

DIGITAL SIGNAGE

HARDENING

04/02/2018

Table of Content

1. About Digital Signage	5
2. Architecture Diagram.....	5
3. Azure Services	7
3.1. Azure blob.....	7
3.2. Azure IoT HUB.....	7
3.3. Azure Web App	7
3.4. Azure Web Job.....	7
3.5. Azure SQL DB	8
4. Definitions	9
5. High Level Deployment Process	10
5.1. ARM Template Definition	10
6. Deployment Costs.....	11
7. Pre-requisites	17
7.1. GUID Generator.....	17
8. ARM Template Input Parameters	18
9. Getting Started	22
9.1. Setting Azure AD Directory and App registration.....	22
9.2. ARM template deployment.....	27
9.3. Deployment Scenario.....	29
9.3.1. Deploy ARM Templates using Azure portal.....	29
9.3.2. Deploy ARM Templates using Azure CLI.....	39
9.3.3. Customize main-template.parameters.json file	39
9.3.4. Create Resource Group for Digital Signage solution	42
9.3.5. Execute the template deployment	42
10. Post Deployment.....	43
11. Digital Signage Dps Player	46
11.1. Installation of Stick Player software on a Virtual machine.....	46
12. Signup to Digital signage UI.....	53

12.1. Add Device.....	55
12.2. Device Group	56
12.2.1. Create Device Group	57
12.2.2. Assign a device to the device group	58
12.3. Content	60
12.3.1. Add Content – Predefined Template	61
12.4. Playlist.....	64
12.4.1. To Add a Playlist.....	64
13. Validation.....	67
13.1. SQL Server verification	67
13.2. Stick VM Cache Verification	73
13.3. DR Validation.....	75
13.3.1. Traffic Manager	76
13.3.2. Sign in to DigitalSignage UI	80
13.3.3. Geo Replication.....	89
13.3.4. Database Restore.....	93
14. Monitoring components	99
14.1. Azure Application Insights.....	99
14.1.1. Live Metrics Stream.....	101
14.1.2. Users	102
14.1.3. Metric Explorer	103
14.1.4. Metric preview	107
14.1.5. Application Map.....	110
14.2. OMS Log Analytics.....	111
14.2.1. SQL Analytics.....	113
14.2.2. Azure Web Apps Analytics	115
14.2.3. Log Search.....	117
14.2.4. IoT HUB	119

14.2.5. Analytics Page.....	119
14.2.6. Usage Page	120
15. Azure Security Center.....	121
15.1. Uses of Azure Security Center.....	122
15.2. Limitations of Azure Security Center	123
15.3. Azure Security Center Pricing Model.....	123
15.4. Monitoring Metrics.....	123
15.5. Difference between OMS and Security Centre	126
16. Access SQL Database using Active Directory.....	128

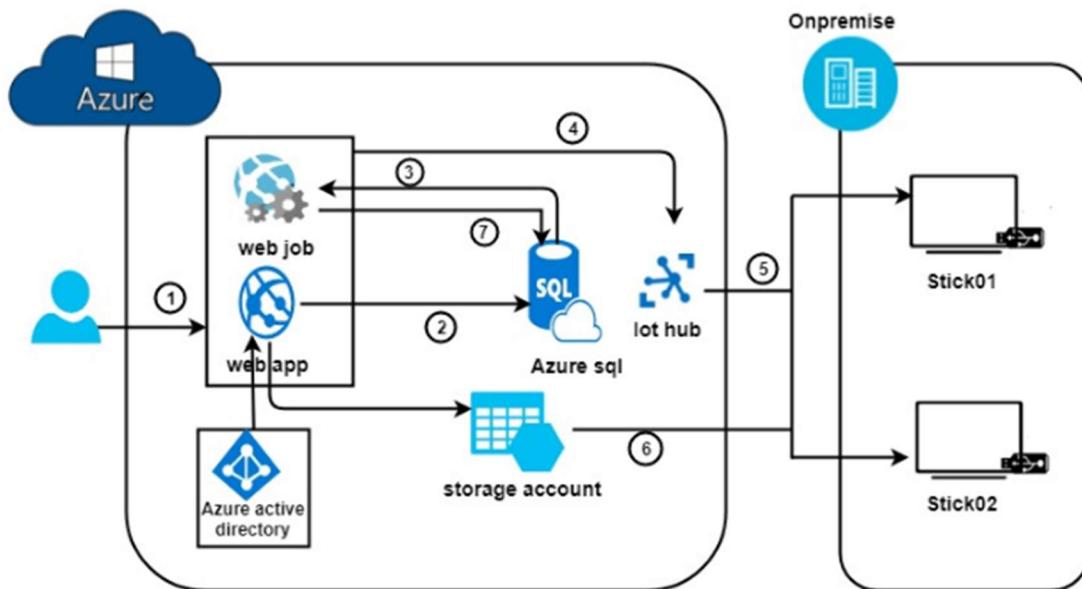
1. About Digital Signage

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.

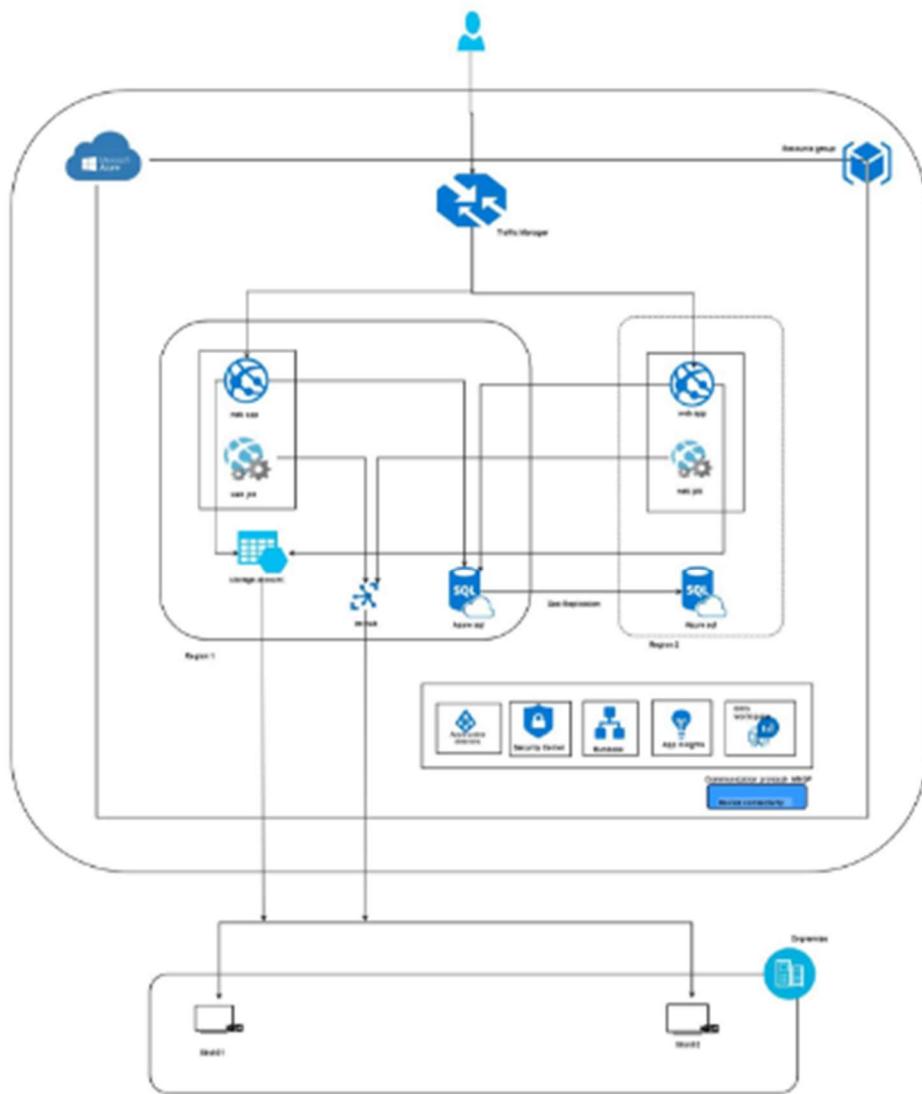
With digital signage, we can get as creative as your imagination allows, and the more innovative your ad, the more attention it's going to draw. Consider the following digital signage campaigns that have really went above and beyond to create a truly innovative customer experience.

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 **Binary Large Object**. 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

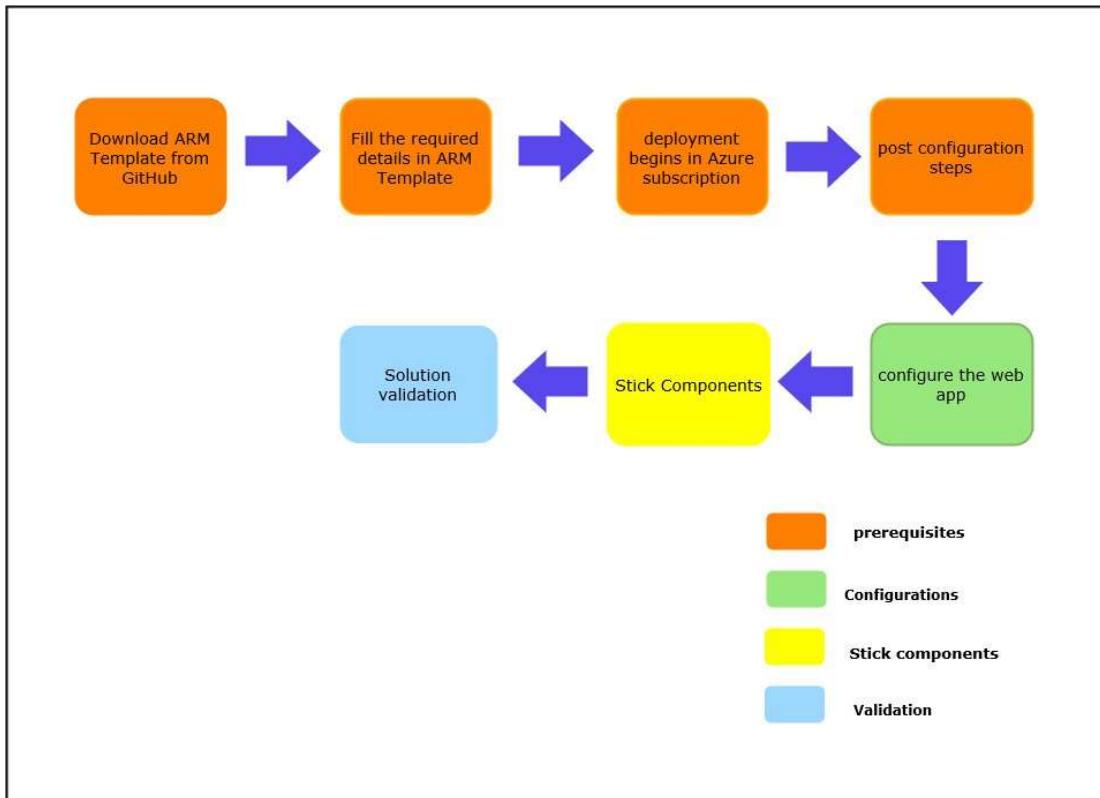
Azure SQL Database is a relational database-as-a service using the Microsoft SQL Server Engine. SQL Database is a high-performance, reliable, and secure database you can use to build data-driven applications and websites in the programming language of your choice, without needing to manage infrastructure.

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:

Secure | <https://www.guidgenerator.com/online-guid-generator.aspx>

Online GUID Generator

How many GUIDs do you want (1-2000):

Uppcase: {} Braces: Hyphens:
Base64 encode: RFC 7515: URL encode:

Generate some GUIDs!

Results:

Use these GUIDs at your own risk! No guarantee of their uniqueness or suitability is given or implied.

What is a GUID?

GUID (or UUID) is an acronym for 'Globally Unique Identifier' (or 'Universally Unique Identifier'). It is a 128-bit integer number used to identify resources. The term GUID is generally used by developers working with Microsoft technologies, while UUID is used everywhere else.

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	
sqlAdministratorLoginP assword	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://projectio t.blob.core.wind ows.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.

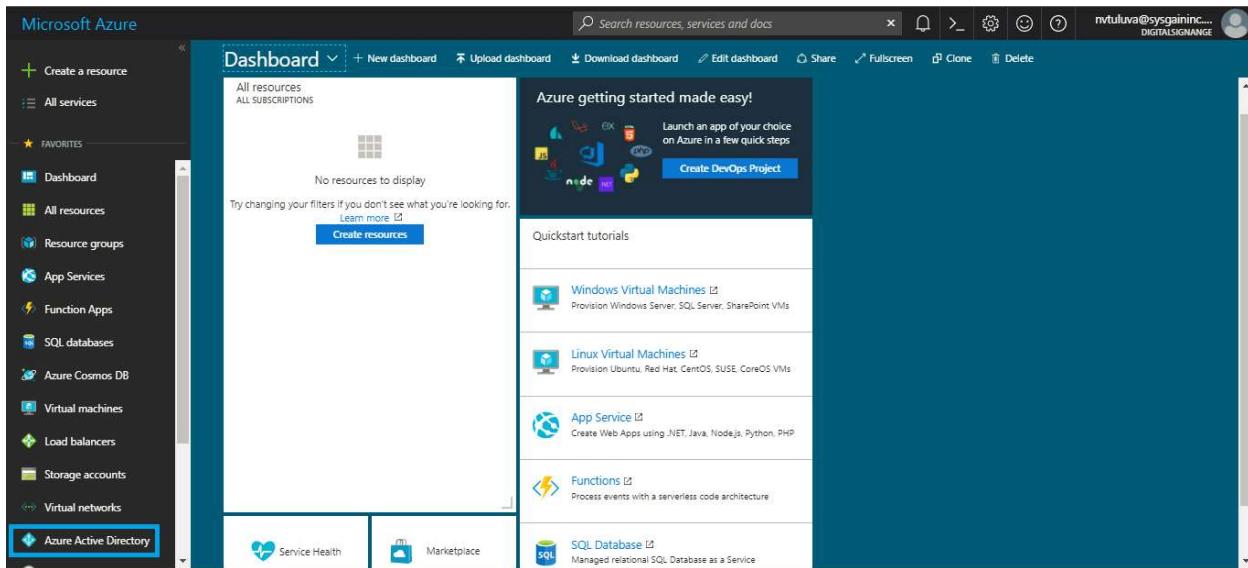
Also Go to settings > Reply URLs provide URL

<https://contentmanagercosfour.trafficmanager.net/> and click on save

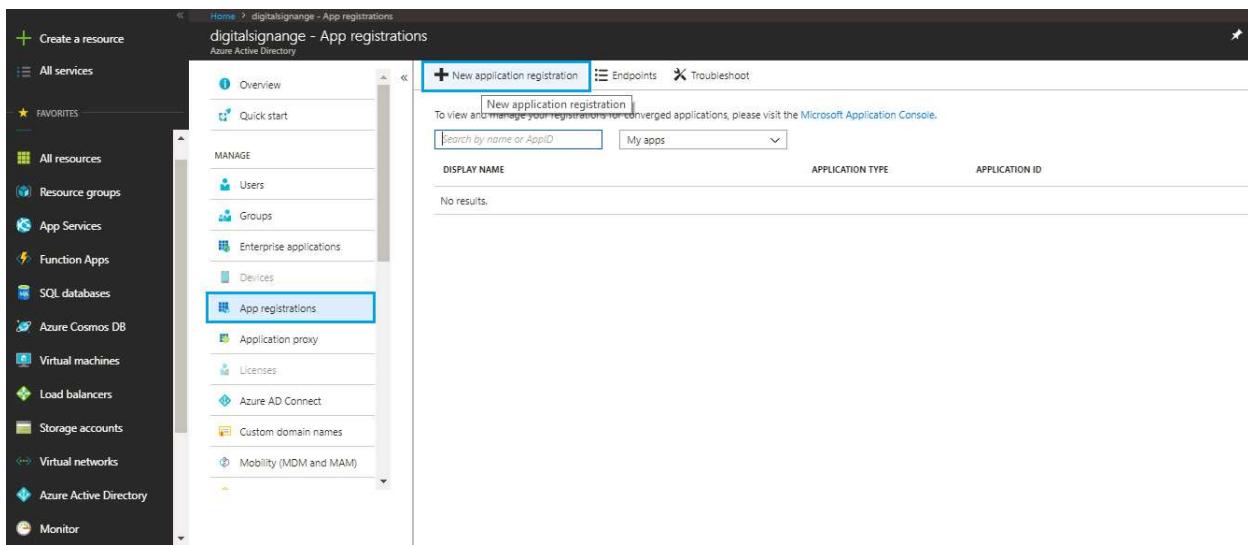
In Costingmodel4 It is important to note that for both the Applications, in the properties sections all the above mentioned URL's should be Trafficmanager URL's

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**.

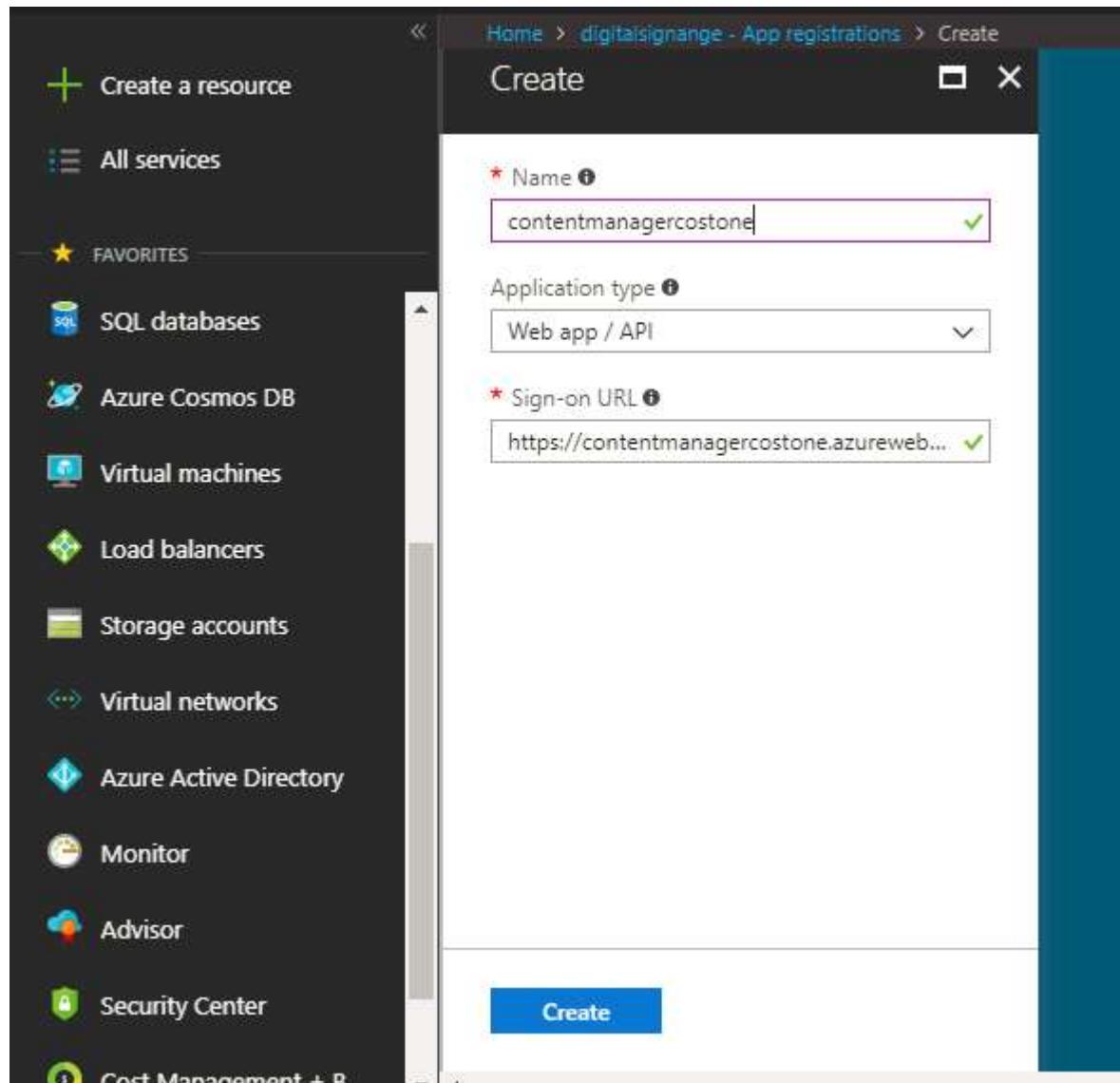


5. In the **Create** page, enter your application's registration information:

- **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

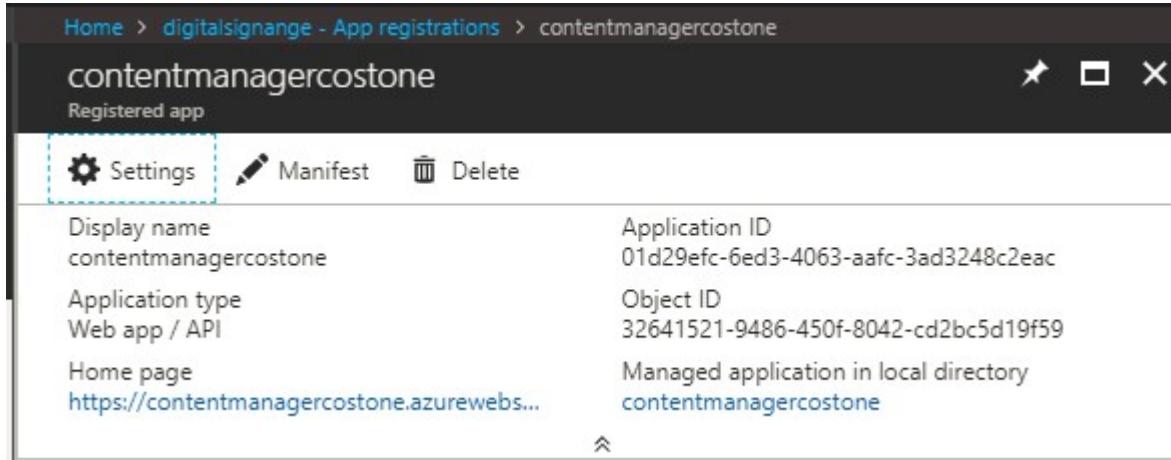
Application type: Web app / API

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

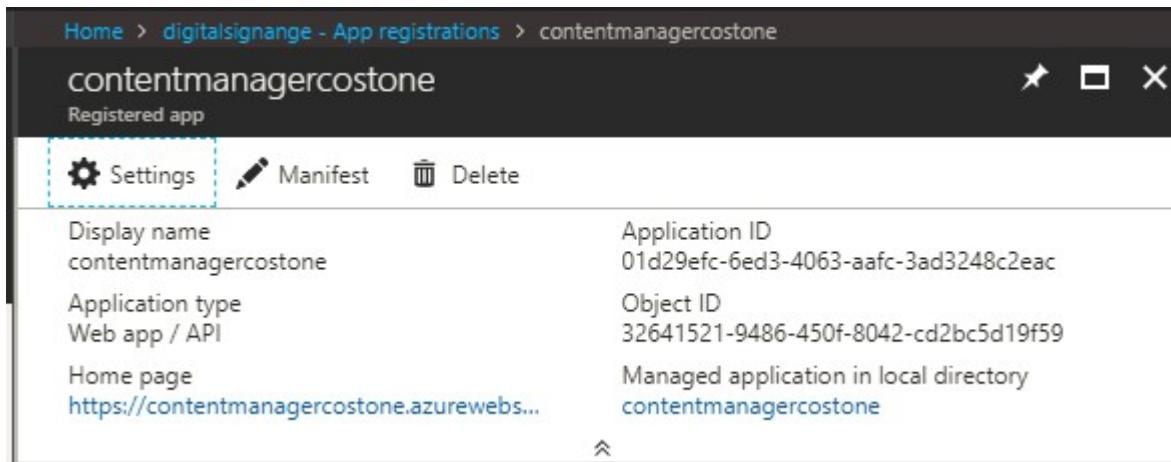
<https://contentmanagercostfour.trafficmanager.net>



Display name contentmanagercostone	Application ID 01d29efc-6ed3-4063-aafc-3ad3248c2eac
Application type Web app / API	Object ID 32641521-9486-450f-8042-cd2bc5d19f59
Home page https://contentmanagercostone.azurewebsites.net	Managed application in local directory contentmanagercostone

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.

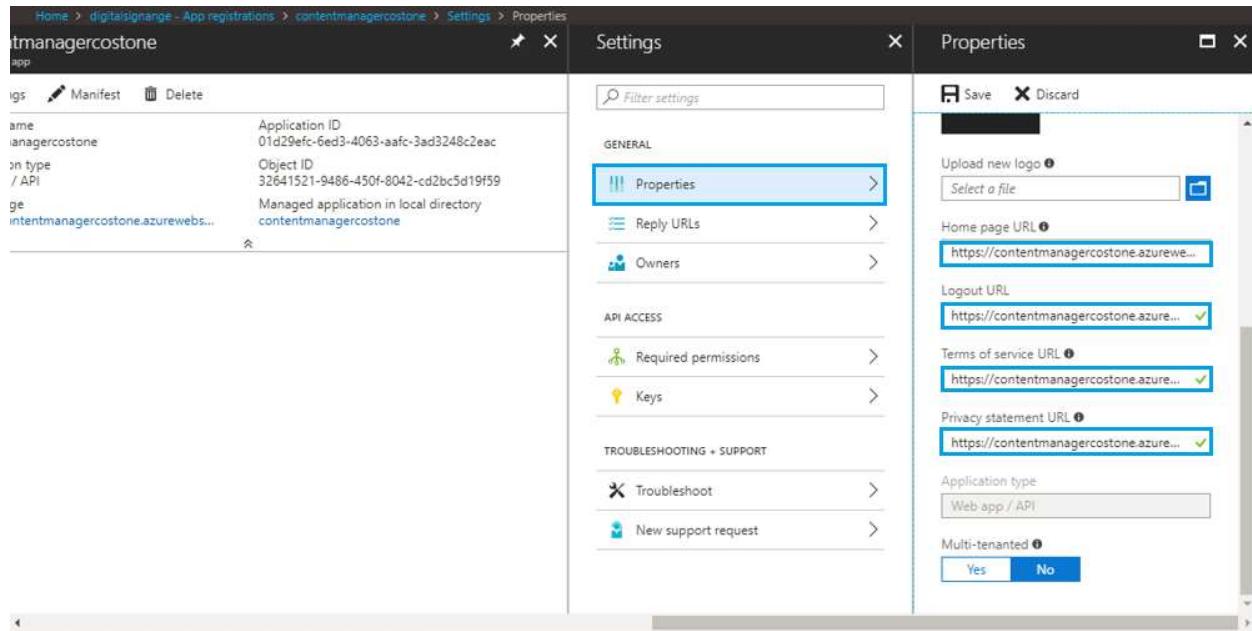


Display name contentmanagercostone	Application ID 01d29efc-6ed3-4063-aafc-3ad3248c2eac
Application type Web app / API	Object ID 32641521-9486-450f-8042-cd2bc5d19f59
Home page https://contentmanagercostone.azurewebsites.net	Managed application in local directory contentmanagercostone

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>

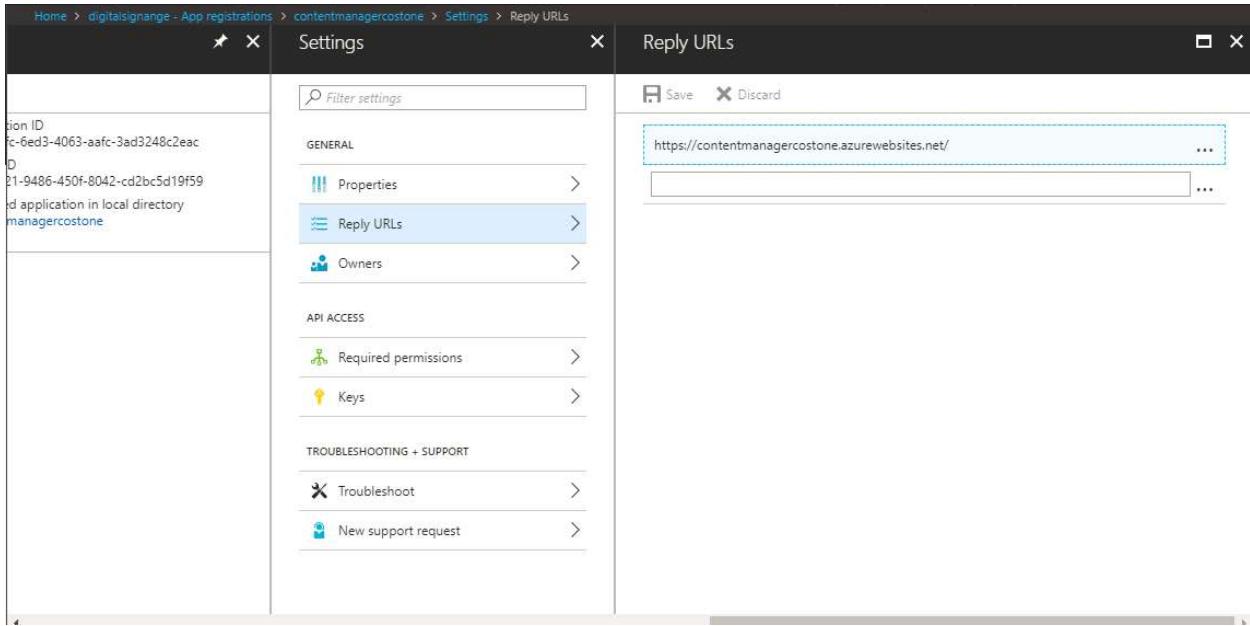


The screenshot shows the Azure portal interface for managing an app registration. On the left, the 'Properties' tab is selected, displaying basic app details like Application ID, Object ID, and the URL https://contentmanagercostone.azurewebsites.net. The 'Settings' tab is also visible. In the center, the 'Properties' section is open, showing various configuration options under 'GENERAL'. The 'Reply URLs' section is highlighted with a blue border. The 'Save' button is visible at the top right of the properties panel.

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>



The screenshot shows the Azure portal interface for managing app registrations. On the left, a sidebar lists settings like Application ID, Properties, Reply URLs, Owners, Required permissions, Keys, Troubleshoot, and New support request. The main pane is titled 'Reply URLs' and contains a single URL entry: `https://contentmanagercostone.azurewebsites.net/`. There are 'Save' and 'Discard' buttons at the top right.

