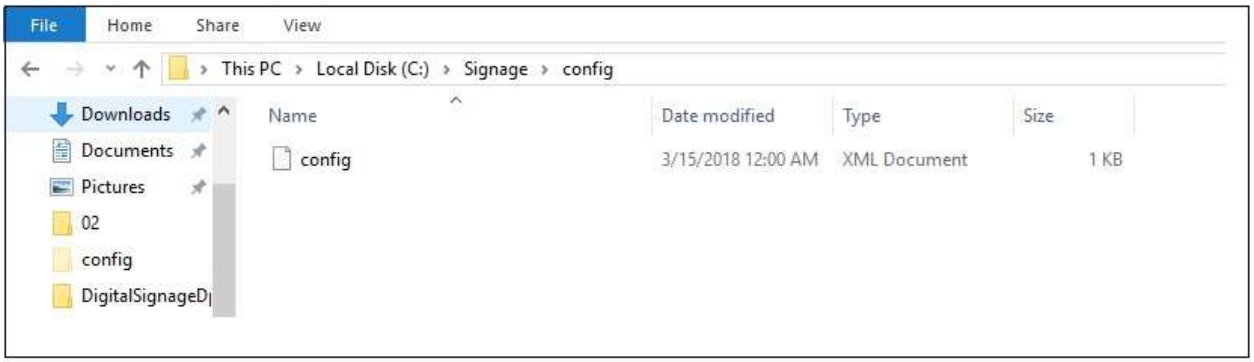
2. Go to **Local Disk (C:) > Signage** to verify.



3. Go to **Local Disk (C:) > Signage > Images** to verify the images

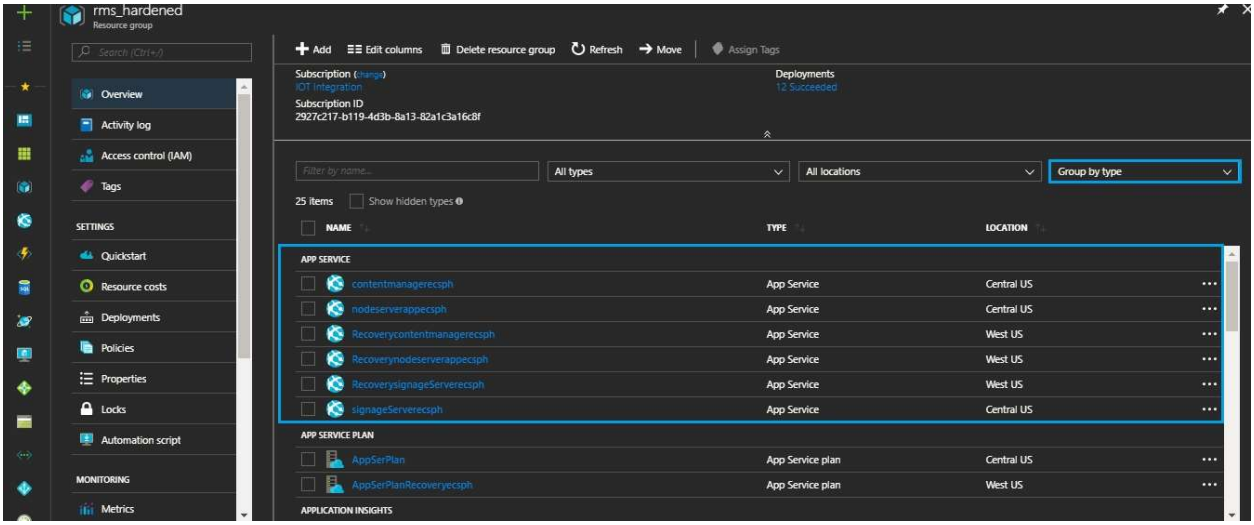


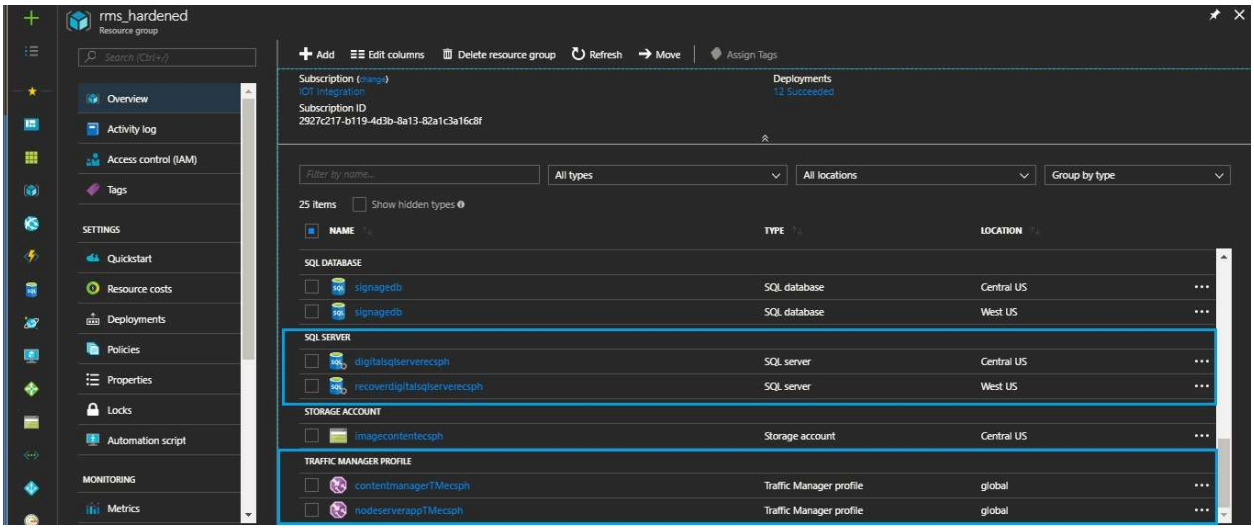
4. Go to **Local Disk (C:) > Signage > Config** to check the config.xml



13.3. DR Validation

1. Go to **Azure portal** > **resource group** > select **group by type** option as shown in the below figure.





Content Manager URLS:

Primary Content Manager URL : https://contentmanagerecsph.azurewebsites.net

Secondary Content Manager URL : https://Recoverycontentmanagerecsph.azurewebsites.net

Node Server URLS:

Primary Node Server URL : https://nodeserverappecsph.azurewebsites.net

Secondary Node Server URL : https://Recoverynodeserverappecsph.azurewebsites.net

Signage Server URLS:

Primary Signage Server URL : https://signageServerecsph.azurewebsites.net

Secondary Signage Server URL : https://RecoverysignageServerecsph.azurewebsites.net

Traffic Manager URLS:

Traffic Manager web app URL : http://contentmanagerTMecsph.trafficmanager.net

Traffic Manager Node Server URL : http://nodeserverappTMecsph.trafficmanager.net

SQL server URLS:

SQL Server URL : digitalsqlserverecsph.database.windows.net

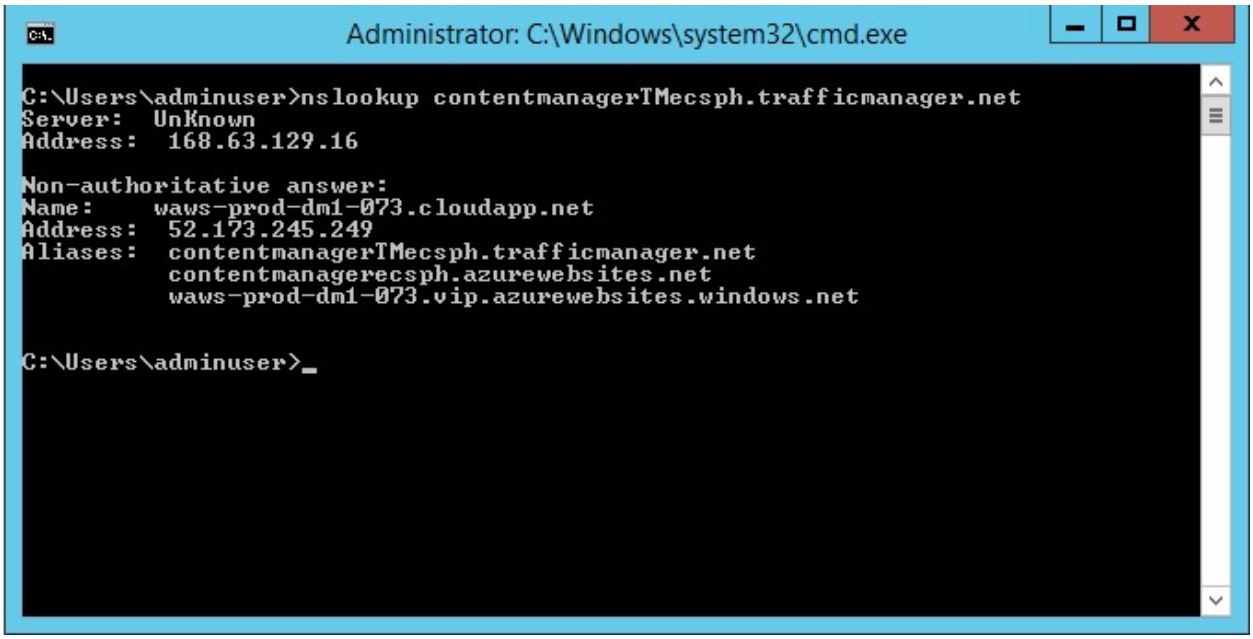
SQL Server URL : recoverdigitalsqlserverecsph.database.windows.net

13.3.1. Traffic Manager

1. Open command prompt & run the following command

`nslookup <trafficmanagerwebappuri>` which is copied from output section.

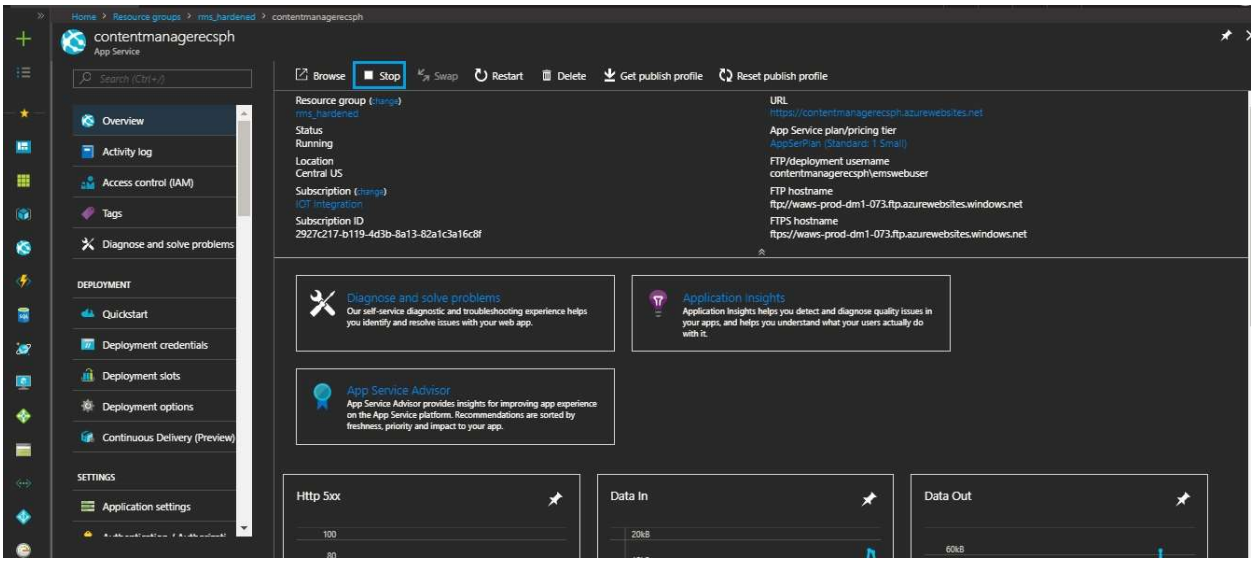
`nslookup contentmanagerTMecsph.trafficmanager.net`



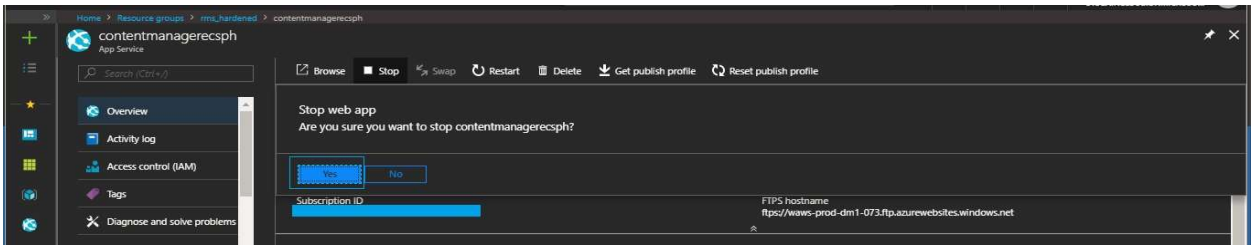
When both Content Manager Applications are up and running. The Traffic redirected Primary Content Manger web app(contentmanagerecsph.azurewebsites.net) as Priority is 1.

2. Stop the Primary Content Manager web app

3. Go to **resource group** > **contentmanagerecsph** > **overview** > **click on stop**



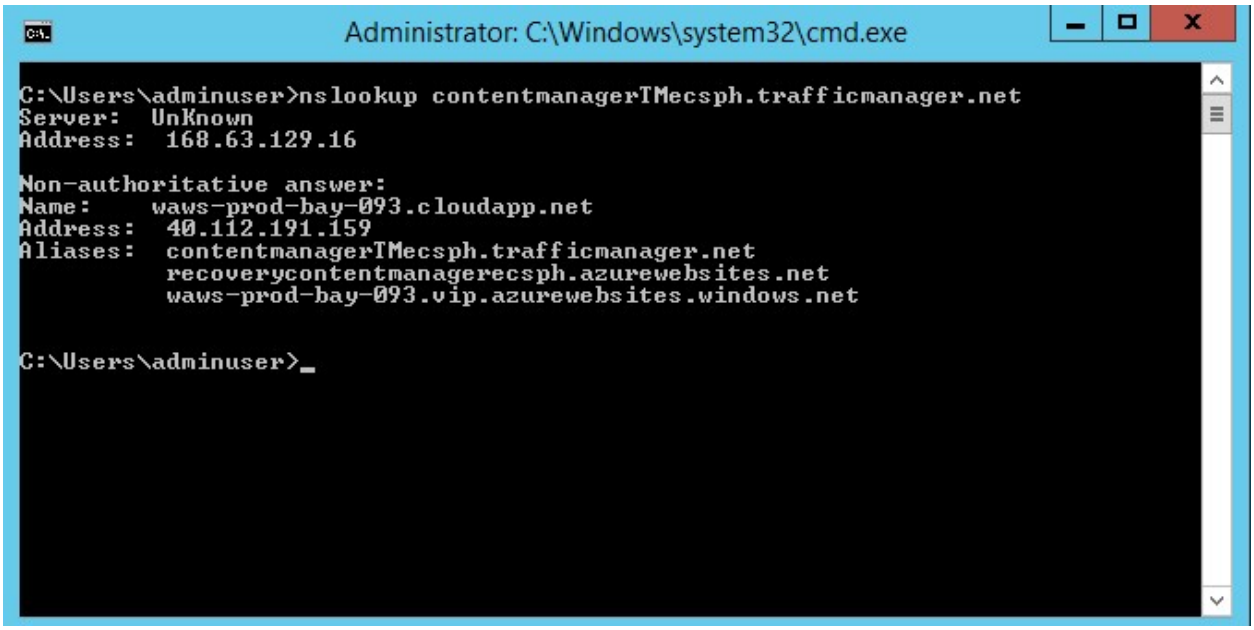
4. Click **Yes** to stop.



5. Open command prompt & run the following command

`nslookup <trafficmanagerwebappuri>` which is copied from output section.

`nslookup contentmanagerTMecsph.trafficmanager.net`

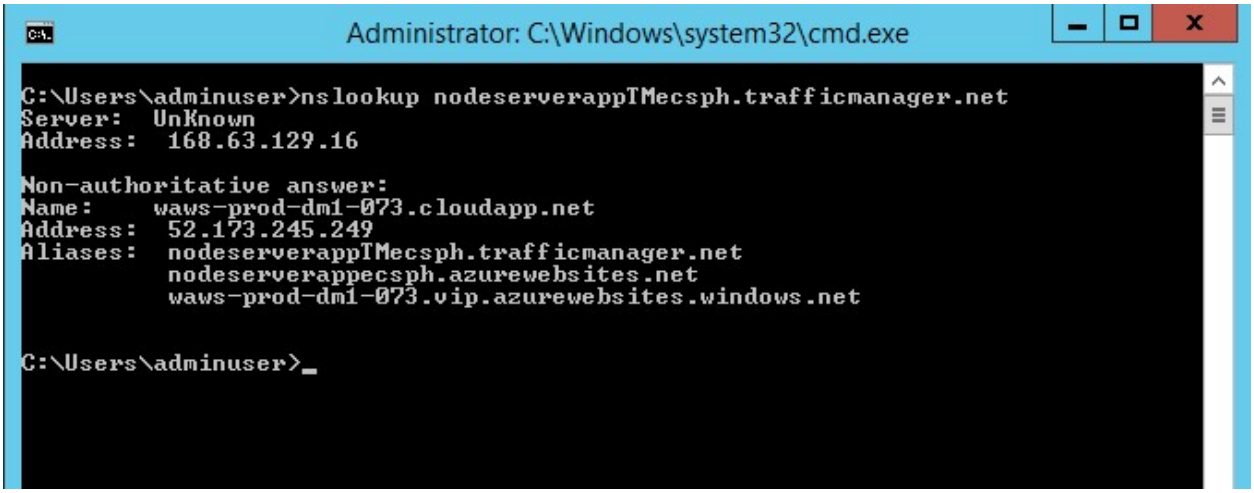


When Primary Content Manager Web Application is stopped. The Traffic Manger redirects data to Secondary Content Manager Web Application (recoverycontentmanagerecsph.azurewebsites.net).

6. Open command prompt & run the following command

`nslookup <trafficmanagernodeserveruri>` which is copied from ouputs section.

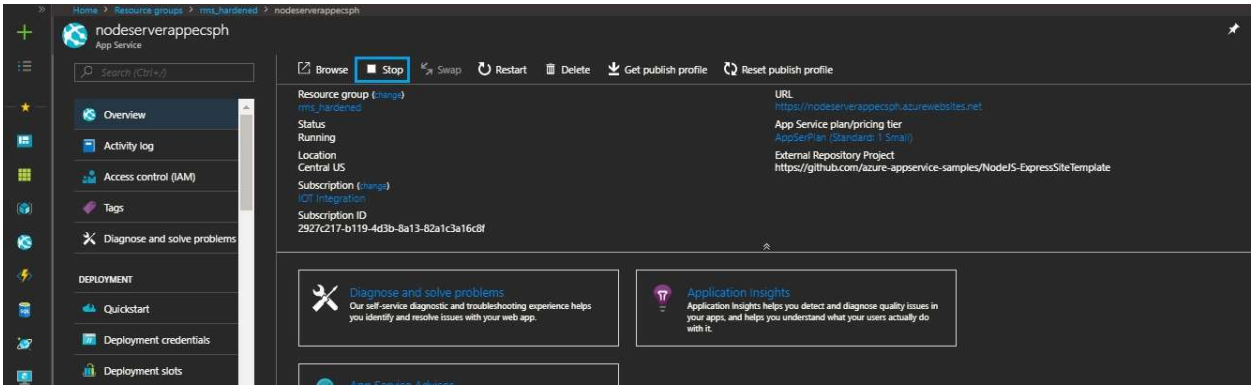
`nslookup nodeserverappTMecsph.trafficmanager.net`



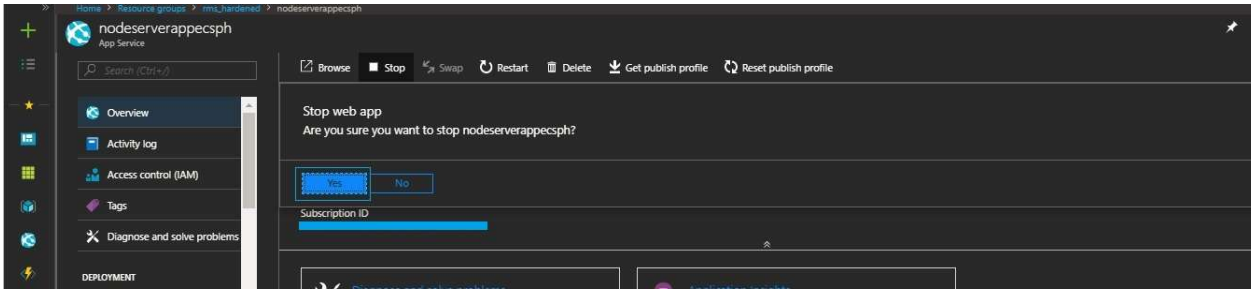
When both Node Server Applications Are up and Running. The Traffic redirected Primary Node server web app(nodeserverappecsph.azurewebsites.net) as Priority is 1.

7. Stop the Primary node server web app

8. Go to **Resource group** > **nodeserverappecsph** > **overview** > click **Stop**



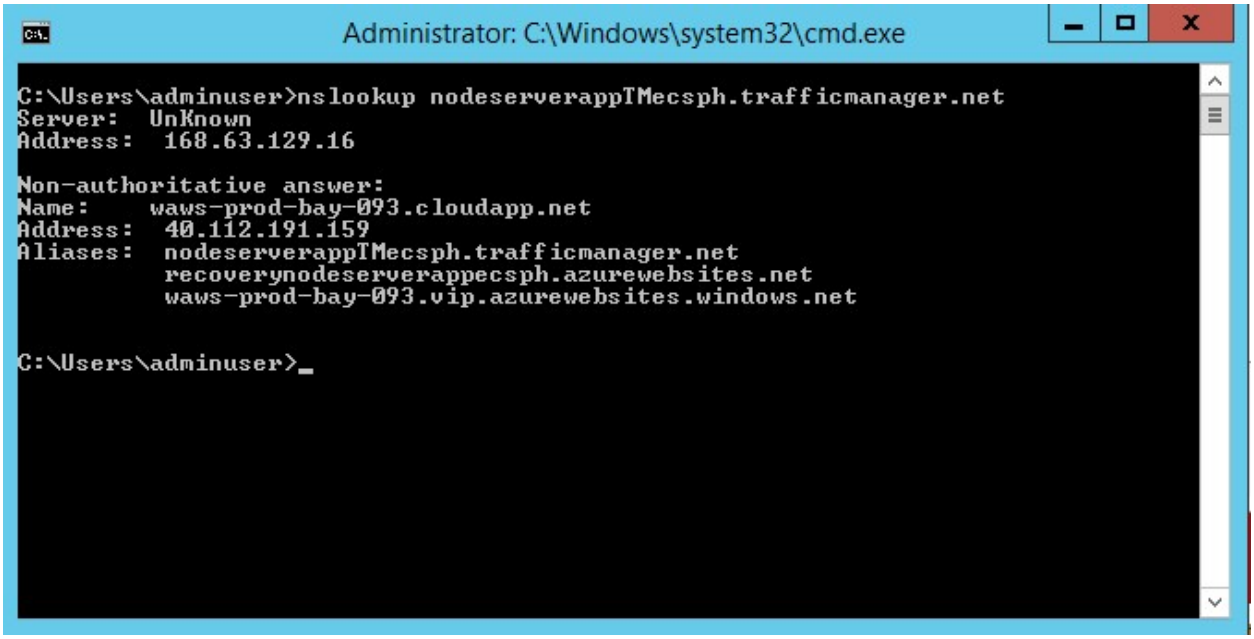
9. Click **Yes** to stop.



10. Open command prompt & run the following command

nslookup <trafficmanagernodeserveruri> which is copied from output section.

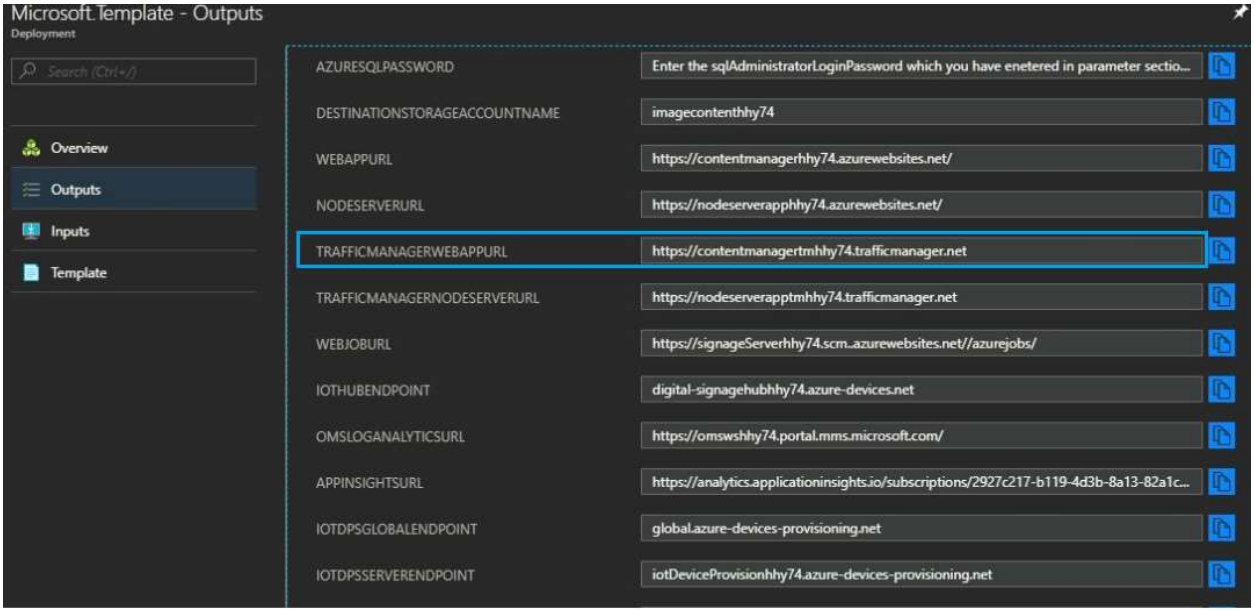
nslookup nodeserverappTMecsph.trafficmanager.net



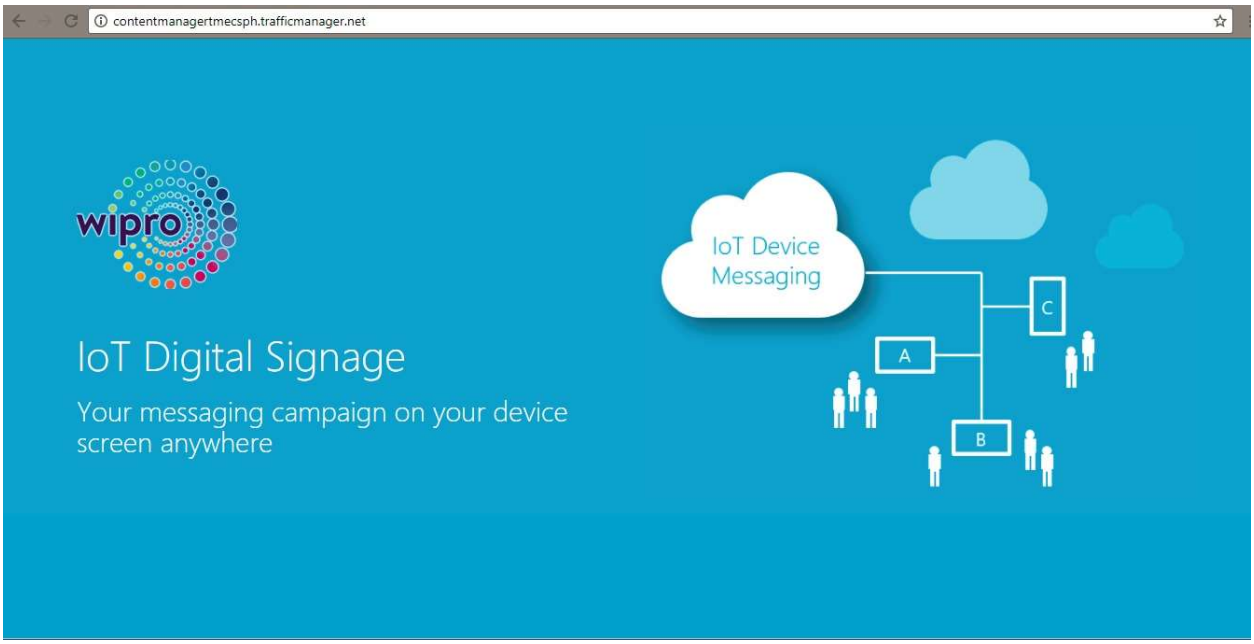
When Primary node server Web Application is stopped. The Traffic Manger redirects the data to Secondary node server web Application(recoverynodeserverappecsph.azurewebsites.net).