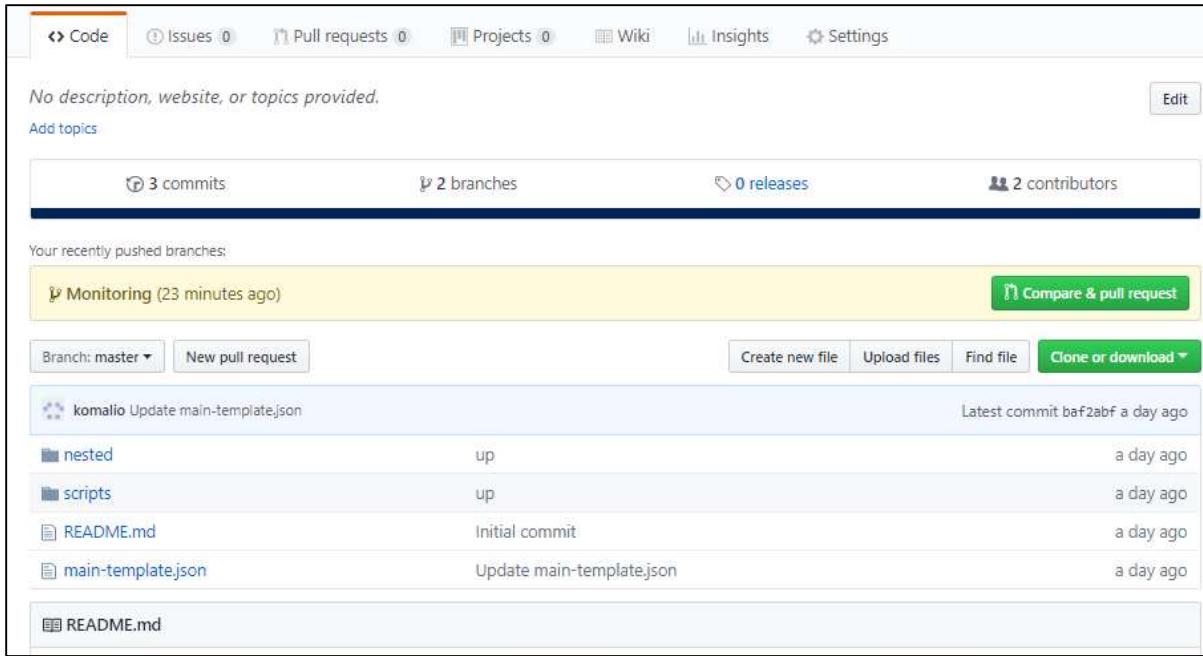
Now you have successfully created **contentmanagercostone** application in your tenant. Note down the **Application ID**, **App Display Name** and **URL**.

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**



No description, website, or topics provided.

Add topics

3 commits 2 branches 0 releases 2 contributors

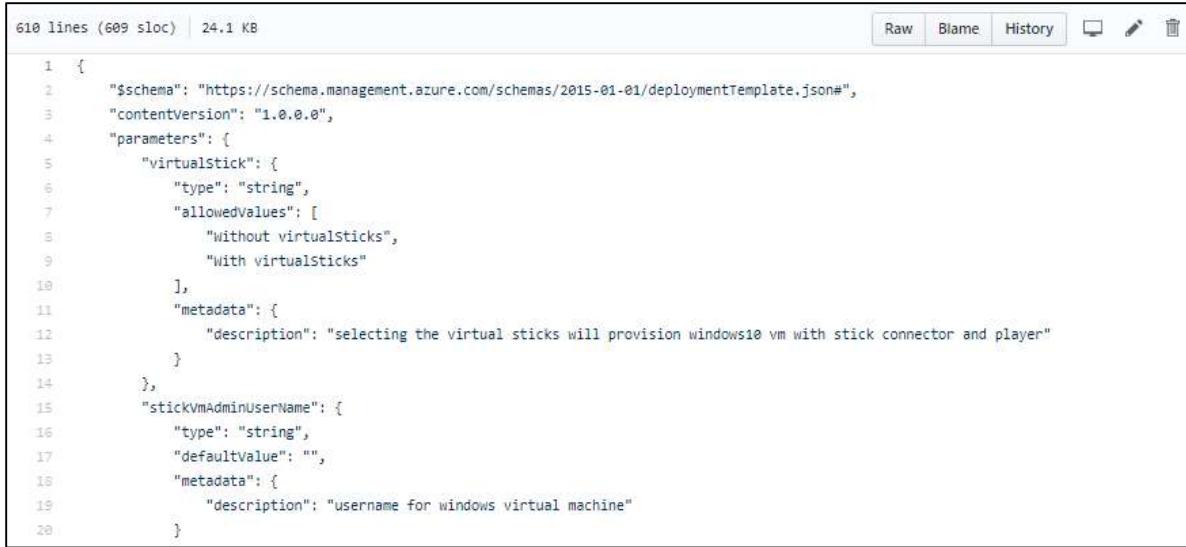
Your recently pushed branches:

Monitoring (23 minutes ago) Compare & pull request

Branch: master New pull request Create new file Upload files Find file Clone or download

komalio	Update main-template.json	Latest commit baf2abf a day ago
nested	up	a day ago
scripts	up	a day ago
README.md	Initial commit	a day ago
main-template.json	Update main-template.json	a day ago
README.md		

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



610 lines (609 sloc) | 24.1 KB

Raw Blame History

```

1  {
2      "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3      "contentVersion": "1.0.0.0",
4      "parameters": {
5          "virtualStick": {
6              "type": "string",
7              "allowedvalues": [
8                  "without virtualSticks",
9                  "With virtualSticks"
10             ],
11             "metadata": {
12                 "description": "selecting the virtual sticks will provision windows10 vm with stick connector and player"
13             }
14         },
15         "stickVMAdminUserName": {
16             "type": "string",
17             "defaultValue": "",
18             "metadata": {
19                 "description": "username for windows virtual machine"
20             }
21     }
22 }
```

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": ""  
        }  
    },  
    "variables": {}  
}
```

9.3. Deployment Scenario

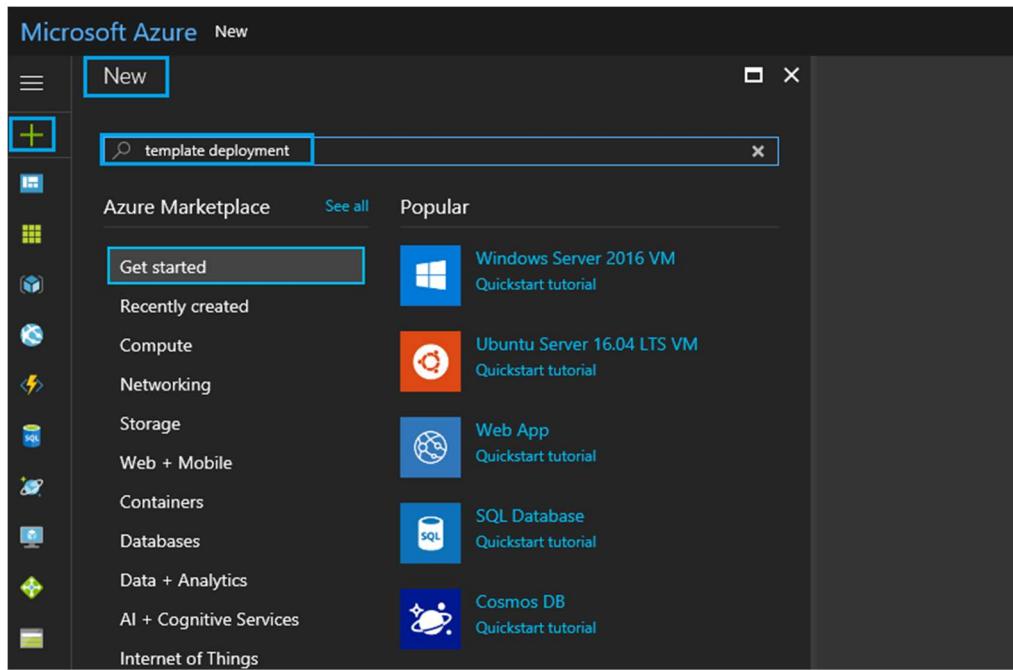
The following sections describes the various scenarios of deployment.

9.3.1. Deploy ARM Templates using Azure portal

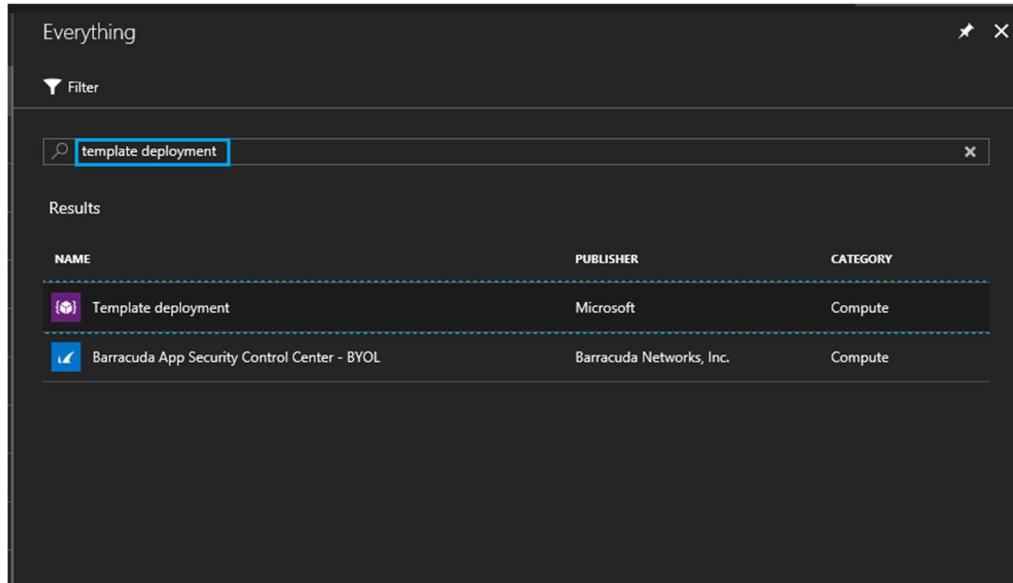
The Resource Manager template you deploy can either be a local file on your machine, or an external file that is in a repository like GitHub.

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

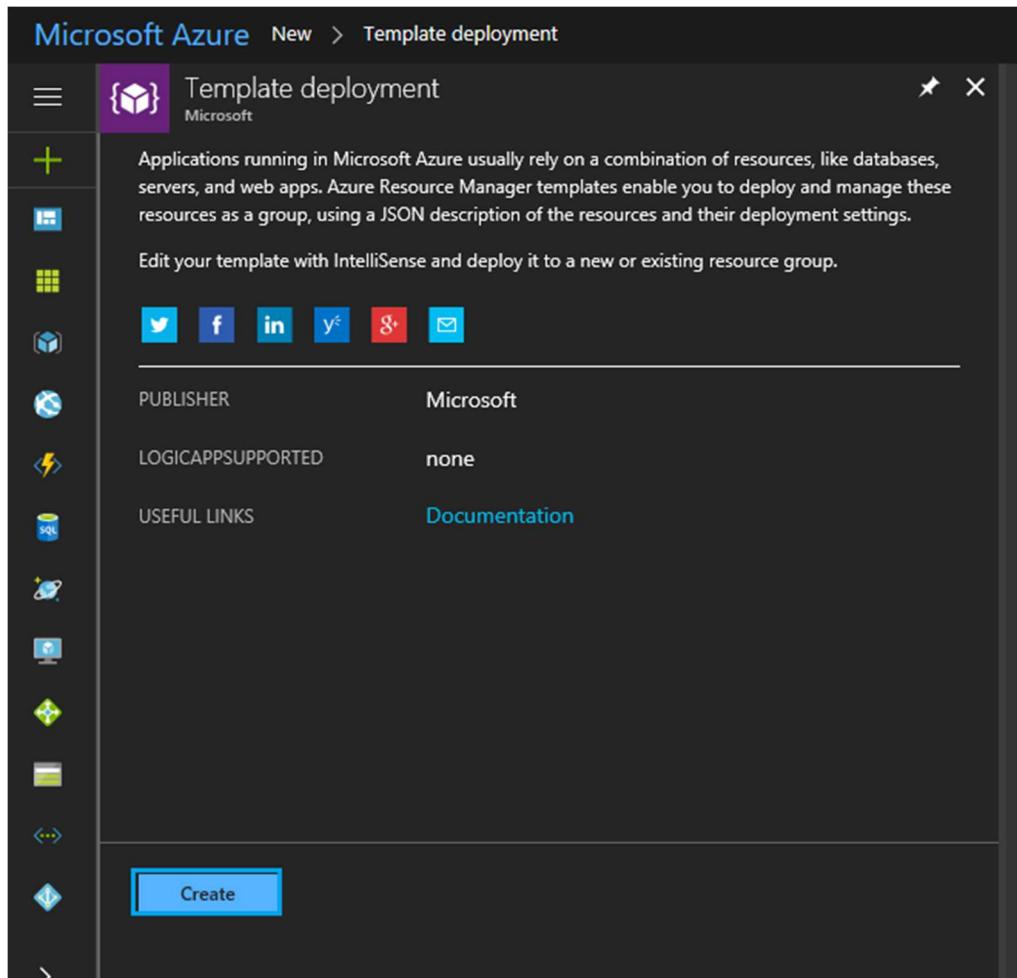
1. Open **Azure portal**, Navigate to **New (+)**, search for the key word **Template deployment**.



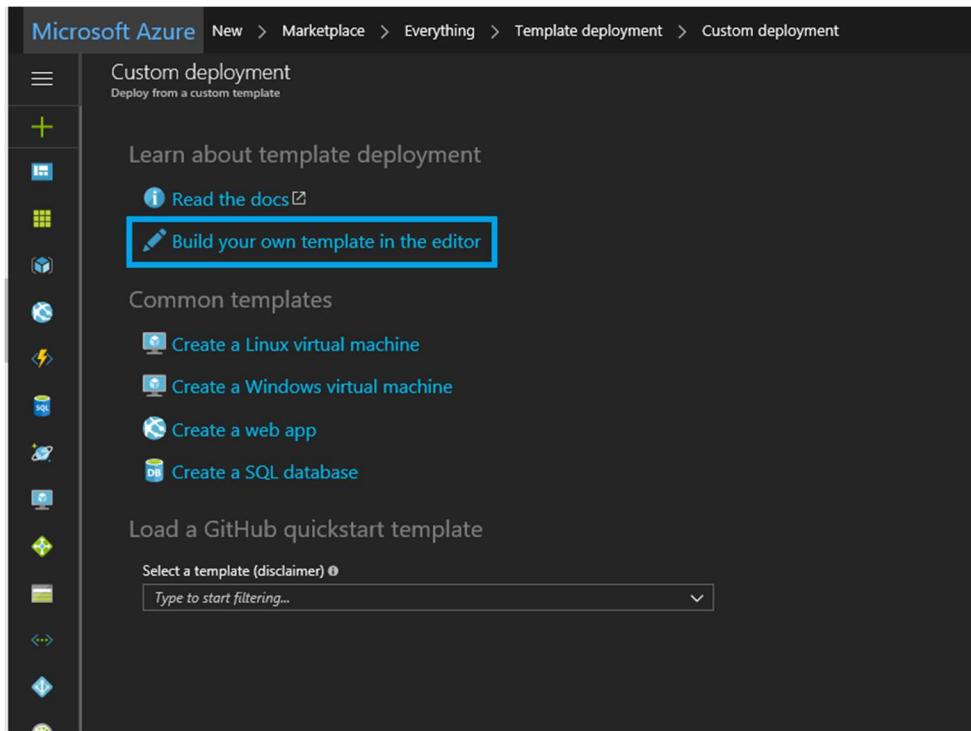
2. The search results are displayed as shown in the following figure, Select **Template deployment**.



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

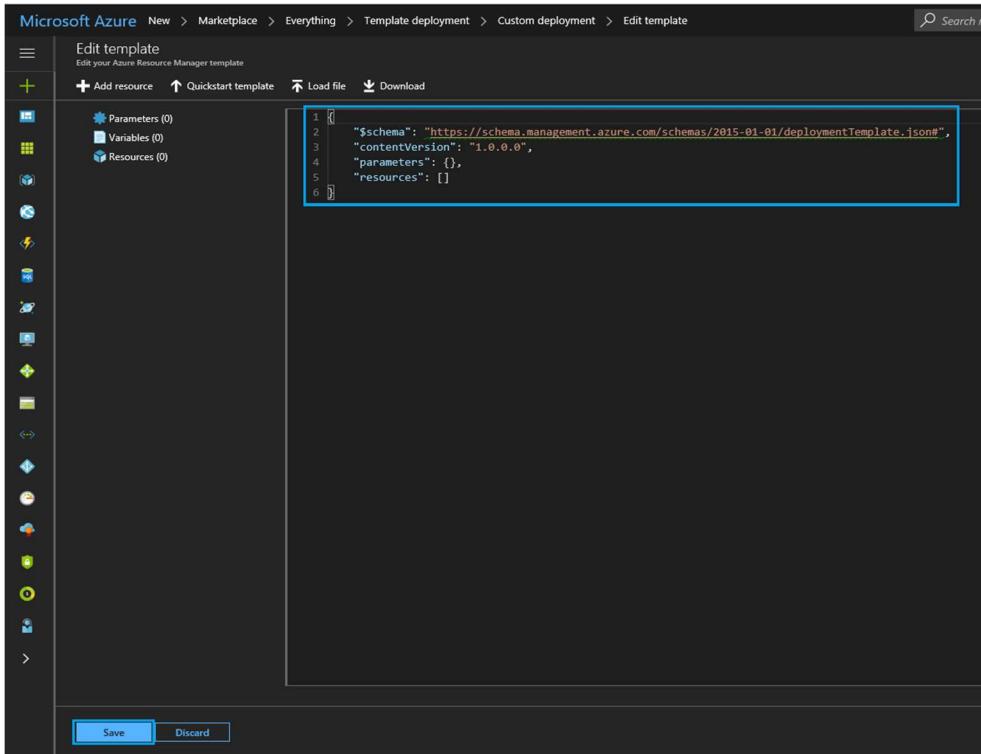


4. Click **Build your own Template in the editor** link as shown in the following figure.



The screenshot shows the Microsoft Azure portal's 'Custom deployment' page. The top navigation bar includes 'New > Marketplace > Everything > Template deployment > Custom deployment'. On the left, there's a sidebar with various icons for creating different Azure resources. The main content area starts with 'Custom deployment' and 'Deploy from a custom template'. Below this is a section titled 'Learn about template deployment' with links to 'Read the docs' and 'Build your own template in the editor' (which is highlighted with a blue border). Further down are sections for 'Common templates' (with links to 'Create a Linux virtual machine', 'Create a Windows virtual machine', 'Create a web app', and 'Create a SQL database') and 'Load a GitHub quickstart template' (with a dropdown menu for selecting a template). A search bar at the bottom right is labeled 'Type to start filtering...'.

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

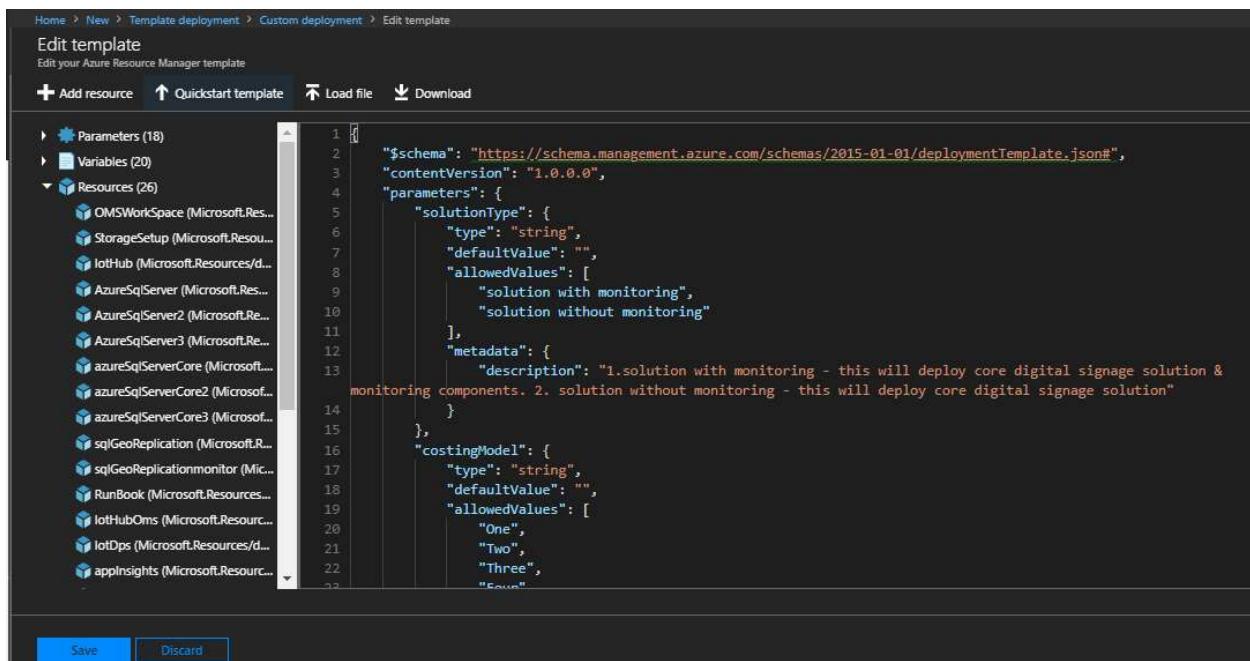


The screenshot shows the 'Edit template' page in the Microsoft Azure portal. The top navigation bar is identical to the previous screenshot. The left sidebar shows 'Parameters (0)', 'Variables (0)', and 'Resources (0)'. The main area is titled 'Edit template' and contains the instruction 'Edit your Azure Resource Manager template'. It features a code editor with the following JSON template:

```
1 [ {  
2     "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
3     "contentVersion": "1.0.0.0",  
4     "parameters": {},  
5     "resources": []  
6 } ]
```

At the bottom of the page are 'Save' and 'Discard' buttons.

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



The screenshot shows the 'Edit template' page in the Azure portal. The top navigation bar includes 'Home', 'New', 'Template deployment', 'Custom deployment', and 'Edit template'. Below the navigation is a toolbar with 'Add resource', 'Quickstart template', 'Load file', and 'Download'. On the left, a sidebar lists 'Parameters (18)', 'Variables (20)', and 'Resources (26)' with a detailed list of resources like OMSWorkSpace, StorageSetup, IoTHub, etc. The main area contains the JSON deployment template code, which defines parameters for 'solutionType' and 'costingModel' with their respective types, default values, allowed values, and descriptions. At the bottom are 'Save' and 'Discard' buttons.

```
1 $schema: "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
2 "contentVersion": "1.0.0.0",
3 "parameters": {
4     "solutionType": {
5         "type": "string",
6         "defaultValue": "",
7         "allowedValues": [
8             "solution with monitoring",
9             "solution without monitoring"
10        ],
11        "metadata": {
12            "description": "1. solution with monitoring - this will deploy core digital signage solution & monitoring components. 2. solution without monitoring - this will deploy core digital signage solution"
13        }
14    },
15    "costingModel": {
16        "type": "string",
17        "defaultValue": "",
18        "allowedValues": [
19            "One",
20            "Two",
21            "Three",
22            "Four"
23        ]
24    }
25 }
```

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 [Edit](#)

* Resource group: Create new Use existing
[Create a resource group](#)

* Location: West US [Edit](#)

SETTINGS

Solution Type [Edit](#)

Costing Model [Edit](#)

Sql Administrator Login [Edit](#)

Pin to dashboard

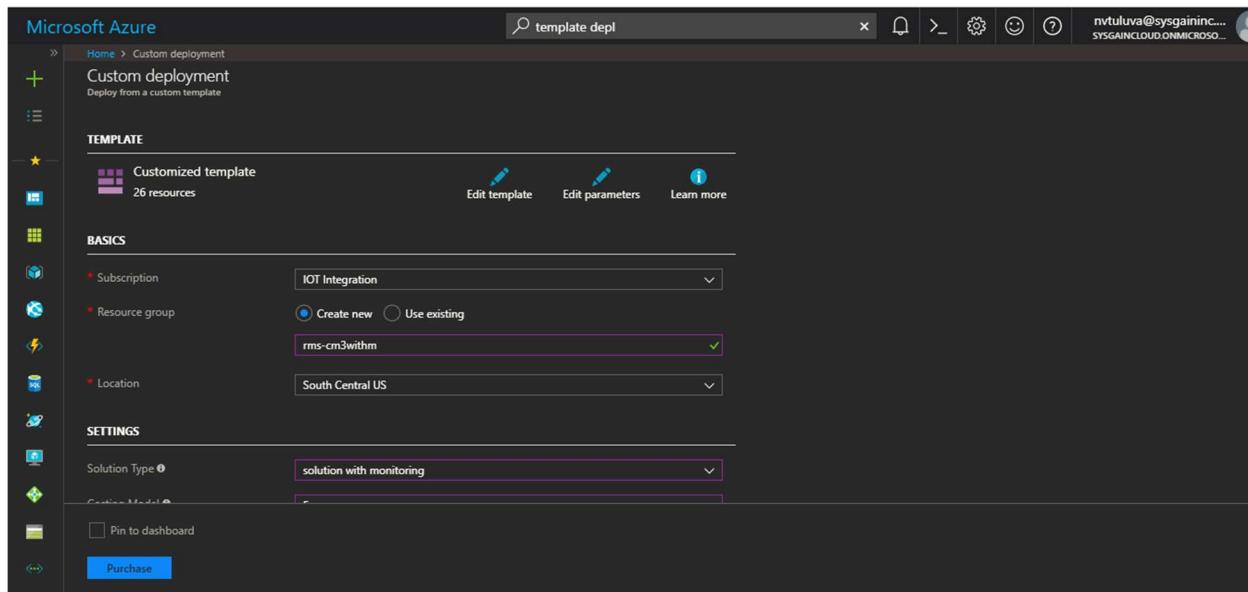
[Purchase](#)

Storage Blob Uri ●	<input type="text" value="https://projectiot.blob.core.windows.net/rms-iot/"/>
Location Dr ●	<input type="text"/>
Content Manager App Name ●	<input type="text"/>
Oms Workspace Region ●	<input type="text" value="eastus"/>
Oms Automation Region ●	<input type="text" value="eastus2"/>
Data Retention ●	<input type="text" value="7"/>
App Insights Location ●	<input type="text" value="westus2"/>
Capacity Units ●	<input type="text" value="1"/>
Iot Dps Region ●	<input type="text" value="eastus"/>
D2c Message Retention In Days Period ●	<input type="text" value="1"/>
D2c Partition Count ●	<input type="text" value="2"/>

Pin to dashboard

Purchase

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



Microsoft Azure

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
rms-cm3withm
- * Location: South Central US

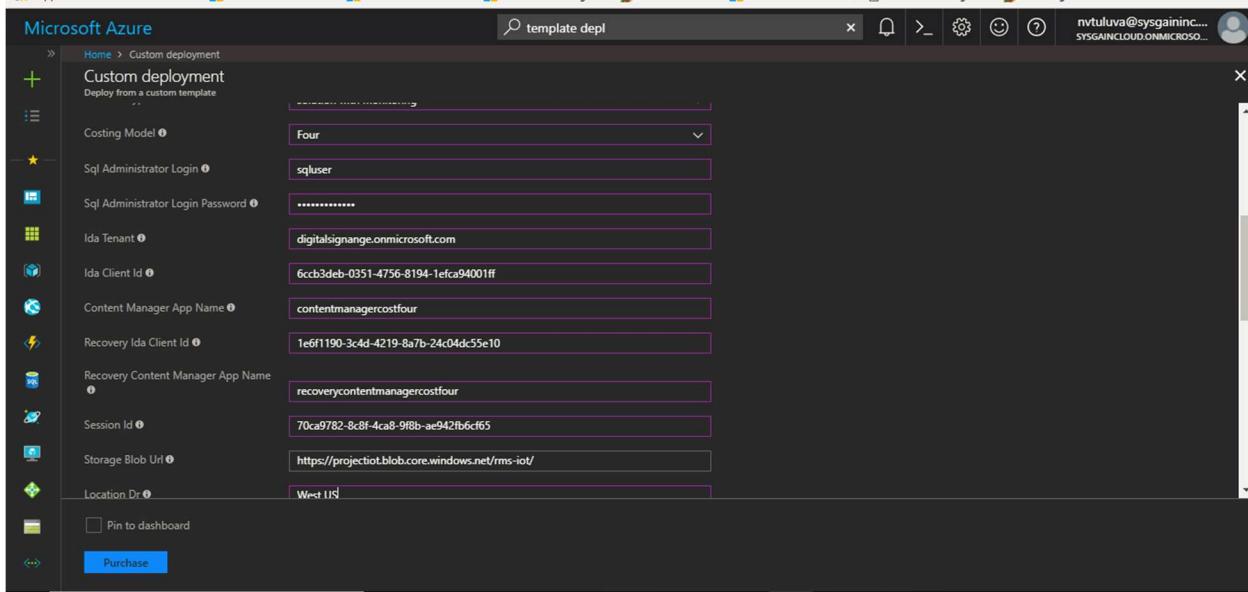
SETTINGS

- Solution Type ●: solution with monitoring

Pin to dashboard

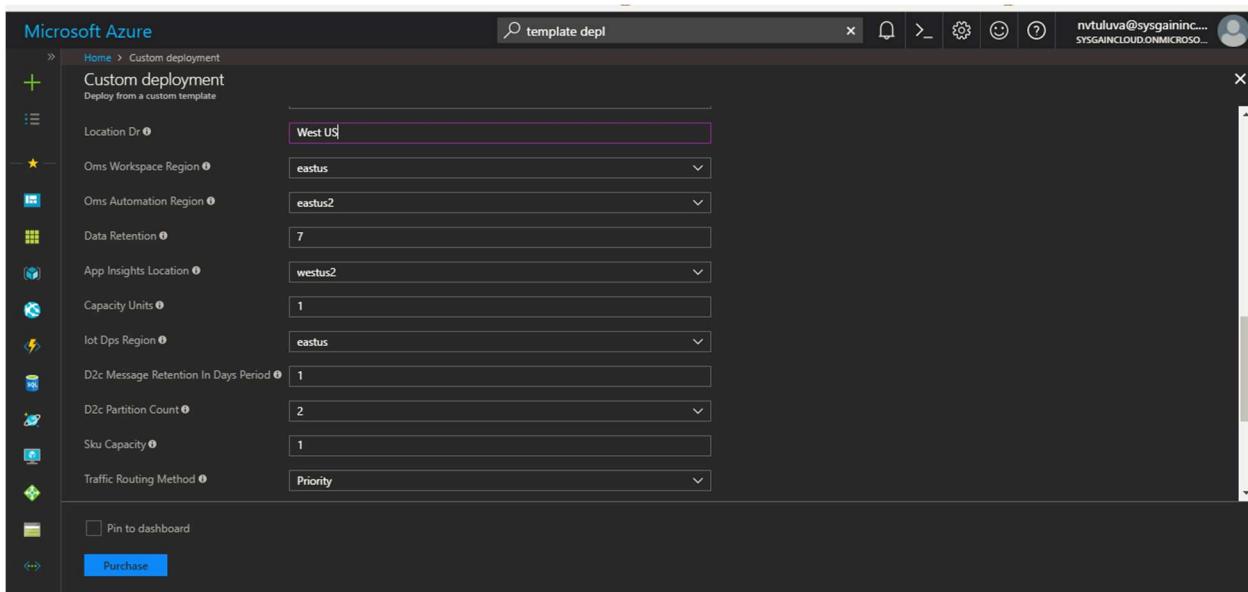
Purchase

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



The screenshot shows the 'Custom deployment' settings page in the Microsoft Azure portal. The 'Session Id' field is highlighted with a purple border, containing the value '70ca9782-8c8f-4ca8-9f8b-ae942fb6cf65'. Other fields include:

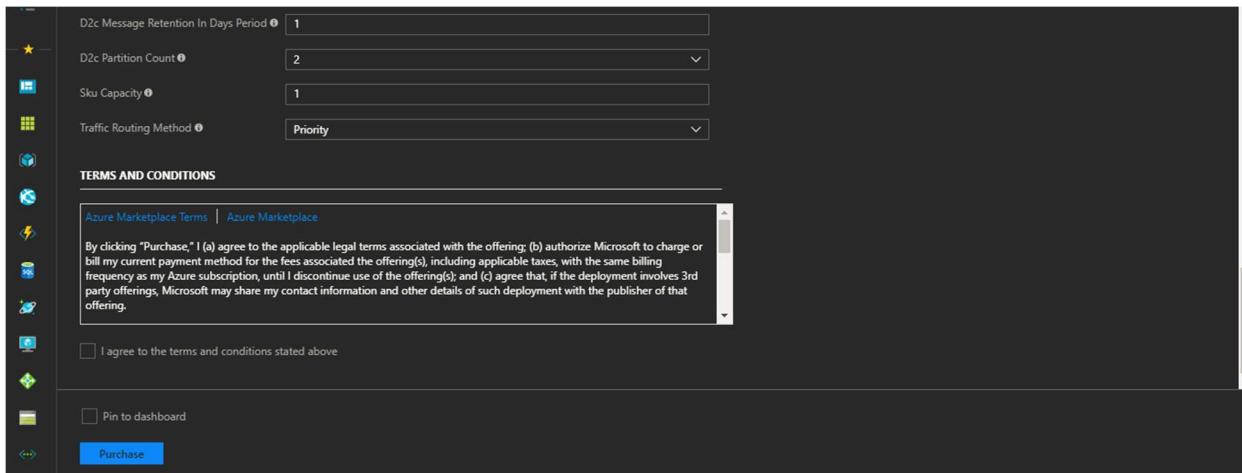
- Costing Model: Four
- Sql Administrator Login: sqluser
- Sql Administrator Login Password: (redacted)
- Ida Tenant: digitalsignage.onmicrosoft.com
- Ida Client Id: 6ccb3deb-0351-4756-8194-1efca94001ff
- Content Manager App Name: contentmanagercostfour
- Recovery Ida Client Id: 1e6f1190-3c4d-4219-8a7b-24c0dc55e10
- Recovery Content Manager App Name: recoverycontentmanagercostfour
- Session Id: 70ca9782-8c8f-4ca8-9f8b-ae942fb6cf65
- Storage Blob Url: https://projectiot.blob.core.windows.net/rms-iot/
- Location Dr: West US



The screenshot shows the 'Custom deployment' settings page in the Microsoft Azure portal. The 'Location Dr' field is highlighted with a purple border, containing the value 'West US'. Other fields include:

- Oms Workspace Region: eastus
- Oms Automation Region: eastus2
- Data Retention: 7
- App Insights Location: westus2
- Capacity Units: 1
- IoT Dps Region: eastus
- D2c Message Retention In Days Period: 1
- D2c Partition Count: 2
- Sku Capacity: 1
- Traffic Routing Method: Priority

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

Subscription (change) IOT Integration Deployment ID 2927c217-b119-4d3b-8a13-82a1c3a16c8f

Filter by name... All types All locations No grouping

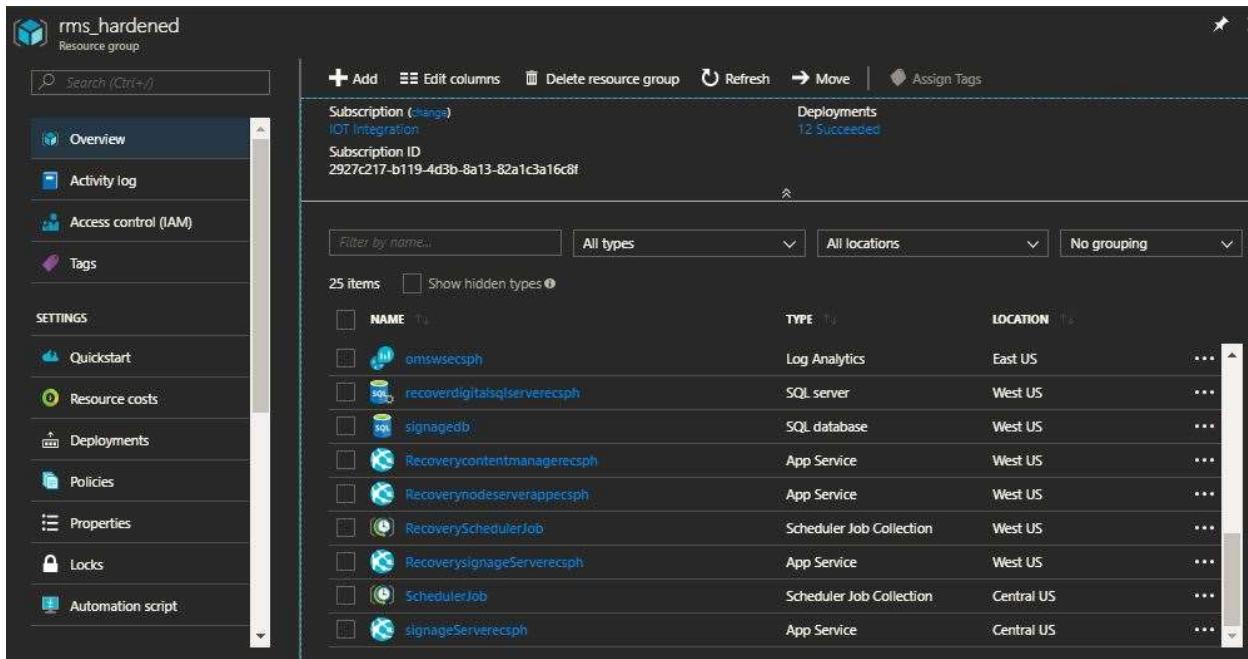
NAME	TYPE	LOCATION
AppInsightsecsp1z33ufme	Application Insights	West US 2
AppServicePlan	App Service plan	Central US
AppServicePlanRecoveryecspfh	App Service plan	West US
AzureSQLAnalytics(omswsecspfh)	Solution	East US
AzureWebAppsAnalytics(omswsecspfh)	Solution	East US
containerCreateecspfh	Automation Account	East US 2
container	Runbook	East US 2
contentmanagerecspfh	App Service	Central US
contentmanagerTMecspfh	Traffic Manager profile	global

rms_hardened Resource group

Subscription (change) IOT Integration Deployment ID 2927c217-b119-4d3b-8a13-82a1c3a16c8f

Filter by name... All types All locations No grouping

NAME	TYPE	LOCATION
digital-signagehubecspfh	IoT Hub	Central US
digitalsqlserverecspfh	SQL server	Central US
signagedb	SQL database	Central US
imagecontentecspfh	Storage account	Central US
iotDeviceProvisionecspfh	Device Provisioning Service	East US
nodeserverappecspfh	App Service	Central US
nodeserverappTMecspfh	Traffic Manager profile	global
omswsecspfh	Log Analytics	East US
recoverdigitalsqlserverecspfh	SQL server	West US



NAME	TYPE	LOCATION
omswsecph	Log Analytics	East US
recoverdigitalsqlserverecph	SQL server	West US
signagedb	SQL database	West US
Recoverycontentmanagerecph	App Service	West US
Recoverymodiserverapprecph	App Service	West US
RecoverySchedulerJob	Scheduler Job Collection	West US
RecoverysignageServerecph	App Service	West US
SchedulerJob	Scheduler Job Collection	Central US
signageServerecph	App Service	Central US

9.3.2. Deploy ARM Templates using Azure CLI

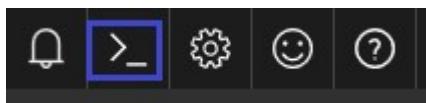
Azure CLI is used to deploy your resources to Azure. The Resource Manager template you deploy, can either be a local file on your machine, or an external file that is in a repository like GitHub.

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

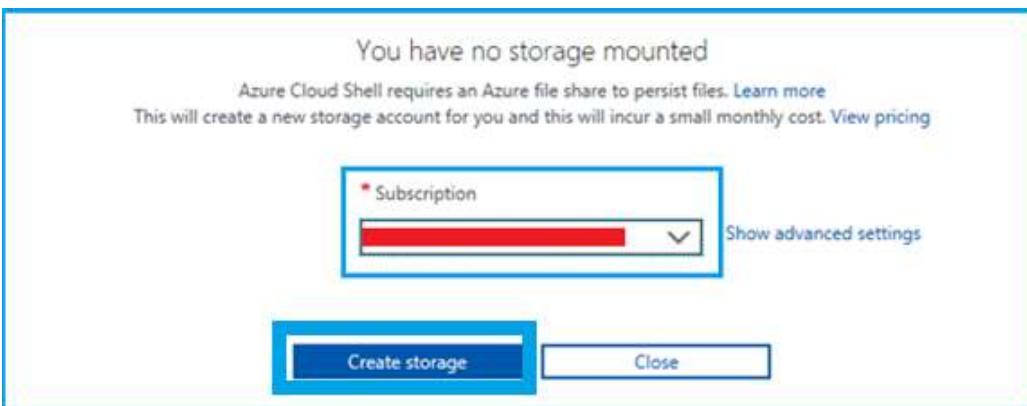
1. Log in to [Azure portal](#).
2. Open the prompt.



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

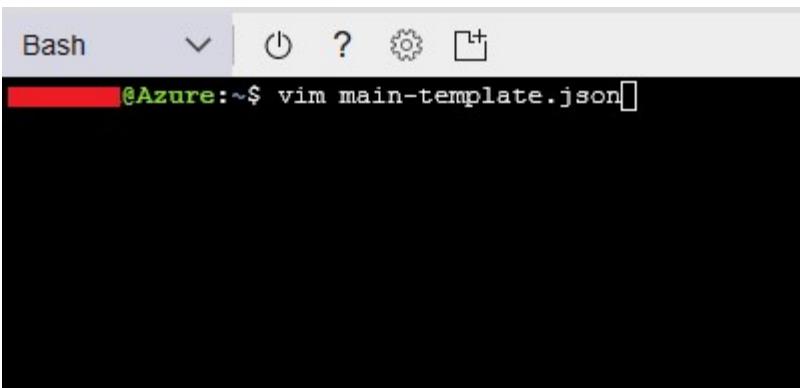


4. Select your preferred **Subscription** from the dropdown list.
5. Click **Create Storage** button as shown in the following figure.

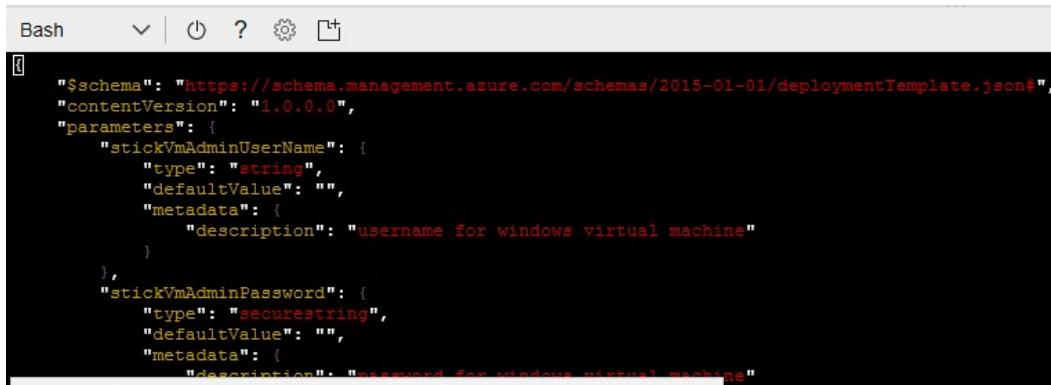


6. Copy **main-template.json** and **main-template.parameters.json** to your Cloud Shell before updating the parameters.
7. Create **main-template.json** using the following command.

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

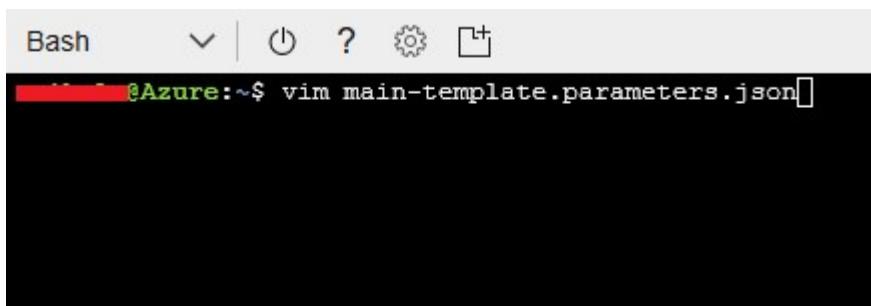


8. Paste your **main-template.json** in editor as shown below and save the file.



```
["$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#", "contentVersion": "1.0.0.0", "parameters": { "stickVmAdminUserName": { "type": "string", "defaultValue": "", "metadata": { "description": "username for windows virtual machine" } }, "stickVmAdminPassword": { "type": "securestring", "defaultValue": "", "metadata": { "description": "password for windows virtual machine" } } }]
```

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

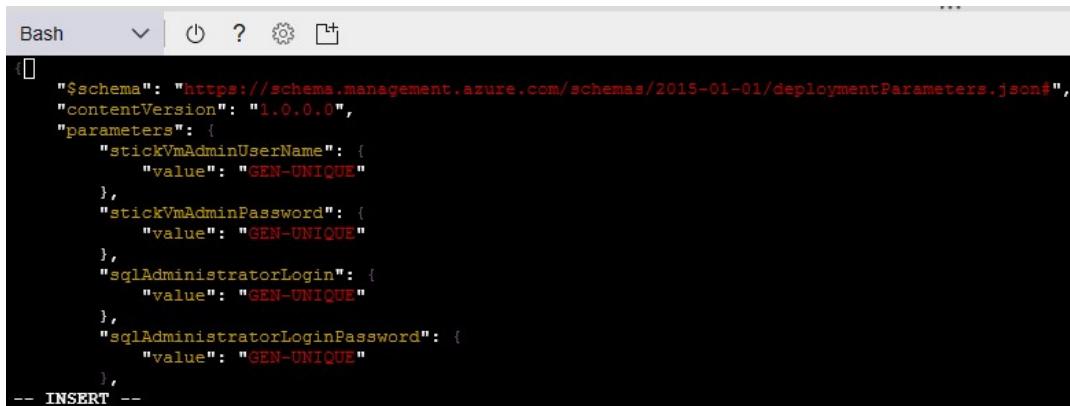


```
@Azure:~$ vim main-template.parameters.json
```

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

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

- a. **sqlAdministratorLogin**
- b. **sqlAdministratorLoginPassword**
- 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**



```
$schema: "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
contentVersion: "1.0.0.0",
parameters: {
    "stickVmAdminUserName": {
        "value": "GEN-UNIQUE"
    },
    "stickVmAdminPassword": {
        "value": "GEN-UNIQUE"
    },
    "sqlAdministratorLogin": {
        "value": "GEN-UNIQUE"
    },
    "sqlAdministratorLoginPassword": {
        "value": "GEN-UNIQUE"
    }
},
-- INSERT --
```

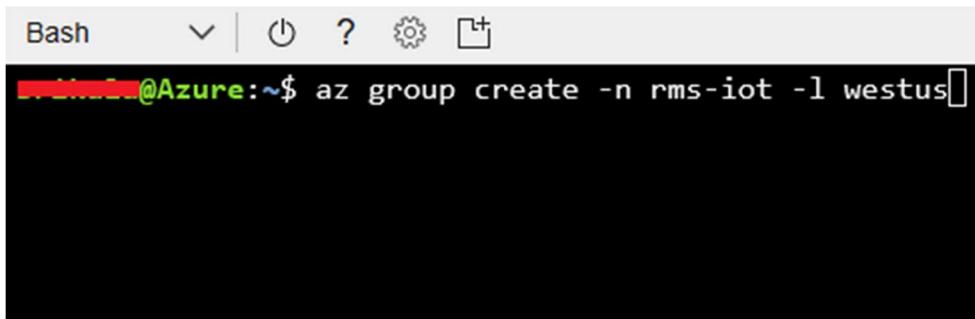
9.3.4. Create Resource Group for Digital Signage solution

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 <***>
```



```
[Azure:~]$ az group create -n rms-iot -l westus
```

9.3.5. Execute the template deployment

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

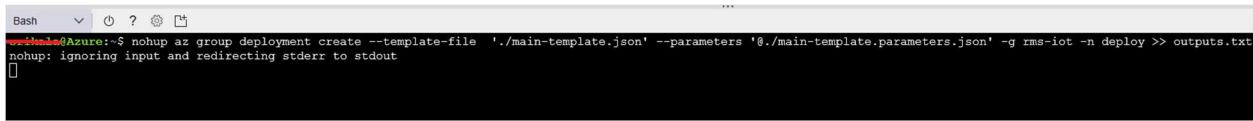
Description: To deploy the ARM Template, you require two files:

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`



A screenshot of a terminal window titled "Bash". The command entered is "nohup az group deployment create --template-file './main-template.json' --parameters '@./main-template.parameters.json' -g rms-iot -n deploy >> outputs.txt". The output shows "nohup: ignoring input and redirecting stderr to stdout".

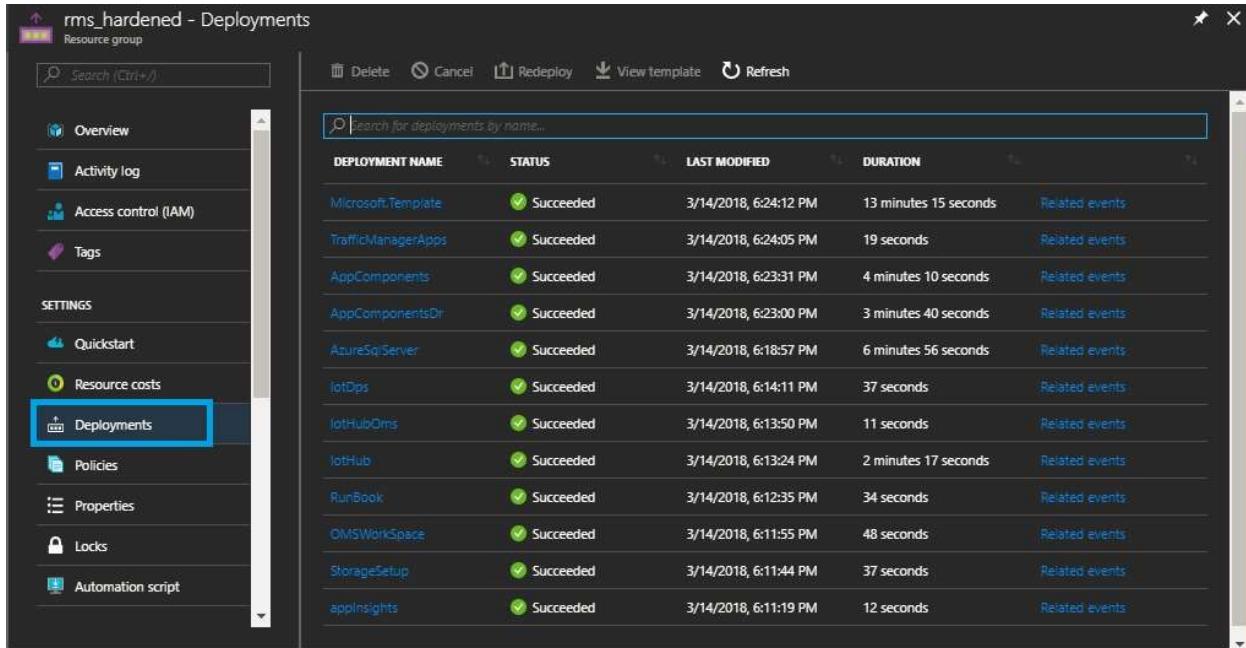
Deployment may take between 15-20 minutes depending on deployment size.

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

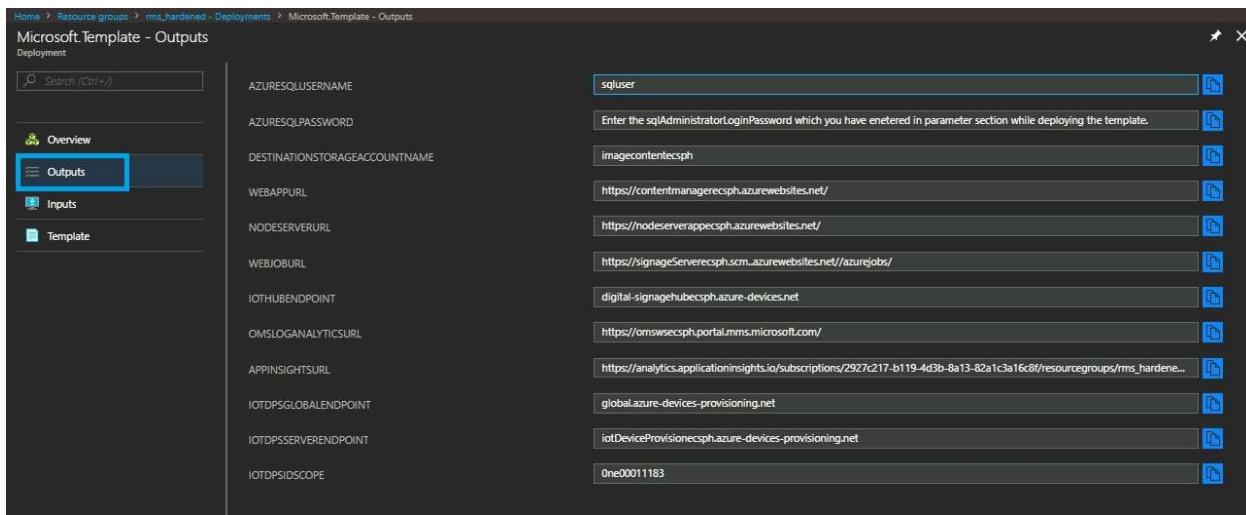
- a. **azureSQLEndpoint**
- b. **azureSQLsignageDBName**
- c. **azureSQLUsername**
- d. **azureSqlPassword**
- e. **stcikVMFQDN**
- f. **stcikVmadminUsername**
- g. **stcikVmAdminPassword**
- h. **destinationStorageAccountName**
- i. **webJobUrl**
- j. **IoTHubEndPoint**
- k. **webAppUrl**
- l. **nodeServerUrl**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

10. Post Deployment

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



DEPLOYMENT NAME	STATUS	LAST MODIFIED	DURATION	RELATED EVENTS
Microsoft.Template	Succeeded	3/14/2018, 6:24:12 PM	13 minutes 15 seconds	Related events
TrafficManagerApps	Succeeded	3/14/2018, 6:24:05 PM	19 seconds	Related events
AppComponents	Succeeded	3/14/2018, 6:23:31 PM	4 minutes 10 seconds	Related events
AppComponentsDri	Succeeded	3/14/2018, 6:23:00 PM	3 minutes 40 seconds	Related events
AzureSqlServer	Succeeded	3/14/2018, 6:18:57 PM	6 minutes 56 seconds	Related events
IoTDPs	Succeeded	3/14/2018, 6:14:11 PM	37 seconds	Related events
IoTHubDm	Succeeded	3/14/2018, 6:13:50 PM	11 seconds	Related events
IoTHub	Succeeded	3/14/2018, 6:13:24 PM	2 minutes 17 seconds	Related events
RunBook	Succeeded	3/14/2018, 6:12:35 PM	34 seconds	Related events
OMSWorkSpace	Succeeded	3/14/2018, 6:11:55 PM	48 seconds	Related events
StorageSetup	Succeeded	3/14/2018, 6:11:44 PM	37 seconds	Related events
appInsights	Succeeded	3/14/2018, 6:11:19 PM	12 seconds	Related events



OUTPUT NAME	VALUE
AZURESQLUSERNAME	sqluser
AZURESQLPASSWORD	Enter the sqAdministratorLoginPassword which you have entered in parameter section while deploying the template.
DESTINATIONSTORAGEACCOUNTNAME	imagecontentecph
WEBAPPURL	https://contentmanagerecph.azurewebsites.net/
NODESERVERURL	https://nodeserverappecph.azurewebsites.net/
WEBJOBUML	https://signageServerecph.scm.azurewebsites.net/azurejobs/
IOTHUBENDPOINT	digital-signagehubecph.azure-devices.net
OMSLOGANALYTICSCURL	https://omsseccph.portal.mms.microsoft.com/
APPINSIGHTSURL	https://analytics.applicationinsights.io/subscriptions/2927c217-b119-4d3b-8a13-82a1c3a16c8f/resourcegroups/rms_hardene...
IOTDPSGLOBALENDPOINT	global.azure-devices-provisioning.net
IOTDPSERVERENDPOINT	iotDeviceProvisionecph.azure-devices-provisioning.net
IOTDPSIDSCOPE	One00011183

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

TRAFFICMANAGERWEBAPPURL

TRAFFICMANAGERNODESERVERURL

IOTDPSIDSCOPE

Microsoft.Template - Outputs

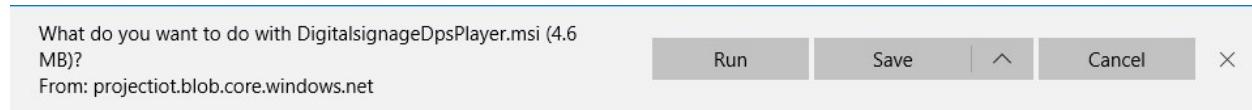
Output Name	Value
DESTINATIONSTORAGEACCOUNTNAME	imagecontentmhhy74
WEBAPPURL	https://contentmanagermhhy74.azurewebsites.net/
NODESERVERURL	https://nodeserverappmhhy74.azurewebsites.net/
TRAFFICMANAGERWEBAPPURL	https://contentmanagermhhy74.trafficmanager.net
TRAFFICMANAGERNODESERVERURL	https://nodeserverapptmhhy74.trafficmanager.net
WEBJOBUURL	https://signageServermhhy74.scm.azurewebsites.net/azurejobs/
IOTHUBENDPOINT	digital-signagehubmhhy74.azure-devices.net
OMSLOGANALYTICSURL	https://omsmhhy74.portal.mms.microsoft.com/
APPINSIGHTSURL	https://analytics.applicationinsights.io/subscriptions/2927c217-b119-4d3b-8a13-82a1c...
IOTDPSGLOBALENDPOINT	global.azure-devices-provisioning.net
IOTDPSSERVERENDPOINT	iotDeviceProvisionmhhy74.azure-devices-provisioning.net
IOTPSIDSCOPE	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.

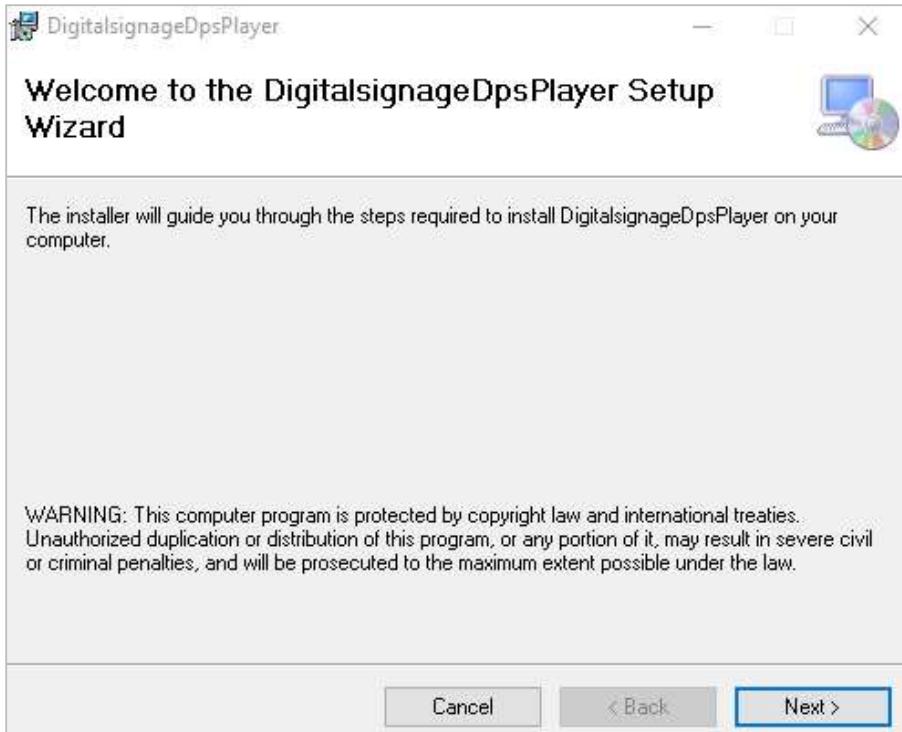
<https://projectiot.blob.core.windows.net/rms-iot/DigitalSignageDpsPlayer.msi>



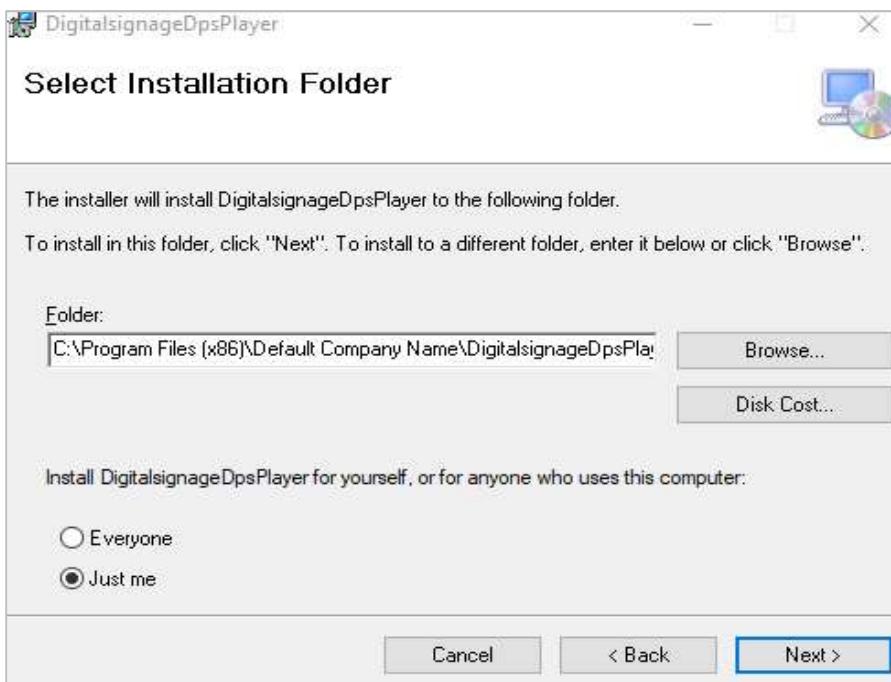
2. Click **More Info**, and select **Run anyway** option.