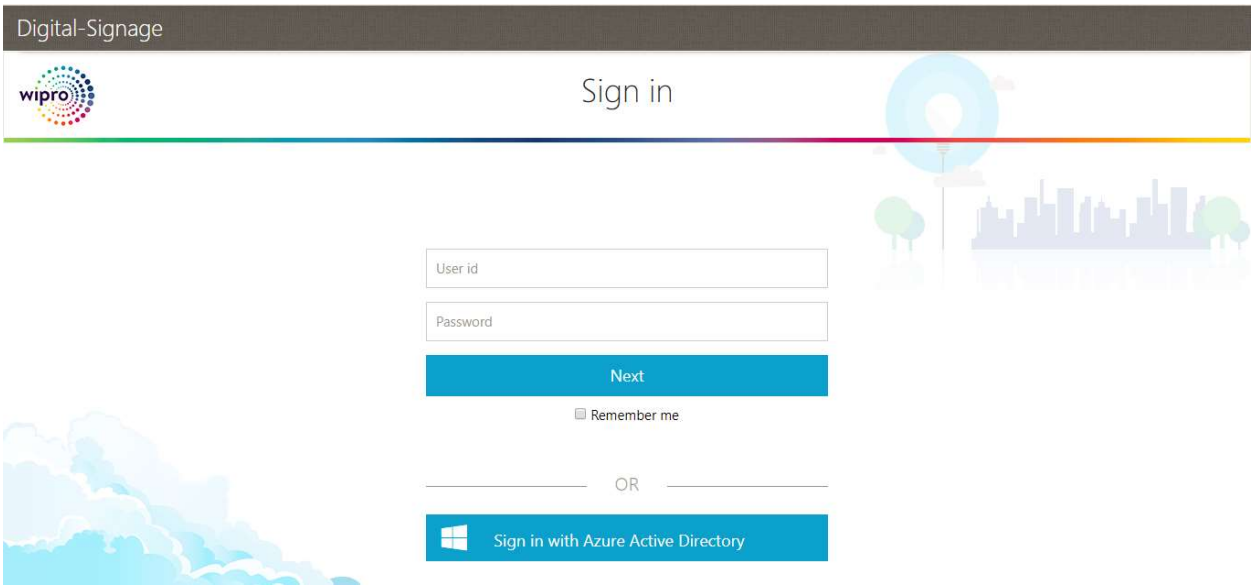
13.3.2. Sign in to DigitalSignage UI

1. Copy and paste the traffic manager web app url from the output section in a browser.
2. Go to **resourcegroup** > **deployments** > **Microsoft Template** > **outputs**
3. Copy the **TRAFFICMANAGERWEBAPPURL** and paste it in a browser.



4. The following page is displayed.

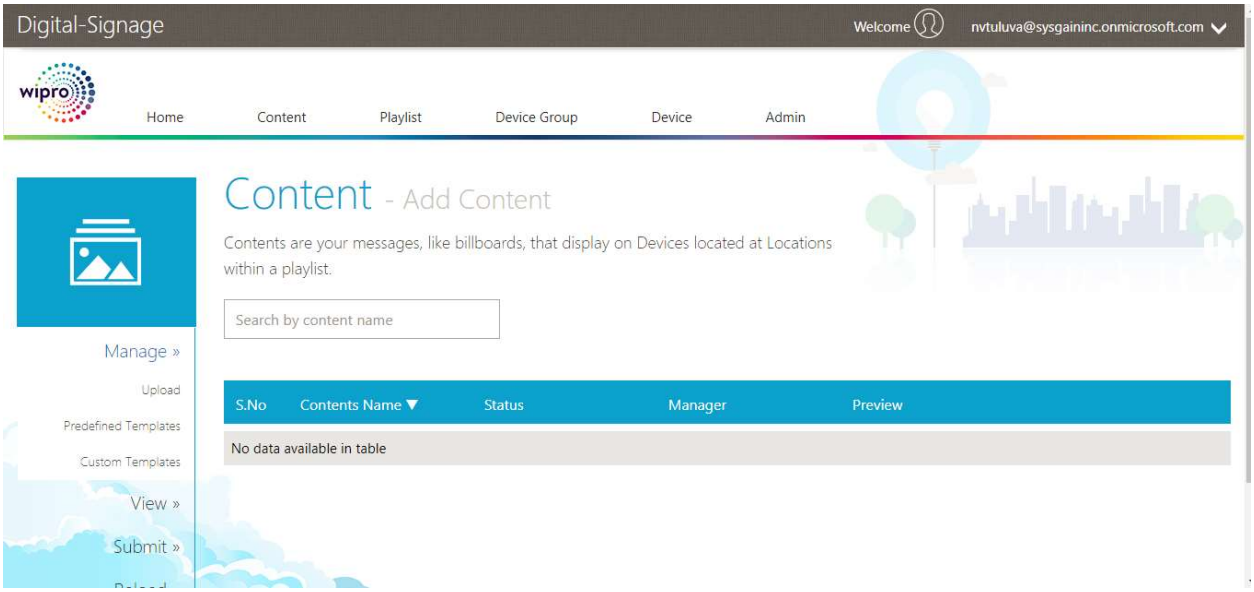




5. Provide User id as ***Admin*** & password as ***Admin*** or sign in using azure AD with your Microsoft account.

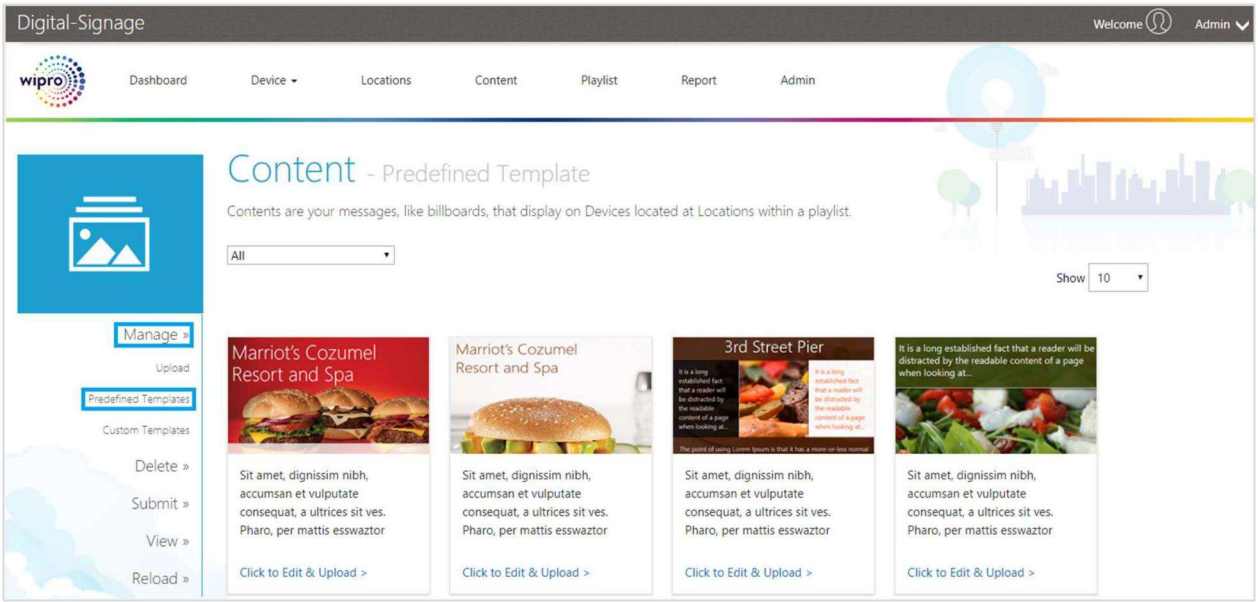
6. The following **Dashboard** appears after successful sign in.

7. Select "**Content**" from the top menu. You can upload your own content, usually an image with text that you have created, or you can select a Template and create your Content with the Template tool.



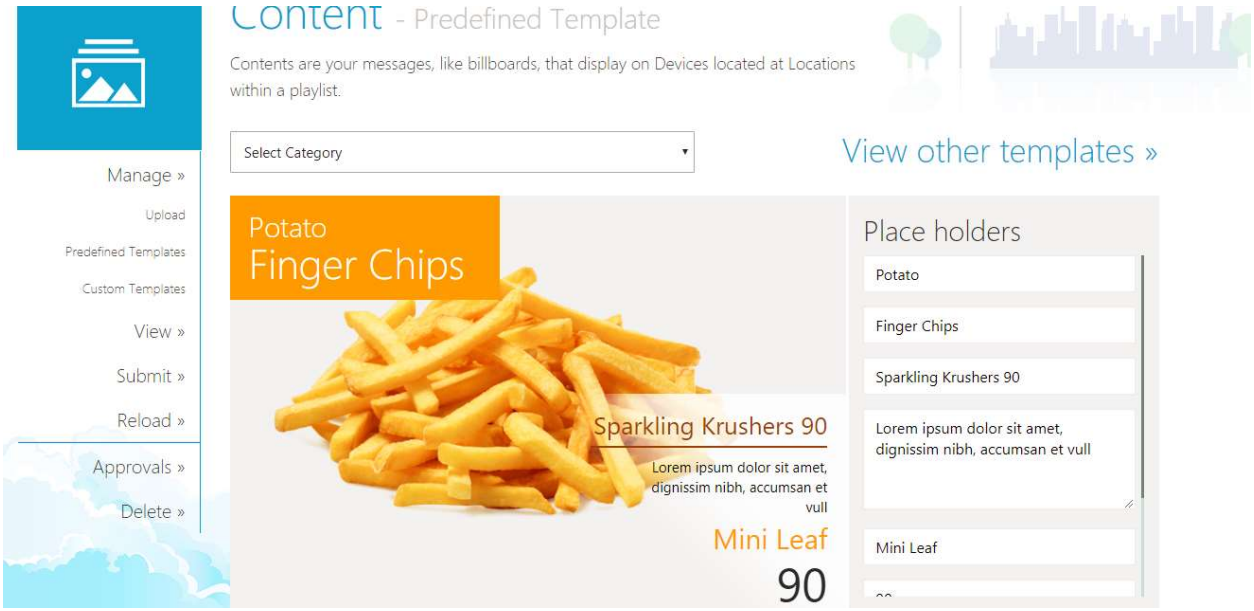
13.3.2.1. Add Content – Predefined Template

1. Select "**Manage** > **Predefined Template**" from the left menu. This is your message composed of images and text that will appear on devices at your Content within your playlist.

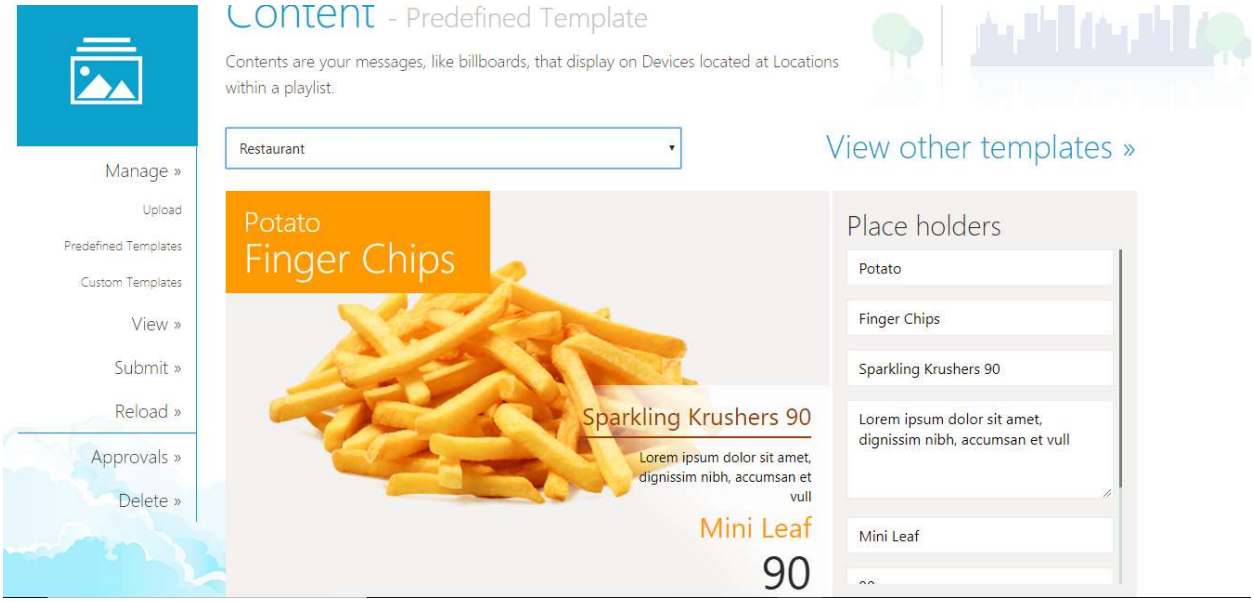


2. Choose a Template and select "**Click to Edit and Upload**." As shown in the following figure.

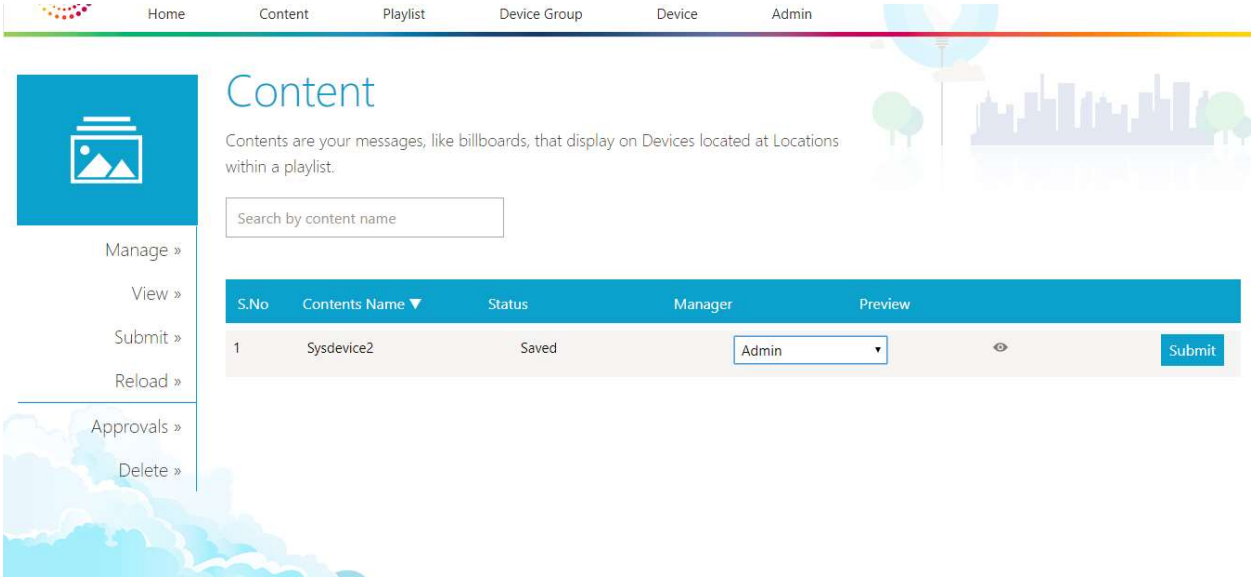
3. Choose a static template to Customize with your images and text.



4. Select the category from the dropdown list as shown in the following figure.

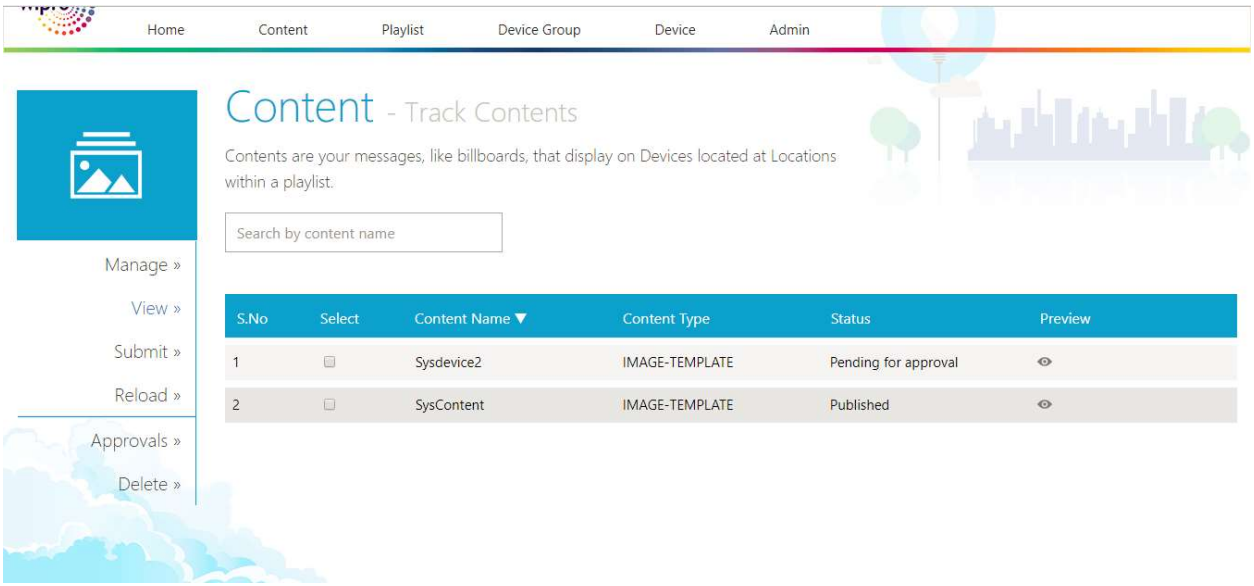


5. In the Place holders section, Enter the Template Name in the field as **Potato, Finger Chips** and click **Save** button the following page is displayed.

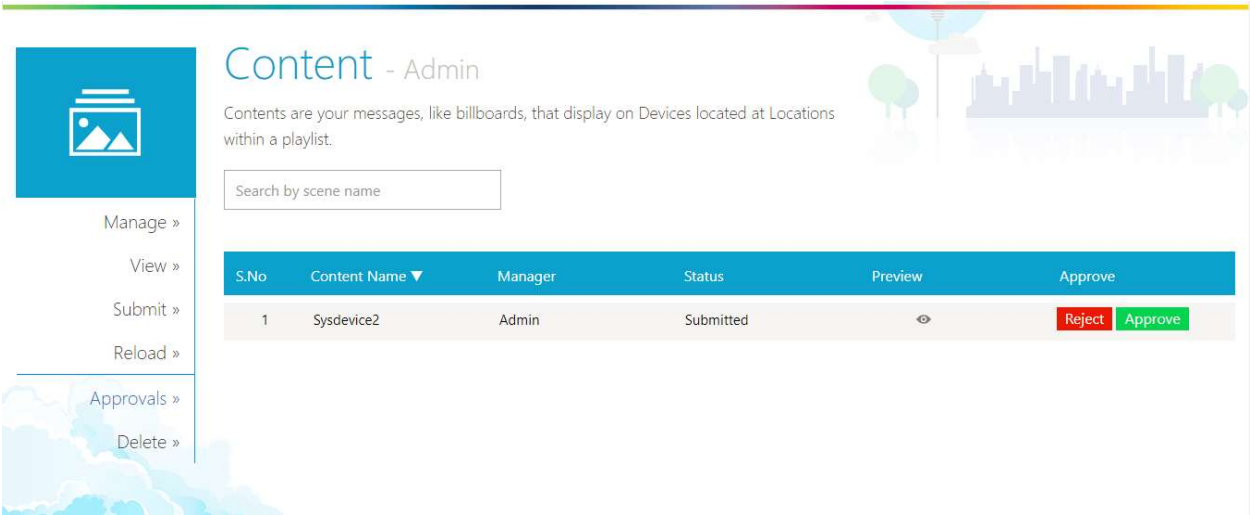


6. Select **Manager** as Admin & Click **Submit** button, the Content page is displayed.

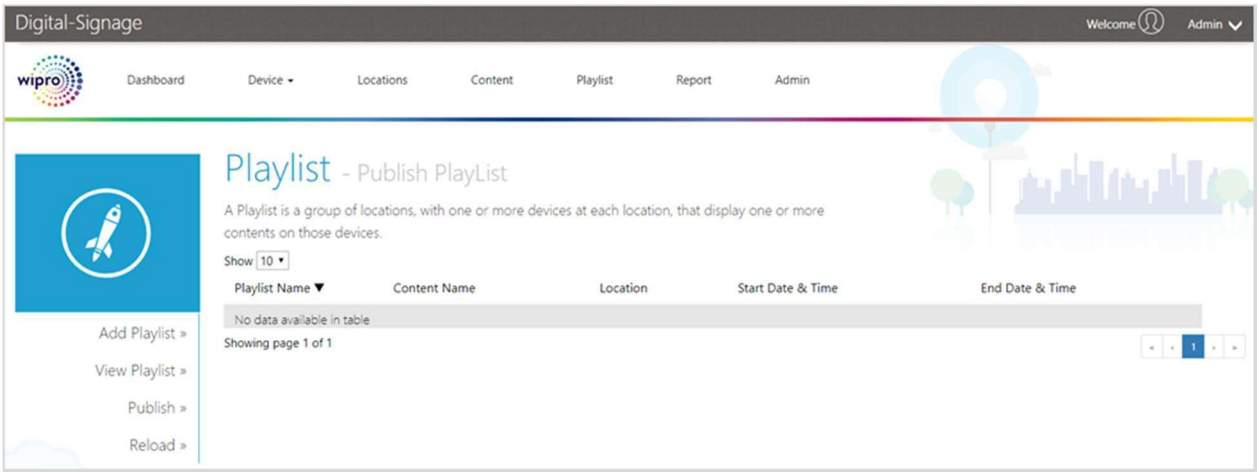
7. Select **View** from the left menu to display the list of contents that are added earlier as shown in the following figure.



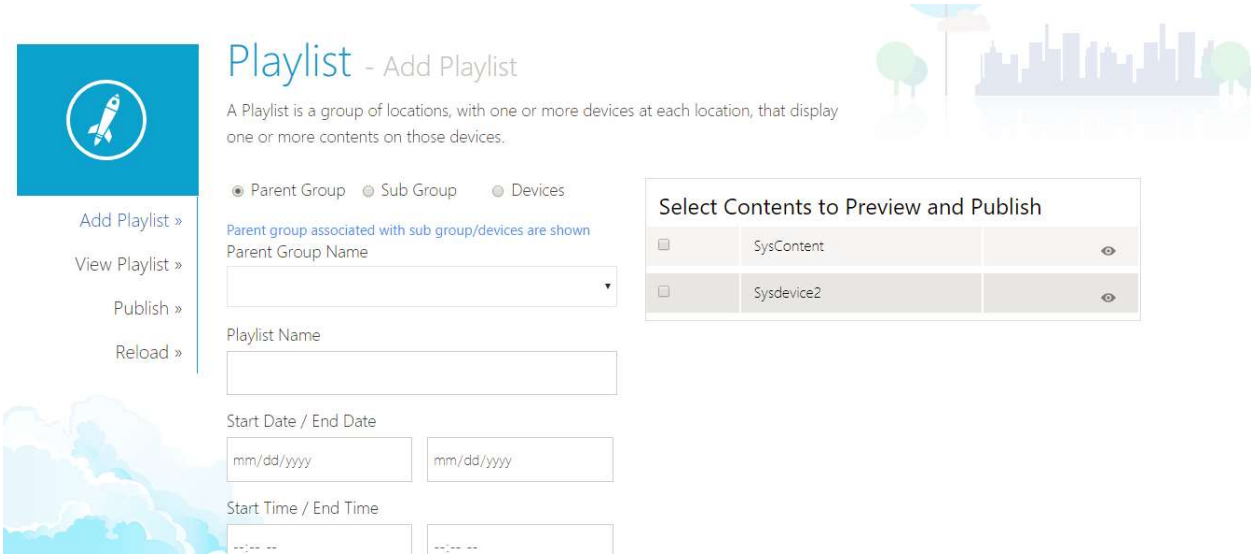
8. Go to **Approvals** section and Click **Approve** button to approve the Content.



9. Select "**Playlist**" from the top menu, the **Publish Playlist** page is displayed as shown in the following figure.

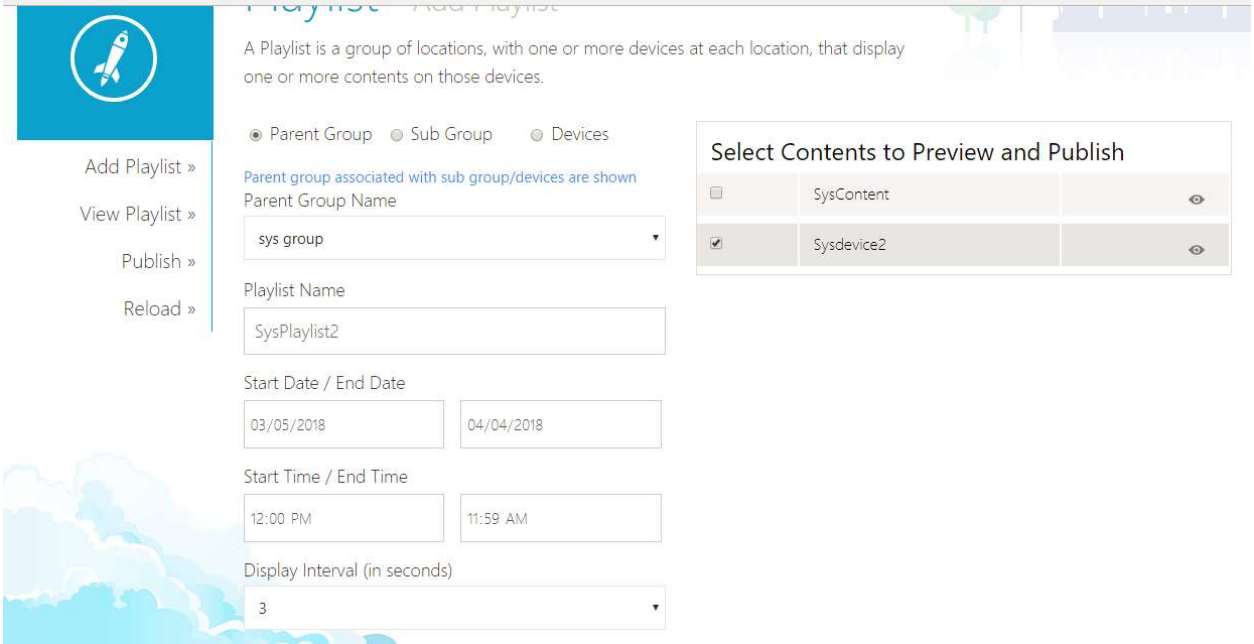


10. Select "**Add Playlist**" from the left menu, the **Add Playlist** page is displayed as shown in the following figure.

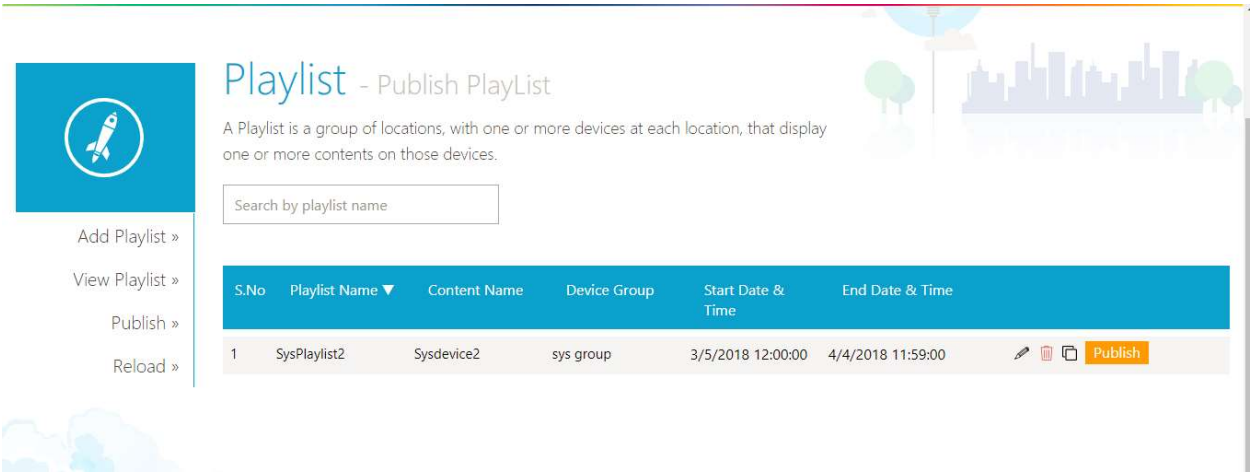


11. In the **Select Contents to Preview and Publish section**, Select one or more check boxes of the content for your Playlist as shown in the following figure.

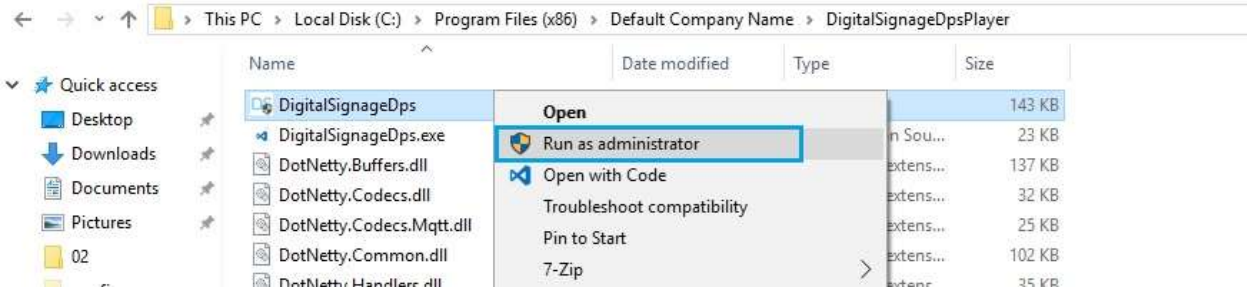
12. Enter the **Playlist Name** in the respective field.
13. Enter the **Start/End Date** and **Start/End Time** in their respective fields.
14. Set the **Display Interval** (In seconds) from the dropdown list.
15. Click **Save** button to save the Playlist is added.



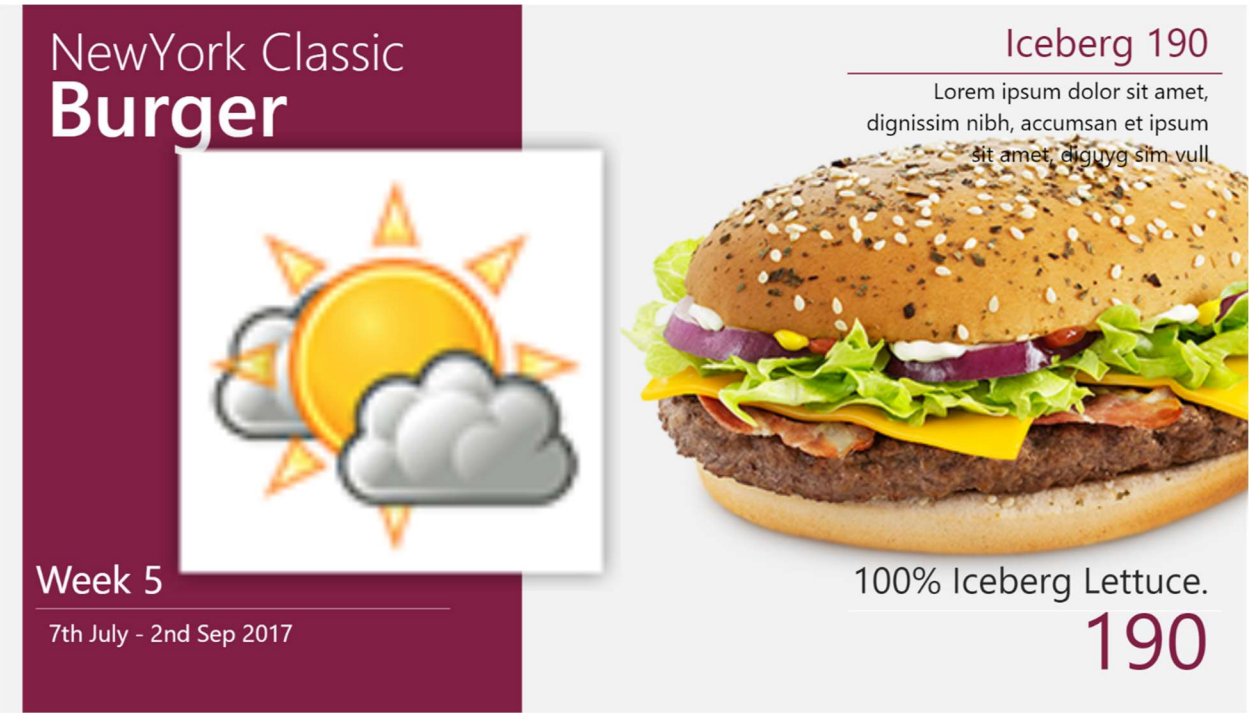
16. Click **Publish** button, a message **"Playlist Published Successfully"** is displayed.



17. Run the DigitalSignage DPS Player

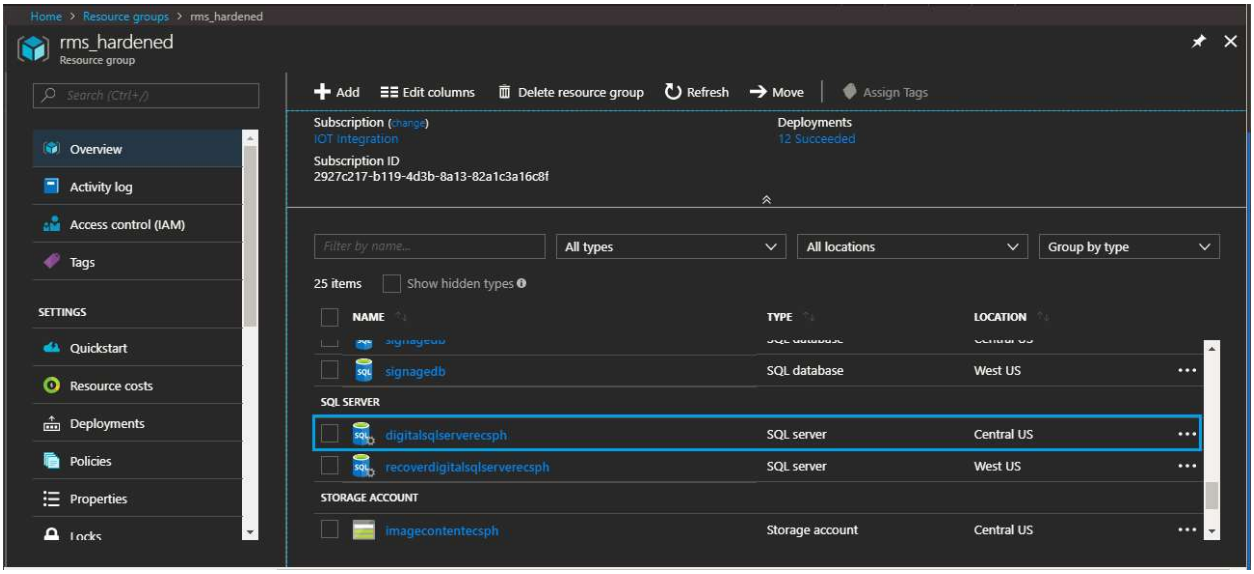


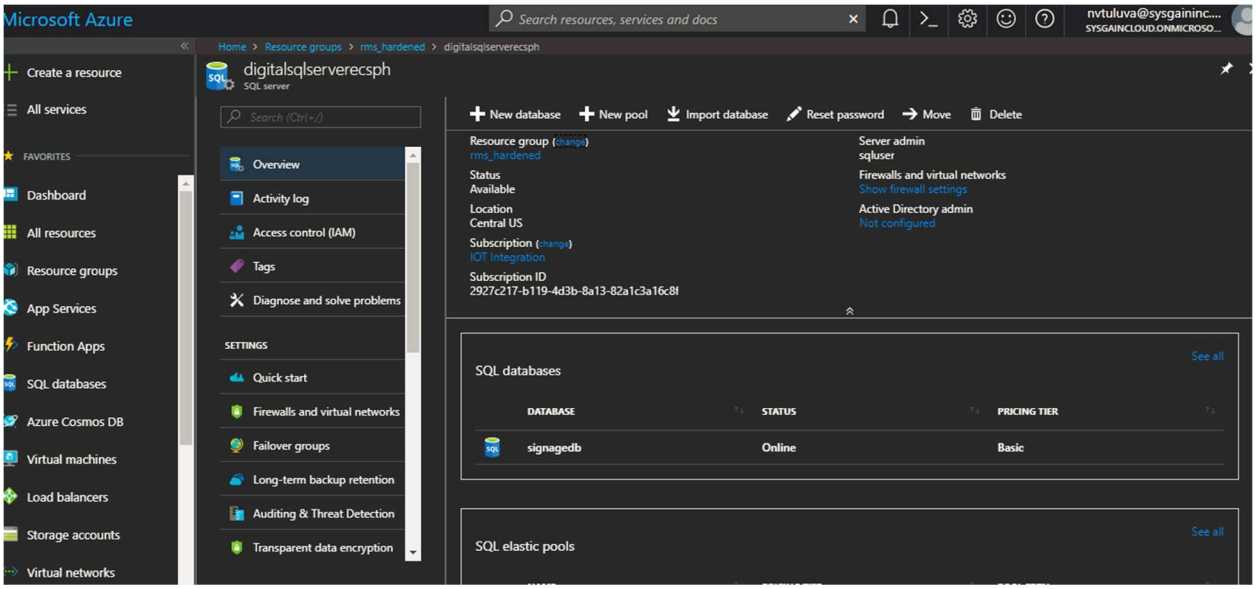
18. Now the two images **NYC Burgers & Potato Finger Chips** are displayed as shown in the following figures.



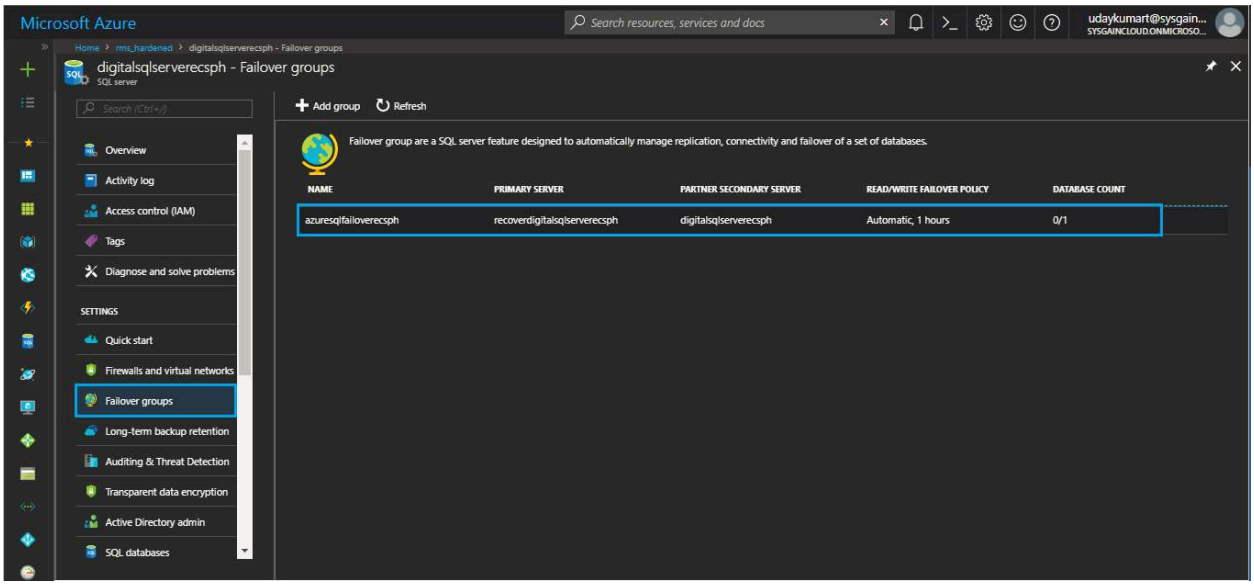
13.3.3. Geo Replication

1. Go to **Resource group > digitalsqlserverecsph**

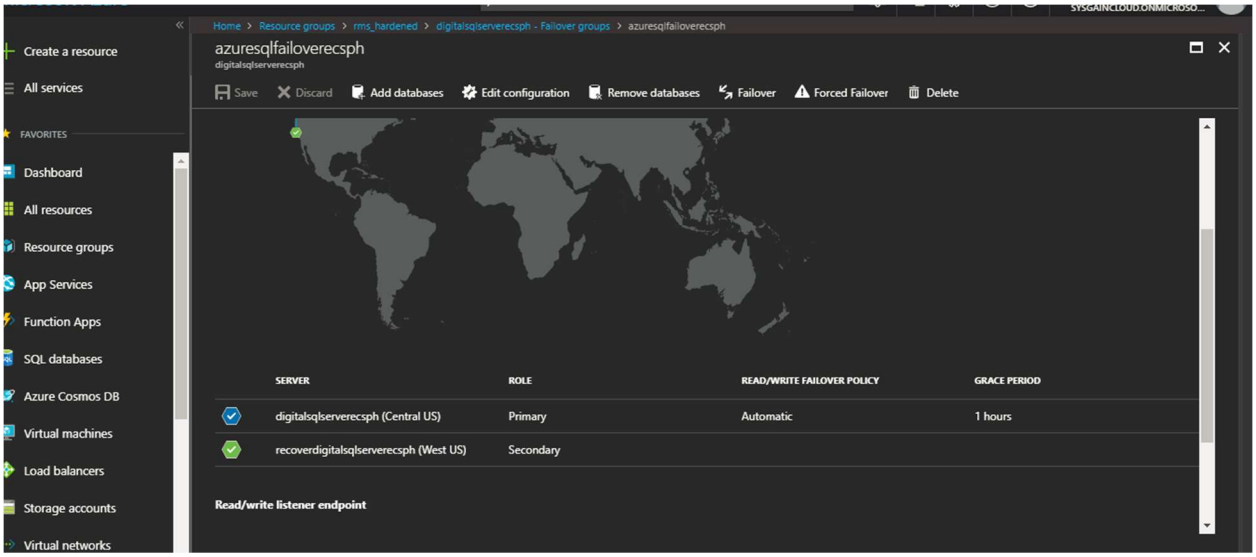




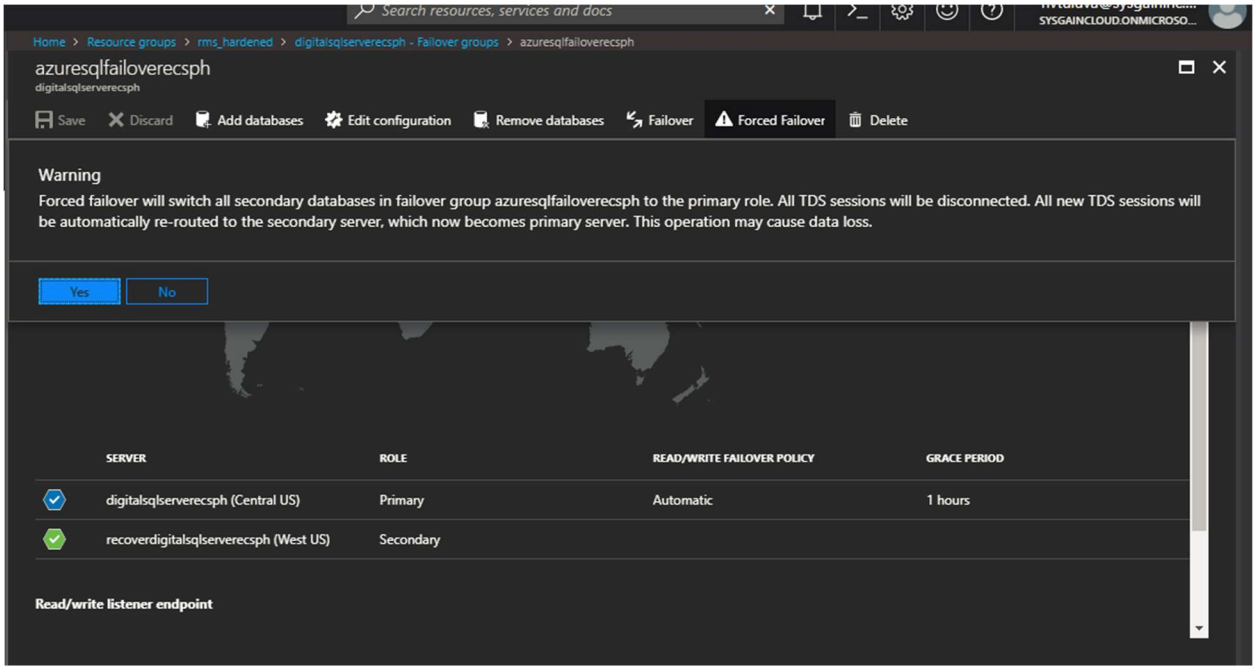
2. In the left side blade, click **Failover groups >** click **azurefailoverecsph**



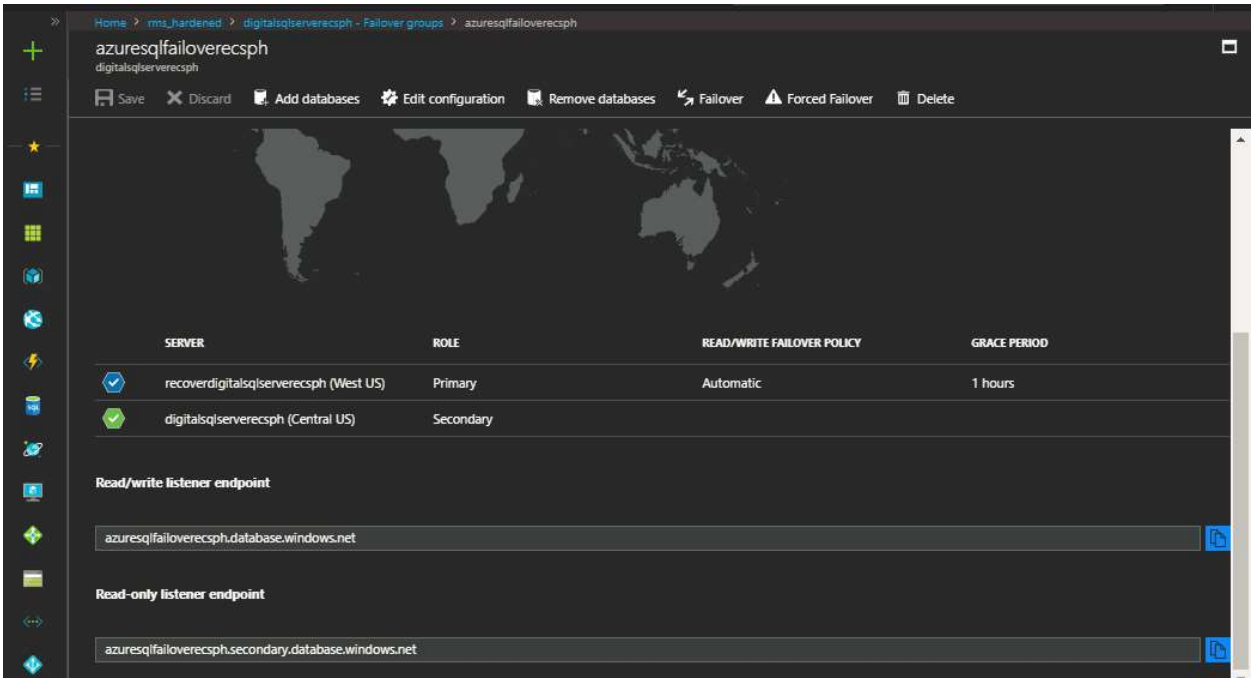
3. As shown in the following figure **digitalsqlserverecsph(Central US)** is primary SQL server and **recover digitalsqlserverecsph (West US)** is secondary SQL server.



4. **Click** on **Force Failover** option and select **Yes.**

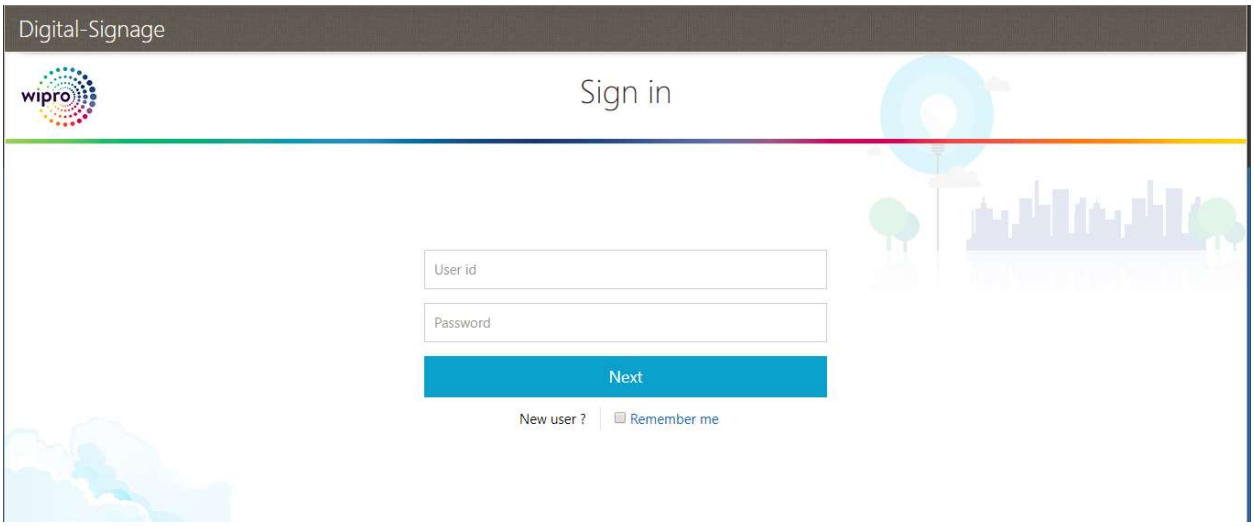


5. Now the **recover digitalsqlserverecsph (West US)** is primary SQL server and **digitalsqlserverecsph(Central US**) is secondary SQL server.



6. Sign in to **DigitalSignage UI**

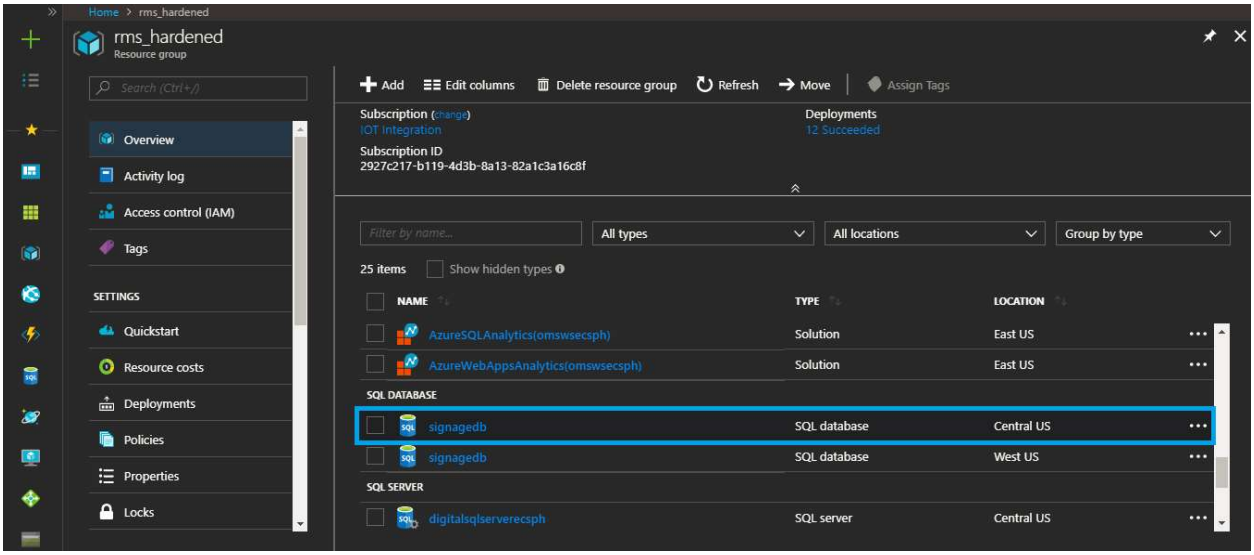
7. Copy and paste the **<TRAFFICMANAGERWEBAPPURL>** from output section and paste it in a browser.



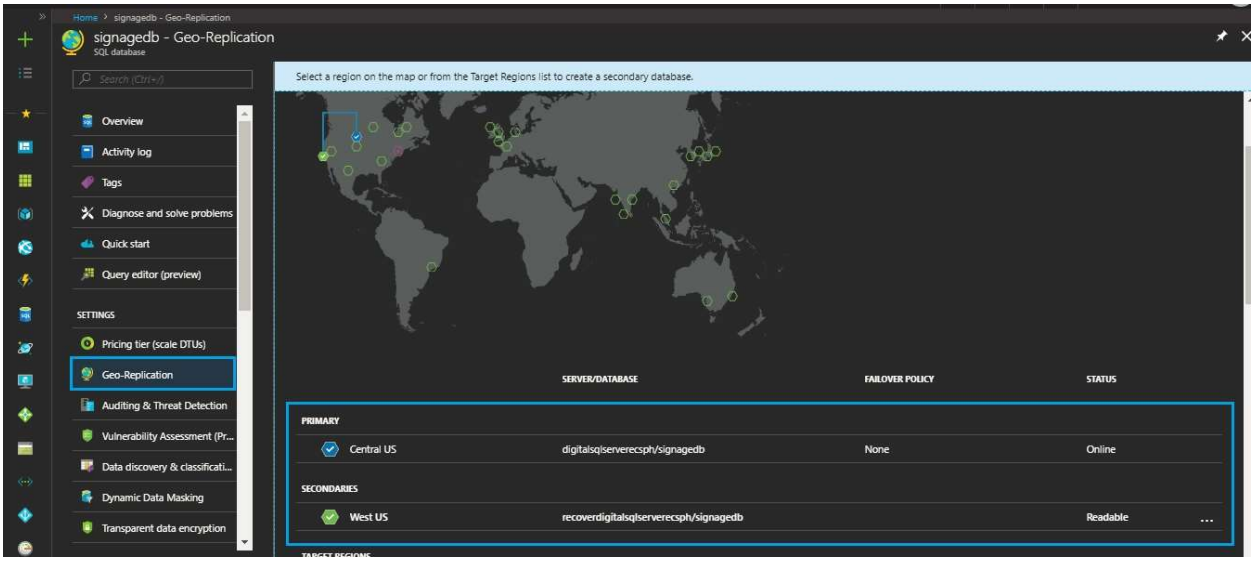
8. Once Login is successful, we can confirm that the recover digitalsqlserverecsph (West US) is working as expected.

13.3.4. Database Restore

1. Go to **Resource group> signagedb**



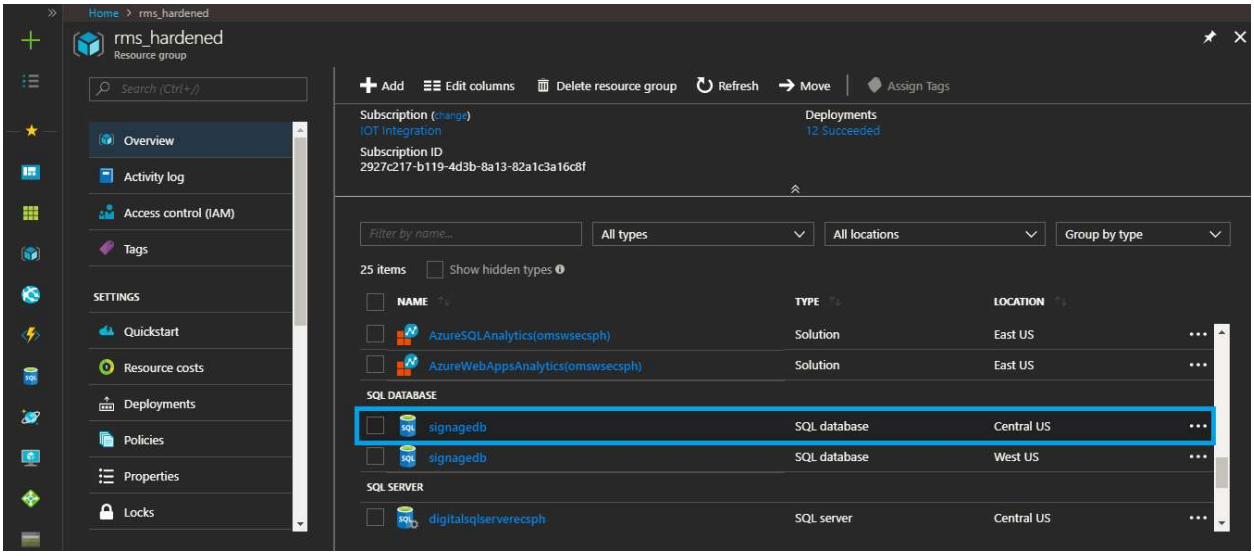
2. Click **Geo Replication** in the left side tab.