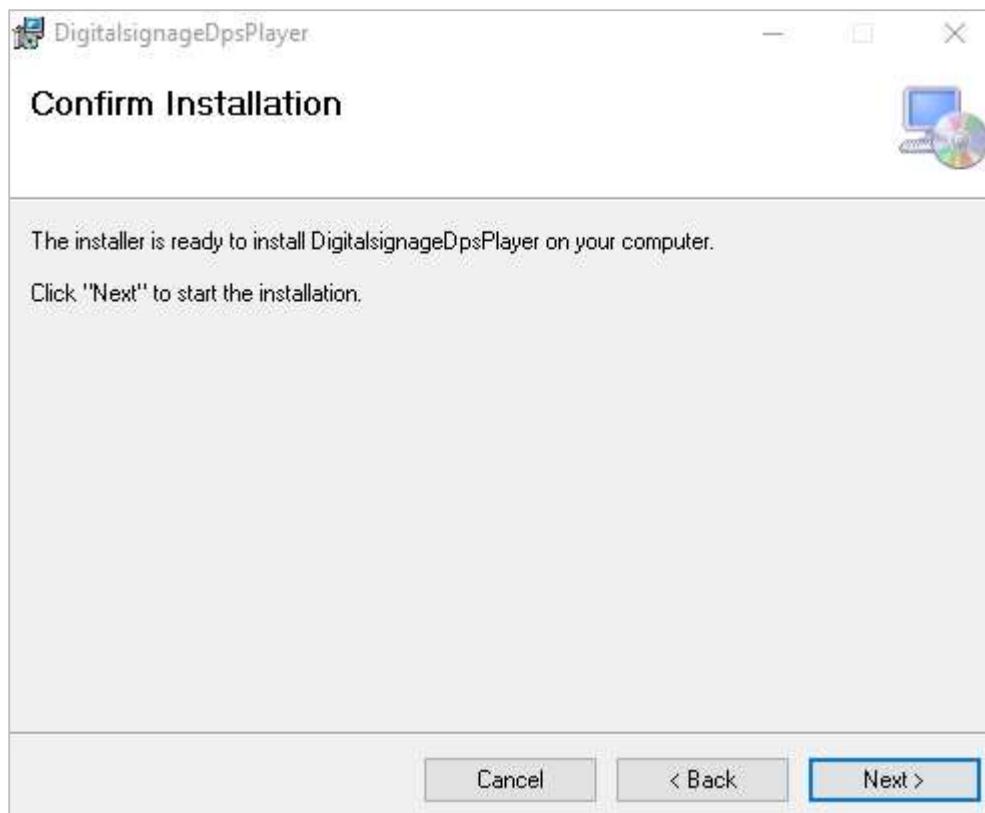
3. Click **Next** button.



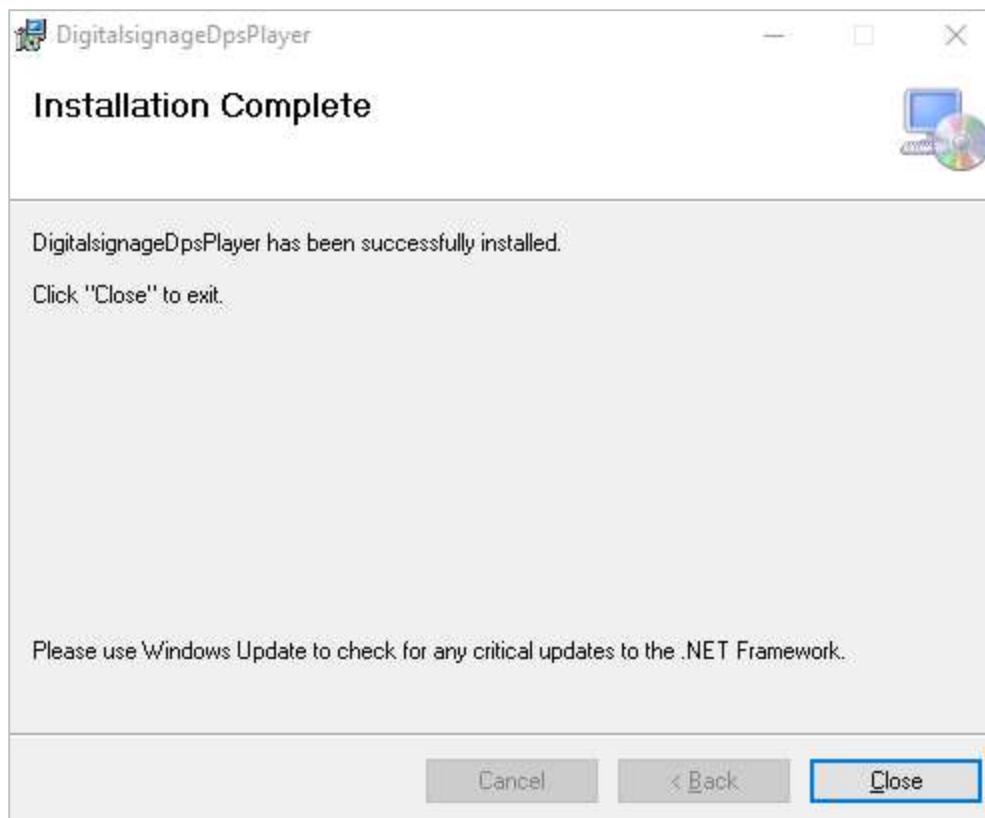
4. Click **Next** button.



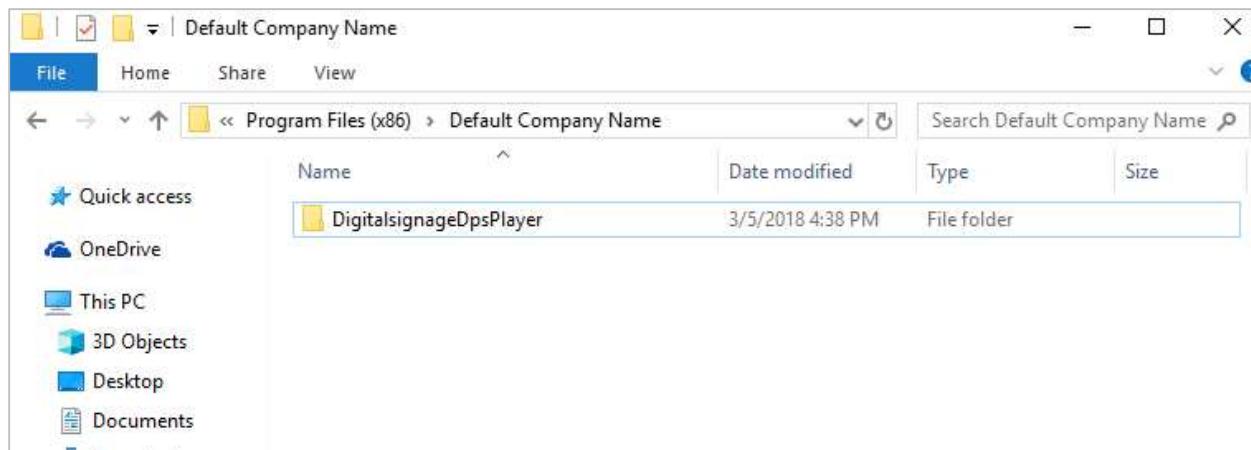
5. Click **Next** button.



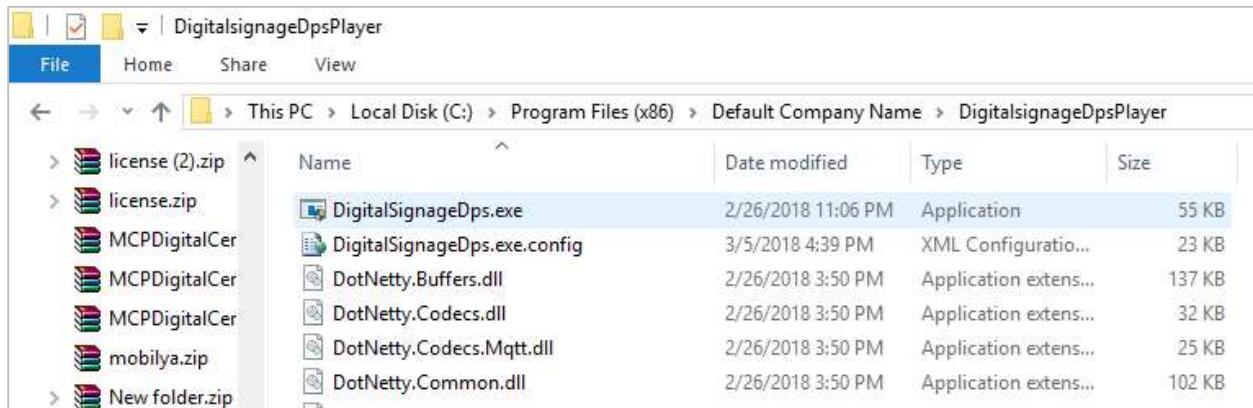
6. Click **YES** in the dialogue box.
7. Click **Close** button.



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

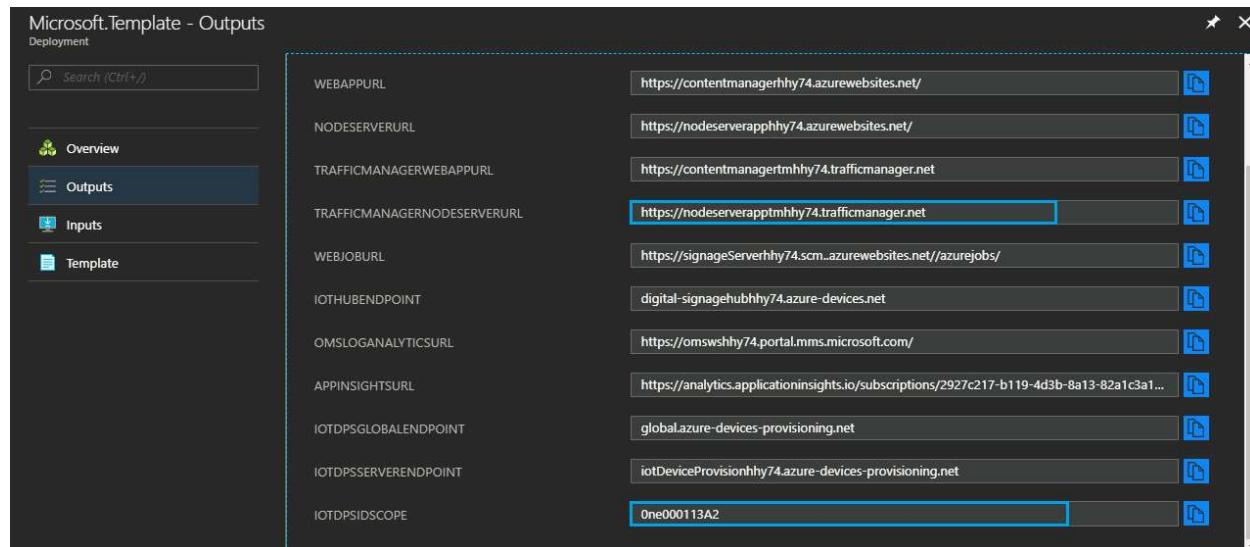


9. Right click on **DigitalSignageDps.exe.config** file folder and open with **notepad++**



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

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



Output Name	Value
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://omswhhy74.portal.mms.microsoft.com/
APPINSIGHTSURL	https://analytics.applicationinsights.io/subscriptions/2927c217-b119-4d3b-8a13-82a1c3a1...
IOTDPGLOBALENDPOINT	globalAzure-devices-provisioning.net
IOTDPSSERVERENDPOINT	iotDeviceProvisionhhy74.azure-devices-provisioning.net
IOTDPSIDSCOPE	One000113A2

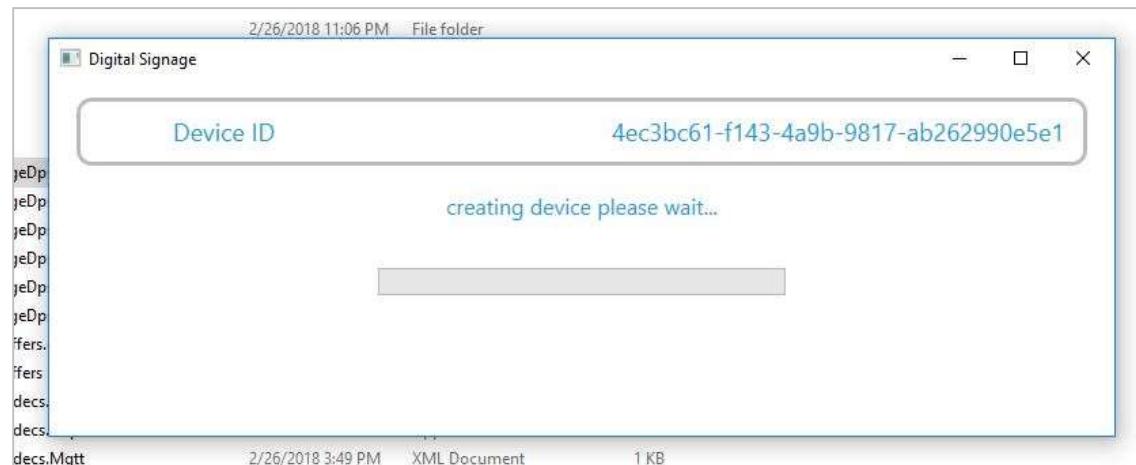
12. Paste the copied **ID Scope** near DeviceProvisioningScopId and **TRAFFICMANAGERWEBAPPURL** near WebApiAddress, and save the file.

```

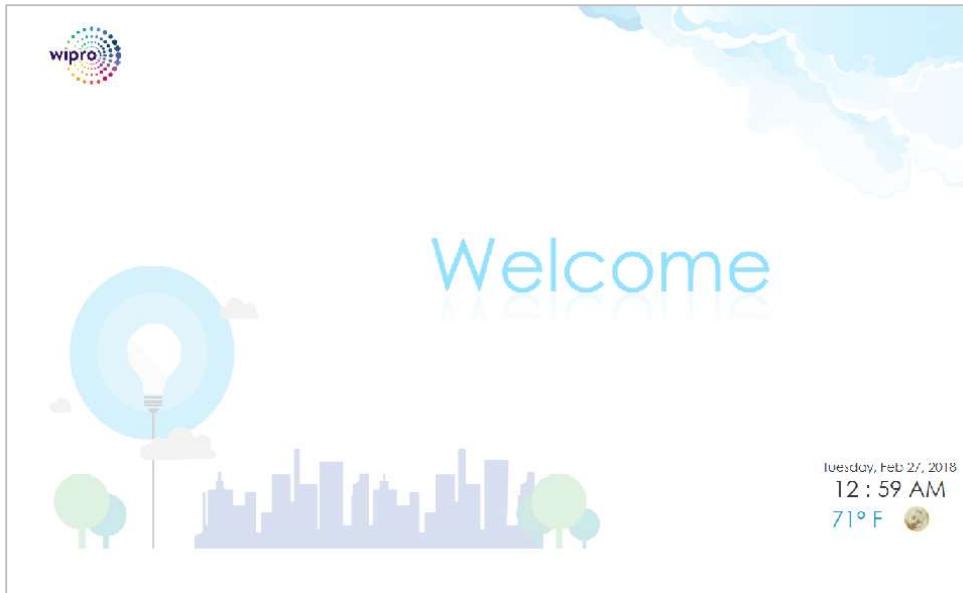
40           <conversionPattern value="%date [%username] - %message%newline" />
41       </layout>
42   </appender>
43   <logger name="Player">
44     <level value="DEBUG" />
45     <appender-ref ref="PlayerLogger" />
46   </logger>
47   <logger name="FaceRecognition">
48     <level value="DEBUG" />
49     <appender-ref ref="FaceRecognitionLogger" />
50   </logger>
51   <logger name="Connector">
52     <level value="DEBUG" />
53     <appender-ref ref="ConnectorLogger" />
54   </logger>
55 </log4net>
56 <appSettings>
57   <add key="WebApiAddress" value="http://nodeserverapptmecph.trafficmanager.net" />
58   <add key="ScopeId" value="One00011183" />
59   <add key="ClientSettingsProvider.ServiceUri" value="" />
60 </appSettings>
61 <startup>
62   <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6.1" />
63 </startup>
64 <runtime>
65   <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
66     <dependentAssembly>
67       <assemblyIdentity name="System.Runtime" culture="neutral" publicKeyToken="b03f5f7f11d50a3a" />
68       <bindingRedirect oldVersion="0.0.0.0-4.1.2.0" newVersion="4.1.2.0" />
69     </dependentAssembly>
70     <dependentAssembly>
71       <assemblyIdentity name="System.Net.Http" culture="neutral" publicKeyToken="b03f5f7f11d50a3a" />

```

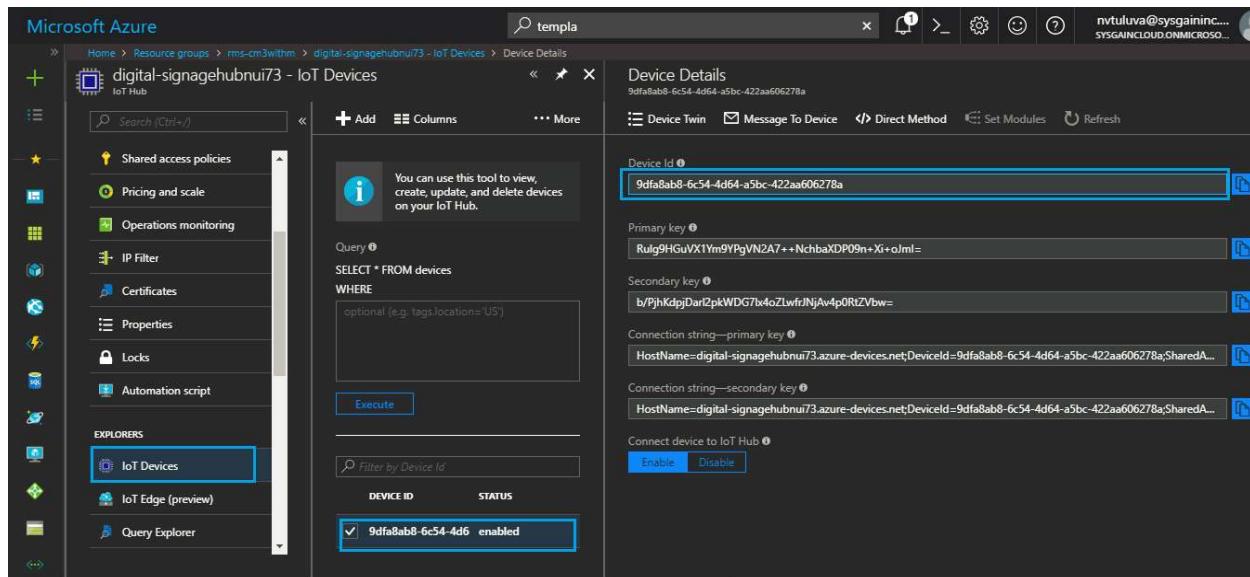
13. Navigate to path **Local Disk (C:) > Program Files (x86) > Default Company Name > DigitalSignageDpsPlayer**, right click **DigitalSignageDps.exe** file and select **run as Administrator**, you can view **Device ID** as shown in the following figure.



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.

A screenshot of the Microsoft Azure portal showing the "Device Details" page for an IoT device. The device ID is highlighted with a blue box: "9dfa8ab8-6c54-4d64-a5bc-422aa606278a". The page includes sections for "Device Twin", "Message To Device", "Direct Method", "Set Modules", and "Refresh". On the left, the "IoT Devices" option is selected in the "EXPLORERS" sidebar. The "Device Id" field contains the same value as the highlighted box. Below it, there are fields for "Primary key" and "Secondary key", each with their respective connection strings. At the bottom, there is a "Connect device to IoT Hub" section with "Enable" and "Disable" buttons, and a checked checkbox for the device ID.

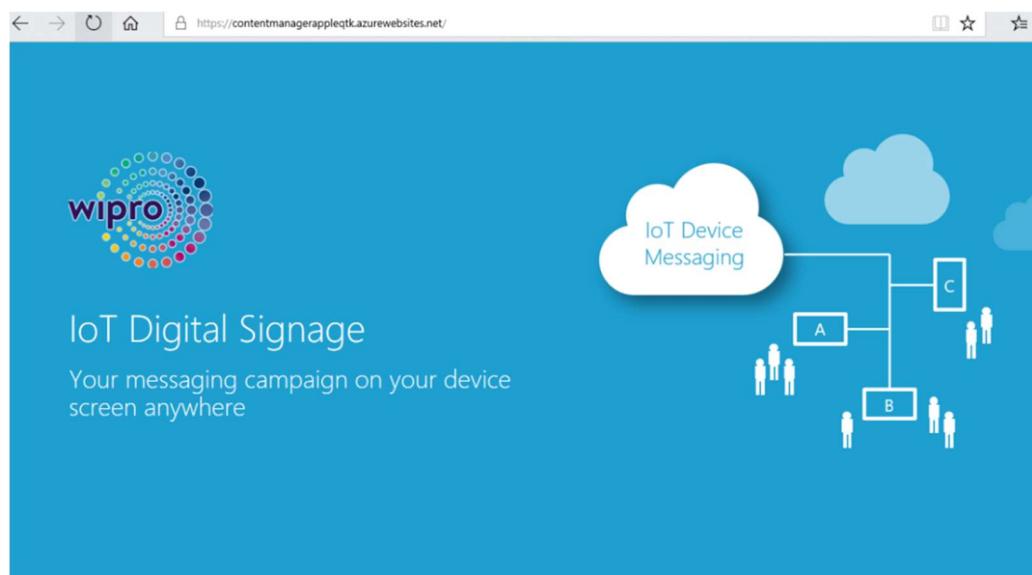
12. Signup to Digital signage UI

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.

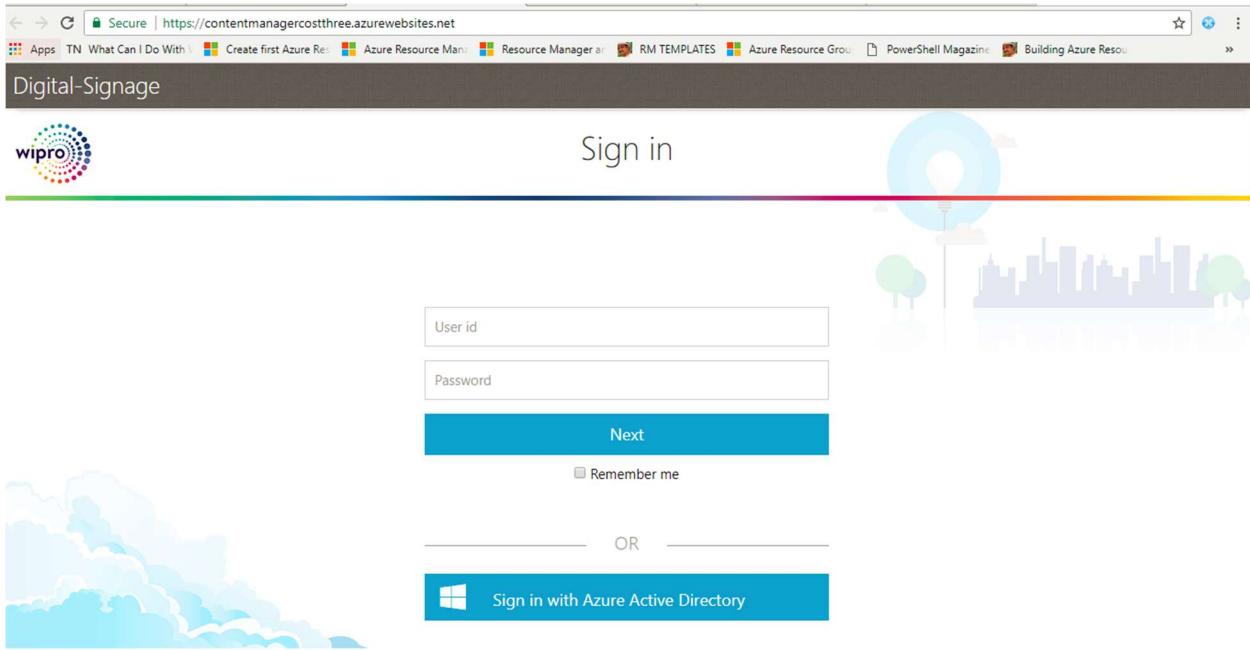
Microsoft Template - Outputs

Parameter	Value
AZURESQLPASSWORD	Enter the sqlAdministratorLoginPassword which you have entered in parameter section
DESTINATIONSTORAGEACCOUNTNAME	imagecontenthy74
WEBAPPURL	https://contentmanagerhy74.azurewebsites.net/
NODESERVERURL	https://nodeserverapphy74.azurewebsites.net/
TRAFFICMANAGERWEBAPPURL	https://contentmanagertmhhy74.trafficmanager.net
TRAFFICMANAGERNODESERVERURL	https://nodeserverappmhhy74.trafficmanager.net
WEBJOBURL	https://signageServerhy74.scm.azurewebsites.net//azurejobs/
IOTHUBENDPOINT	digital-signagehubhy74.azure-devices.net
OMSLOGANALYTICSURL	https://omswhhy74.portal.mms.microsoft.com/
APPINSIGHTSURL	https://analytics.applicationinsights.io/subscriptions/2927217-b119-4d3b-8a13-82a1c...
IOTDPGLOBALENDPOINT	global.azure-devices-provisioning.net
IOTDPSSERVERENDPOINT	iotDeviceProvisionhy74.azure-devices-provisioning.net

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.



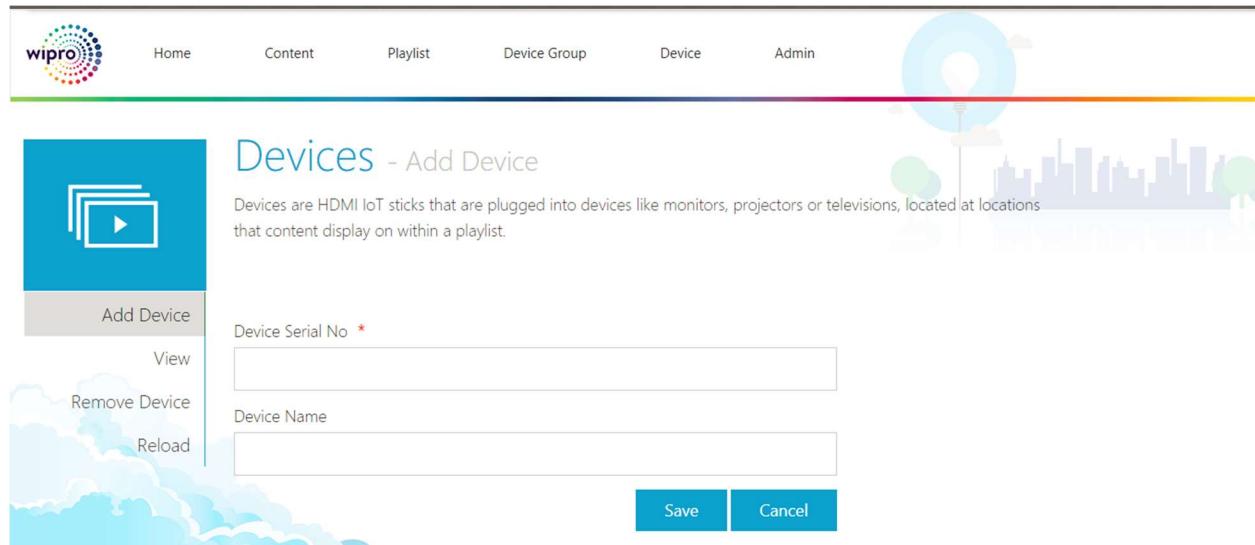
6. Once you login the **Home** page is displayed as shown in the following figure.



12.1. Add Device

To add device, follow the below steps,

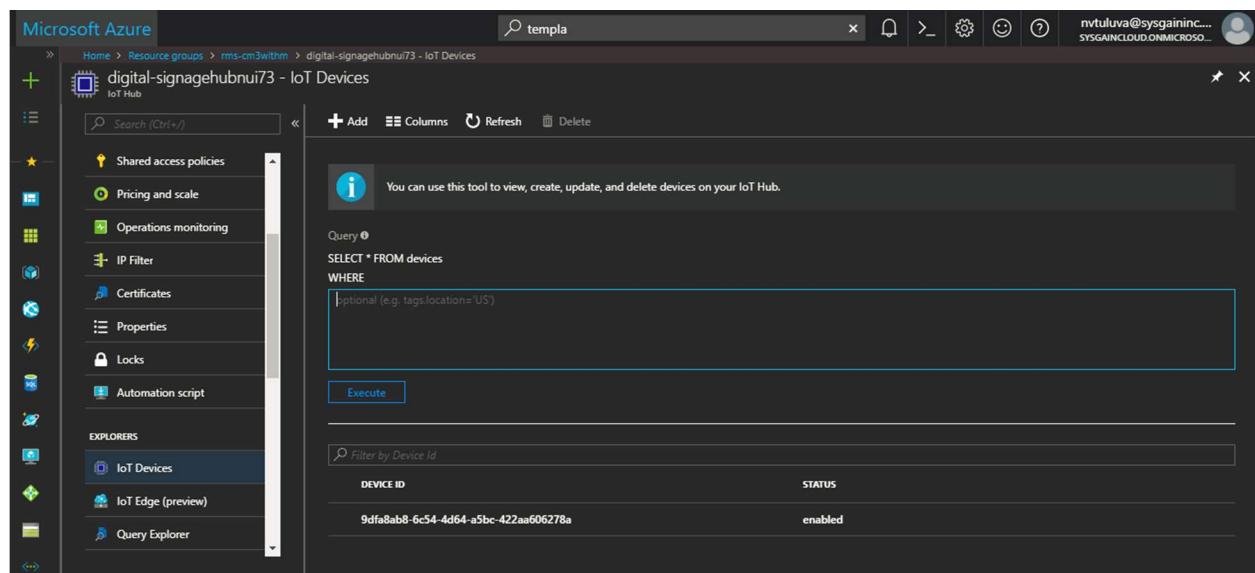
1. Click “**Device**” from top of menu **Devices** page is displayed as shown in the following figure.



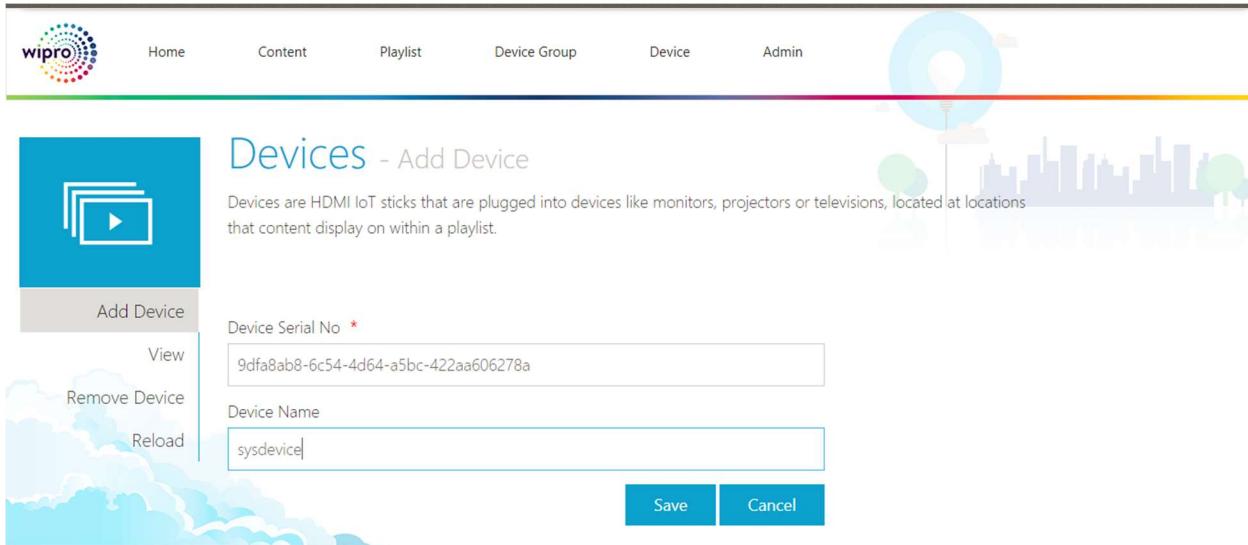
2. Select **Add Device** option from the left menu.