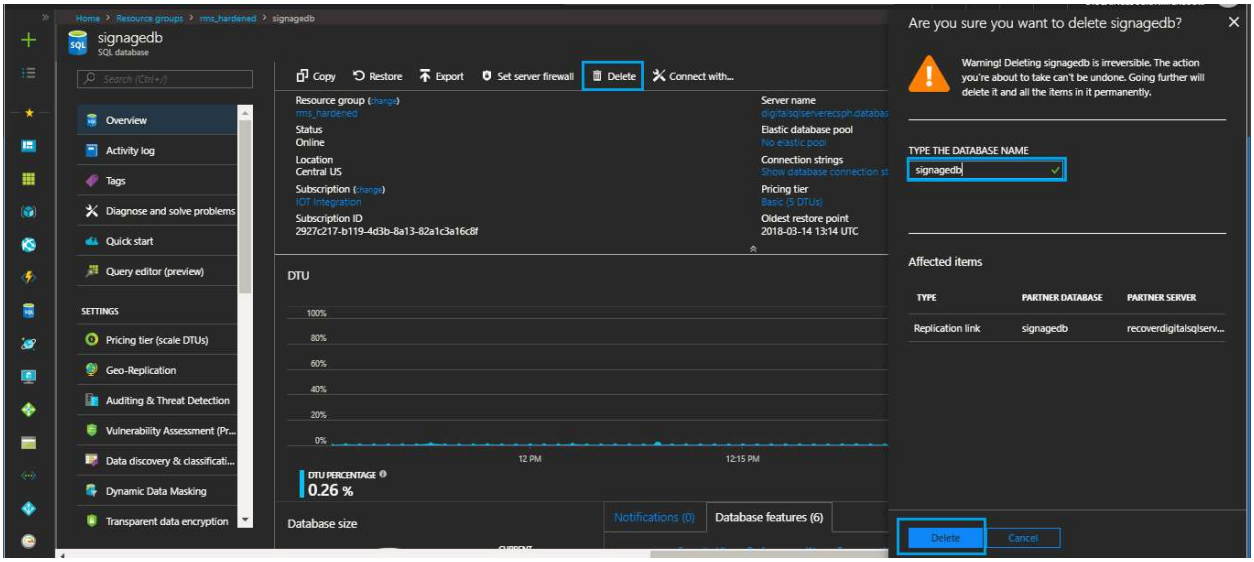
3. In the above figure **digitalsqlserverecsph/signagedb** is primary database and **recoverdigitalsqlserverecsph/signagedb** is secondary database.

4. Delete the primary database.

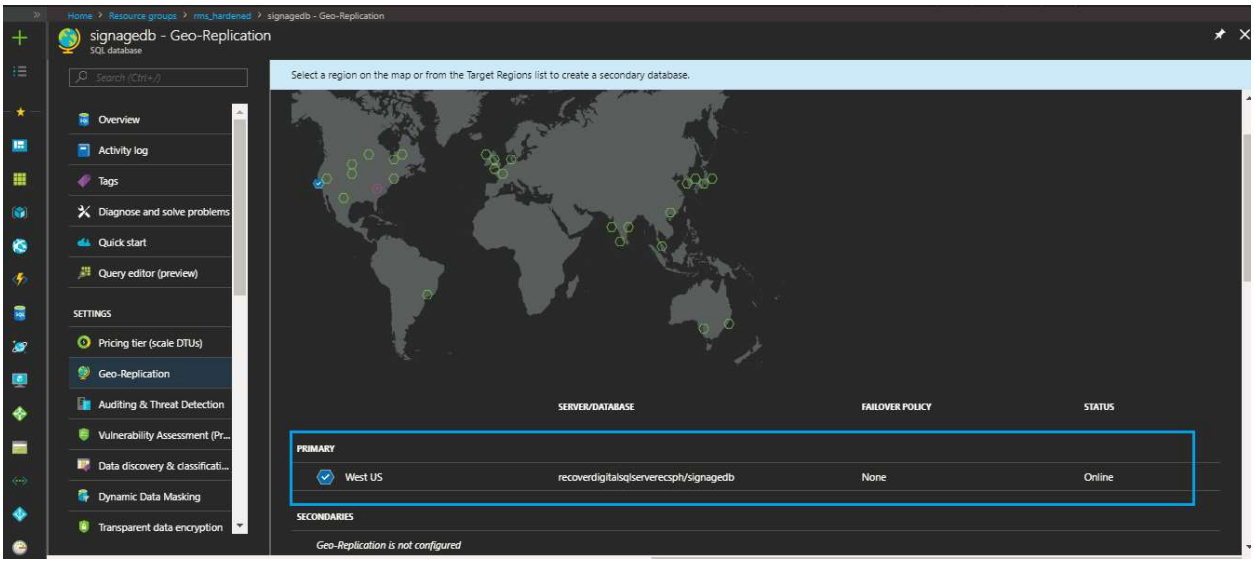
5. Go to **Resource group> signagedb**



6. Click **Delete** option, type the **<database name> "signagedb"** and click **Delete.**



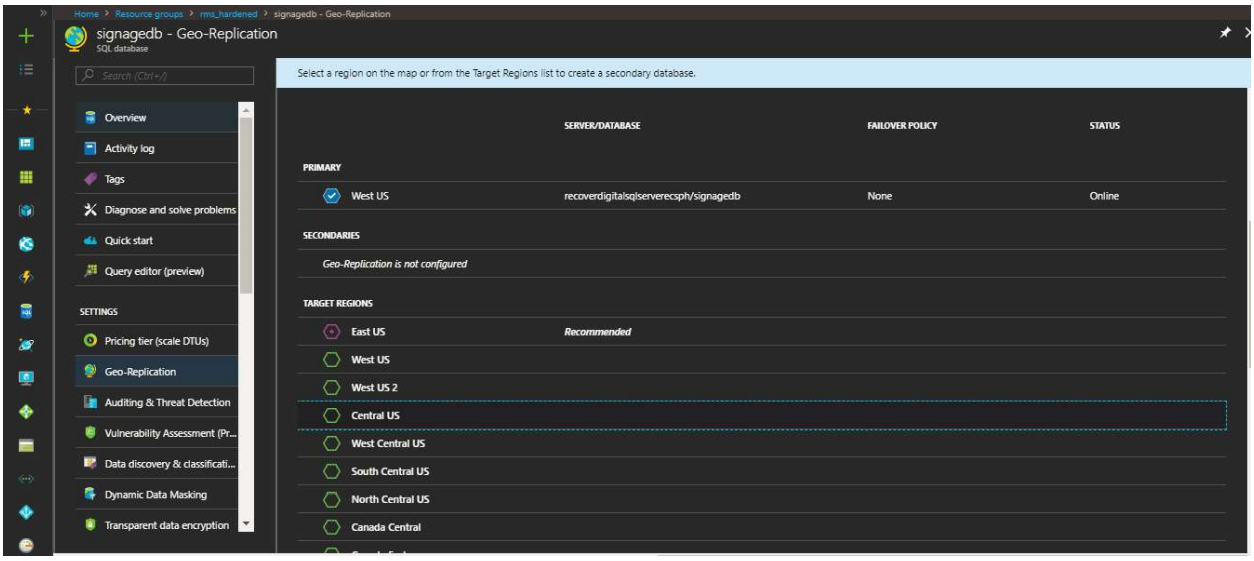
7. Go to **resourcegroup > signagedb >** click **Geo replication**

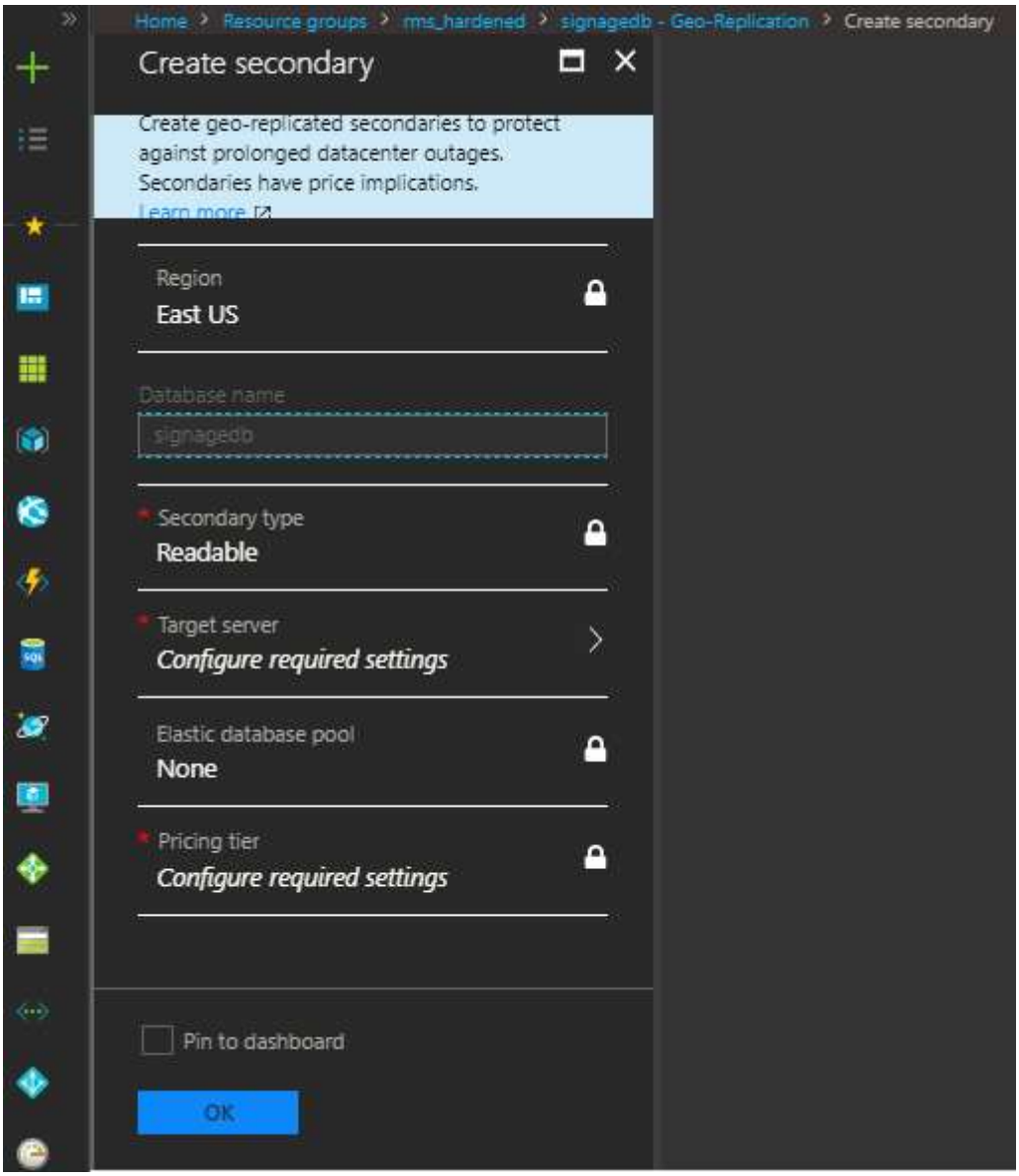


8. Now in the above figure **recoverdigitalsqlserverecsph/signagedb** is the primary database.

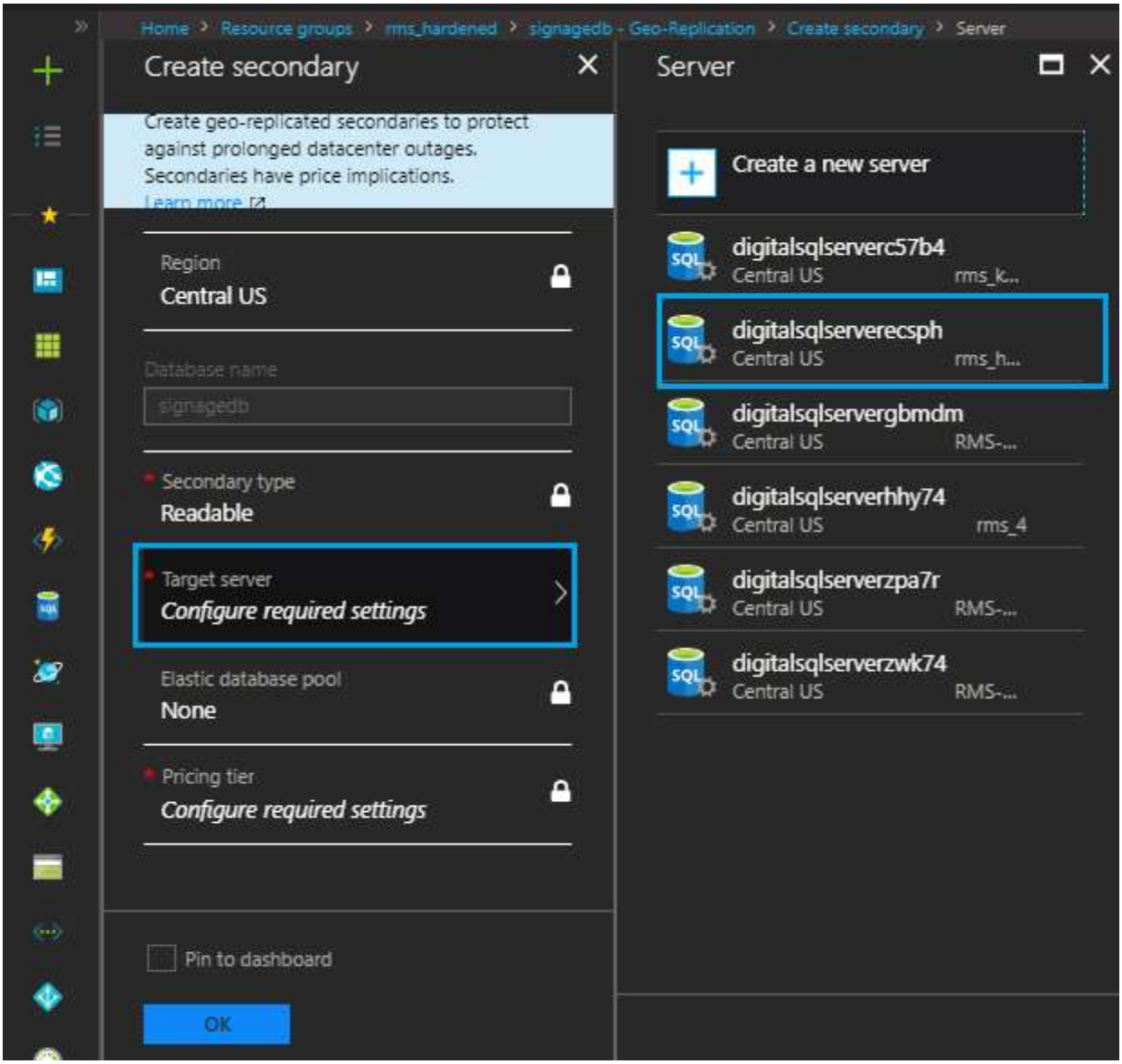
9. Create another secondary database from this new primary database.

10. Select a target region where you want your secondary database.


Home > Resource groups > rms_hardened > signagedb - Geo-Replication
signagedb - Geo-Replication
SQL database
Search (Ctrl+/)
Overview
Activity log
Tags
Diagnose and solve problems
Quick start
Query editor (preview)
SETTINGS
Pricing tier (scale DTUs)
Geo-Replication
Auditing & Threat Detection
Vulnerability Assessment (Pr...
Data discovery & classificati...
Dynamic Data Masking
Transparent data encryption
Select a region on the map or from the Target Regions list to create a secondary database.
SERVER/DATABASE
FAILOVER POLICY
STATUS
PRIMARY
West US
recoverdigitalsqlserverecsph/signagedb
None
Online
SECONDARIES
Geo-Replication is not configured
TARGET REGIONS
East US
Recommended
West US
West US 2
Central US
West Central US
South Central US
North Central US
Canada Central

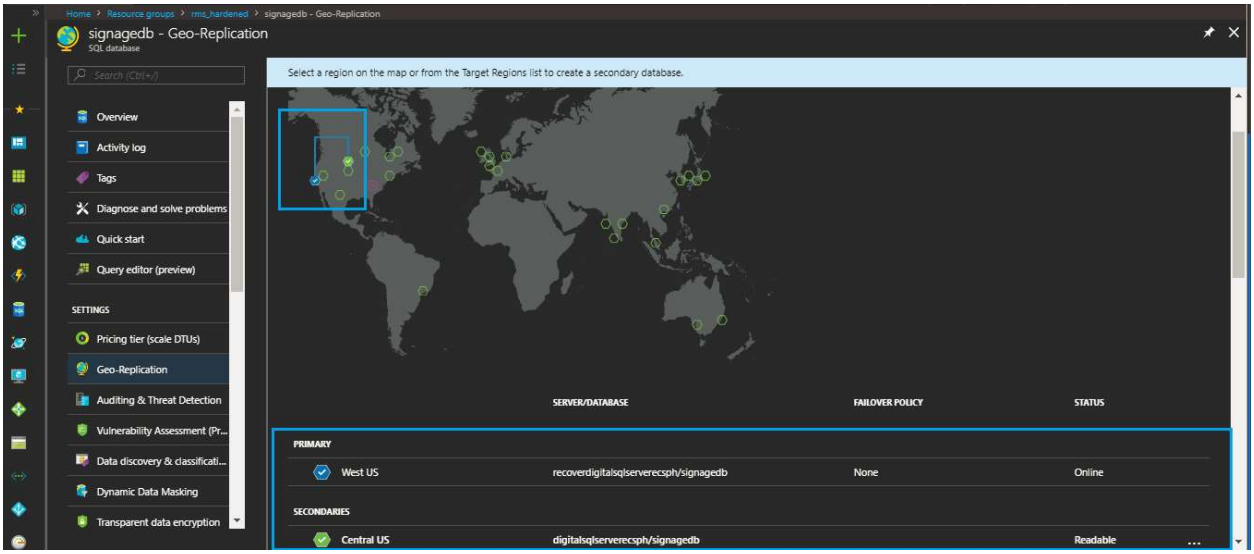


11. Click **Configure required settings >** select an existing server or create a new server.



12. Click **OK** button.

13. Now you can see that we have created a new replicated database in the Central US region as shown in the following figure.



14. Monitoring components

14.1. Azure Application Insights

Application Insights is an extensible Application Performance Management (APM) service for web developers on multiple platforms. This is used to monitor your live web application and to automatically detect performance anomalies. It includes a powerful analytics tools to help you diagnose issues and to understand what users do with your app.

An overview of Application Insights, an Azure based service which makes it possible to monitor any application to know about its availability, failures and performance.

It works for apps on a wide variety of platforms including some of below.

- .NET
- Node.js
- J2EE
- hosted on-premises or in the cloud

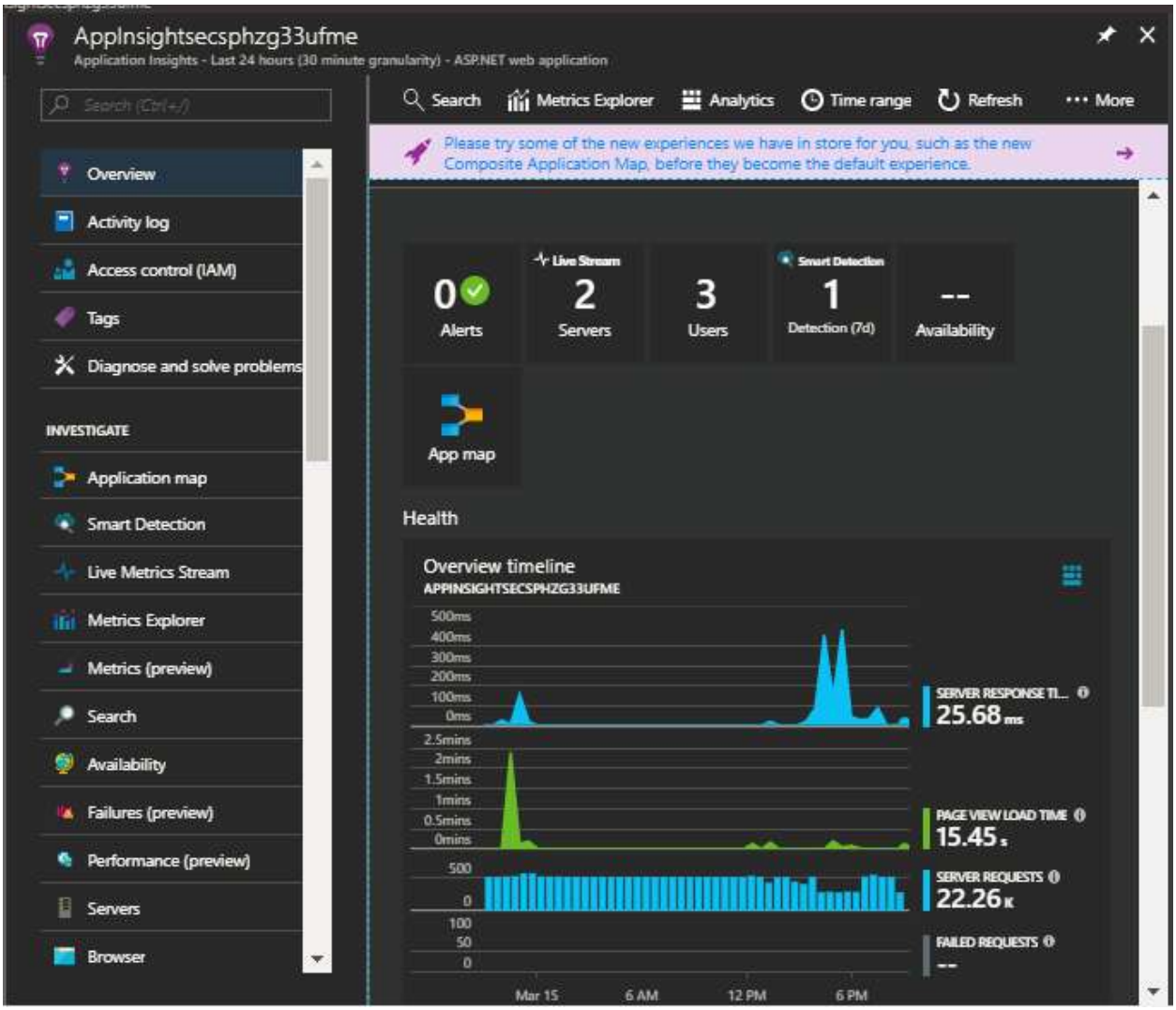
What does Application Insights monitor?

- Request rates, response times, and failure rates
- Dependency rates, response times, and failure rates
- Exceptions
- Page views and load performance
- AJAX calls

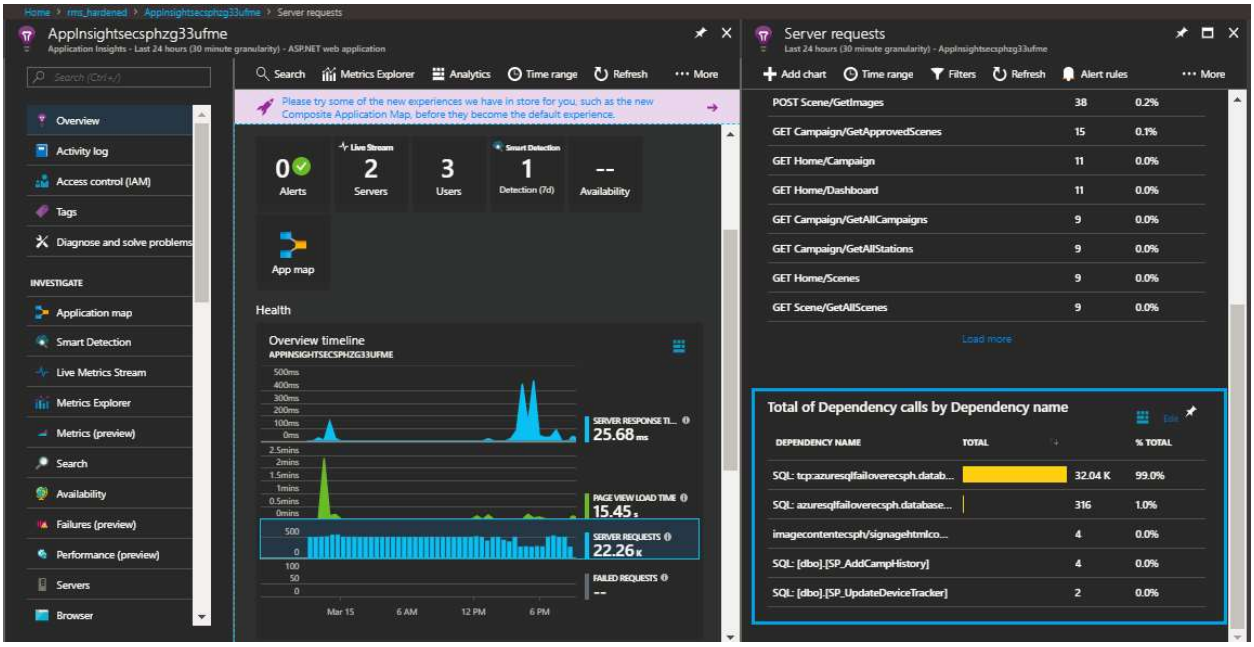
- User and session counts
- Performance counters
- Performance counters
- Host diagnostics from Docker or Azure
- Diagnostic trace logs
- Custom events and metrics

Application Insights

1. Go to **Azure portal > Resource Group > RMS_monitoring > Application Insights**
2. Click the **Application Insights** icon in the deployed resource group.
3. The following page is displayed with **Server Response Time, Page View Load Time, Server Requests** graphs.

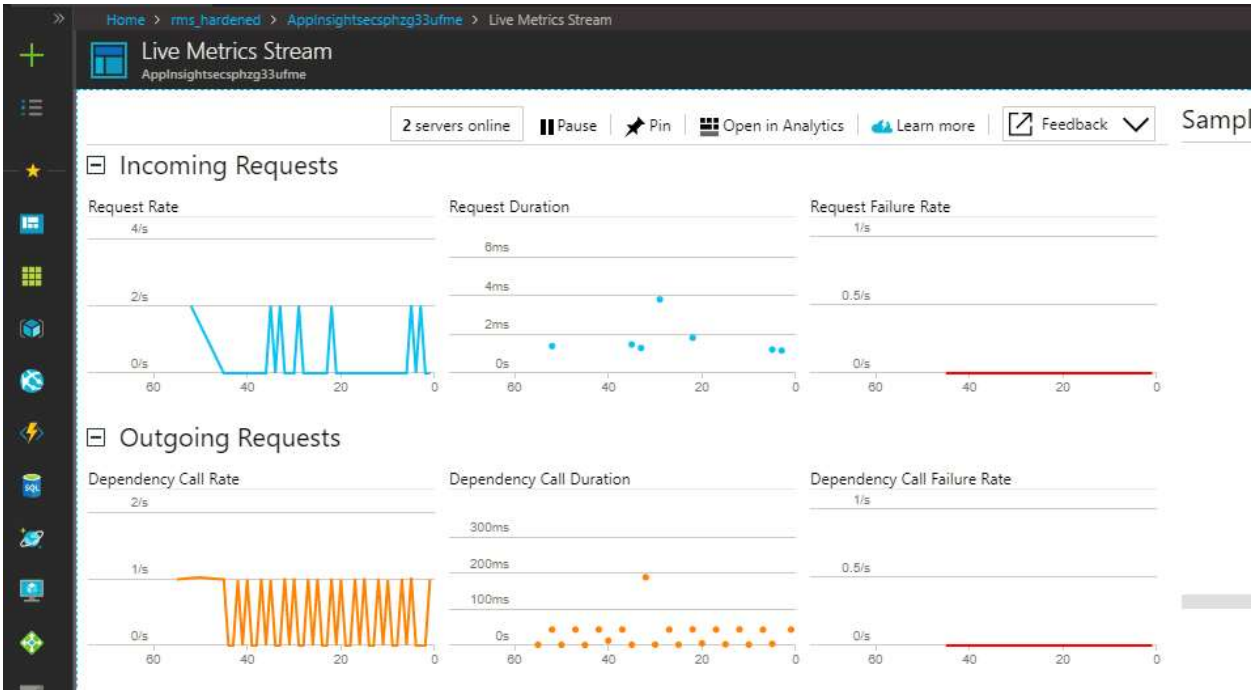


4. To view the Server Request Logs of web job, click **Server Requests**.



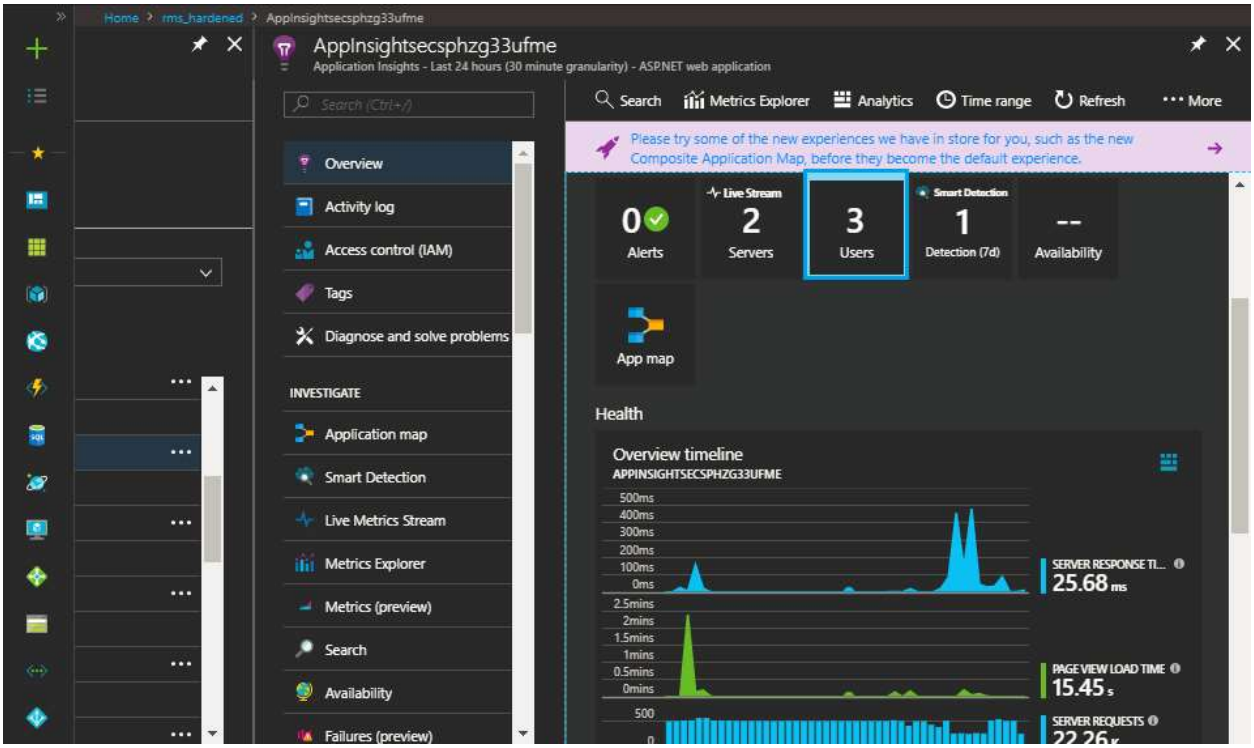
14.1.1. Live Metrics Stream

Click **Live Metric Stream** to view the incoming requests, outgoing requests, overall health and servers of the web application.

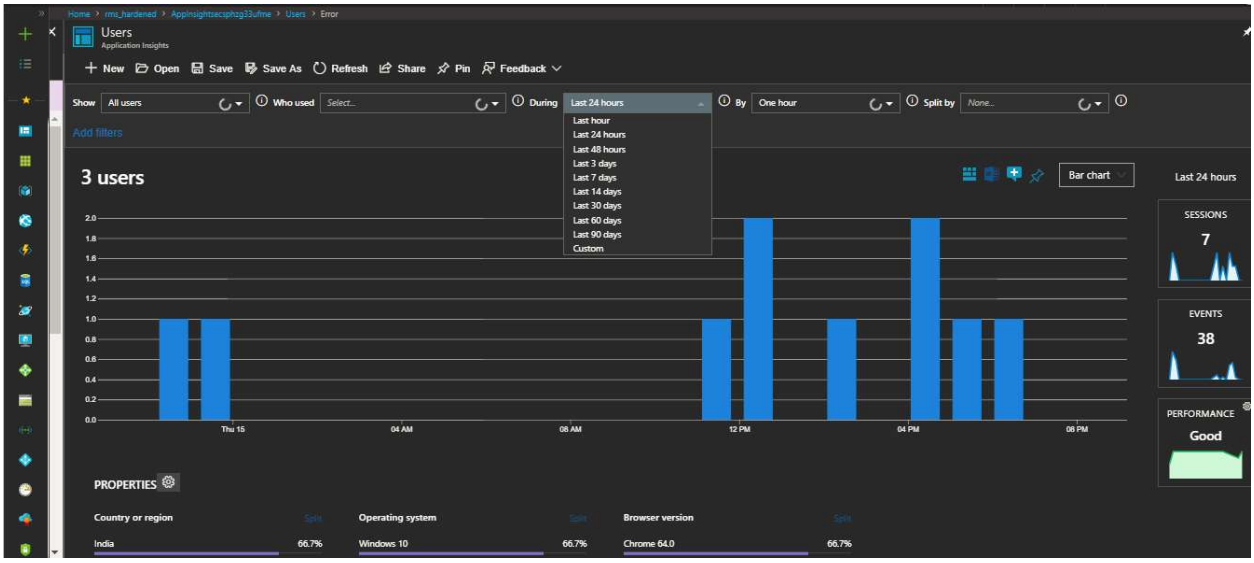


14.1.2. Users

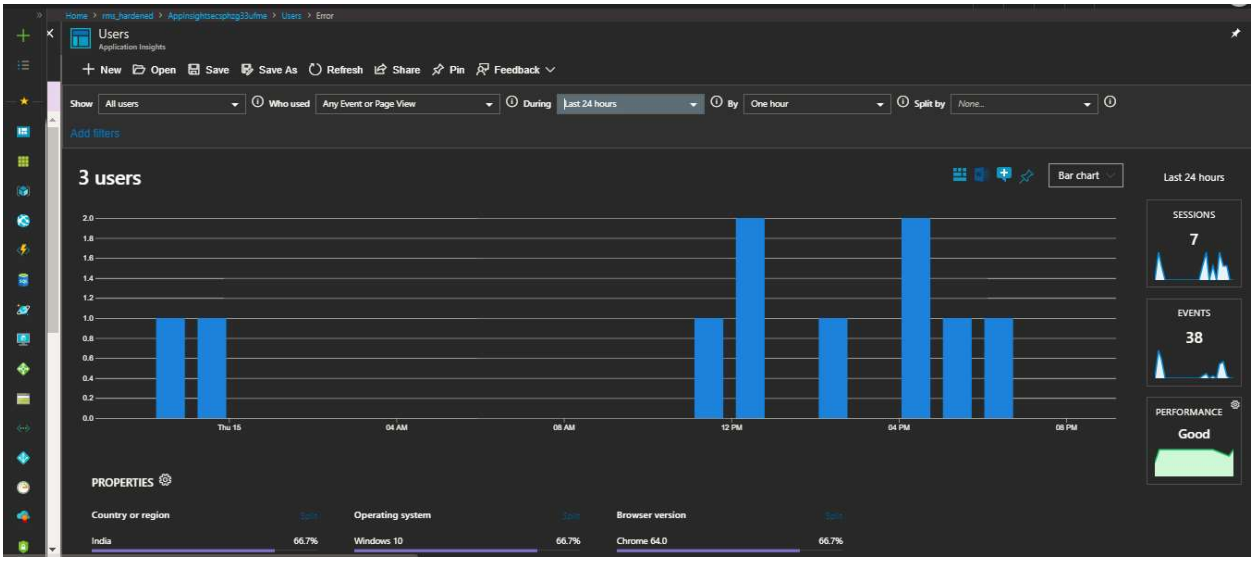
1. Click **Users** to view the number of users connected to the web application and to see the number of sessions that are running in the web application.



2. Select the required duration from the drop-down list as shown in the following figure.



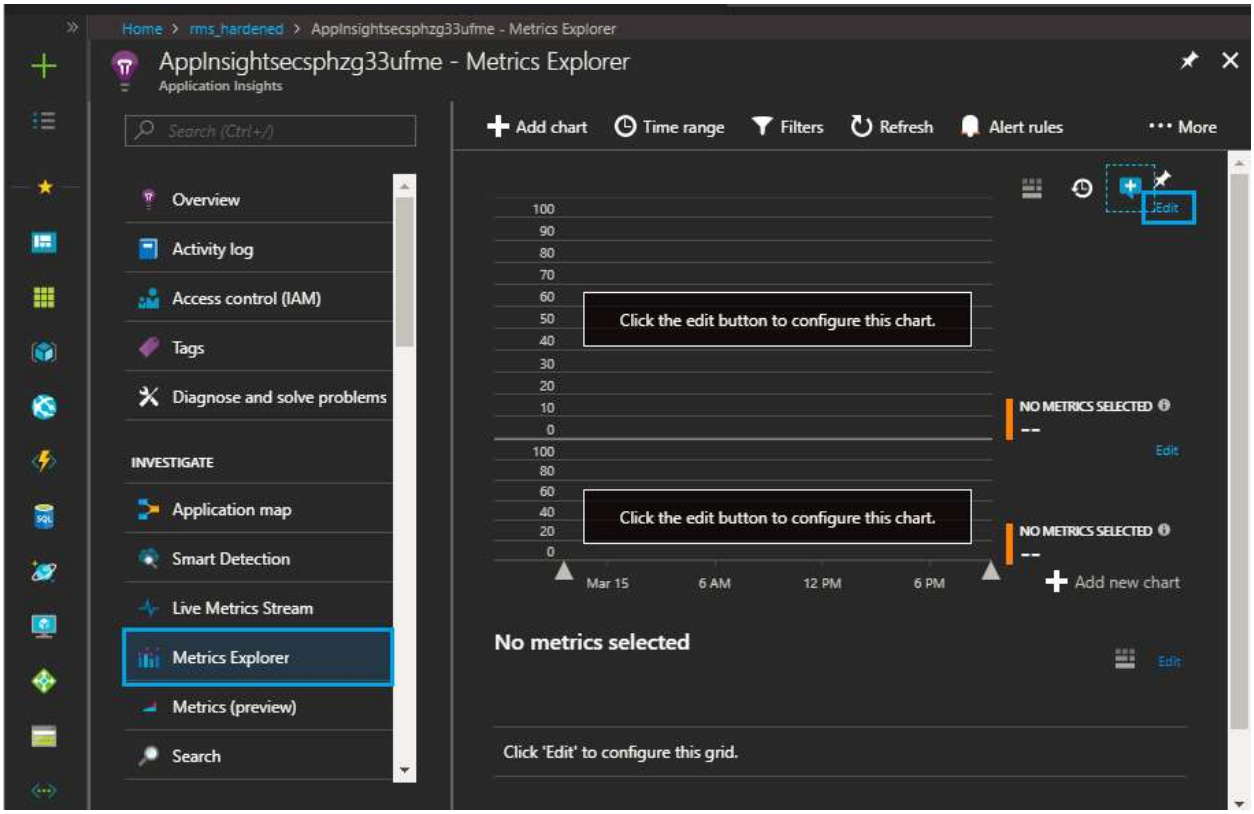
3. In this you also have other options like **Who used**, **Duration, By** and **split by** in to set the metrics as per your requirement.



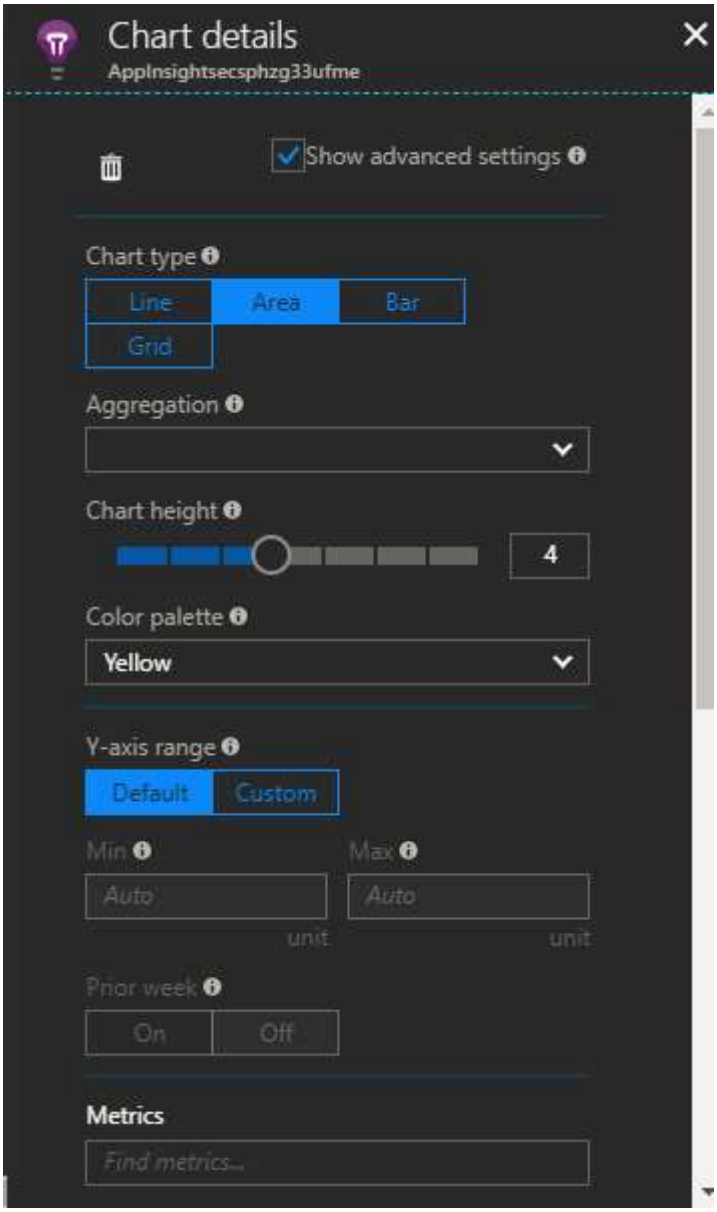
14.1.3. Metric Explorer

1. Select the **Metric Explorer** option from the left menu.

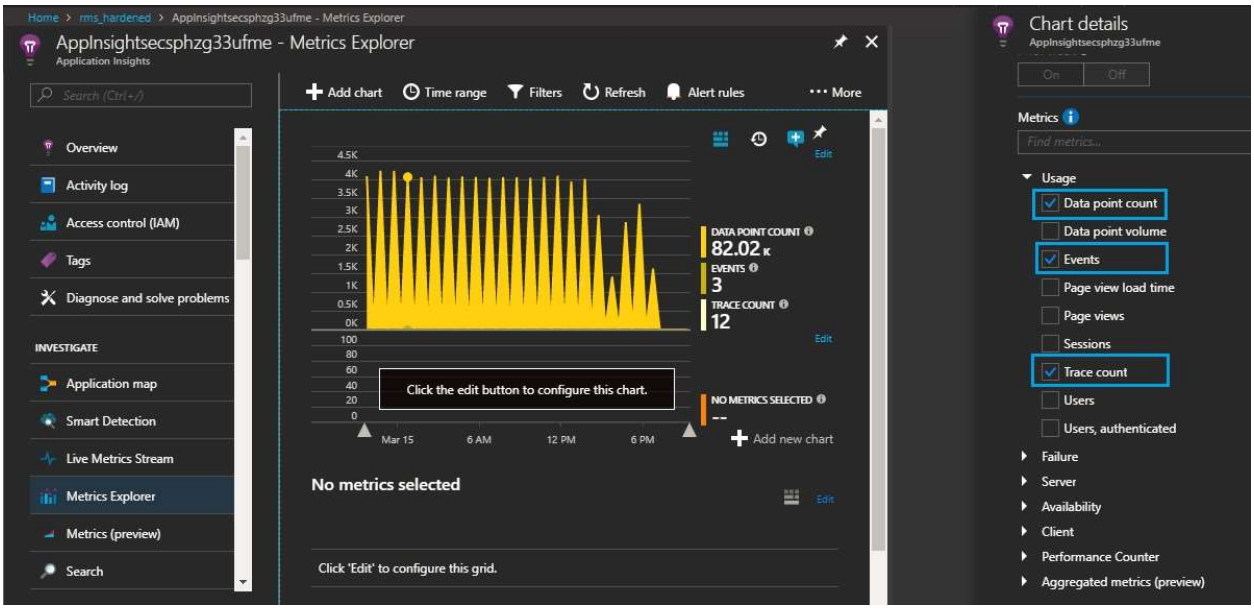
2. Click the **Edit** link on the top right corner as shown in the following figure.



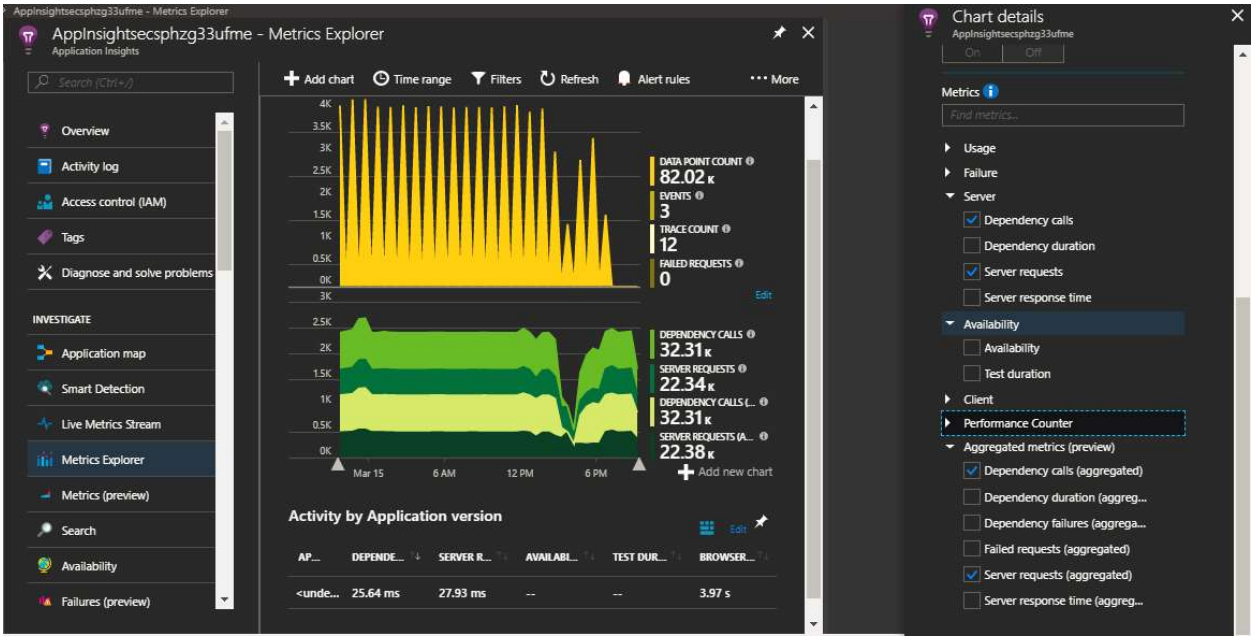
3. **Chart details** page is displayed on the right side. Set the details as per requirement.



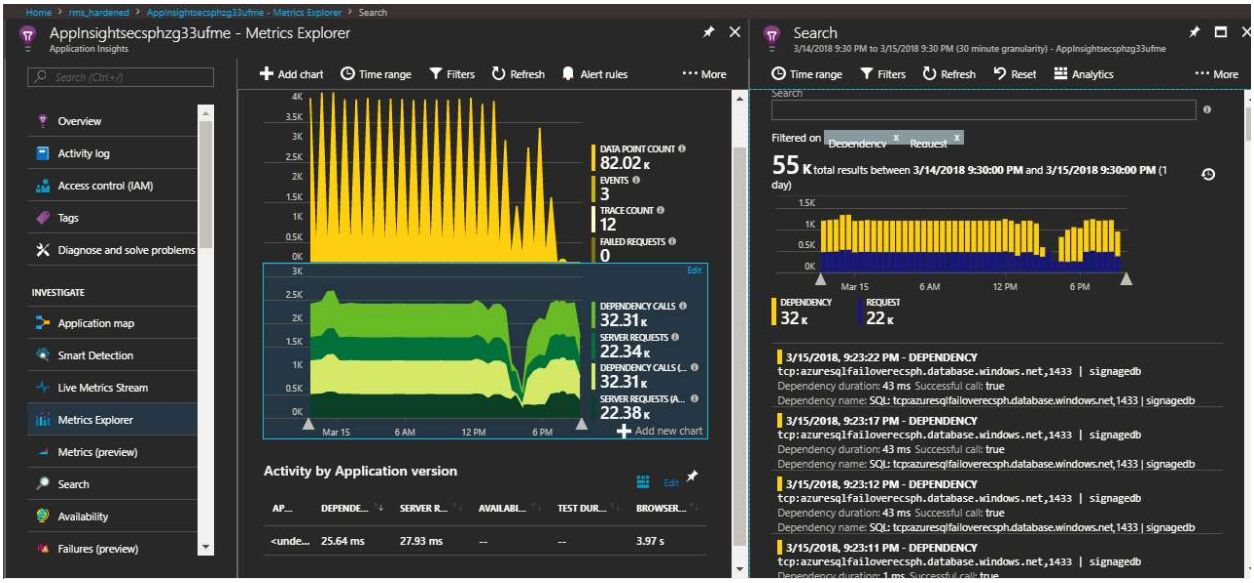
4. Scroll down in the **Chart Details** page, you can see the **Metrics**, select check boxes of the required metrics as shown in the following figure.



5. Similarly, you can get the metrics for **Server, Client, Failure, Availability, Performance Counter** and **Aggregated metrics**.

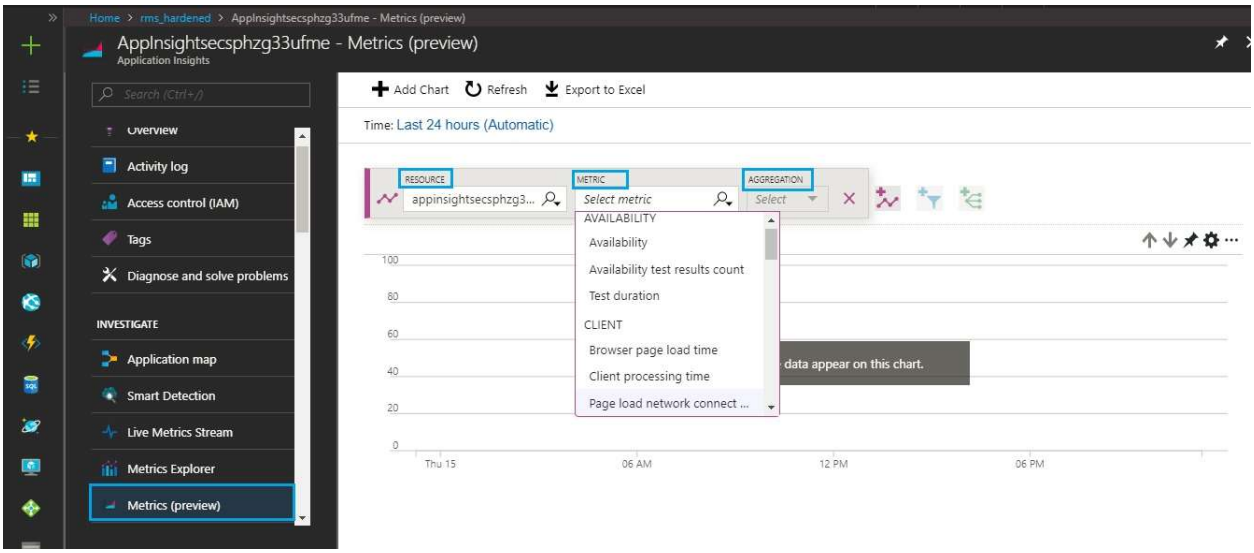


6. To check the logs, click the required chart for which you want to see the logs of each request as shown in the following figure.

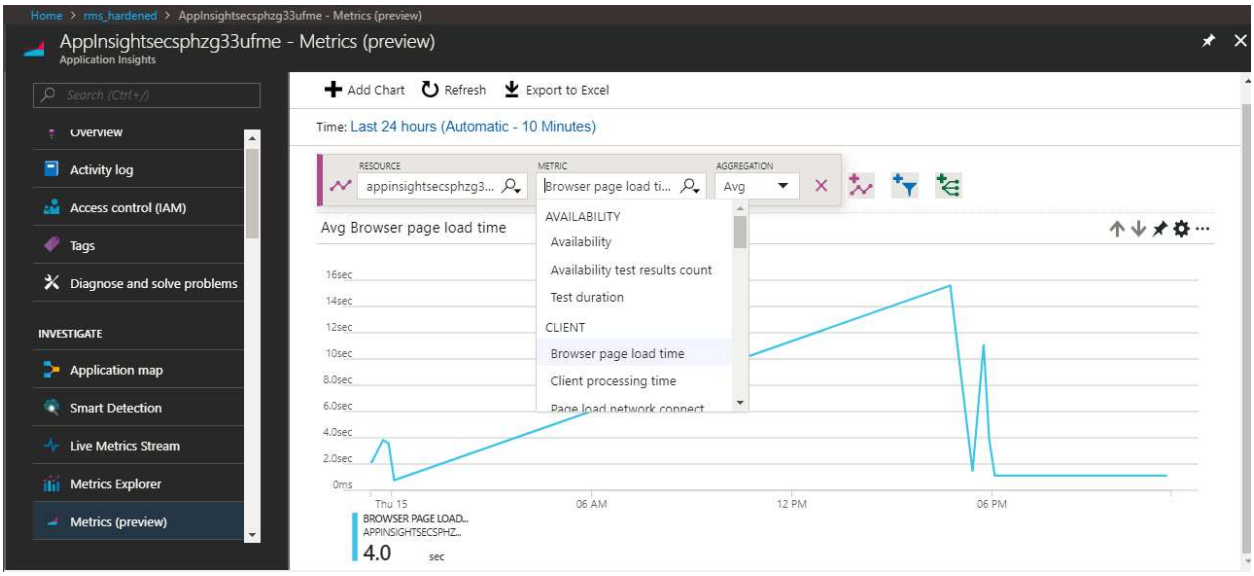


14.1.4. Metric preview

1. Select **Metric Explorer** from the left menu.
2. Select the resource from the drop-down list, select the metric and the aggregation as per requirement.