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.

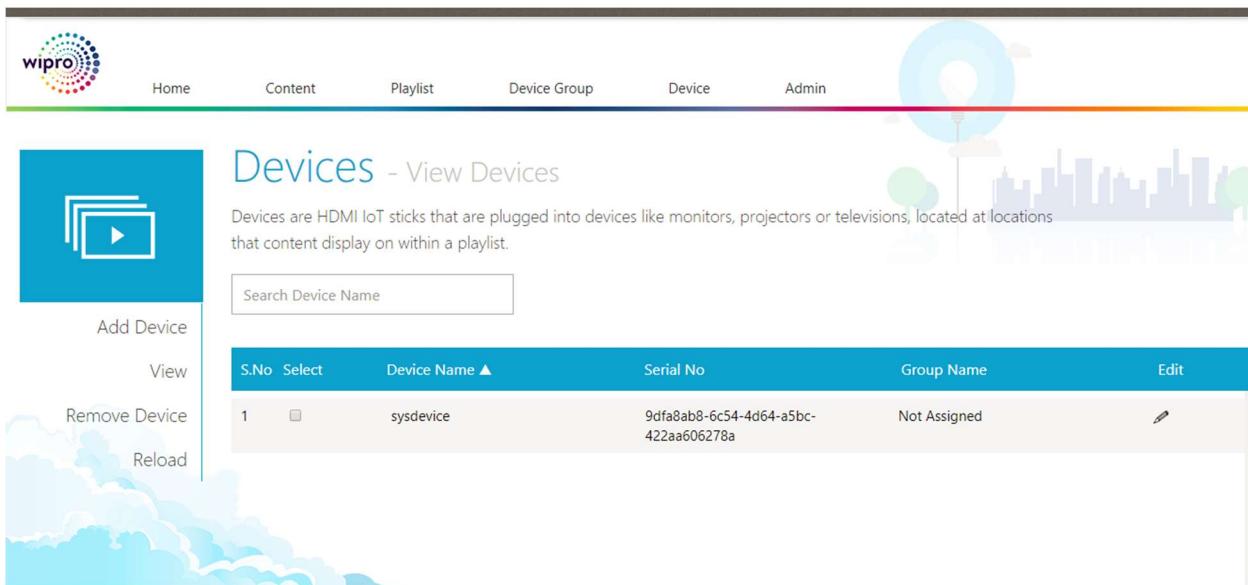


Device Serial No *

Device Name

Save **Cancel**

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



S.No	Select	Device Name ▲	Serial No	Group Name	Edit
1	<input type="checkbox"/>	sysdevice	9dfa8ab8-6c54-4d64-a5bc-422aa606278a	Not Assigned	

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

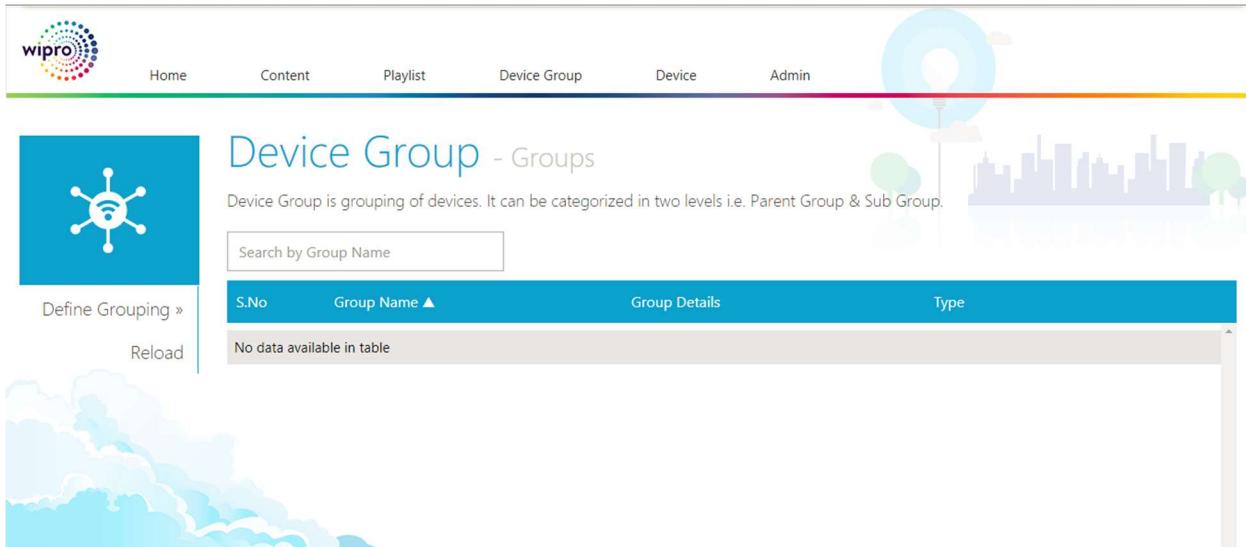
example: "**digitalsignageiothubid**" which was saved in earlier step.

12.2. Device Group

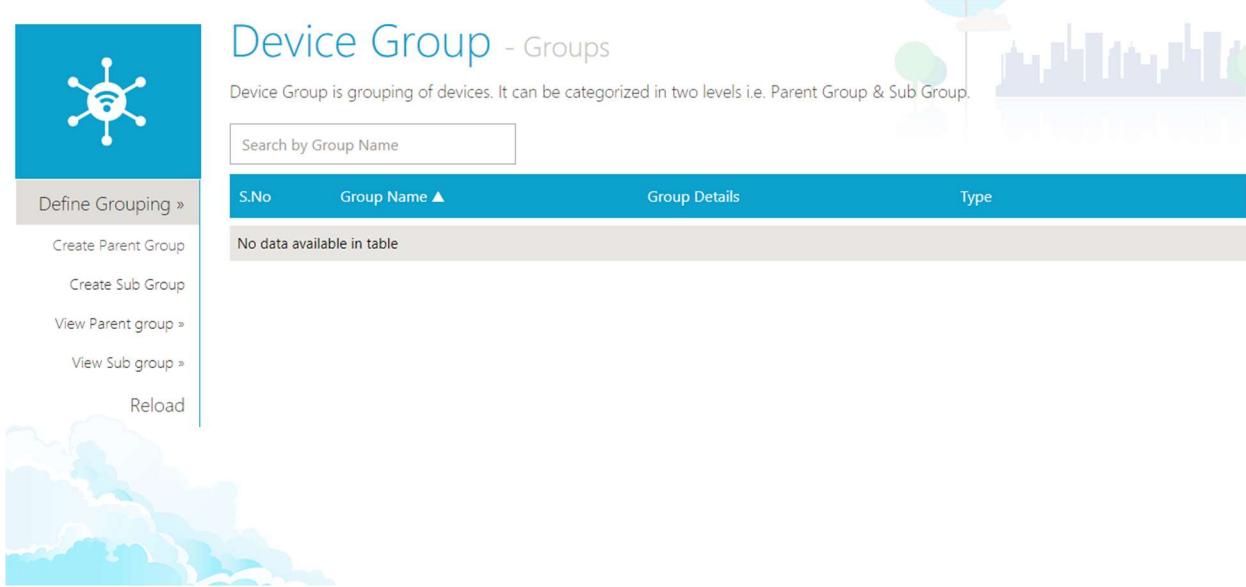
1. Select "**Device Group**" from the top menu

12.2.1. Create Device Group

- 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.

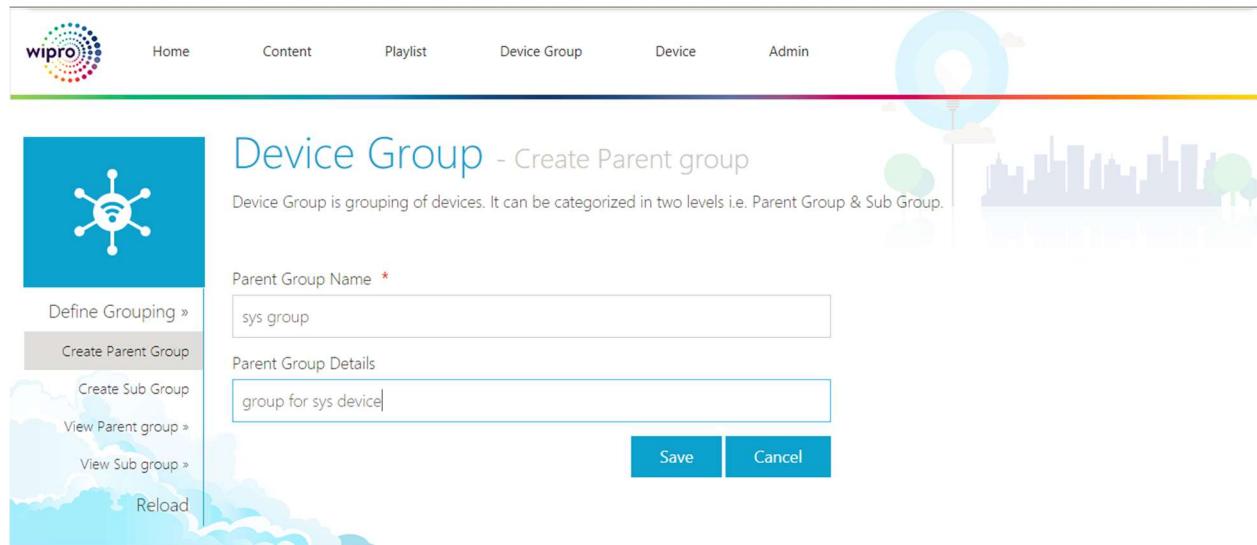


The screenshot shows the 'Device Group - Groups' page. At the top, there is a navigation bar with links: Home, Content, Playlist, Device Group (which is the active tab), Device, and Admin. Below the navigation bar, there is a search bar labeled 'Search by Group Name'. A table is present with columns: S.No, Group Name ▲, Group Details, and Type. A message 'No data available in table' is displayed below the table. On the left side, there is a sidebar with a blue icon and the following options: Define Grouping », Create Parent Group, Create Sub Group, View Parent group », View Sub group », and Reload.



This screenshot is identical to the one above, showing the 'Device Group - Groups' page. The main difference is the expanded sidebar on the left, which includes additional options: 'Define Grouping »', 'Create Parent Group', 'Create Sub Group', 'View Parent group »', 'View Sub group »', and 'Reload'.

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



Device Group - Create Parent group

Device Group is grouping of devices. It can be categorized in two levels i.e. Parent Group & Sub Group.

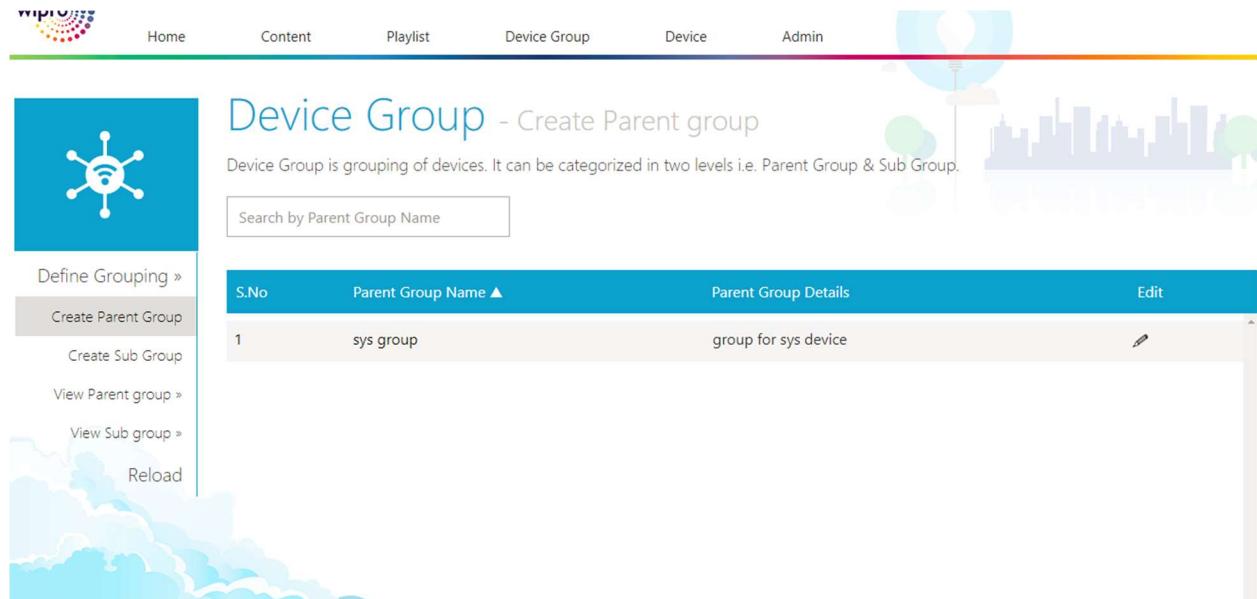
Parent Group Name *

Parent Group Details

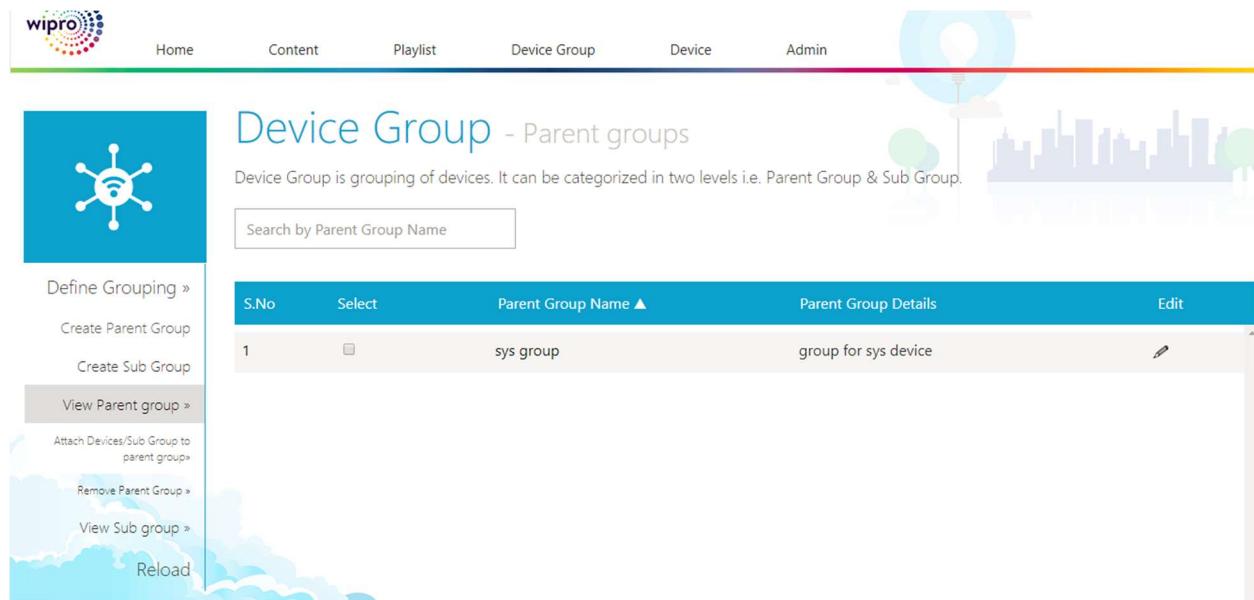
Save Cancel

12.2.2. Assign a device to the device group

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



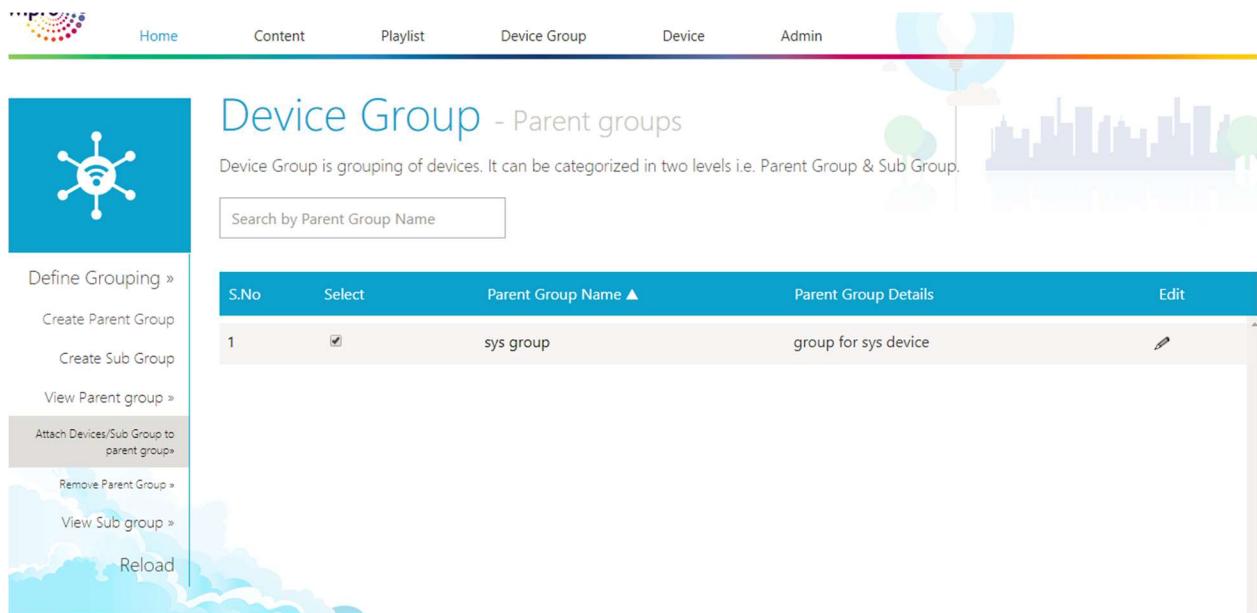
S.No	Parent Group Name	Parent Group Details	Edit
1	sys group	group for sys device	



The screenshot shows the 'Device Group - Parent groups' page. The left sidebar has a 'View Parent group' button highlighted. The main area displays a table with the following data:

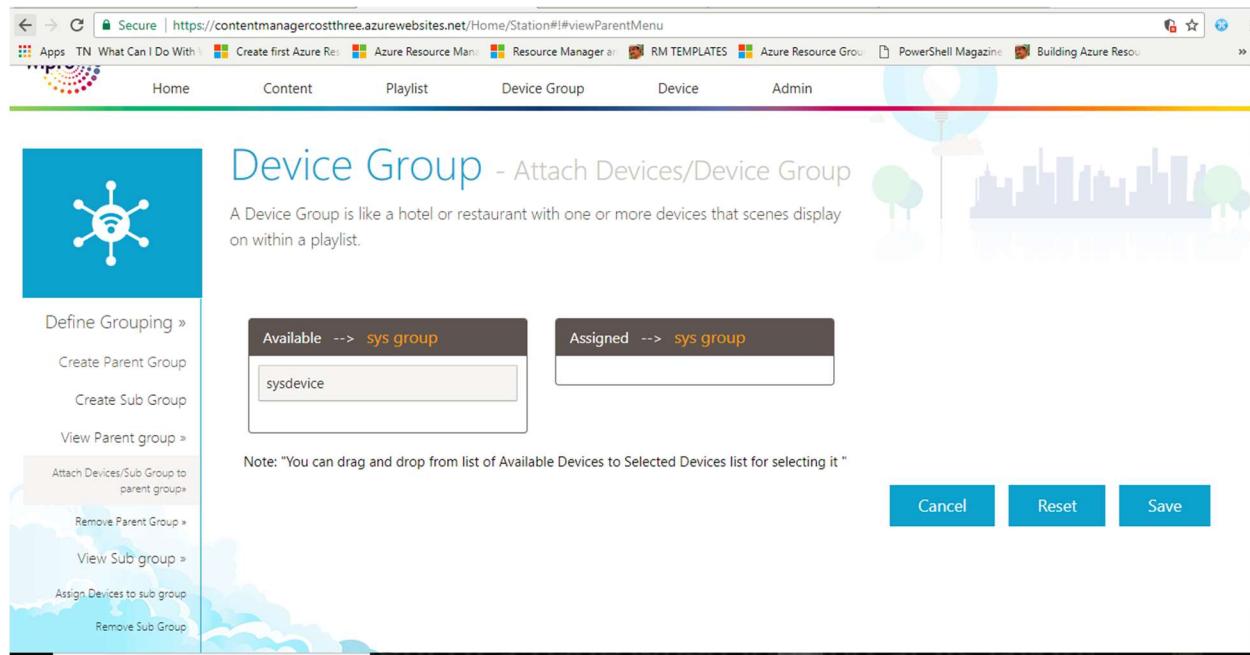
S.No	Select	Parent Group Name ▲	Parent Group Details	Edit
1	<input type="checkbox"/>	sys group	group for sys device	

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



The screenshot shows the same 'Device Group - Parent groups' page, but the 'Select' checkbox for the first row ('sys group') is now checked. The table data remains the same as in the previous screenshot.

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



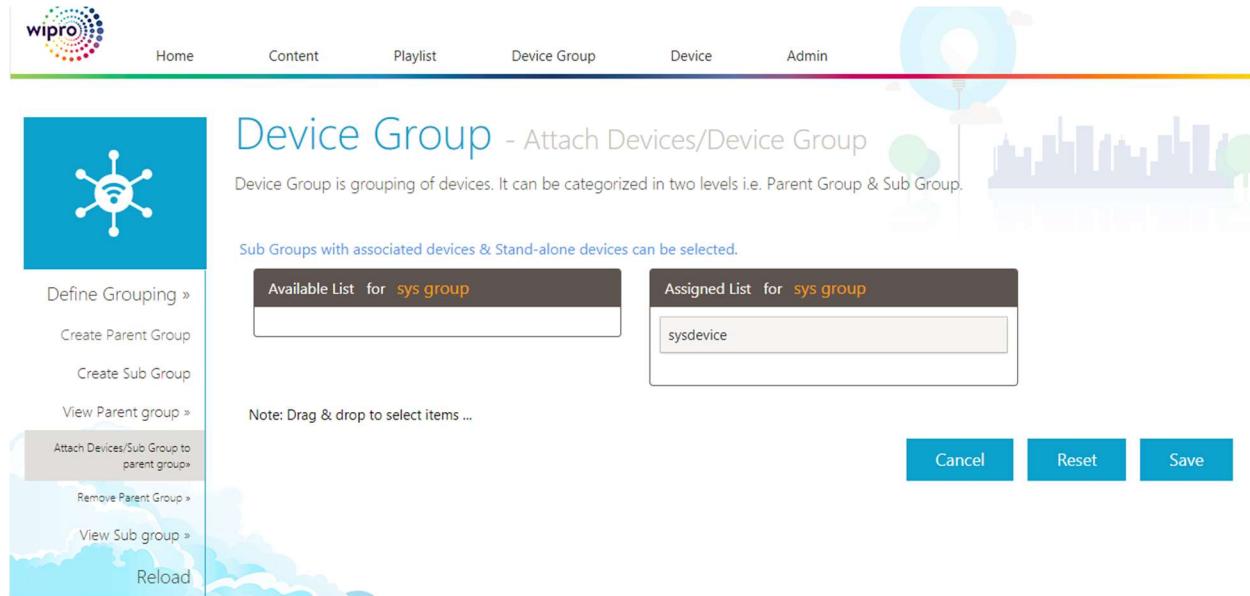
A Device Group is like a hotel or restaurant with one or more devices that scenes display on within a playlist.

Available --> sys group
Assigned --> sys group

Note: "You can drag and drop from list of Available Devices to Selected Devices list for selecting it"

Cancel Reset Save

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



Device Group is grouping of devices. It can be categorized in two levels i.e. Parent Group & Sub Group.

Sub Groups with associated devices & Stand-alone devices can be selected.

Note: Drag & drop to select items ...

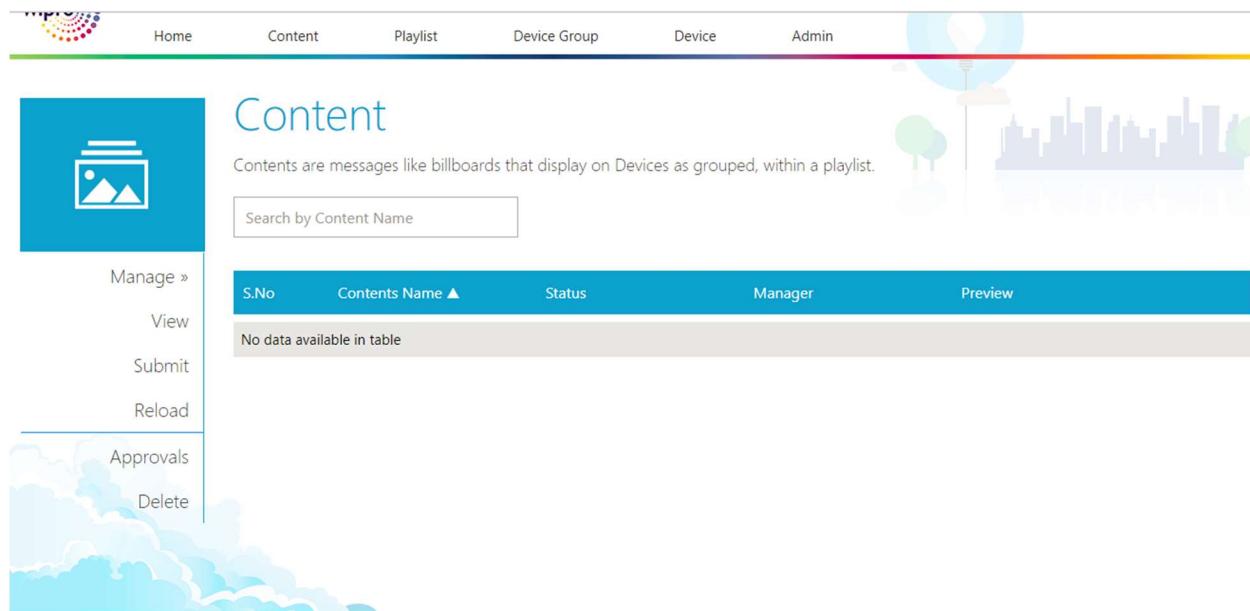
Available List for sys group
Assigned List for sys group

sysdevice

Cancel Reset Save

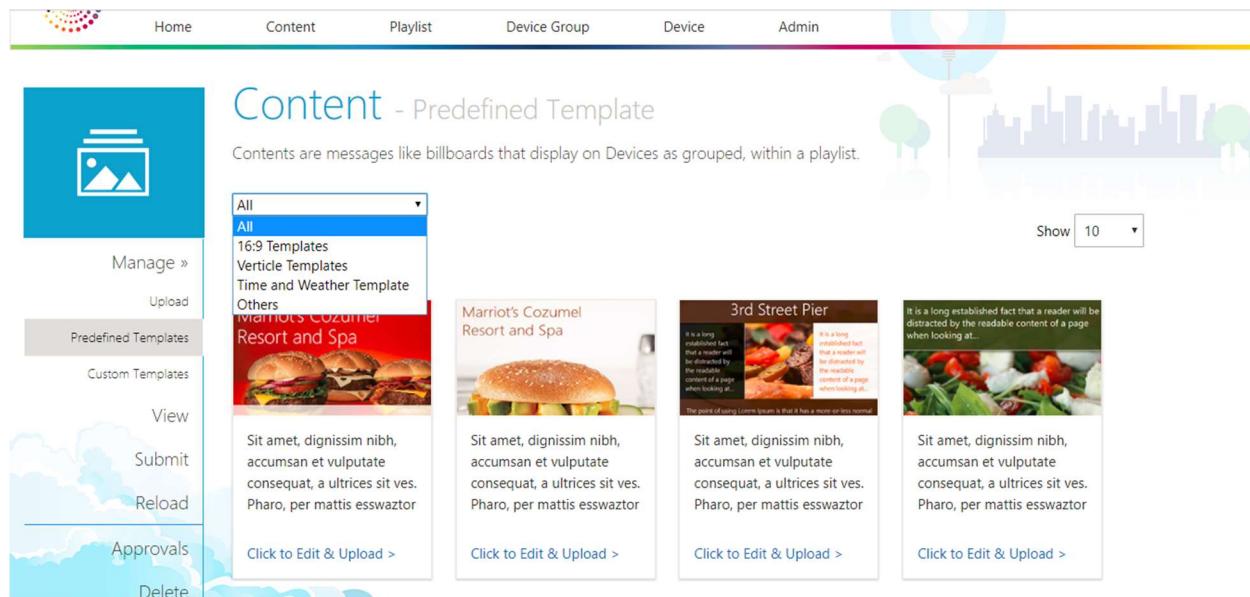
12.3. Content

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.



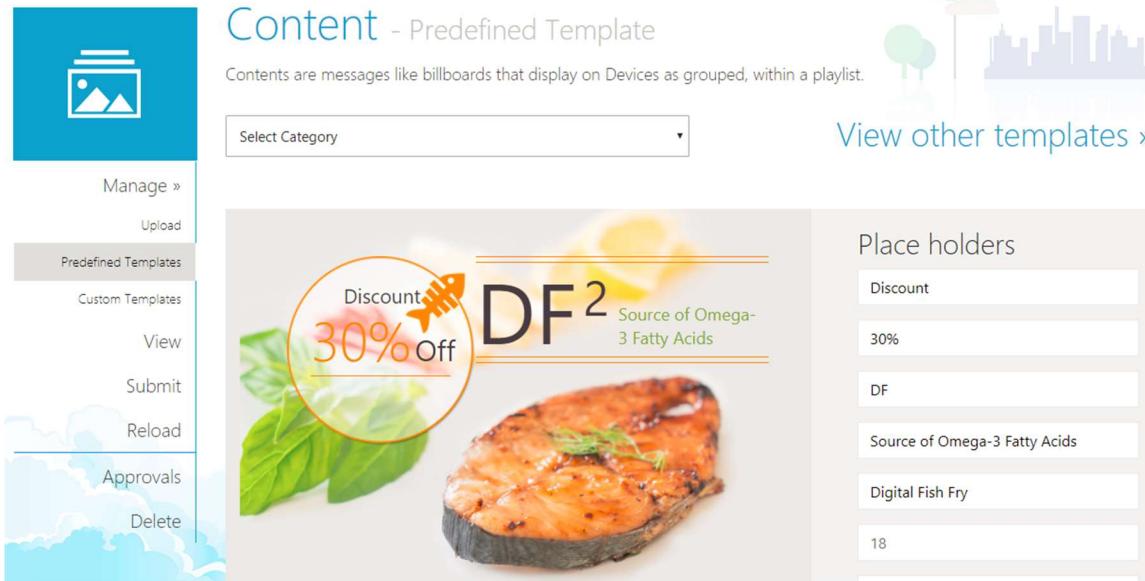
12.3.1. Add Content – Predefined Template

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.