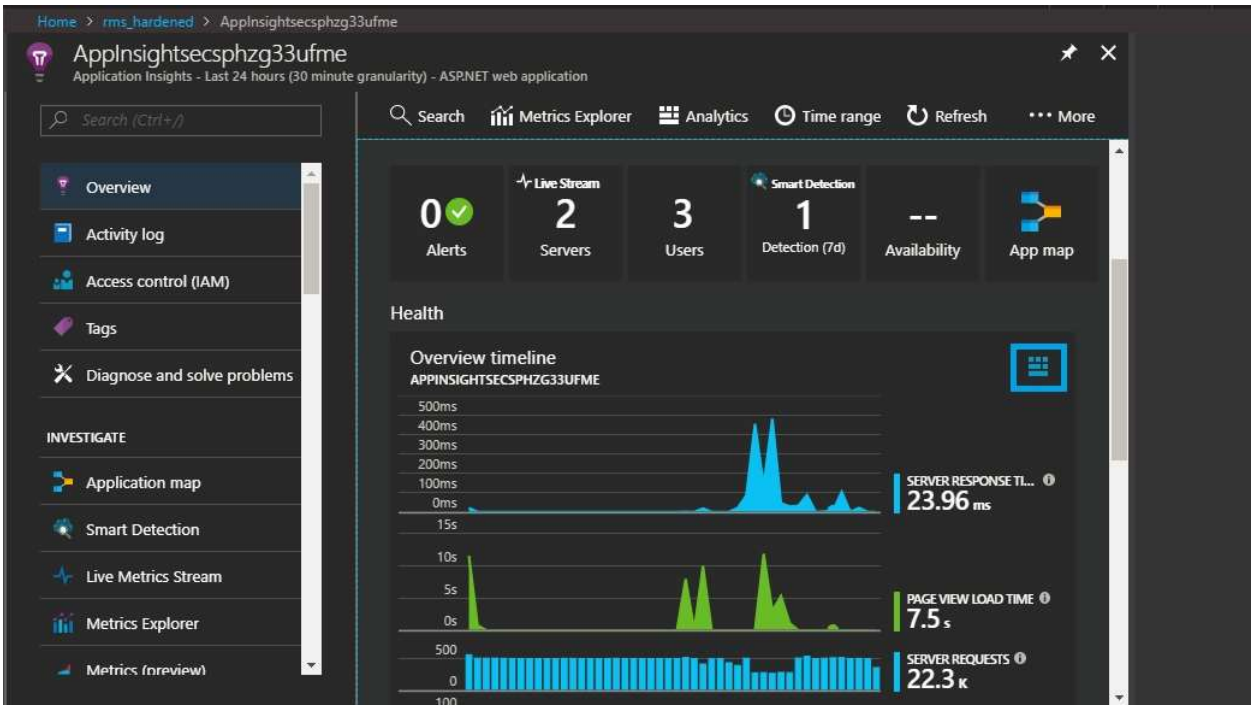


3. The graph is displayed as per the selected metric and aggregation.

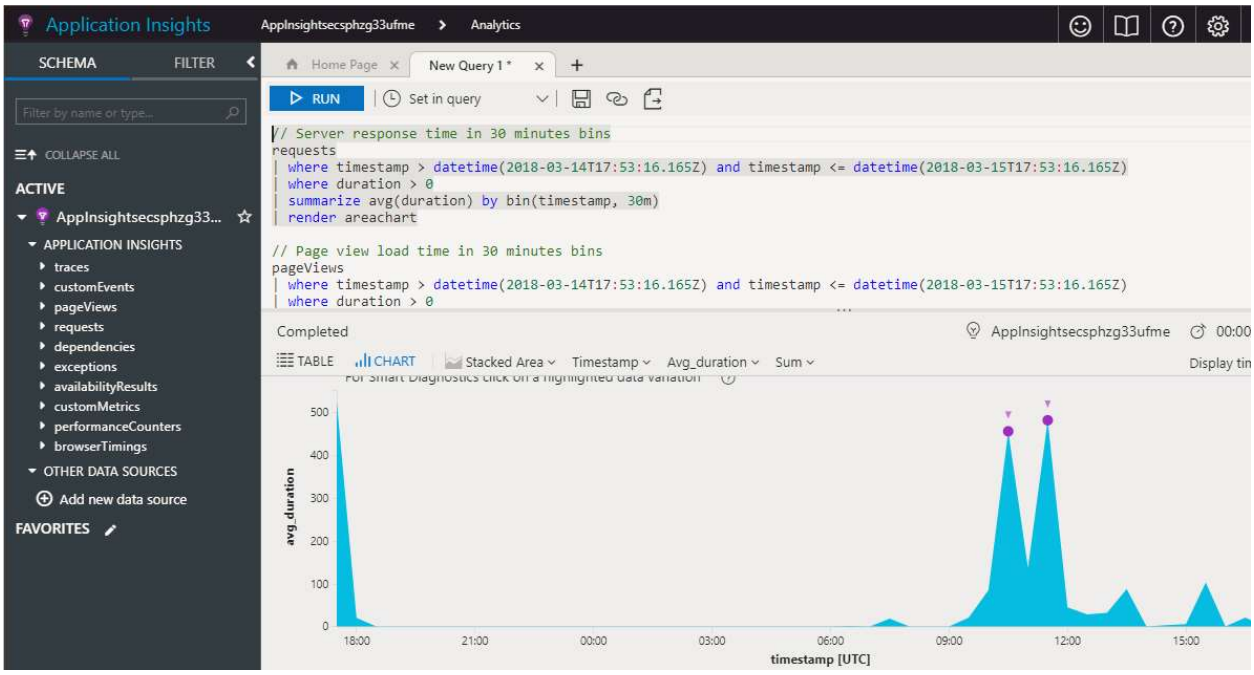


4. User can use the **Usage Customized Query** to view the metrics.

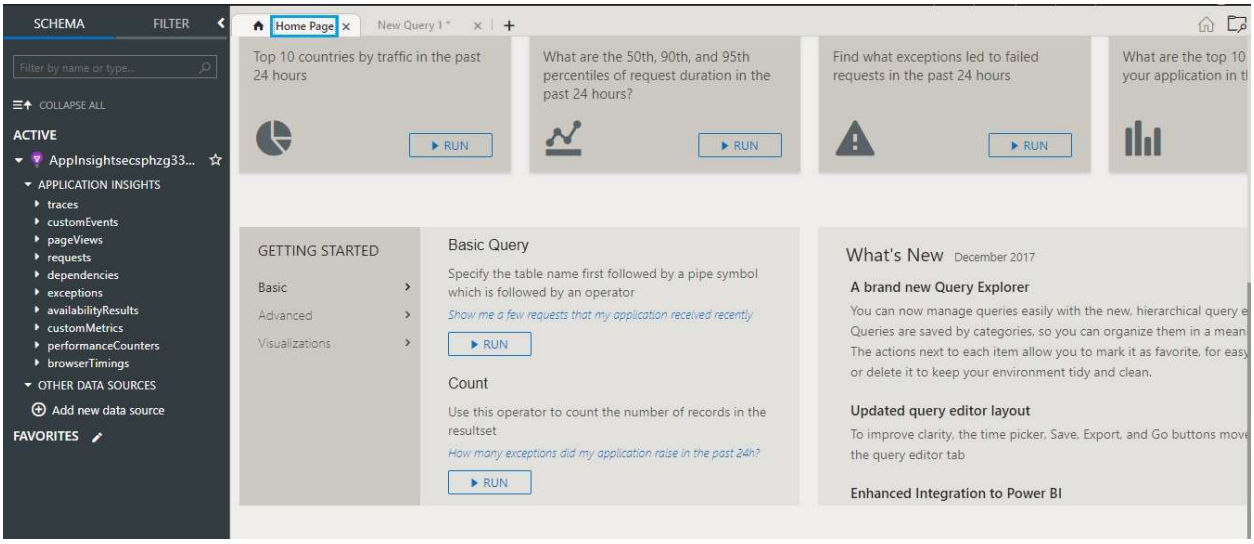
5. Click the icon on the top right corner of the **Overview timeline** section as shown in the following figure.



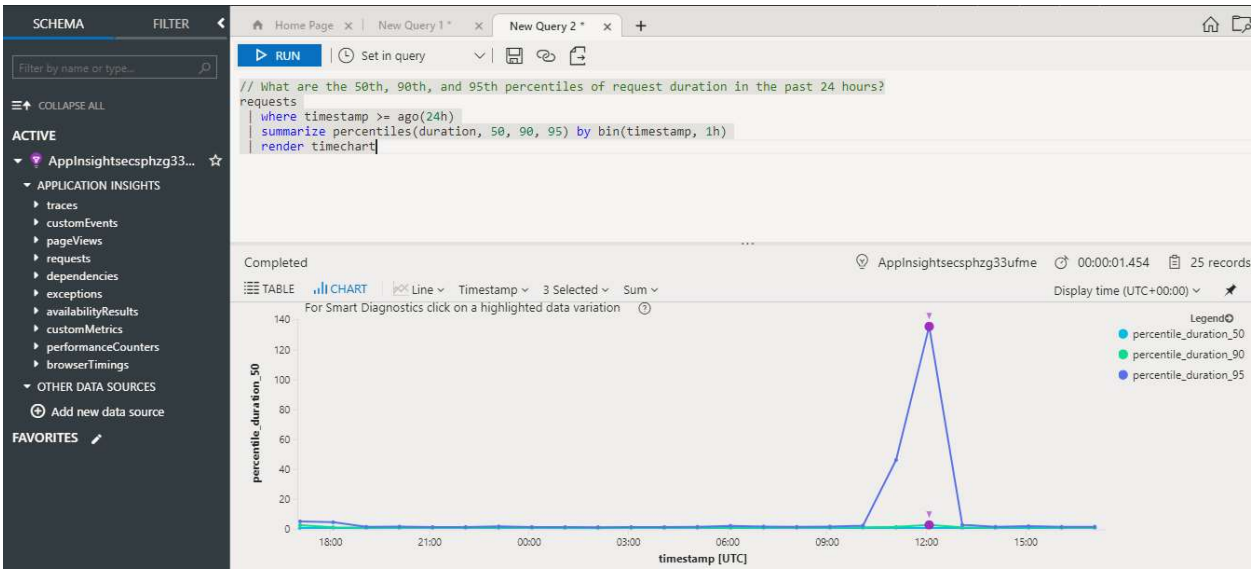
6. A new tab with some default queries & chart for the same are displayed as shown in the following figure.



7. Click **Home Page** which is in left side of top menu and scroll down to view the default basic queries, Click **RUN** as per user requirement.

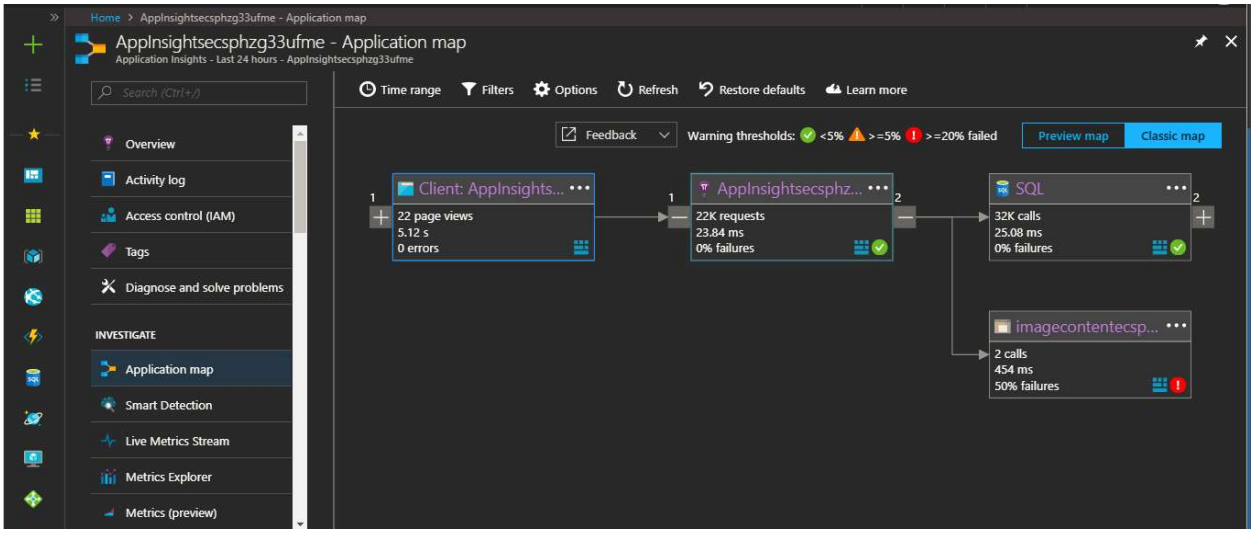


8. Click **RUN** in the Performance section to display default queries & charts.

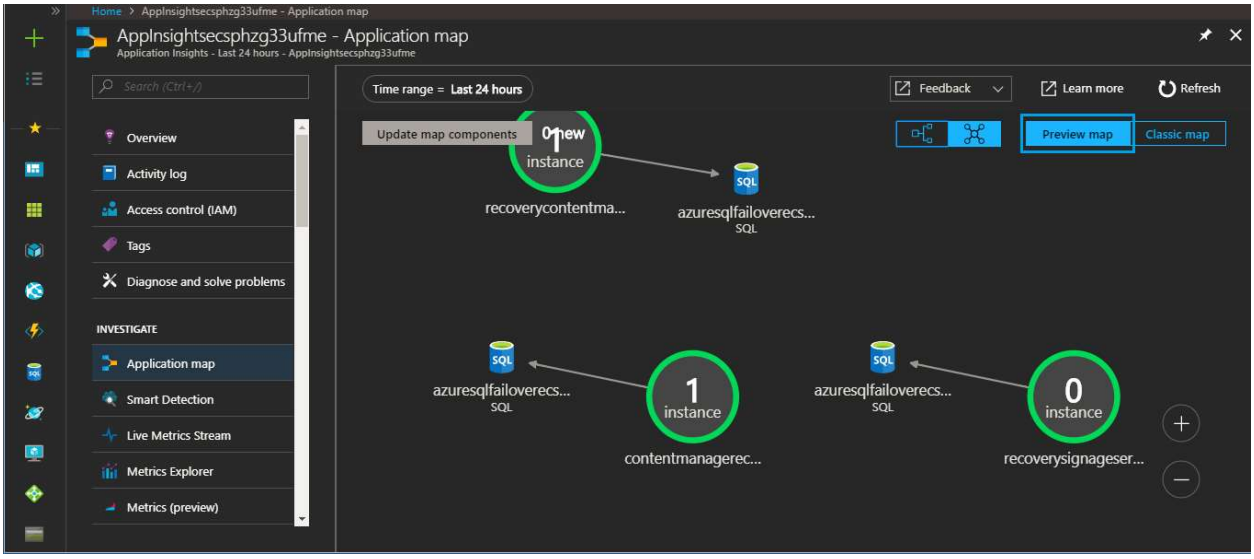


14.1.5. Application Map

1. Application Map helps you to spot the performance bottlenecks or failure hotspots across all components distributed in the application.
2. Click **Application map** as shown in the following figure.
3. Click **Preview map** on the top-right corner to switch back to **Preview map** from the **Classic map**.
4. Click the **Classic map**, the application map is displayed as shown in the following figure.



5. Click **Preview map** the application map is displayed as shown in the following figure.



14.2. OMS Log Analytics

Operations Management Suite (also known as OMS) is a collection of management services that were designed in the cloud from the start. Rather than deploying and managing on-premises resources, OMS components are entirely hosted in Azure.

What is Log Analytics?

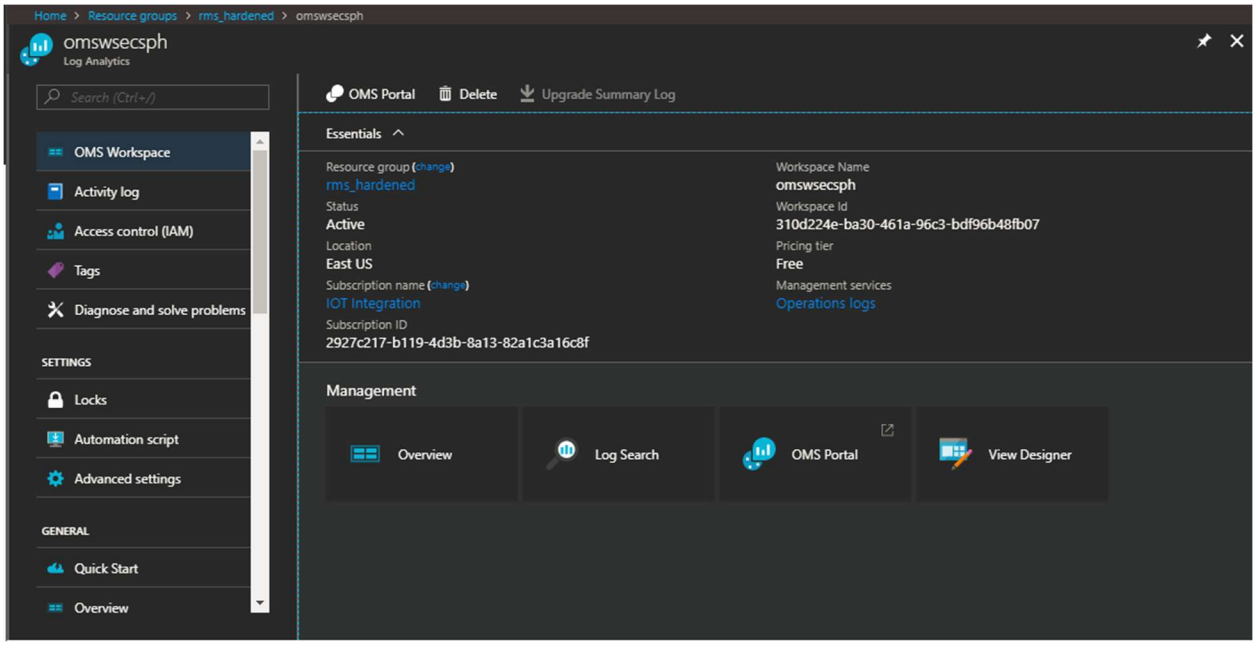
Log Analytics is a service in Operations Management Suite (OMS) that monitors your cloud and on-premises environments to maintain their availability and performance. It collects data generated by resources in your cloud and on-premises environments and from other monitoring tools to provide analysis across multiple sources.

OMS are helpful to monitor SQL Database, Web Apps and Other Azure Components

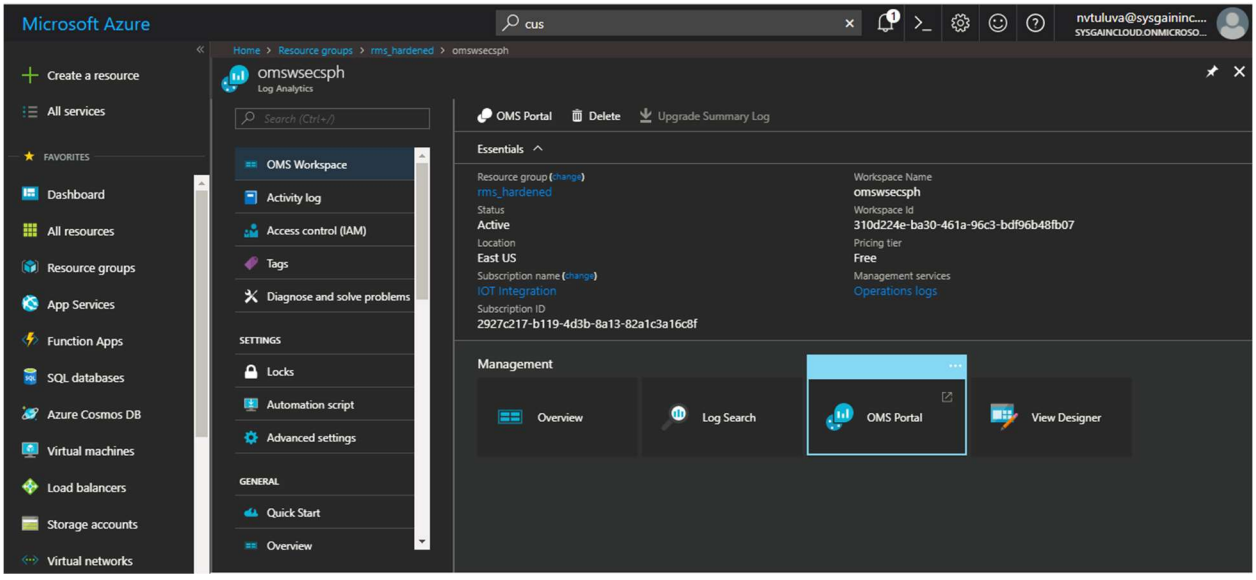
In this Deployment we are using below two solutions.

- Azure SQL Analytics
- Azure Web Apps Analytics

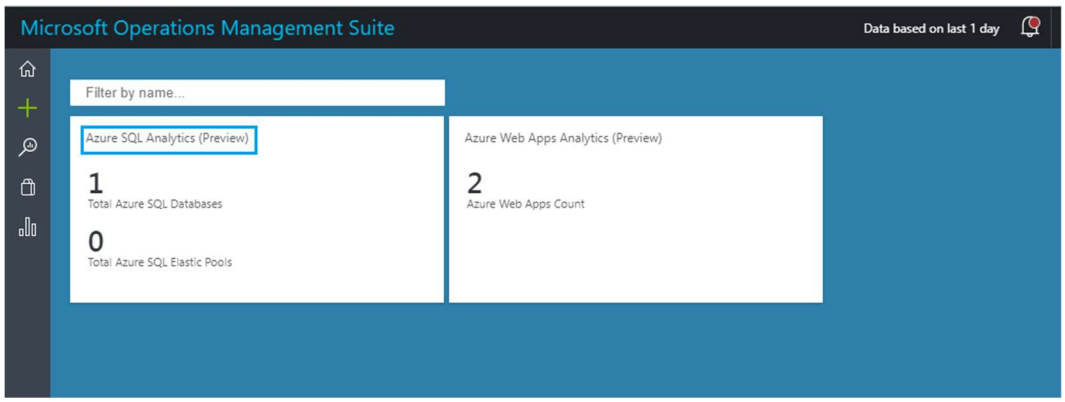
1. Go to **Azure portal > Resource group > Deployments> Microsoft.Template.** Get the **OMS Portal URL** from the **Outputs** section as shown in the following figure.



2. Click **OMS Portal** as shown in the following figure.



3. Open **OMS log analytics** portal by copying the URL in the output section in new tab where user is already logged into azure portal.



14.2.1. SQL Analytics

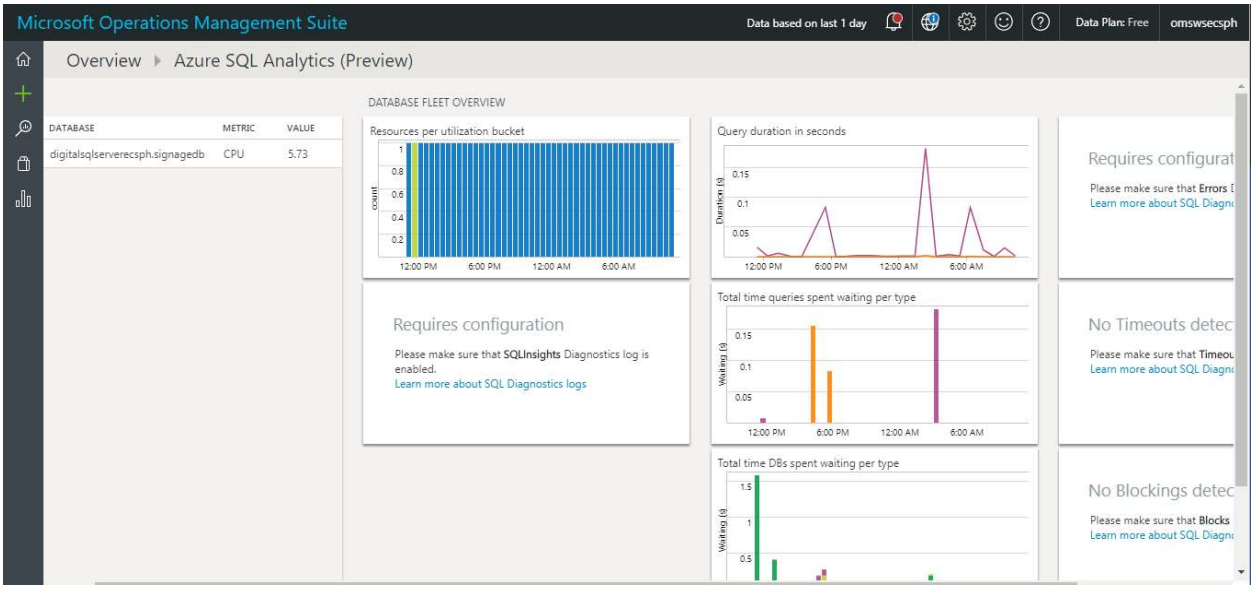
Azure SQL Analytics solution in Azure Log Analytics collects and visualizes important SQL Azure performance metrics.

The dashboard includes the overview of all databases that are monitored through different perspectives. Selecting any of the tiles, opens a drill-down report into the specific perspective. Once the perspective is selected, the drill-down report is opened.

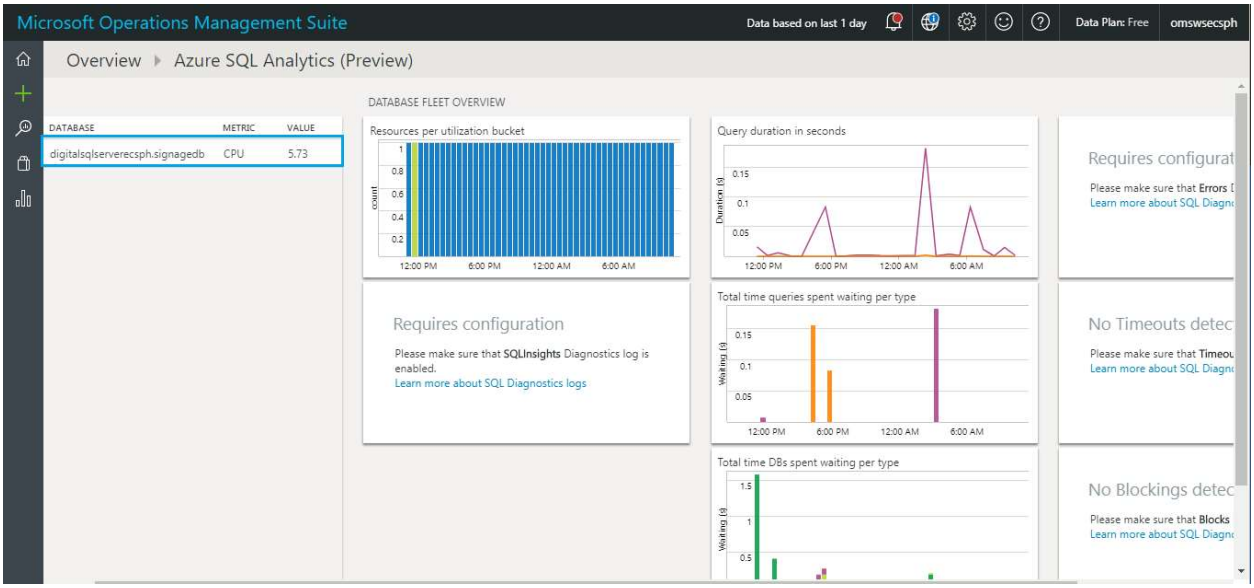
Using this solution, we can find out below metrics:

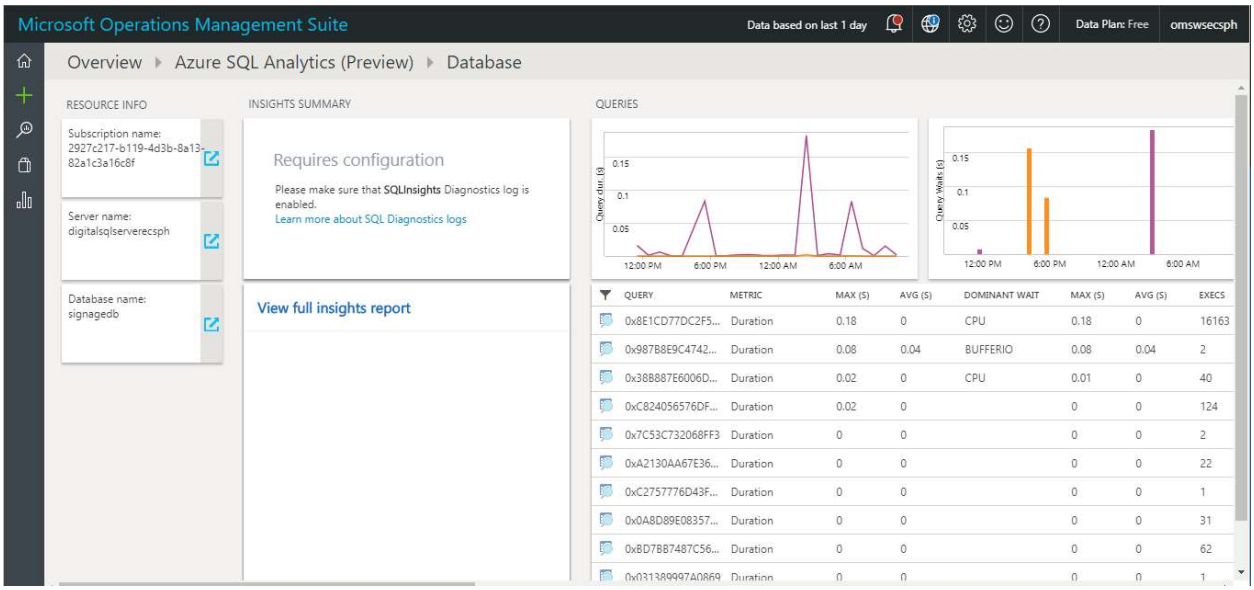
- List of SQL Servers
- List of Databases
- Database Usage
- Query Duration
- Resource Utilization Like Storage, CPU percent, Deadlock and Physical data read
- Etc.

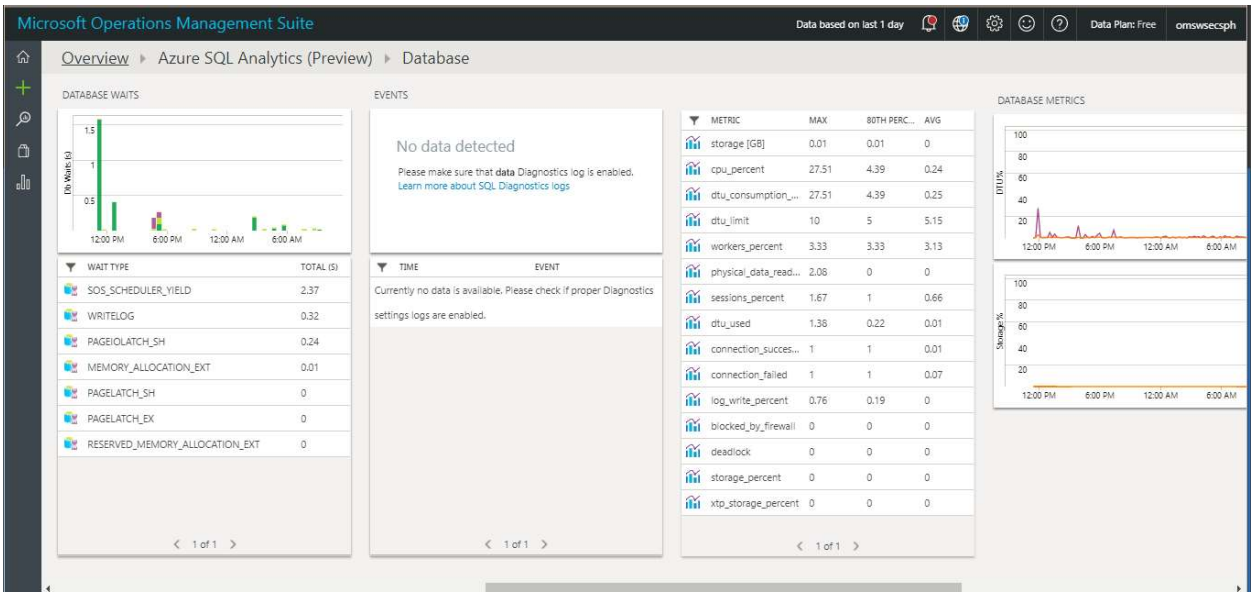
1. Click the **Azure SQL Analytics (Preview)** link the analytics page is displayed as shown in the following figure.