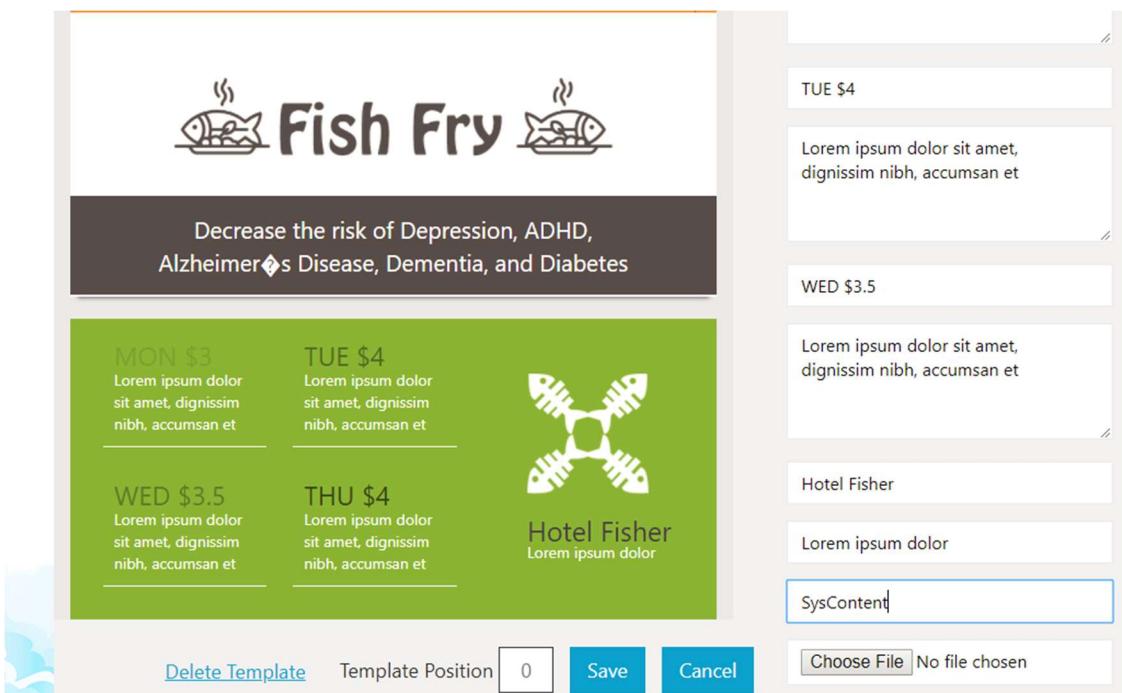


2. Choose a Template and select “**Click to Edit and Upload.**” As shown in the following figure. Choose a static template to Customize with your images and text.

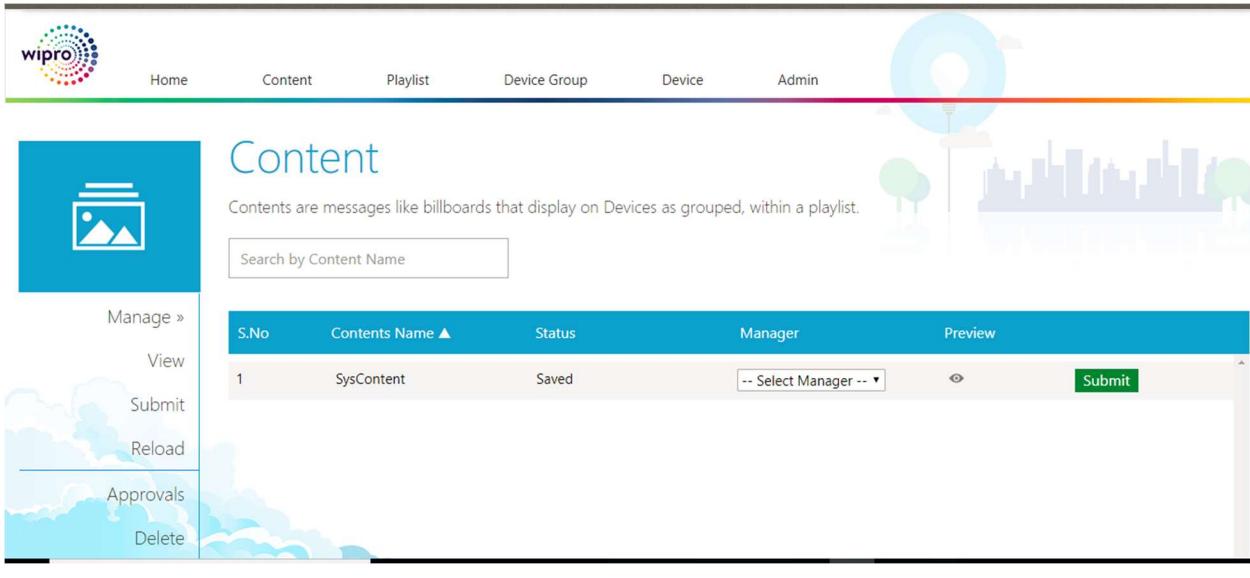
3. Select the category from the dropdown list as shown in the above figure.



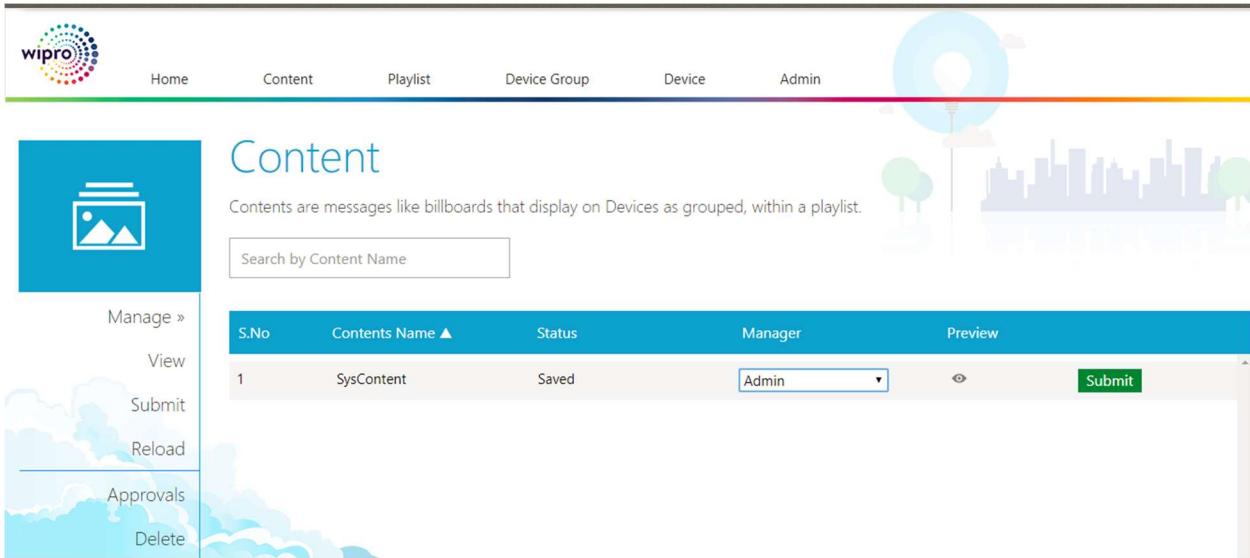
4. In the **Place holders** section, Enter the **Template Name** in the field and click **Save** button.



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

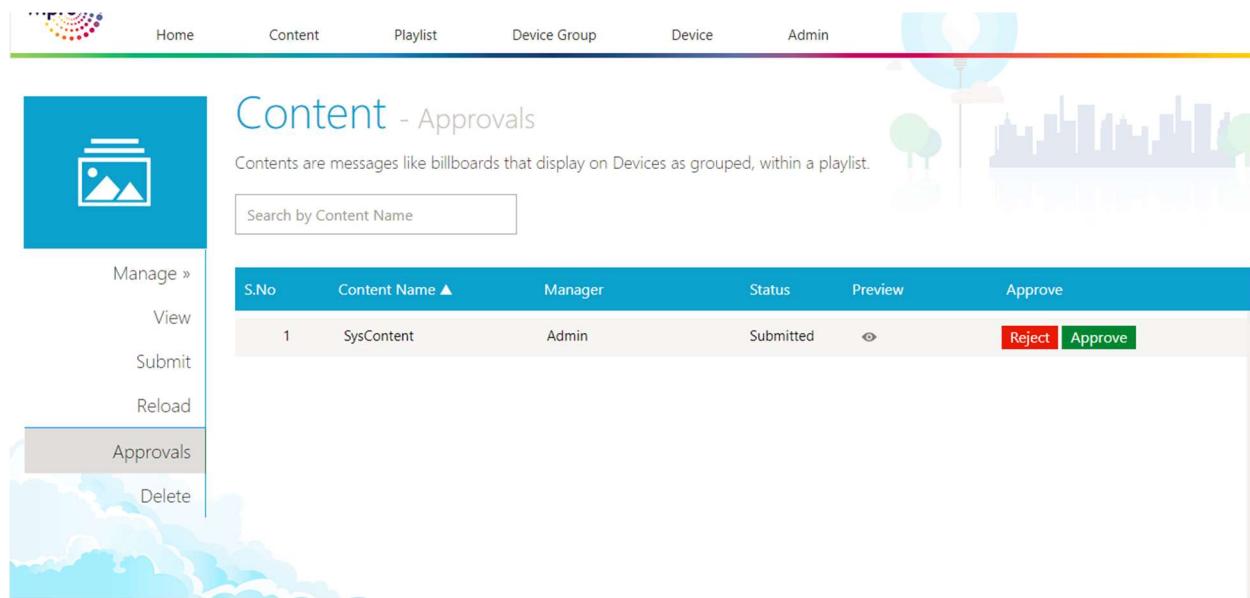


S.No	Contents Name ▲	Status	Manager	Preview
1	SysContent	Saved	-- Select Manager --	 



S.No	Contents Name ▲	Status	Manager	Preview
1	SysContent	Saved	Admin	 

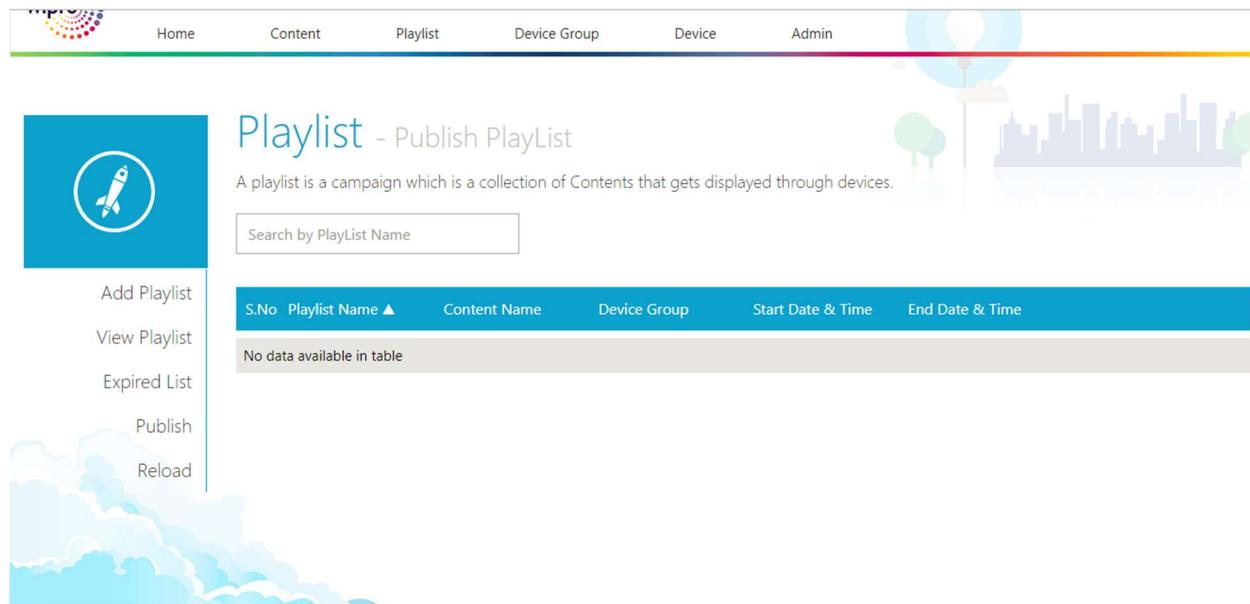
6. Select **View** from the left menu to display the list of contents that are added earlier.
7. Click **Approvals** to check the contents which are pending for Approval by the Admin.



S.No	Content Name ▲	Manager	Status	Preview	Approve
1	SysContent	Admin	Submitted		Reject Approve

12.4. Playlist

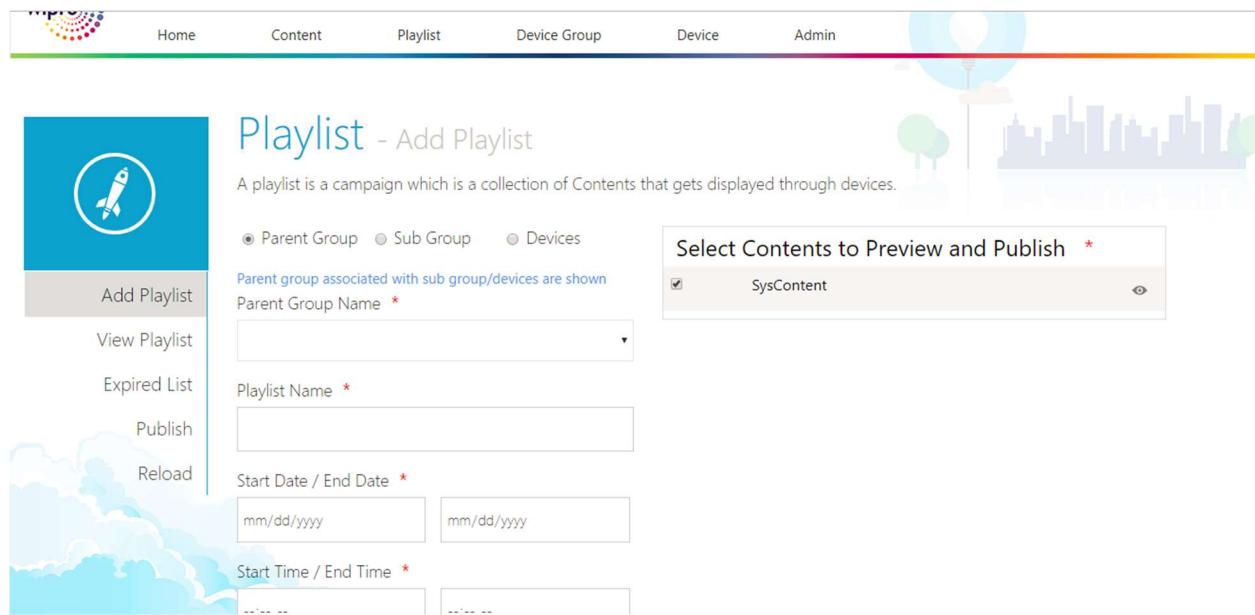
Select “**Playlist**” from the top menu, the publish playlist page is displayed as shown in the following figure.



S.No	Playlist Name ▲	Content Name	Device Group	Start Date & Time	End Date & Time
No data available in table					

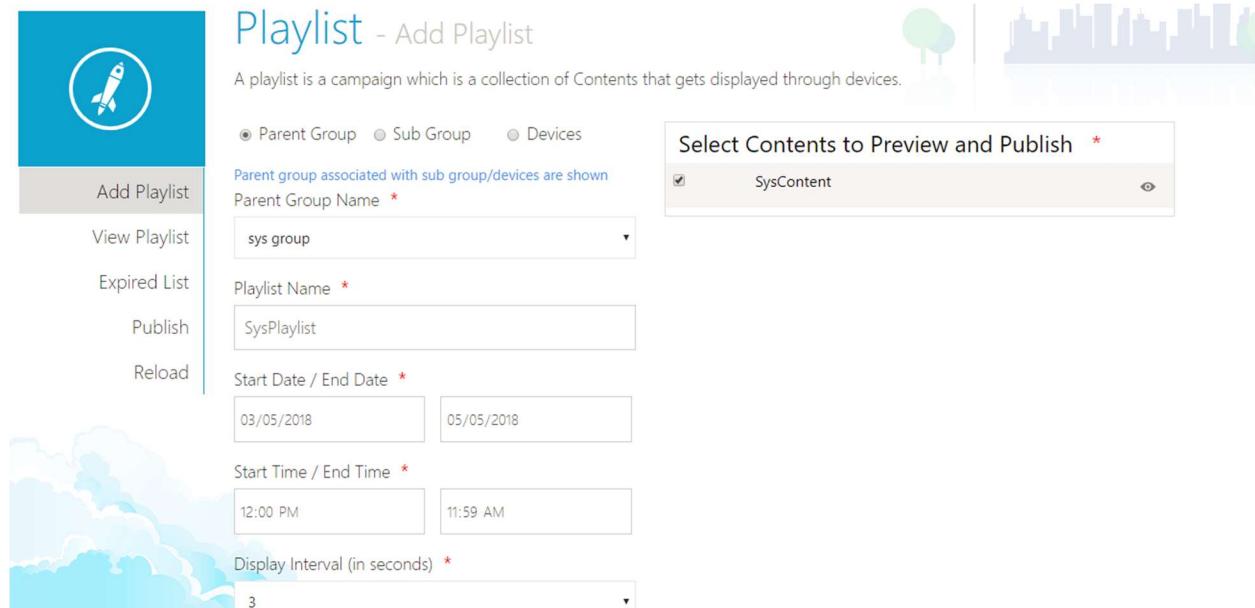
12.4.1. To Add a Playlist

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

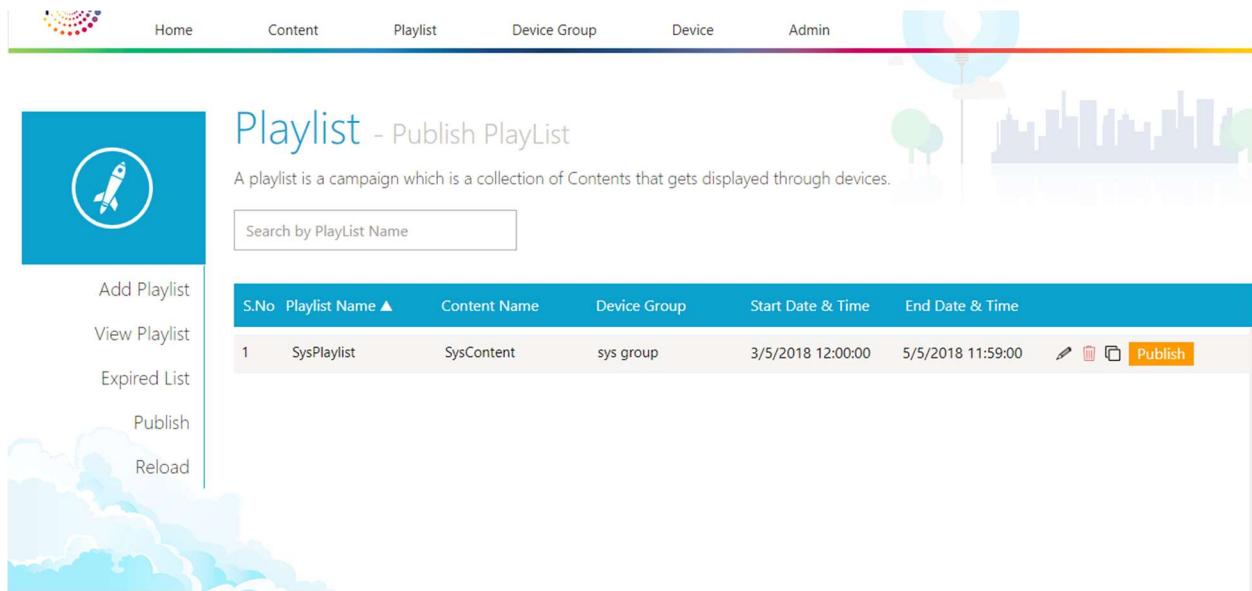


12.4.1.1. Define the settings for the playlist

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.



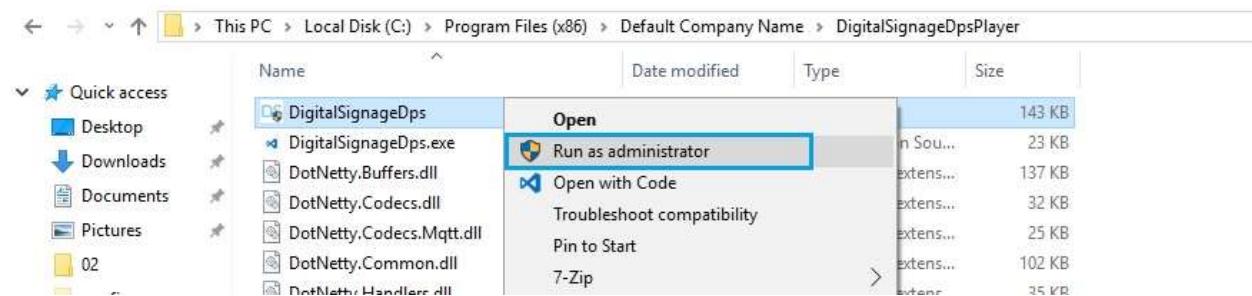
2. Enter the **Playlist Name** in the respective field.
3. Enter the **Start/End Date** and **Start/End Time** in their respective fields.
4. Set the **Display Interval (In seconds) and Frequency** from the dropdown list.
5. Click **Save** button to save the Playlist is added,
6. Click **Publish** button,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



A playlist is a campaign which is a collection of Contents that gets displayed through devices.

S.No	Playlist Name	Content Name	Device Group	Start Date & Time	End Date & Time
1	SysPlaylist	SysContent	sys group	3/5/2018 12:00:00	5/5/2018 11:59:00

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

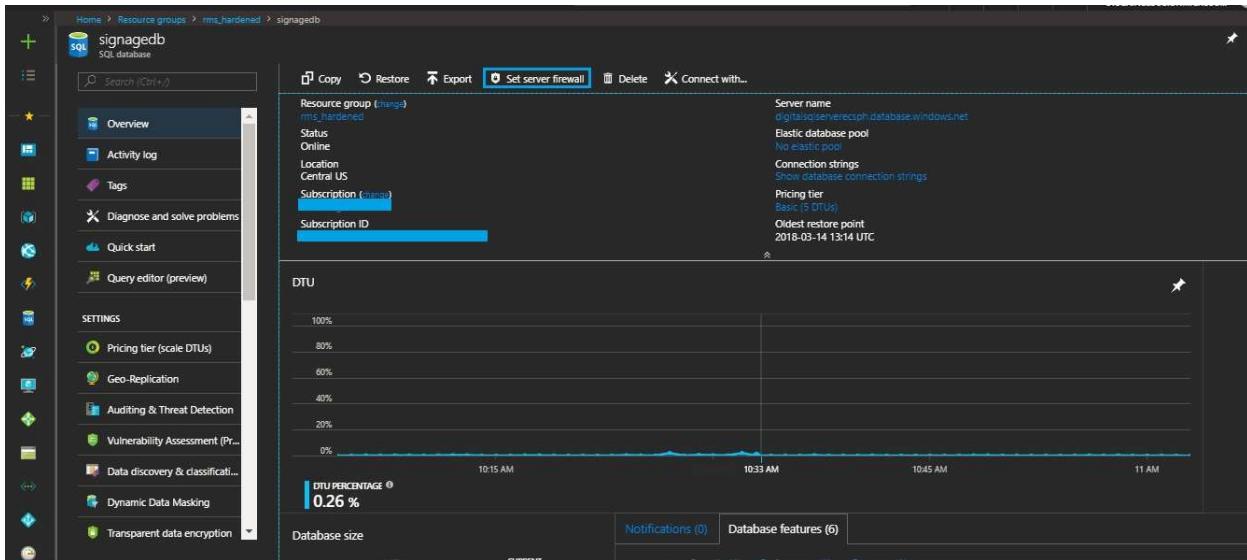




13. Validation

13.1. SQL Server verification

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

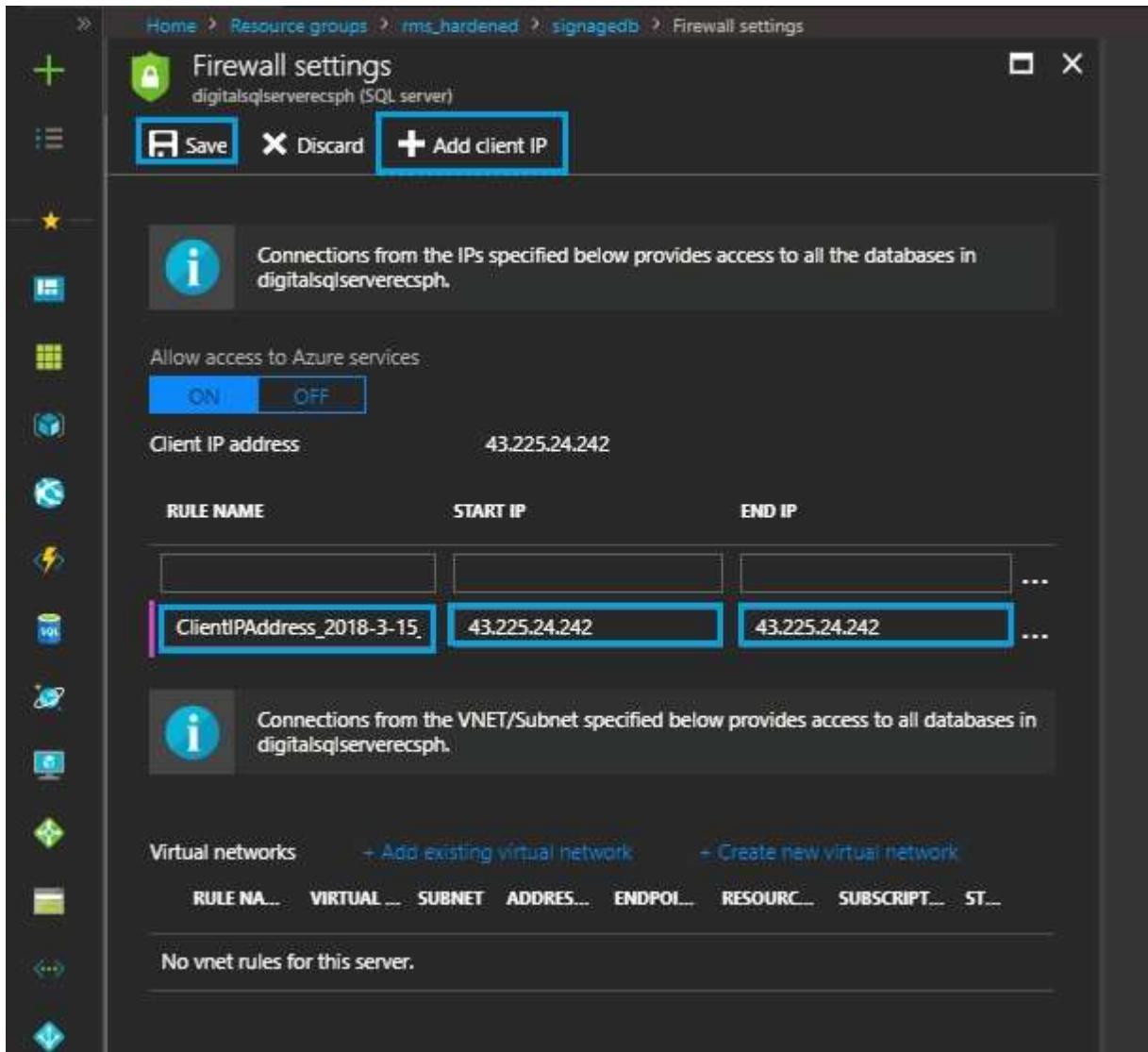


The screenshot shows the Azure portal interface for managing a SQL database named 'signagedb'. The left sidebar lists various database management options like Overview, Activity log, Tags, and Query editor. The main panel displays the 'Overview' tab for the resource group 'rms_hardened'. Key details shown include:

- Resource group: rms_hardened
- Status: Online
- Location: Central US
- Subscription: (new)
- Subscription ID: [redacted]
- Server name: digitalserverccph.database.windows.net
- Elastic database pool: No elastic pool
- Connection strings: Show database connection strings
- Pricing tier: Basic (5 DTUs)
- Oldest restore point: 2018-03-14 13:14 UTC

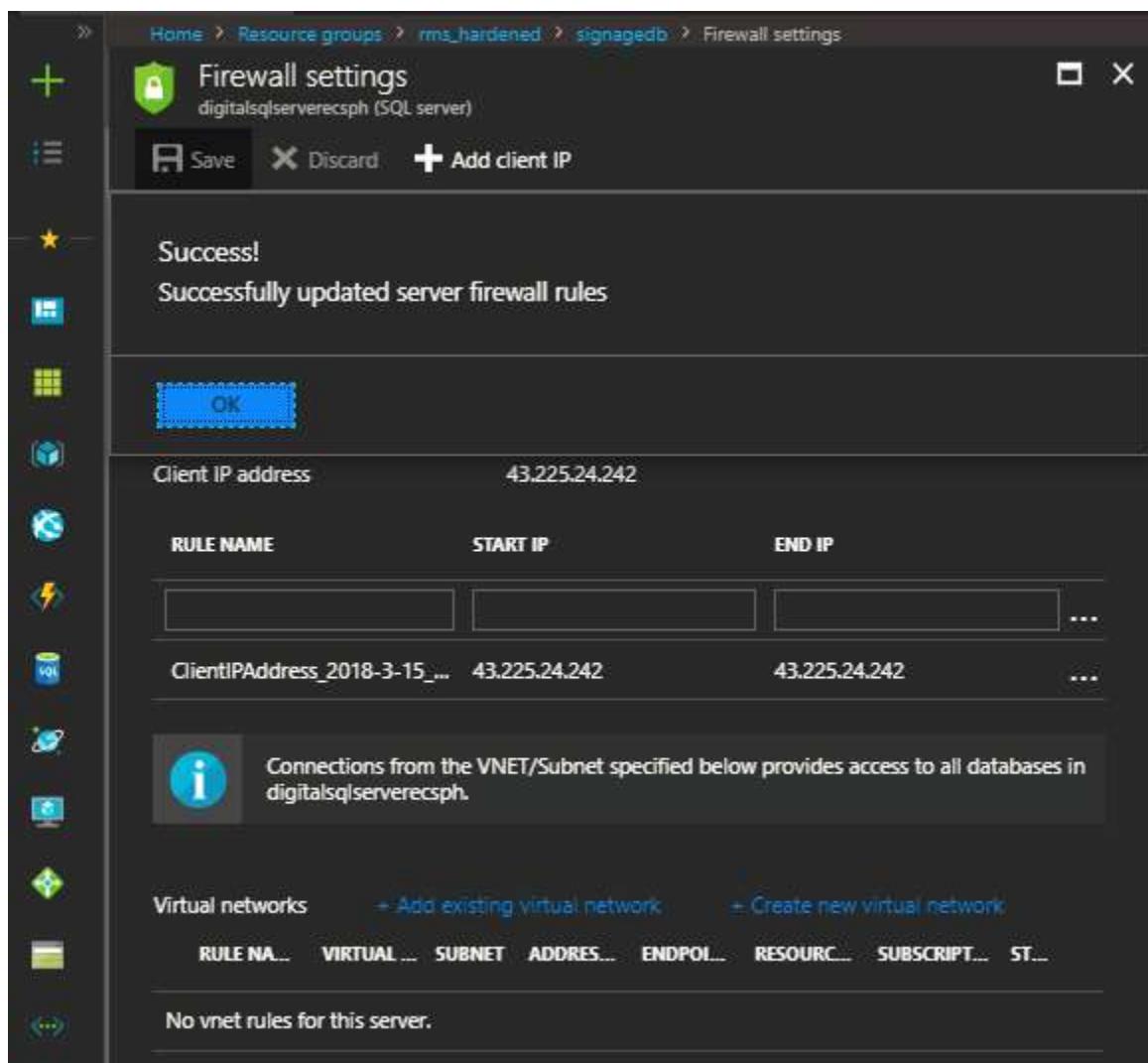
Below this, there's a chart titled 'DTU' showing usage over time, with a value of 0.26% indicated at the bottom.

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

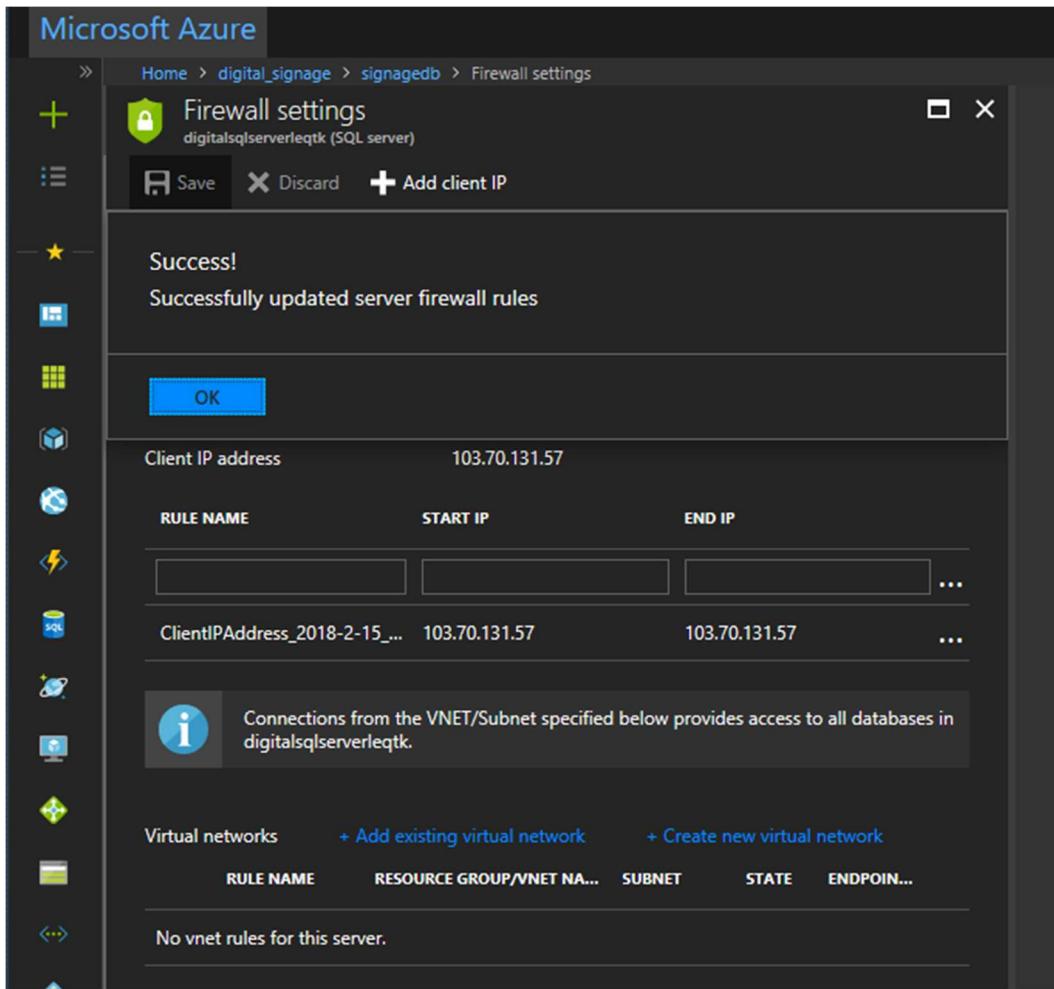


The screenshot shows the 'Firewall settings' blade for a SQL server named 'digitalsqlserverecph'. At the top, there are 'Save' and 'Discard' buttons, and a prominent blue 'Add client IP' button which is highlighted with a blue box. Below this, a tooltip explains that connections from specified IPs provide access to all databases. An 'Allow access to Azure services' toggle switch is set to 'ON'. A table lists a single rule: 'ClientIPAddress_2018-3-15' with 'START IP' 43.225.24.242 and 'END IP' 43.225.24.242. Further down, another section for 'Virtual networks' is shown with a table header: 'RULE NA...', 'VIRTUAL...', 'SUBNET...', 'ADDRES...', 'ENDPOI...', 'RESOURC...', 'SUBSCRIPT...', 'ST...'. A message at the bottom states 'No vnet rules for this server.'

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

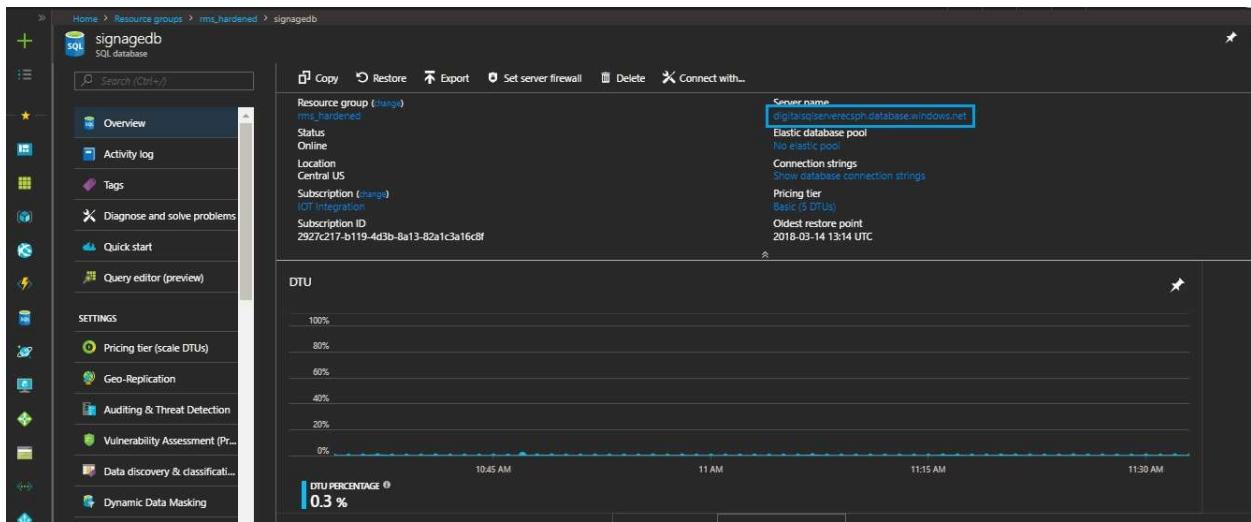


The screenshot shows the 'Firewall settings' page for a SQL server named 'digitalsqlserverecsph'. The top navigation bar includes 'Home', 'Resource groups', 'rms_hardened', 'signagedb', and 'Firewall settings'. Below the title, there are 'Save', 'Discard', and 'Add client IP' buttons. A success message states 'Successfully updated server firewall rules'. An 'OK' button is present. The main table displays a single rule: 'ClientIPAddress_2018-3-15...' with 'START IP' 43.225.24.242 and 'END IP' 43.225.24.242. A tooltip explains that VNET/Subnet access provides access to all databases. At the bottom, there are buttons for 'Virtual networks', 'Add existing virtual network', 'Create new virtual network', and columns for 'RULE NAME', 'VIRTUAL...', 'SUBNET', 'ADDRESS...', 'ENDPOL...', 'RESOURCE...', 'SUBSCRIPT...', and 'ST...'. A note at the bottom states 'No vnet rules for this server.'



The screenshot shows the Microsoft Azure Firewall settings page for a SQL server named 'digitalsqlserverleqtk'. A success message 'Successfully updated server firewall rules' is displayed. Below it, a table lists a single rule: 'Client IP address' 103.70.131.57. The table has columns for RULE NAME, START IP, and END IP. A note below the table states: 'Connections from the VNET/Subnet specified below provides access to all databases in digitalsqlserverleqtk.' At the bottom, there are buttons for Virtual networks, Add existing virtual network, and Create new virtual network.

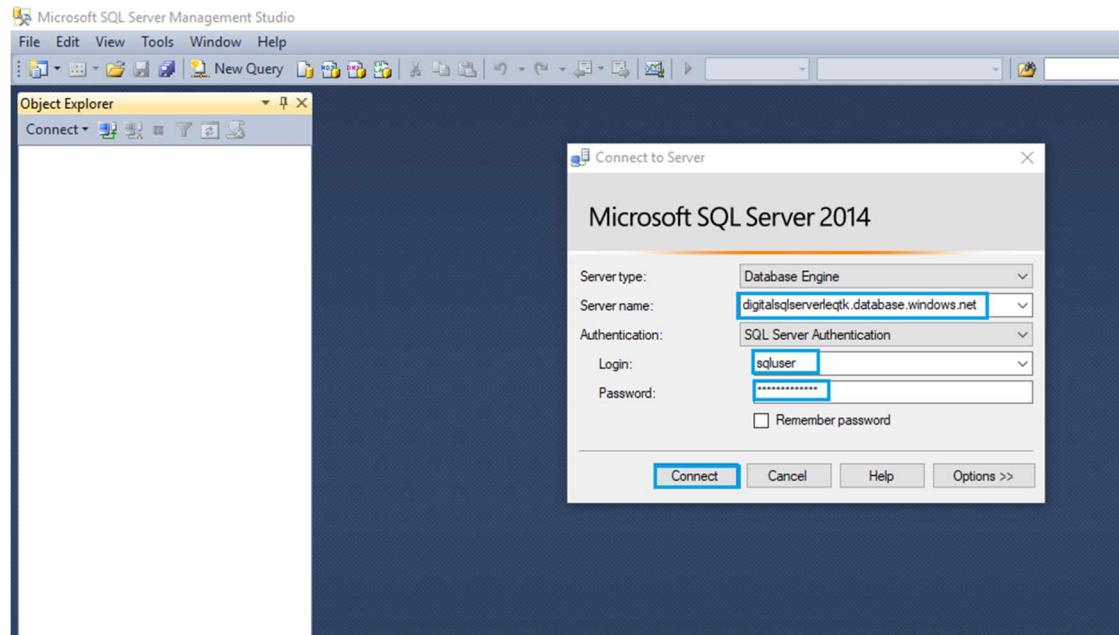
4. Open **Azure portal** and copy the server name.



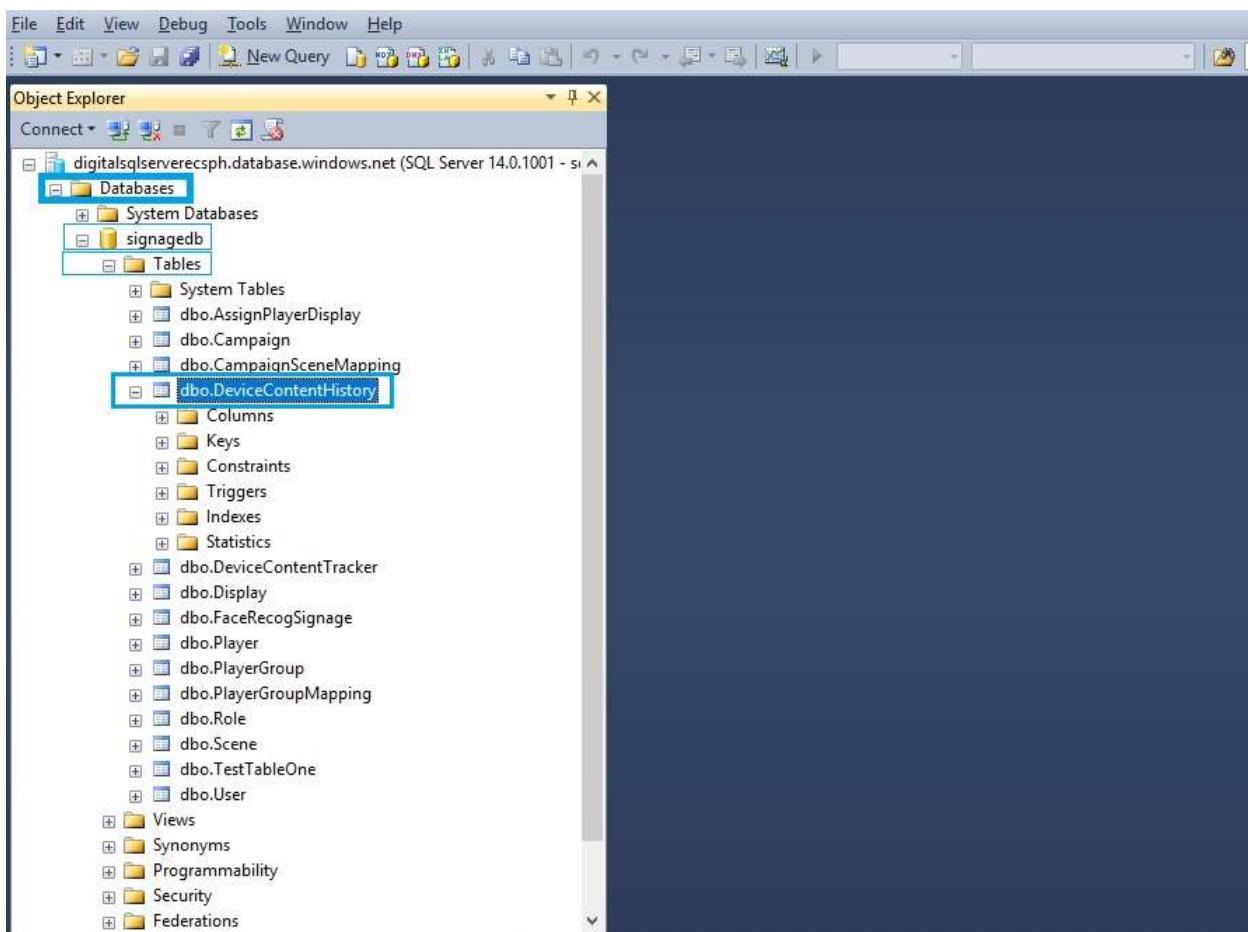
The screenshot shows the Azure portal's overview page for a SQL database named 'signededb'. The 'Server name' field is highlighted and contains the value 'digitalsqlserverleqph.database.windows.net'. Other details shown include the status 'Online', location 'Central US', and a DTU usage chart at the bottom.

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

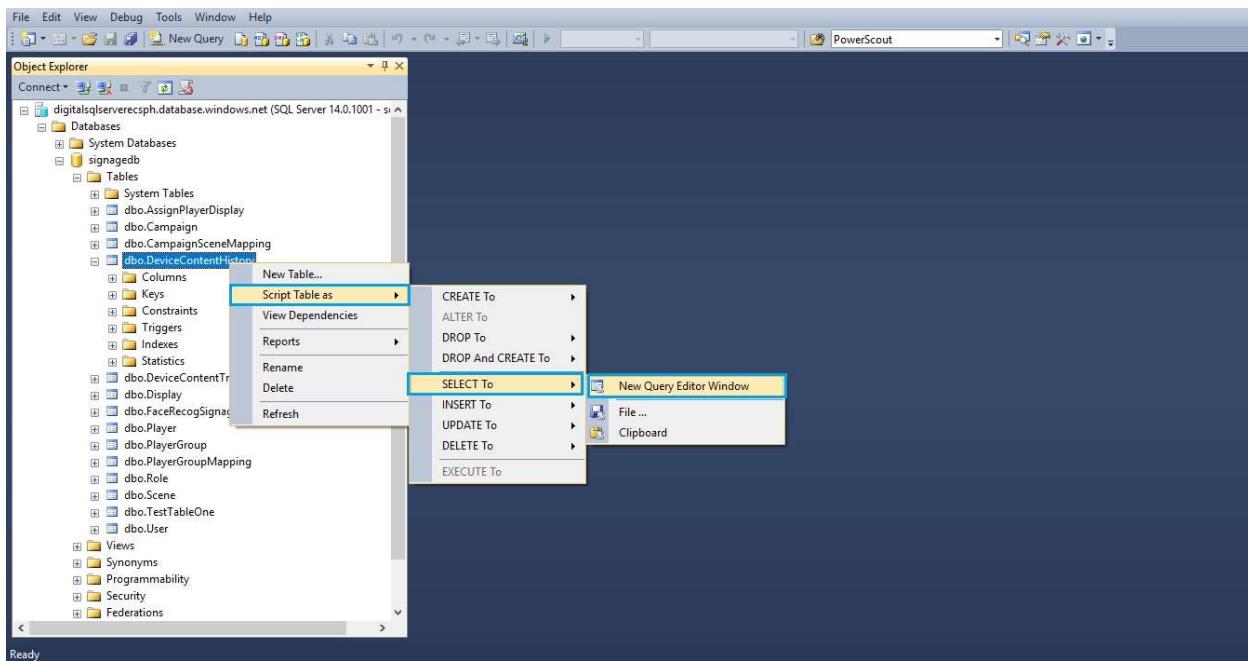
6. Enter the Login and password which are provided for SQL at the time of template deployment and click **Connect** button.



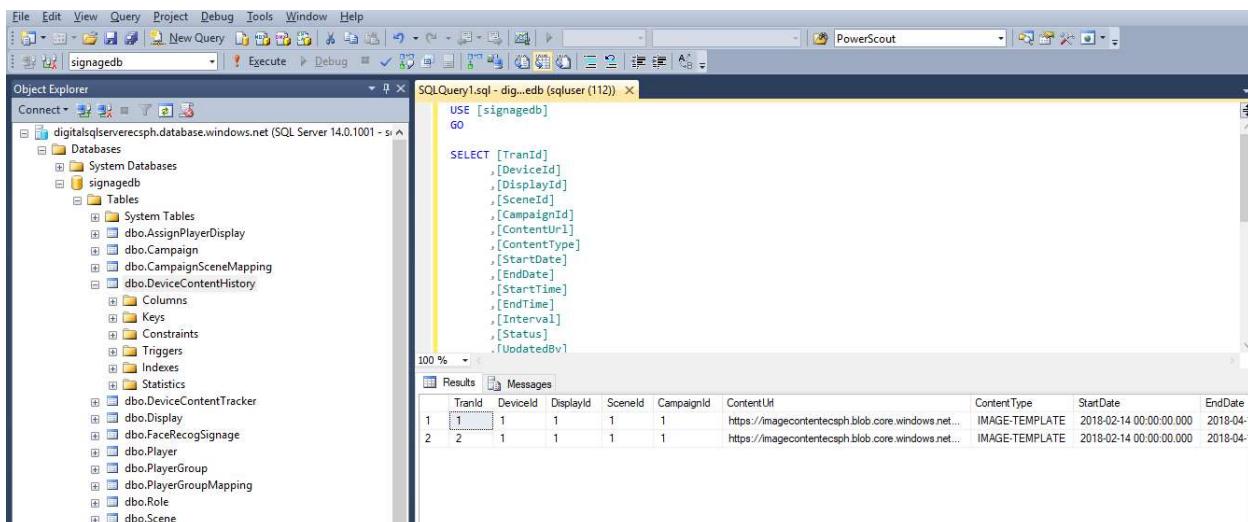
7. Navigate to **Databases > System Databases > Tables** and select the table as shown in the following figure.



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

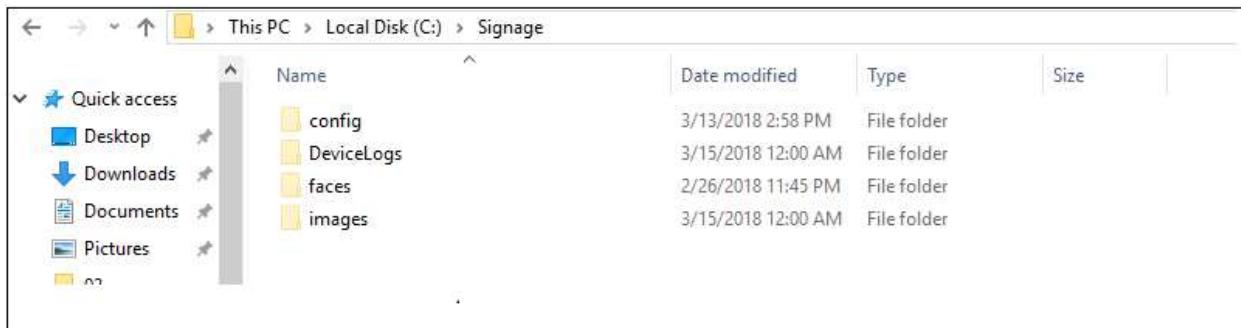


9. The table is displayed as shown in the following figure.

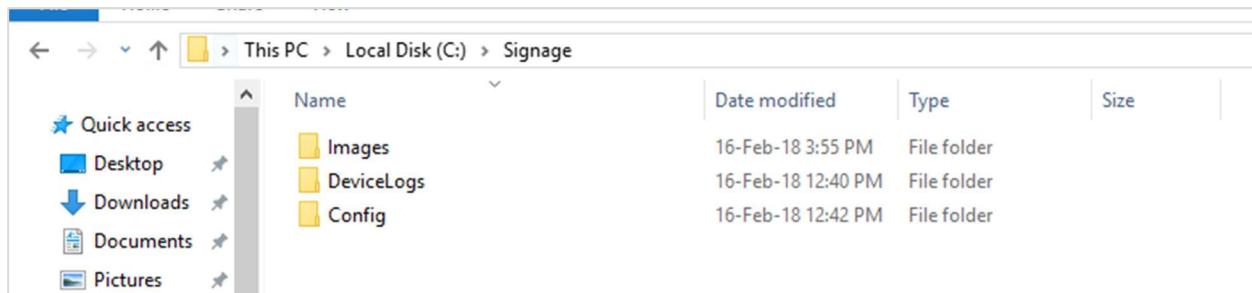


13.2. Stick VM Cache Verification

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



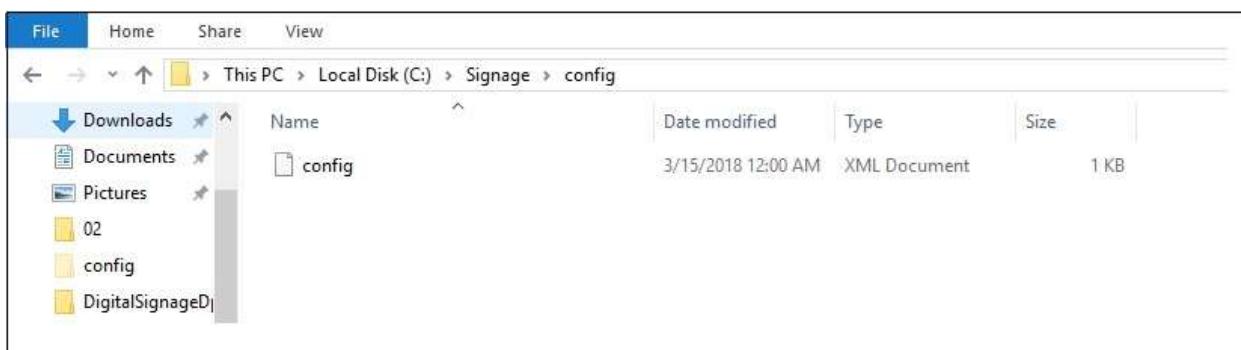
2. Go to **Local Disk (C:) > Signage** to verify.



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

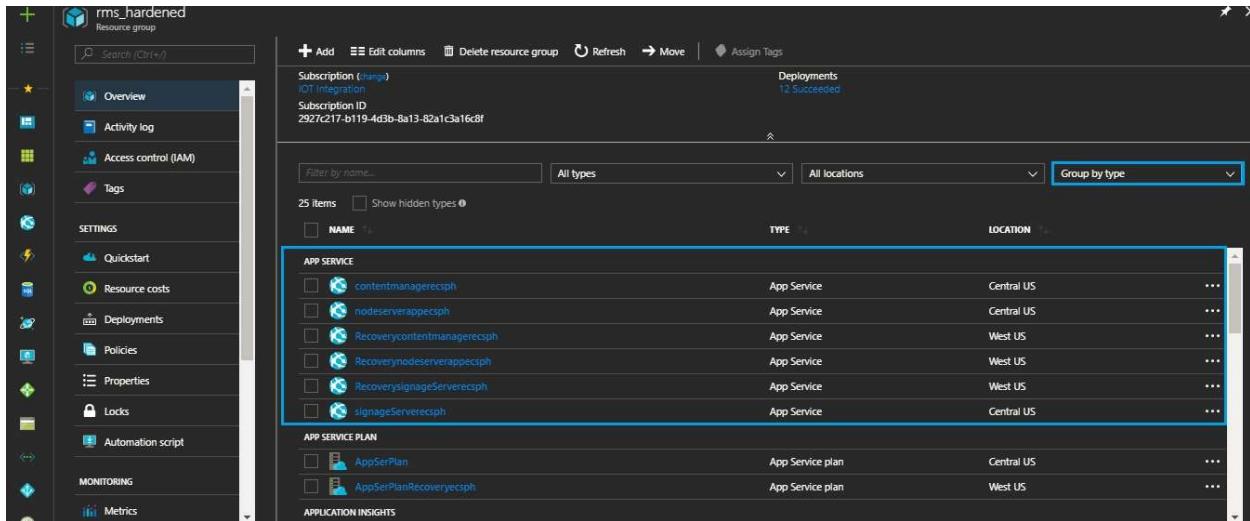


4. Go to **Local Disk (C:) > Signage > Config** to check the config.xml

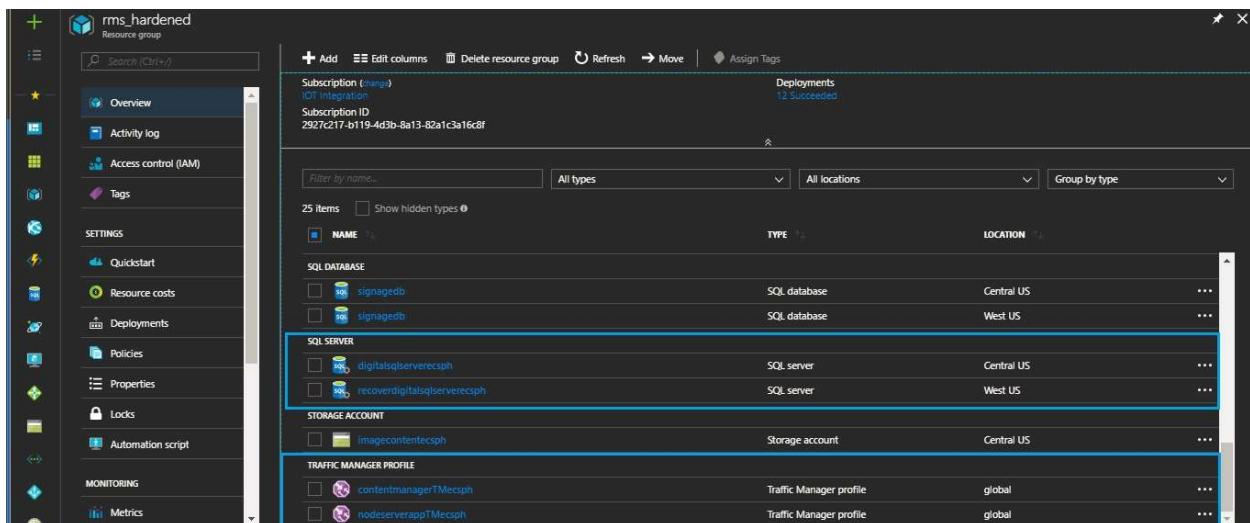


13.3. DR Validation

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



The screenshot shows the Azure portal interface for the 'rms_hardened' resource group. The left sidebar contains navigation links like Overview, Activity log, Access control (IAM), Tags, SETTINGS, Quickstart, Resource costs, Deployments, Policies, Properties, Locks, Automation script, MONITORING, and Metrics. The main area displays a table of resources grouped by type. The 'Group by type' dropdown menu is open, with 'All types' selected. The table includes columns for NAME, TYPE, and LOCATION. Resources listed under APP SERVICE include contentmanagerecsph, nodeserverappcsph, Recoverycontentmanagerecsph, Recoverynodeserverappcsph, RecoverysignageServercsph, and signagewServercsph, all categorized as App Service and located in Central US or West US. APP SERVICE PLAN entries show AppServicePlan and AppServicePlanRecoverycsph in Central US and West US respectively. There are also sections for APPLICATION INSIGHTS, SQL DATABASE, and other service types.



This screenshot shows the same 'rms_hardened' resource group overview as the previous one, but with a different grouping. The 'Group by type' dropdown is again highlighted. The table now groups resources by type, such as SQL DATABASE, SQL SERVER, STORAGE ACCOUNT, and TRAFFIC MANAGER PROFILE. It lists multiple instances of signededb, digitalsqlservercsph, and recoverdigitalsqlservercsph under SQL DATABASE. Under SQL SERVER, there are two entries for signagewServercsph. The storage account section contains imagecontentcsph, and the traffic manager profile section contains contentmanagerTMecsph and nodeserverappTMecsph. All resources are located in Central US or West US.