2. Click **digitalsqlserverft5zx** to open the database page as shown in the following figure.







14.2.2. Azure Web Apps Analytics

The Azure Web Apps Analytics (Preview) solution provides insights into your Azure Web Apps by collecting different metrics across all your Azure Web App resources.

Using the solution, you can view the:

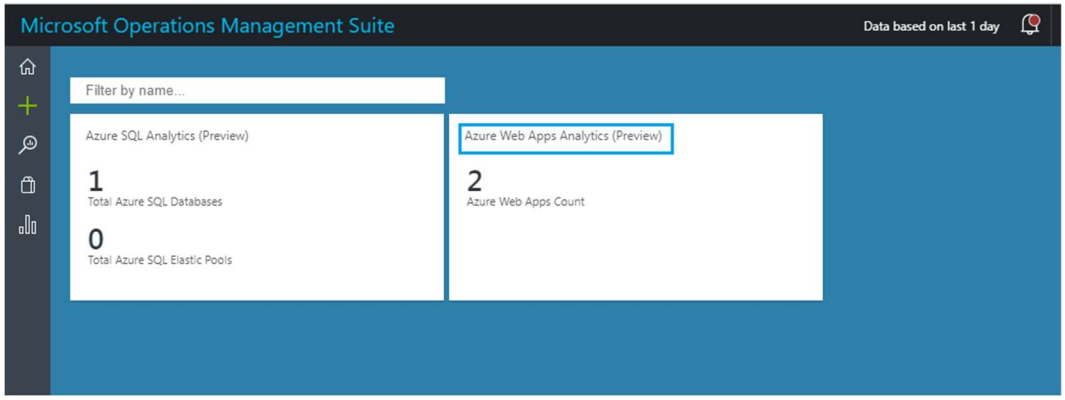
- Top Web Apps with the highest response time
- Number of requests across your Web Apps, including successful and failed requests
- Top Web Apps with highest incoming and outgoing traffic

- Top service plans with high CPU and memory utilization
- Azure Web Apps activity log operations

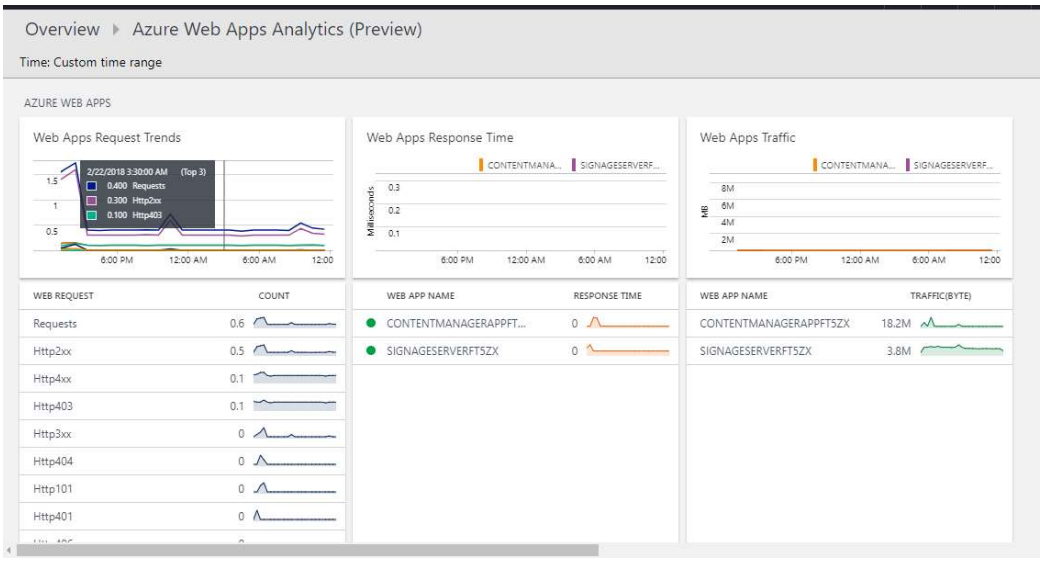
Azure Web Apps metrics like

- Average Memory Working Set
- Average Response Time
- Bytes Received/Sent
- CPU Time
- Requests
- Memory Working Set
- Httpxxx

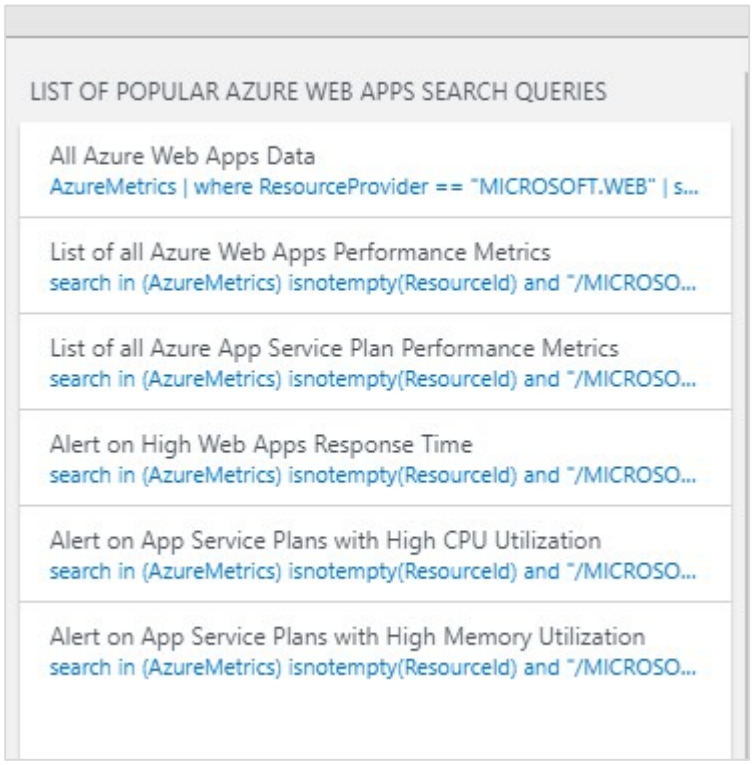
1. Open the **Microsoft Operations management Suite**.



2. Click the **Azure Web Apps Analytics (Preview)** link the following page is displayed.



3. Use the horizontal scroll bar at the bottom of the page to get more insights on web apps.



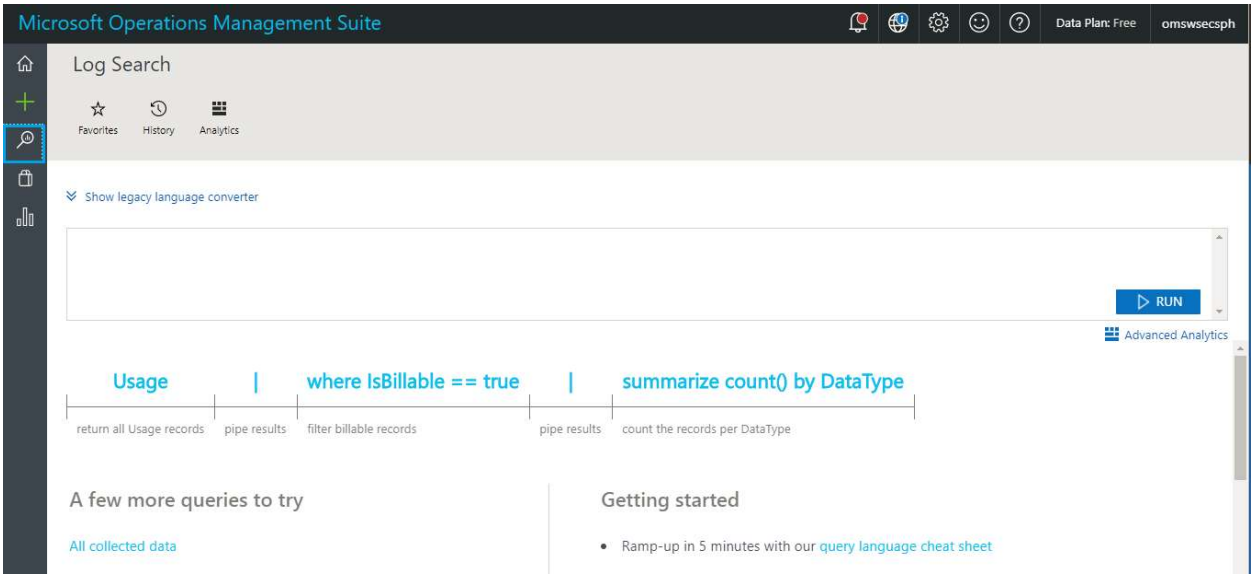
14.2.3. Log Search

Log search to retrieve any data from Log Analytics. Whether you're analyzing data in the portal, configuring an alert rule to be notified of a condition, or retrieving data using the Log Analytics.

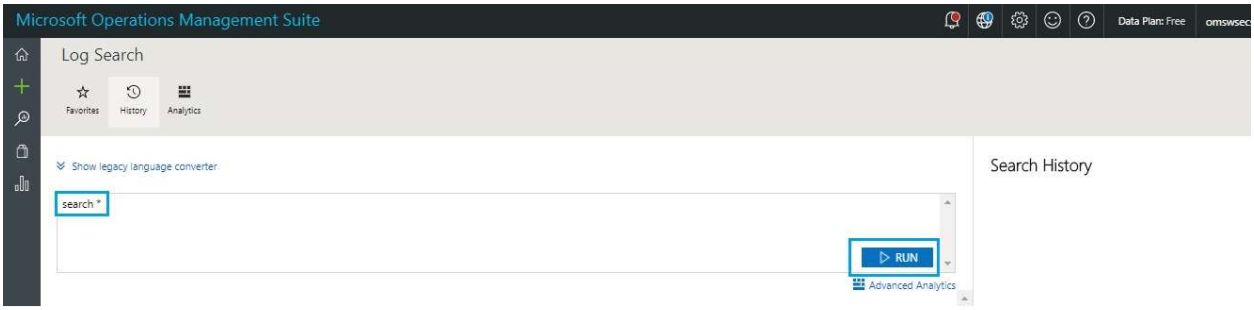
Perform interactive analysis of data in the repository in the Azure portal or the Advanced Analytics portal.

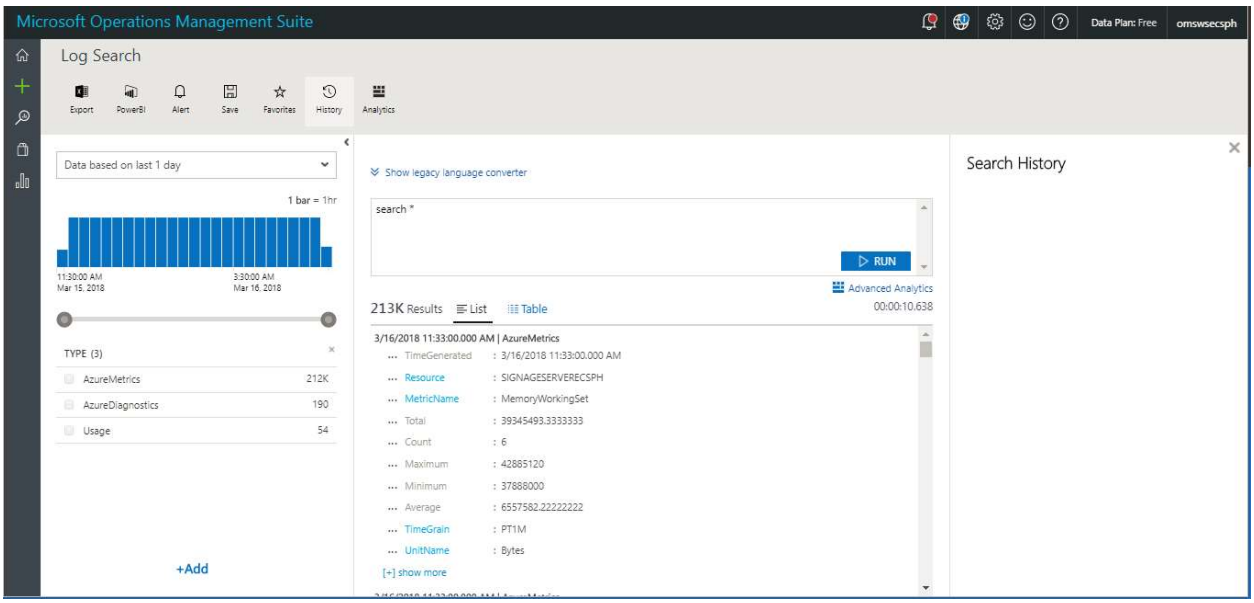
Create visualizations of data to be included in user dashboards with View Designer. Log searches provide the data used by tiles and visualization parts in each view.

1. Go to homepage, Click **Log Search** the following search page is displayed as shown in the following figure.



2. Enter key word **search *** in the box, the details are displayed below the box as shown in the following figure.





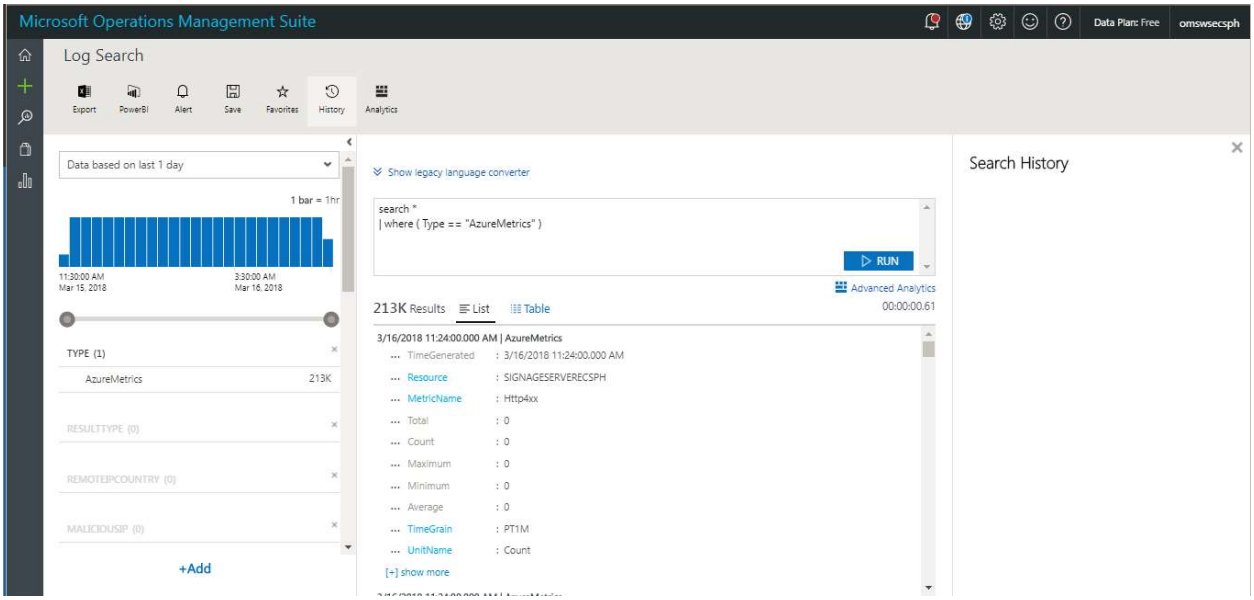
14.2.4. IoT HUB

Go to **Log Search** page and enter the below query.

search *

| where (Type == "AzureMetrics")

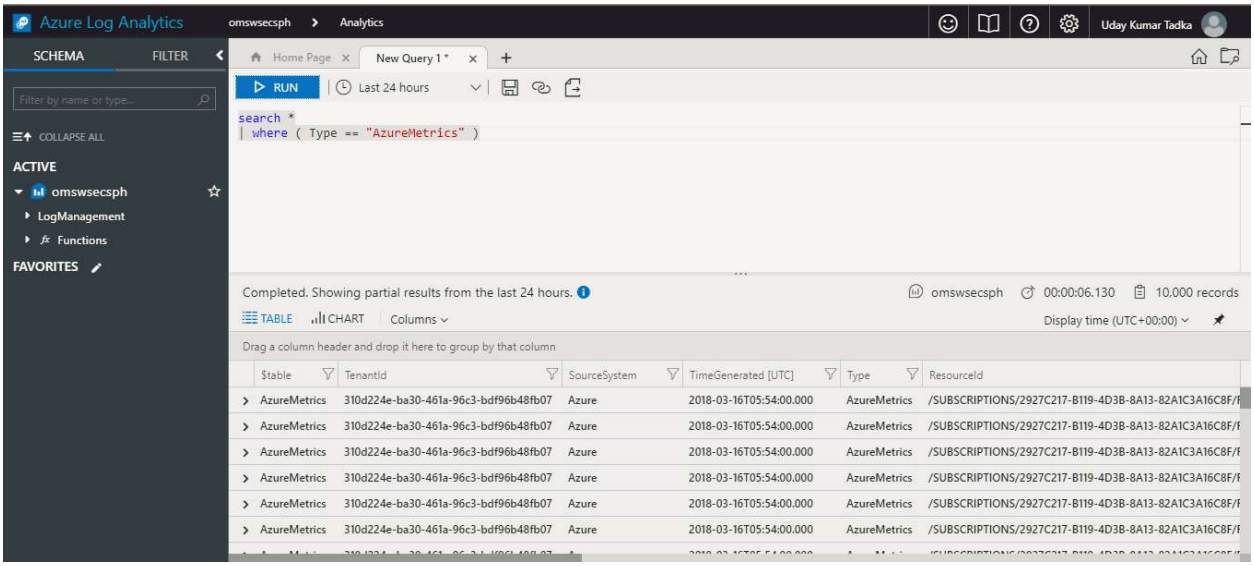
| search "DIGITAL-SIGNAGEHUBFT5ZX" to display the data relevant to IoT HUB as shown in the following figure.



14.2.5. Analytics Page

Analytics portal is a web tool to write and execute Azure Log Analytics queries. Performs interactive analysis of data in the repository in the Azure portal or the Advanced Analytics portal. Create visualizations of data to be included in user dashboards with View Designer. Log searches provide the data used by tiles and visualization parts in each view.

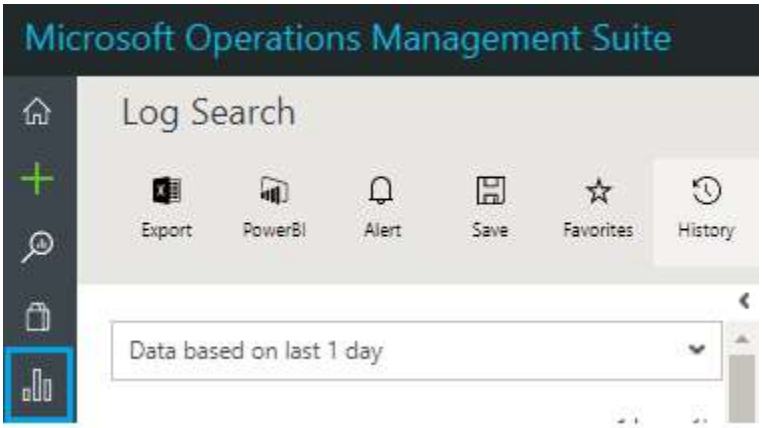
Click **Analytics** to view the charts and tables.

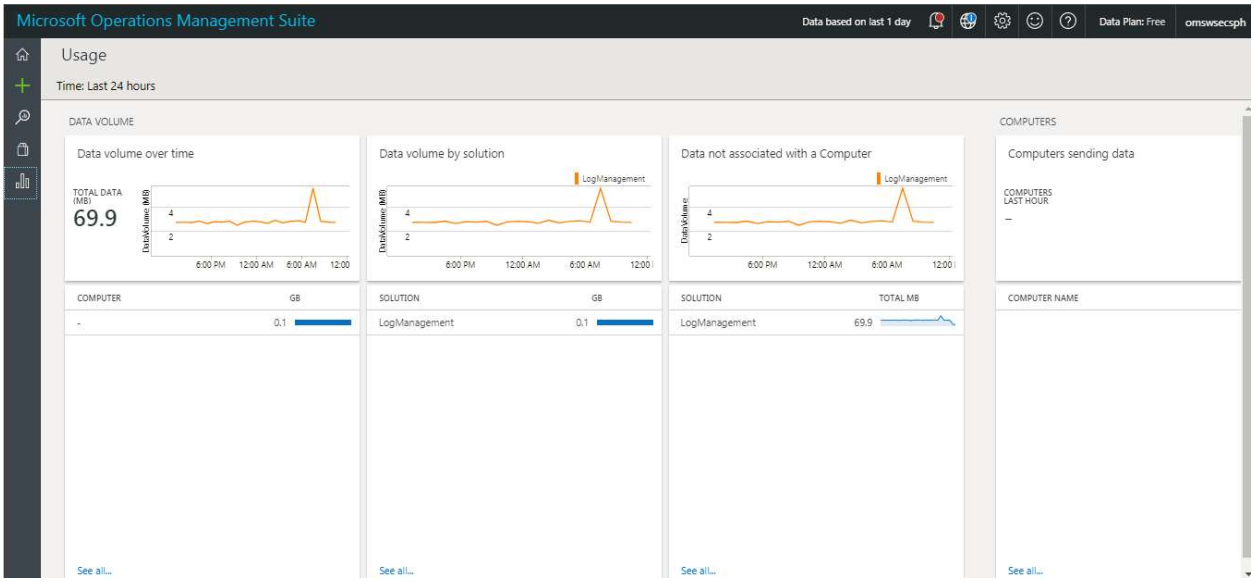


14.2.6. Usage Page

Usage page provides the utilization of OMS Workspace. In the Usage page the details such as data volume utilization, Computers connected to workspace are displayed.

Click **Usage** icon to view the utilization of the OMS workspace.





15. Azure Security Center

What is Azure Security Center?

Azure Security Center helps you prevent, detect, and respond to threats with increased visibility into and control over the security of your Azure resources. It provides integrated security monitoring and policy management across your subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.

Azure Security Center analyzes data from the following sources to provide visibility into your security state, identify vulnerabilities and recommend mitigations, and detect active threats:

- **Azure Services:** Uses information about the configuration of Azure services you have deployed by communicating with that service's resource provider.
- **Network Traffic:** Uses sampled network traffic metadata from Microsoft's infrastructure, such as source/destination IP/port, packet size, and network protocol.
- **Partner Solutions:** Uses security alerts from integrated partner solutions, such as firewalls and antimalware solutions.
- **Virtual Machines and Servers:** Uses configuration information and information about security events, such as Windows event and audit logs, IIS logs, syslog messages, and crash dump files from your virtual machines. In addition, when an alert is created, Azure Security Center may generate a snapshot of the VM disk affected and extract machine

artifacts related to the alert from the VM disk, such as a registry file, for forensics purposes.

Why use Security Center?

Security Center provides below features to manage infrastructure.

- Centralized policy management
- Continuous security assessment
- Actionable recommendations
- Advanced cloud defenses
- Prioritized alerts and incidents
- Integrated security solutions

Which Azure resources are monitored by Azure Security Center?

Azure Security Center monitors the following Azure resources:

- Virtual machines (VMs)
- Azure Virtual Networks
- Azure SQL service
- Azure Storage account
- Azure Web Apps (in App Service Environment)
- Partner solutions integrated with your Azure subscription such as a web application firewall on VMs and on App Service Environment

15.1. Uses of Azure Security Center

- Monitor security across on-premises and cloud workloads
- Apply policy to ensure compliance with security standards
- Find and fix vulnerabilities before they can be exploited
- Use access and application controls to block malicious activity
- Leverage advanced analytics and threat intelligence to detect attacks
- Simplify investigation for rapid threat response
- Analyze and investigate incidents
- Detect threats before they happen
- Streamline security audits
- Automatic data collection
- Efficient data storage

15.2. Limitations of Azure Security Center

- Azure Security Center is only capable of Monitoring Virtual Machine, SQL Server, Storage Account.
- Using Security Center IoT HUB, Web Applications and other Azure Resources can't be monitored.

15.3. Azure Security Center Pricing Model

FEATURES	FREE (AZURE RESOURCES ONLY)	STANDARD (HYBRID AND AZURE RESOURCES)
Security policy, assessment and recommendations	✔	✔
Connected partner solutions	✔	✔
Security event collection and search	- -	✔
Just in time VM Access	- -	✔
Adaptive application controls	- -	✔
Advanced threat detection for networks, VMs/servers and Azure services	- -	✔
Built-in and custom alerts	- -	✔
Threat intelligence	- -	✔
Included Data	Not applicable	500 MB per day[1]
Price	Free	$15 / node[2] / month

15.4. Monitoring Metrics

Azure Security Center analyzes the security state of your Azure resources. When Security Center identifies potential security vulnerabilities, it creates recommendations that guide you through the process of configuring the needed controls.

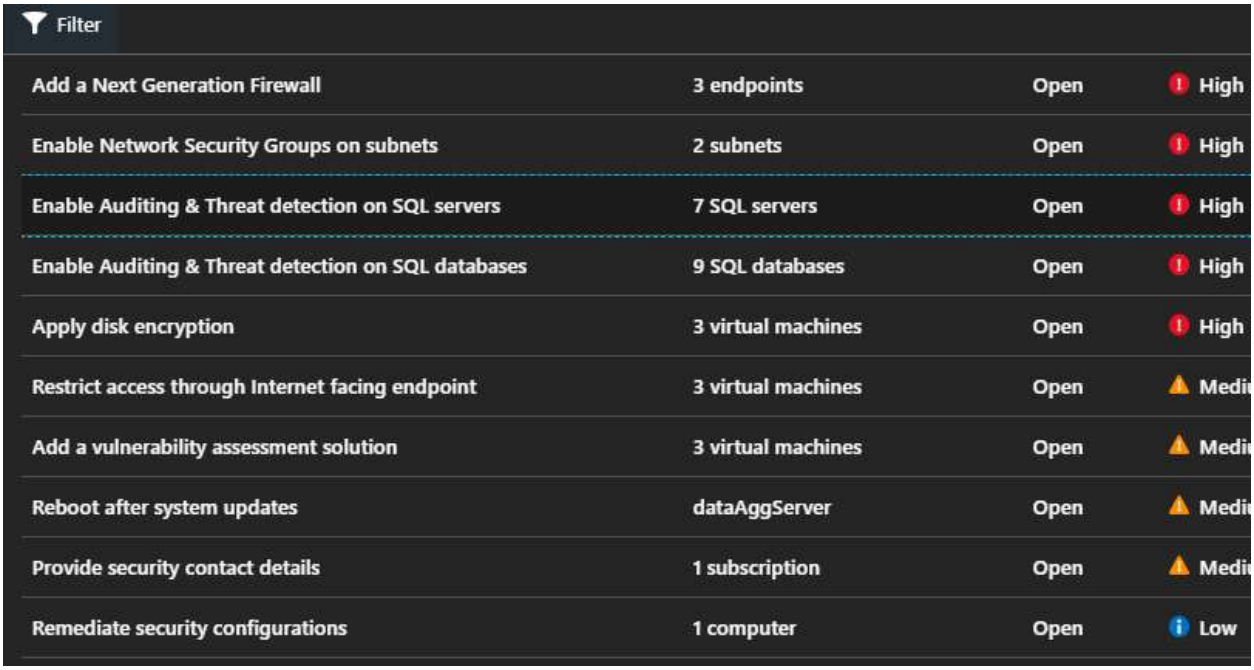
Protecting Azure SQL service and data in Azure Security Center

Available SQL service and data recommendations

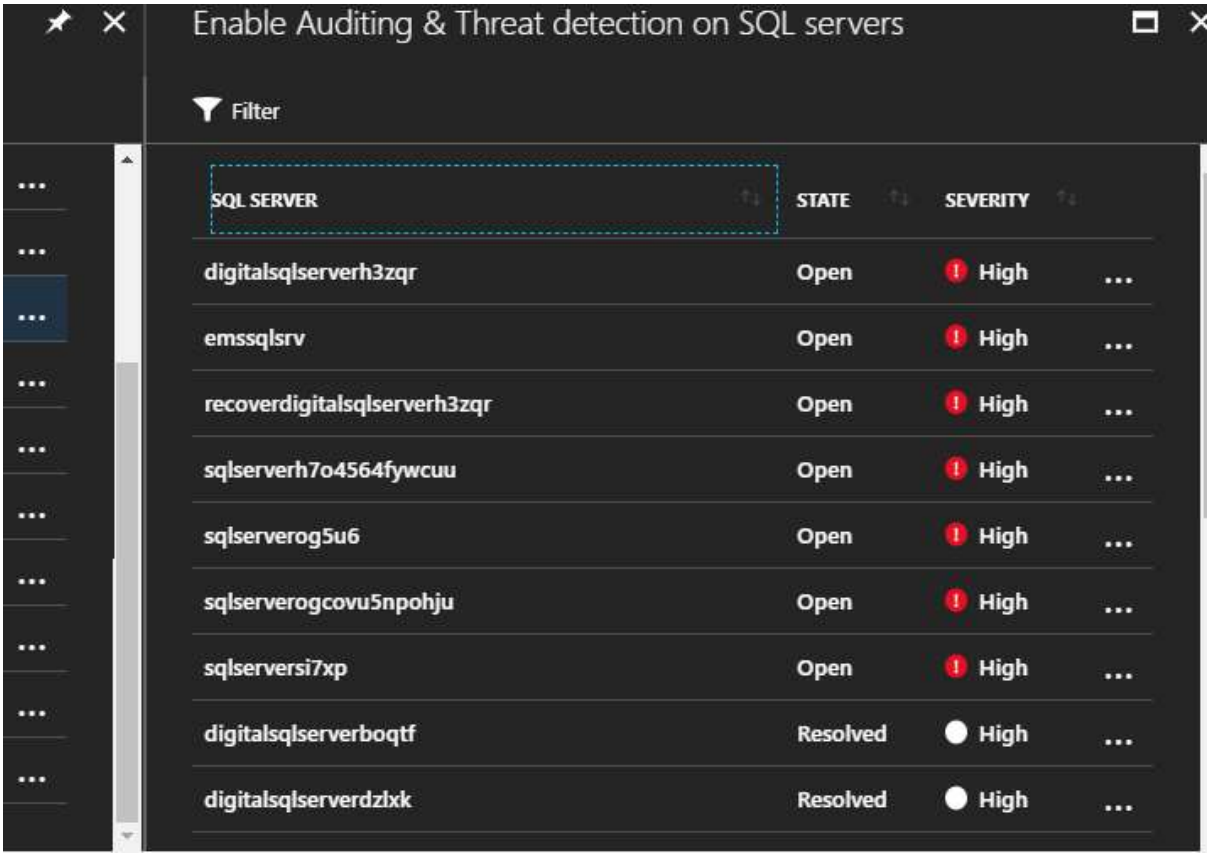
- Enable auditing and threat detection on SQL servers
- Enable auditing and threat detection on SQL databases
- Enable Transparent Data Encryption on SQL databases
- **Enable auditing and threat detection on SQL servers**

To Enable auditing and threat detection on SQL servers follow the below steps:

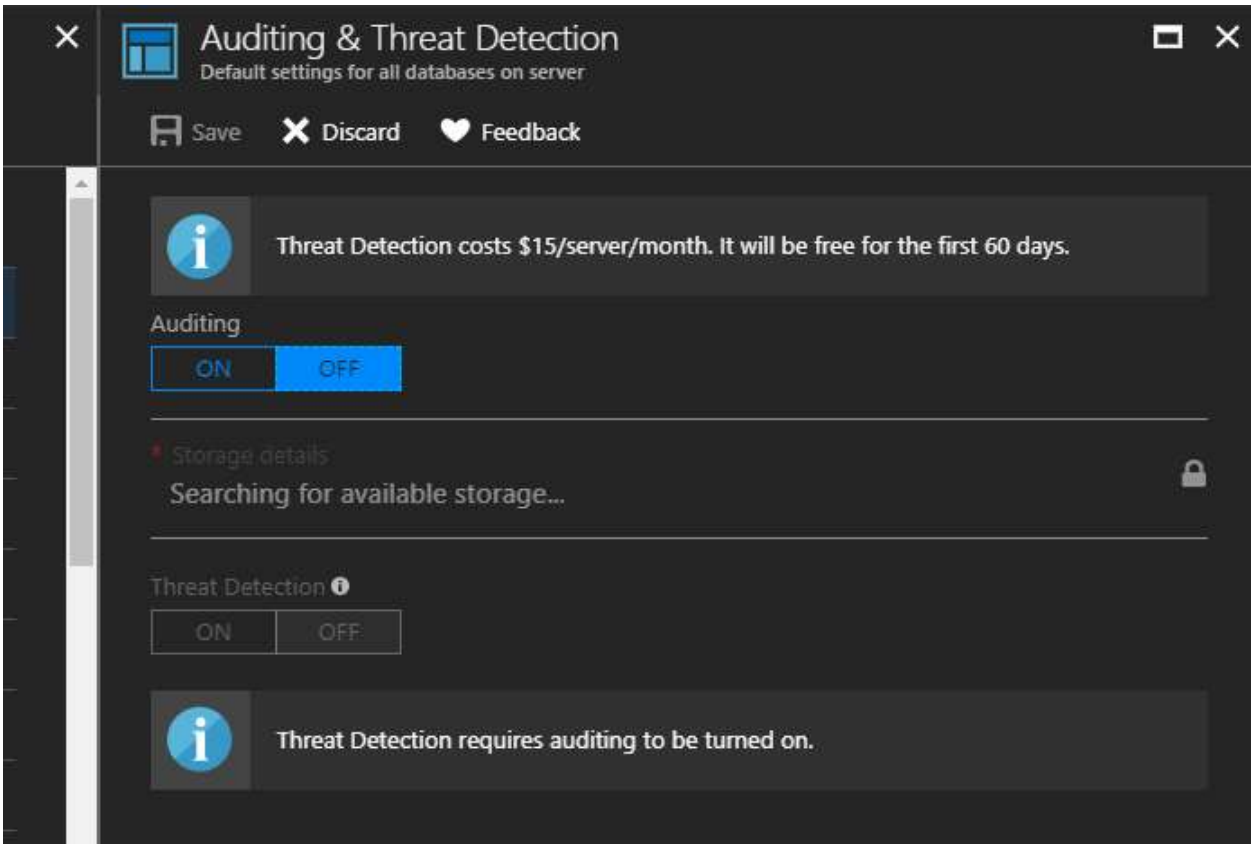
1. Click **Enable auditing and threat detection on SQL servers** as shown in the following figure.



2. The list of servers are displayed as shown in the following figure. Choose the required **SQL Server**.



3. A New page is displayed, where we can configure **Audit & Threat Detection**.



4. After Choosing Storage Account Select **ON** for both **Auditing** and **Threat Detection**.
5. Set Security Policy to enable SQL Auditing and Threat Detection and SQL transparent data encryption. Similarly **Enable auditing and threat detection on SQL databases.**

15.5. Difference between OMS and Security Centre

Azure Security Center focuses on preventing, detecting, and responding to threats with increased visibility and control over the security of a customer's Azure resources – it is a narrower view but a more in-depth one focused on just security.

Microsoft recently unified Azure Security Center (ASC) and the Operations Management Suite (OMS). This means ASC now offers the same functionality as OMS plus a few additional features.

- Recover deleted or overwritten files from network shares
- Eliminate time consuming restores from backup
- Continuous data protection for easy, instant file recovery

- Supports end user self-service

Operations Management Suite (OMS) is an online service from Microsoft which covers four major areas: Log Analytics, Automation, Backup, and Site Recovery. The last three encompass the corresponding Azure services:

Log Analytics gathers data using the Microsoft Monitoring Agent (MMA). It gets the data from your on-premises or cloud-hosted resources and lets you search and analyze large amounts of data quickly.

Azure Security Center **(ASC)** on the other hand is an Azure service that monitors your Windows and Linux computers across both Azure (and other clouds) and on-premises workloads for true hybrid monitoring. The aim here is to apply security policies across all workloads, continuously assess compliance with policy, and provide actionable recommendations to deal with security vulnerabilities.

Note that the free tier of ASC only covers Azure resources, whereas the Standard tier can deal with hybrid workloads as well. Also, just-in-time (JIT) virtual machine (VM) access, threat intelligence, and a few other features are only available in the Standard tier.

ASC includes the same capabilities as the OMS Security & Compliance solution. This collects security events (and lets you search across them lightning fast). It displays dashboards for system update status, antivirus (AV) status, and identity and access. ASC adds policies, recommendations to help fix vulnerabilities, automatic discovery of new Azure resources, additional monitoring of VMs, and network, storage, and SQL configuration in Azure.

Azure Security Center Data Replication

Data Captured through Azure Security Center will be stored in same Geo Region to Support compliance.

VM Geo	Workspace Geo
United States, Brazil, Canada	United States
Europe, United Kingdom	Europe
Asia Pacific, Japan, India	Asia Pacific
Australia	Australia

What are security policies?

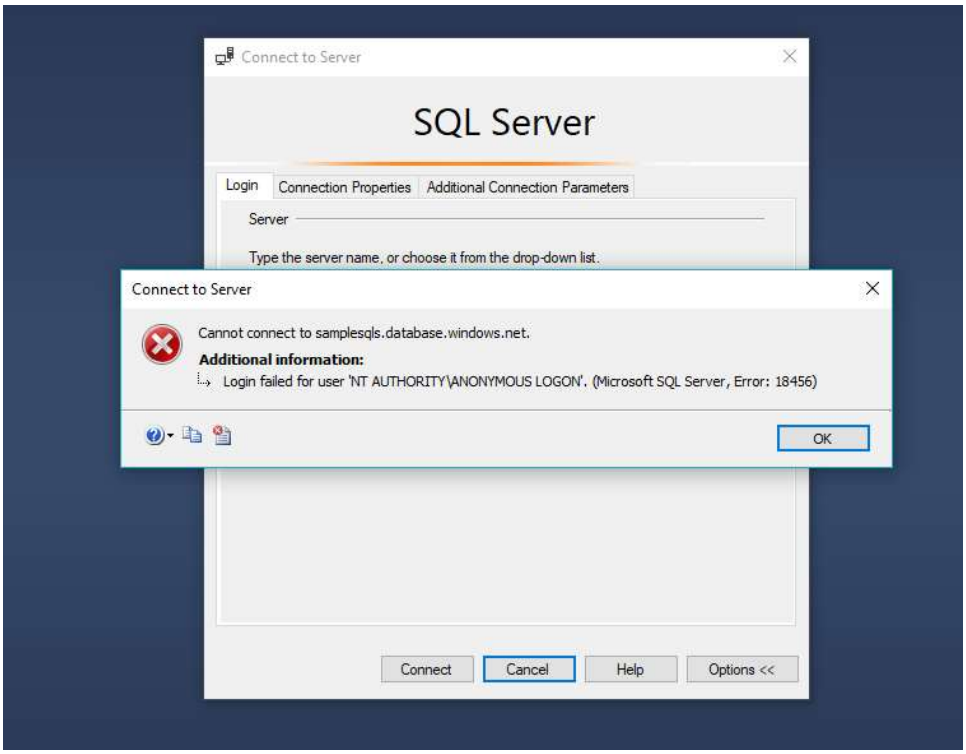
A security policy defines the desired configuration of your workloads and helps ensure compliance with company or regulatory security requirements. In Azure Security Center, you can

define policies for your Azure subscriptions and tailor them to your type of workload or the sensitivity of your data.

Security Center policies contain the following components:

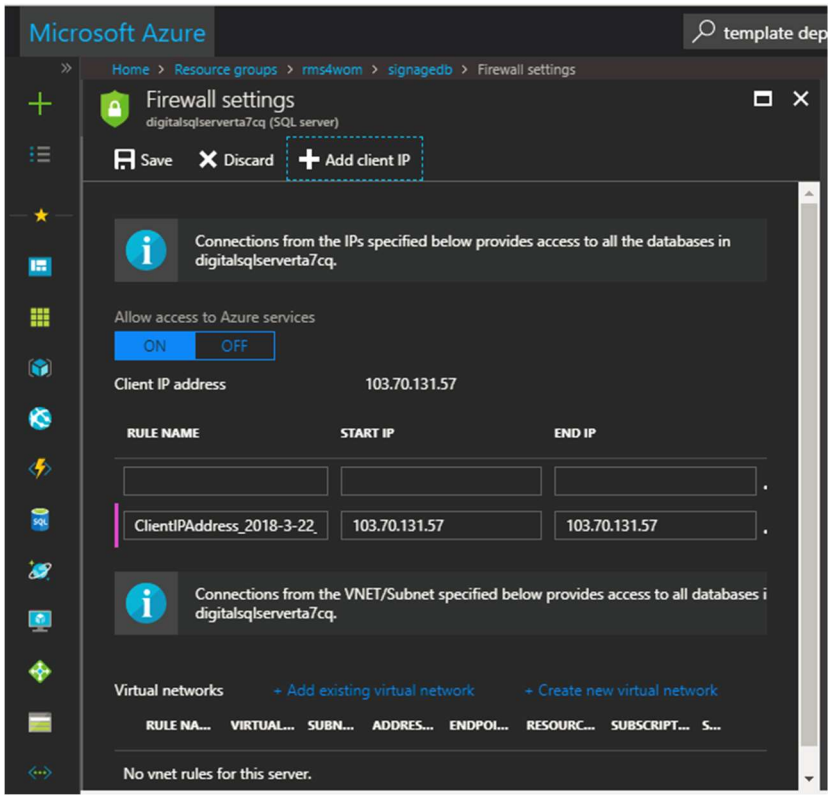
- Data collection
- Security policy
- Email notifications
- Pricing tier

16. Access SQL Database using Active Directory

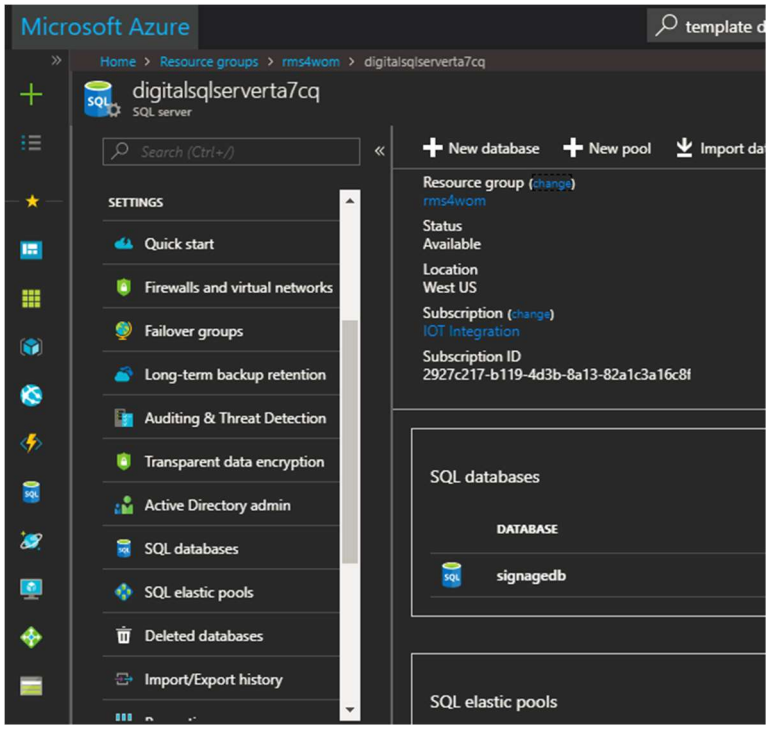


To Enable Firewall settings:

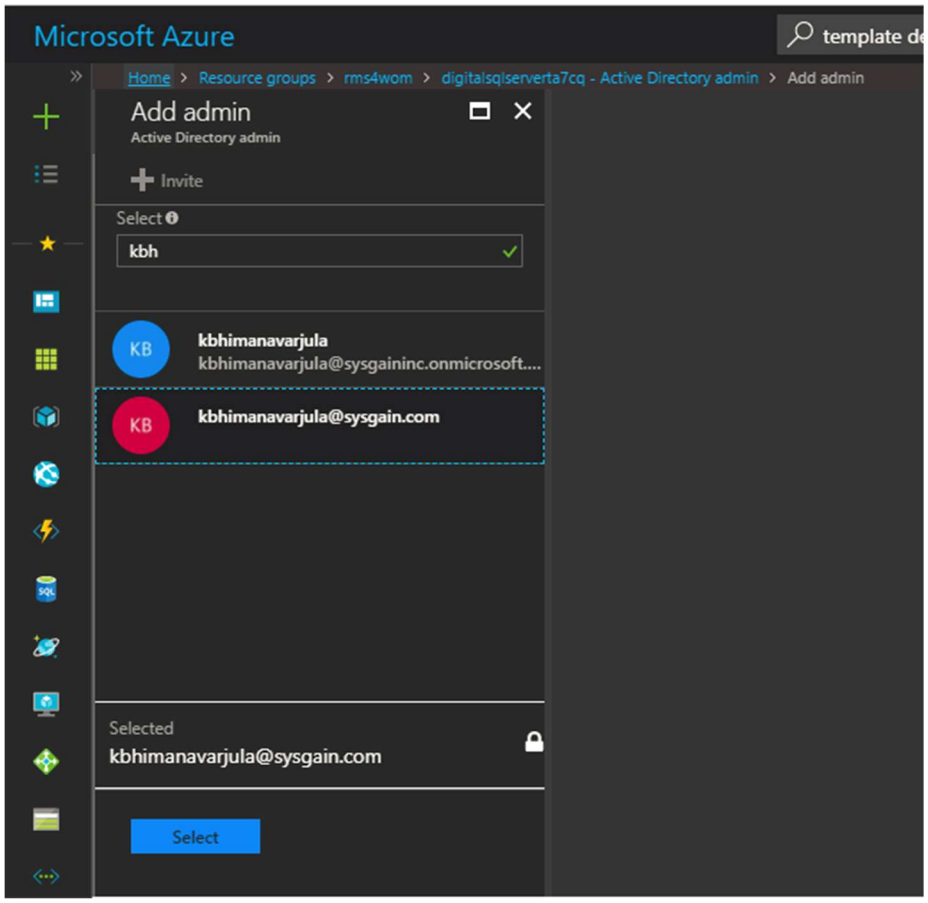
1. Go to the resource group and select the database click **Firewall Setting** ,click **Add Client IP** and click **Save** as shown in the following figure.

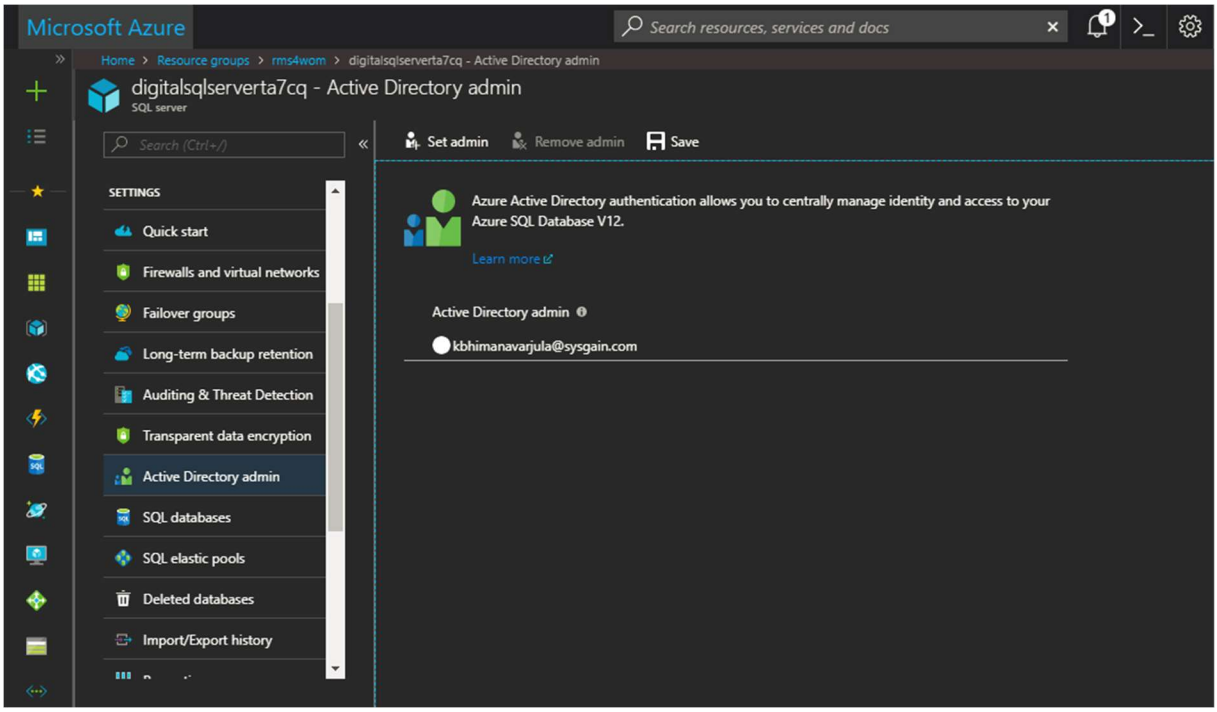


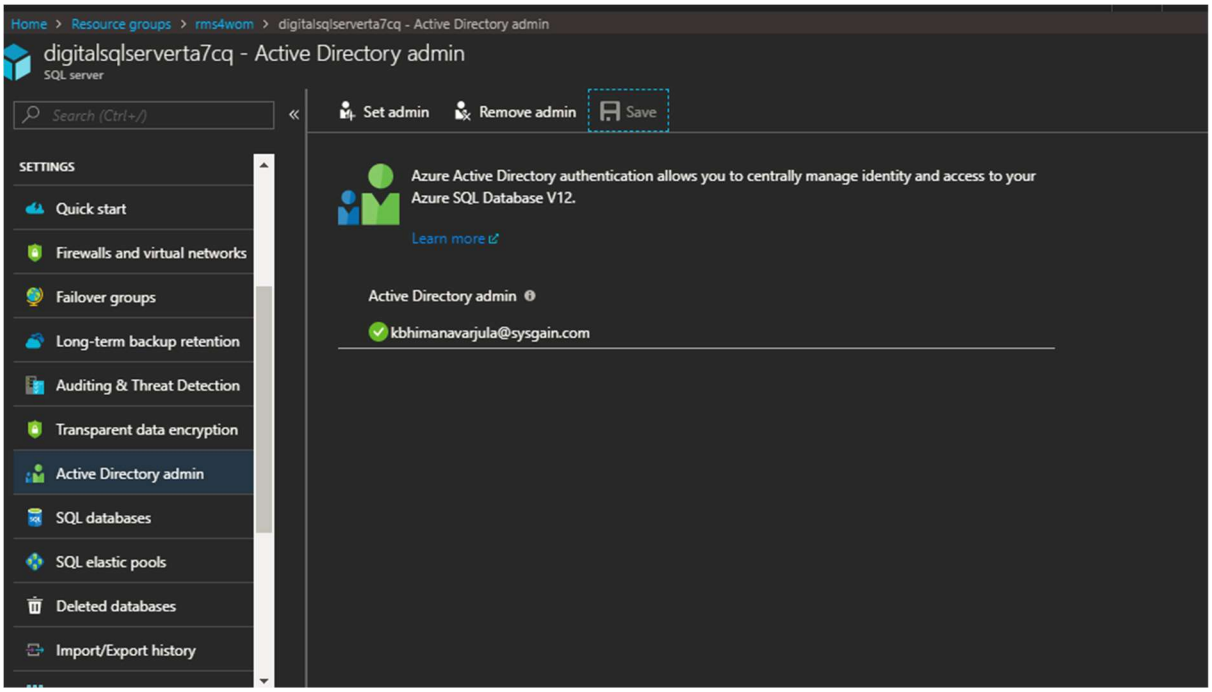
2. Select your **Sql Server** from the **Azure Portal** and click **Active Directory Admin**



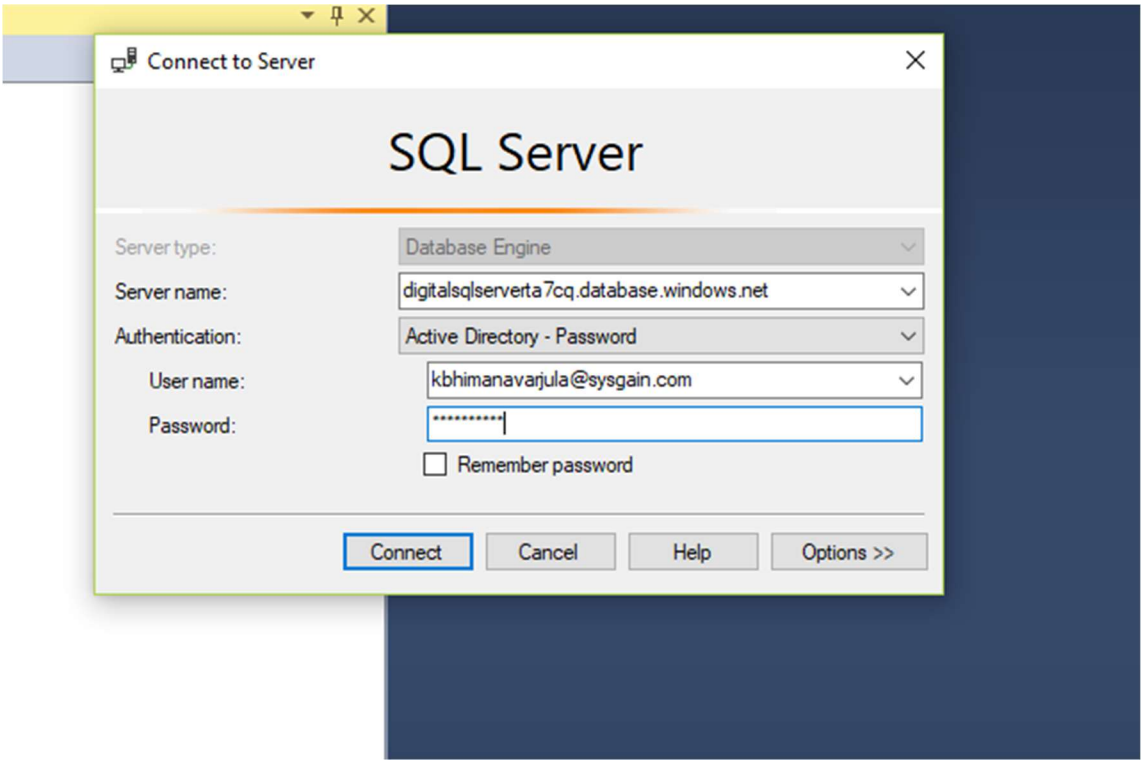
3. Select the **Admin Id** as shown in the following figure and click **Set Admin** and **Save**

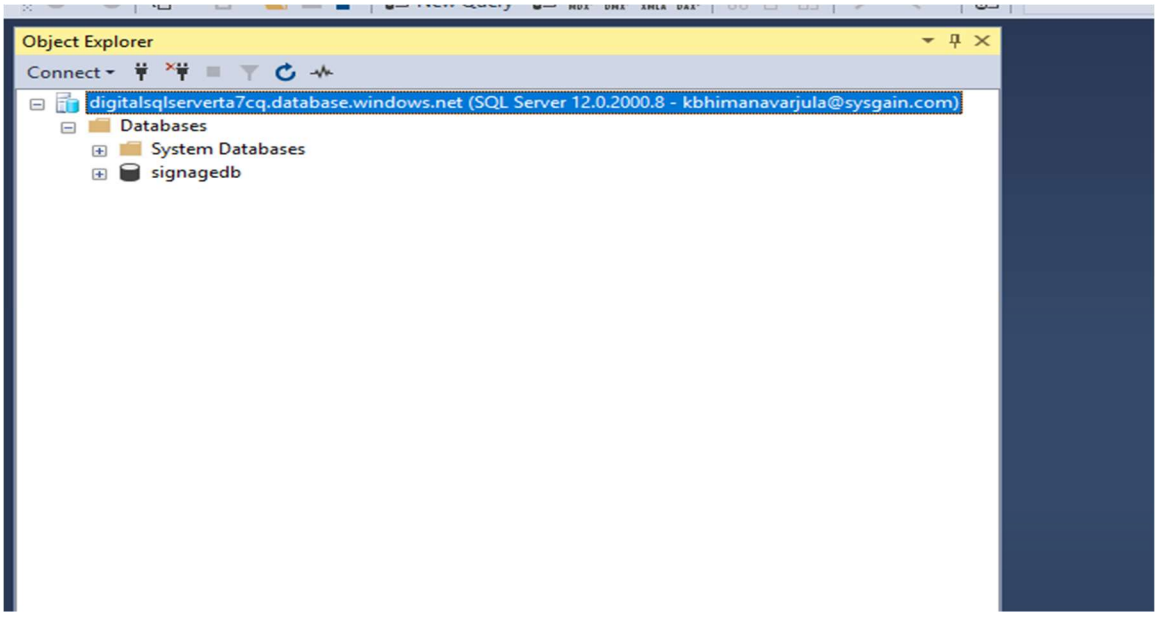






4. Now you will be able to **Acess Sql Server** using AD authentication as shown in the following figure.





End of the Document

Thank You

Visit us at www.Sysgain.com