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

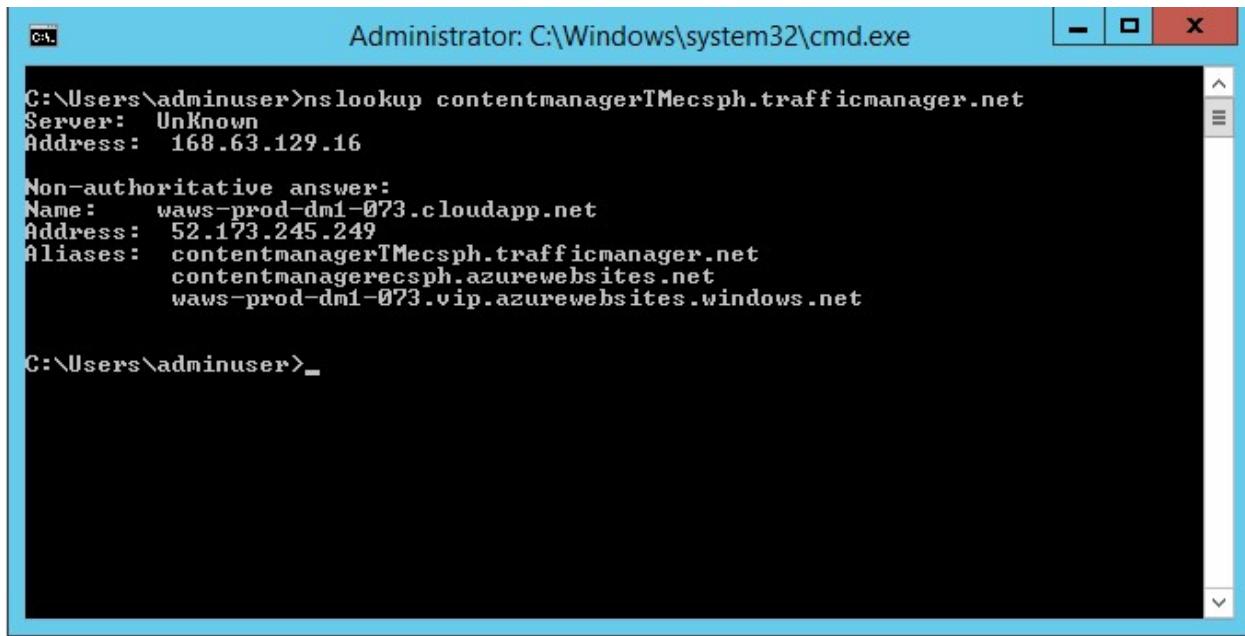
SQL Server URL : recoverdigitalsqlserverecsph.database.windows.net

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`



```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\adminuser>nslookup contentmanagerTMeCSph.trafficmanager.net
Server: Unknown
Address: 168.63.129.16

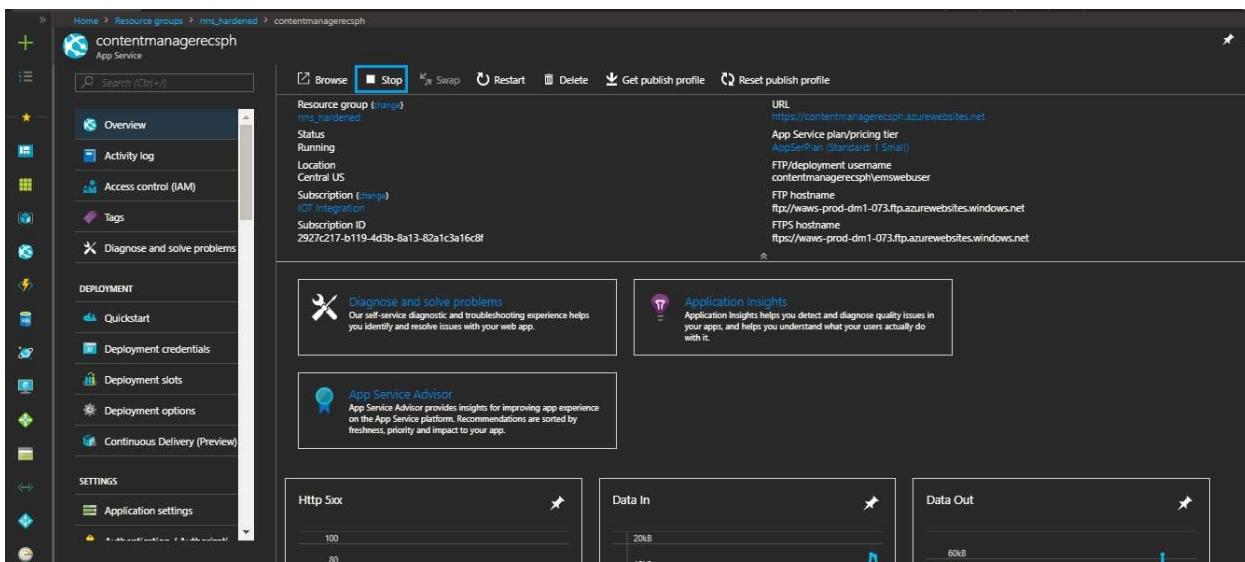
Non-authoritative answer:
Name: waws-prod-dm1-073.cloudapp.net
Address: 52.173.245.249
Aliases: contentmanagerTMeCSph.trafficmanager.net
contentmanagerecsph.azurewebsites.net
waws-prod-dm1-073.vip.azurewebsites.windows.net

C:\Users\adminuser>_

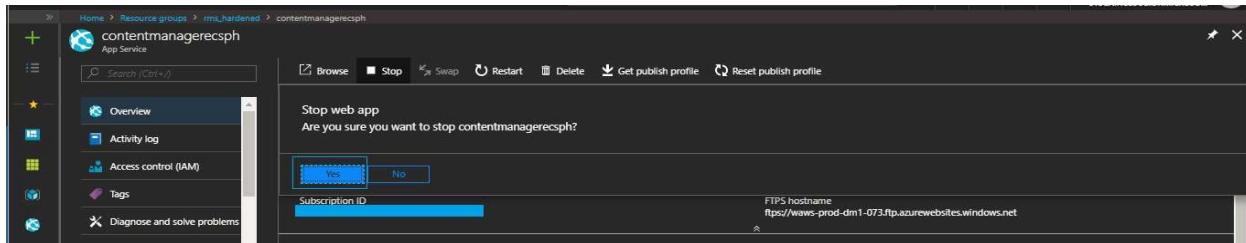
```

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**



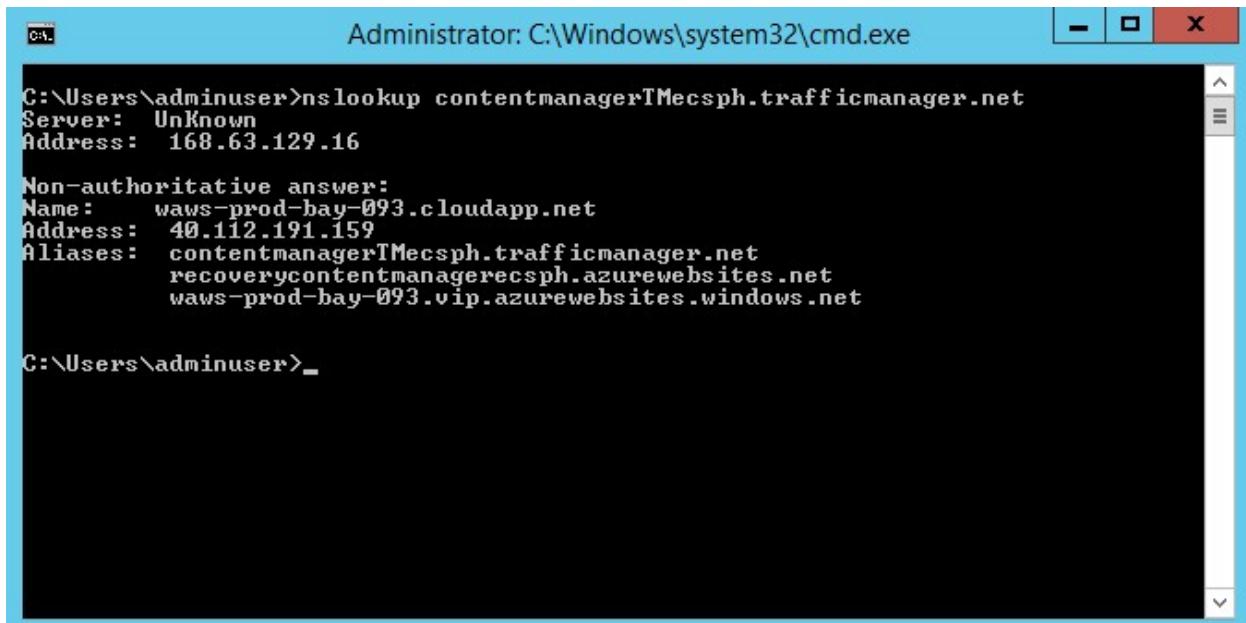
4. Click **Yes** to stop.



5. Open command prompt & run the following command

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

```
nslookup contentmanagerTMecsph.trafficmanager.net
```



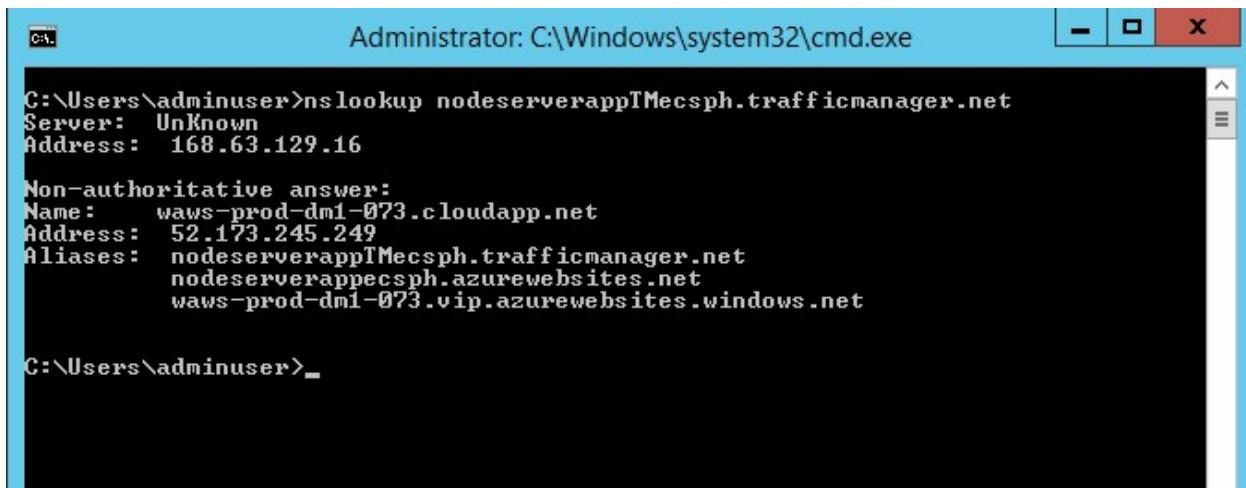
When Primary Content Manager Web Application is stopped. The Traffic Manger redirects data to Secondary Content Manager Web Application
(recoverycontentmanagerecsph.azurewebsites.net).

6. Open command prompt & run the following command

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

```
nslookup nodeserverappTMecsph.trafficmanager.net
```

RMS Hardening



```
Administrator: C:\Windows\system32\cmd.exe

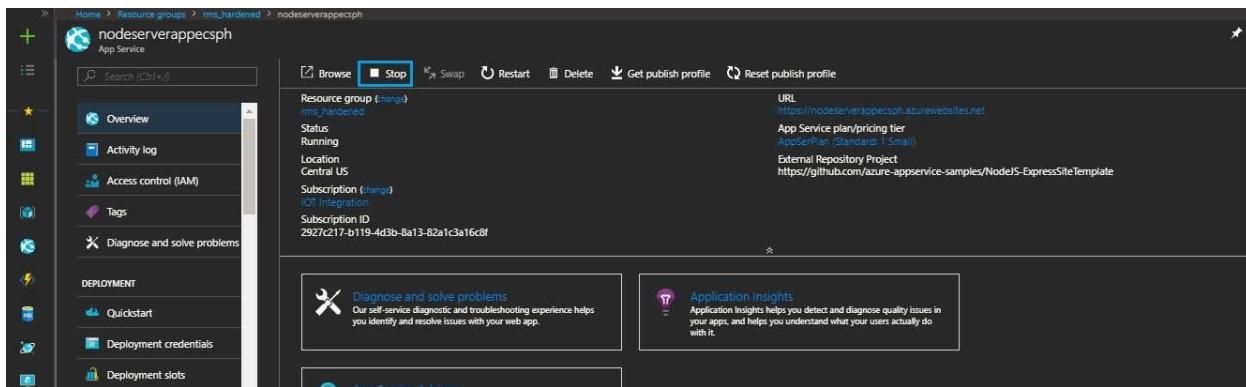
C:\Users\adminuser>nslookup nodeserverappTMeCSph.trafficmanager.net
Server: Unknown
Address: 168.63.129.16

Non-authoritative answer:
Name: waws-prod-dm1-073.cloudapp.net
Address: 52.173.245.249
Aliases: nodeserverappTMeCSph.trafficmanager.net
nodeserverappecsph.azurewebsites.net
waws-prod-dm1-073.vip.azurewebsites.windows.net

C:\Users\adminuser>
```

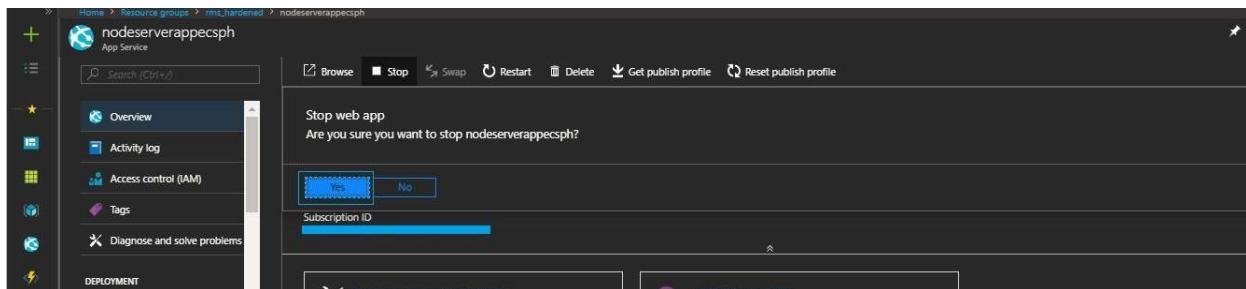
When both Node Server Applications Are up and Running. The Traffic redirected Primary Node server web app(nodeserverappecsph.azurewebsites.net) as Priority is 1.

7. Stop the Primary node server web app
8. Go to **Resource group > nodeserverappecsph > overview > click Stop**



The screenshot shows the Azure portal's 'Overview' page for the 'nodeserverappecsph' app service. The 'Stop' button is highlighted in blue, indicating it is selected. Other buttons visible include 'Swap', 'Restart', 'Delete', 'Get publish profile', and 'Reset publish profile'. The page displays basic information such as the resource group ('rms_hardened'), status ('Running'), location ('Central US'), subscription ('Standard'), and a link to the GitHub repository for the Node.js Express Site Template.

9. Click **Yes** to stop.

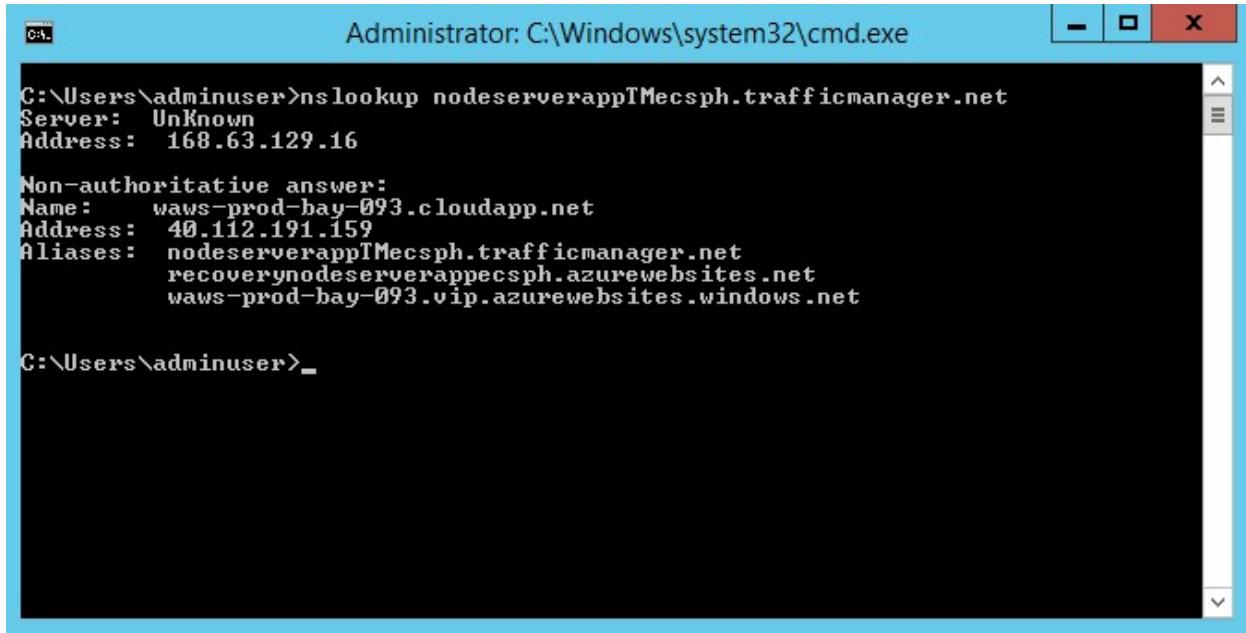


The screenshot shows a confirmation dialog box in the Azure portal asking 'Are you sure you want to stop nodeserverappecsph?'. Below the question are two buttons: 'Yes' (highlighted in blue) and 'No'. The background shows the 'Overview' page of the 'nodeserverappecsph' app service, with the 'Stop' button also visible.

10. Open command prompt & run the following command

nslookup <trafficmanagernodeserveruri> which is copied from output section.

nslookup nodeserverappTMecsph.trafficmanager.net



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\adminuser>nslookup nodeserverappTMecsph.trafficmanager.net
Server: UnKnown
Address: 168.63.129.16

Non-authoritative answer:
Name: waws-prod-bay-093.cloudapp.net
Address: 40.112.191.159
Aliases: nodeserverappTMecsph.trafficmanager.net
recoverynodeserverappcsph.azurewebsites.net
waws-prod-bay-093.vip.azurewebsites.windows.net

C:\Users\adminuser>_
```

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

13.3.2. Sign in to DigitalSignage UI

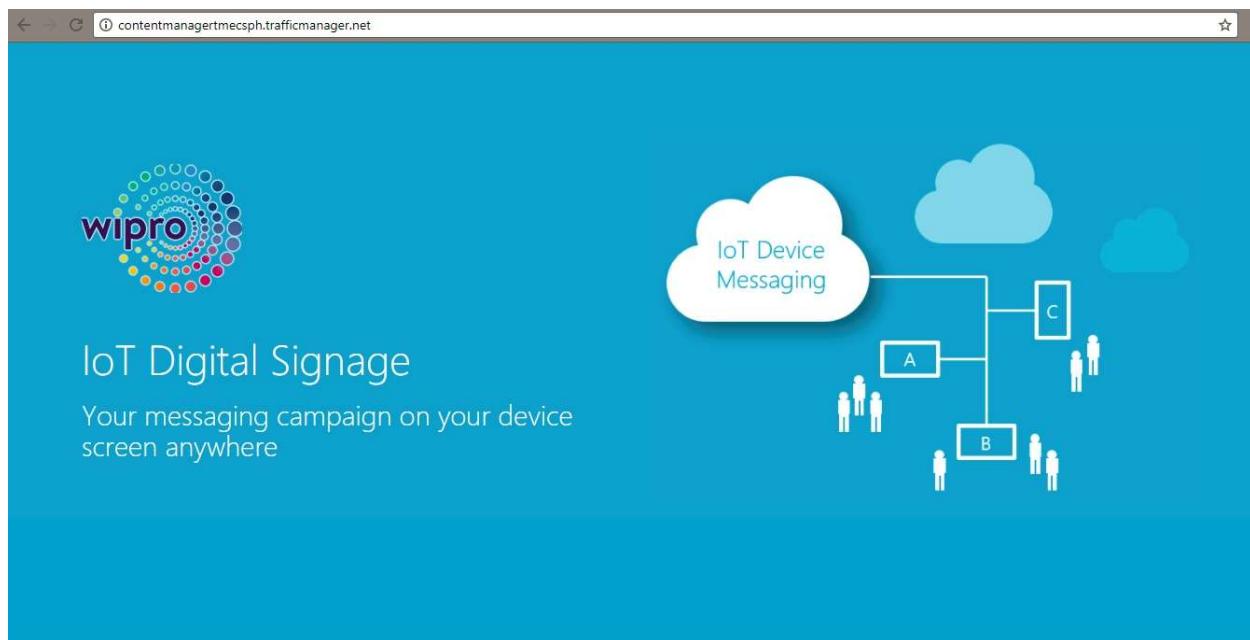
1. Copy and paste the traffic manager web app url from the output section in a browser.
2. Go to **resourcegroup > deployments > Microsoft Template > outputs**
3. Copy the **TRAFFICMANAGERWEBAPPURL** and paste it in a browser.

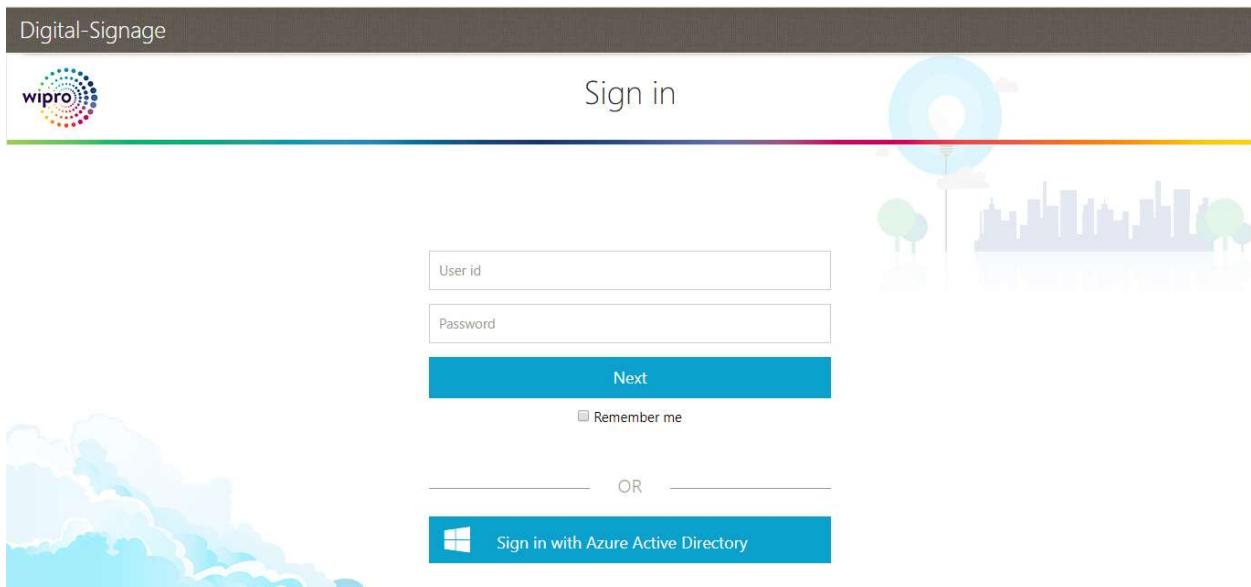
Microsoft Template - Outputs

Deployment

AZURESQLPASSWORD	Enter the sqlAdministratorLoginPassword which you have entered in parameter section
DESTINATIONSTORAGEACCOUNTNAME	imagecontentmhhy74
WEBAPPURL	https://contentmanagermhhy74.azurewebsites.net/
NODESERVERURL	https://nodeserverapphhy74.azurewebsites.net/
TRAFFICMANAGERWEBAPPURL	https://contentmanagertmhhy74.trafficmanager.net
TRAFFICMANAGERNODESERVERURL	https://nodeserverapptmhhy74.trafficmanager.net
WEBJOBURL	https://signageServermhhy74.scm.azurewebsites.net//azurejobs/
IOTHUBENDPOINT	digital-signagehubmhhy74.azure-devices.net
OMSLOGANALYTICSURL	https://omswhhy74.portal.mms.microsoft.com/
APPINSIGHTSURL	https://analytics.applicationinsights.io/subscriptions/2927c217-b119-4d3b-8a13-82a1c...
IOTDPSGLOBALENDPOINT	global.azure-devices-provisioning.net
IOTDPSSERVERENDPOINT	iotDeviceProvisionmhhy74.azure-devices-provisioning.net

4. The following page is displayed.

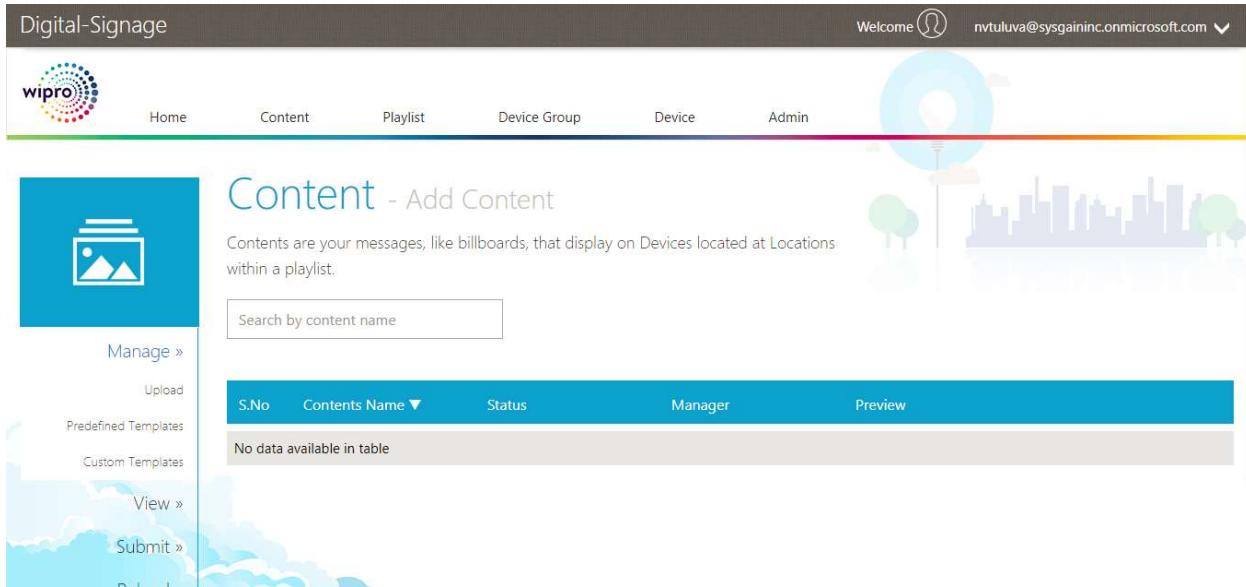




5. Provide User id as **Admin** & password as **Admin** or sign in using azure AD with your Microsoft account.
6. The following **Dashboard** appears after successful sign in.



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.



Digital-Signage

Welcome nvtuluva@sysgaininc.onmicrosoft.com Admin

wipro Home Content Playlist Device Group Device Admin

Content - Add Content

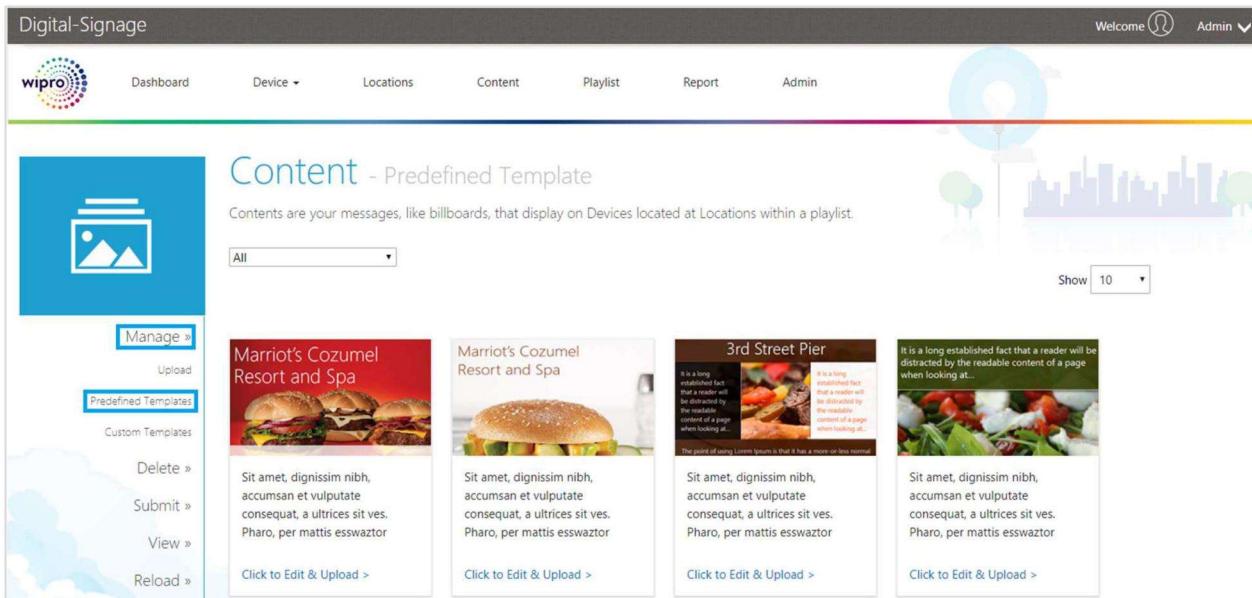
Contents are your messages, like billboards, that display on Devices located at Locations within a playlist.

Search by content name

S.No	Contents Name ▼	Status	Manager	Preview
No data available in table				

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.



Digital-Signage

Welcome nvtuluva@sysgaininc.onmicrosoft.com Admin

wipro Dashboard Device Locations Content Playlist Report Admin

Content - Predefined Template

Contents are your messages, like billboards, that display on Devices located at Locations within a playlist.

All Show 10

 Marriot's Cozumel Resort and Spa Sit amet, dignissim nibh, accumsan et vulputate consequat, a ultrices sit ves. Pharo, per mattis esswaztor Click to Edit & Upload >	 3rd Street Pier It is a long established fact that a reader will be distracted by the readable content of a page when looking at... Click to Edit & Upload >	 Marriot's Cozumel Resort and Spa Sit amet, dignissim nibh, accumsan et vulputate consequat, a ultrices sit ves. Pharo, per mattis esswaztor Click to Edit & Upload >
---	--	---

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.

Content - Predefined Template

Contents are your messages, like billboards, that display on Devices located at Locations within a playlist.

Select Category ▾

Potato Finger Chips



Sparkling Krushers 90
Lorem ipsum dolor sit amet, dignissim nibh, accumsan et vull
Mini Leaf 90

Place holders

- Potato
- Finger Chips
- Sparkling Krushers 90
- Mini Leaf
- ...

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

Content - Predefined Template

Contents are your messages, like billboards, that display on Devices located at Locations within a playlist.

Select Category ▾

Potato Finger Chips

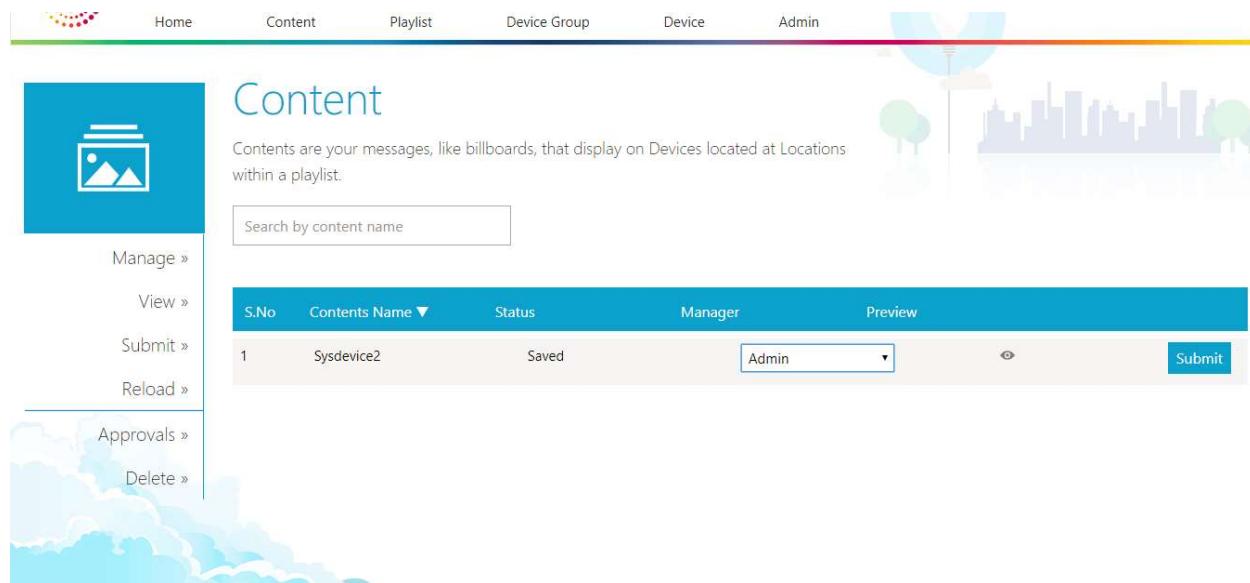


Sparkling Krushers 90
Lorem ipsum dolor sit amet, dignissim nibh, accumsan et vull
Mini Leaf 90

Place holders

- Potato
- Finger Chips
- Sparkling Krushers 90
- Mini Leaf
- ...

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.



Content

Contents are your messages, like billboards, that display on Devices located at Locations within a playlist.

Search by content name

S.No	Contents Name ▼	Status	Manager	Preview
1	Sysdevice2	Saved	Admin	

Manage »

View »

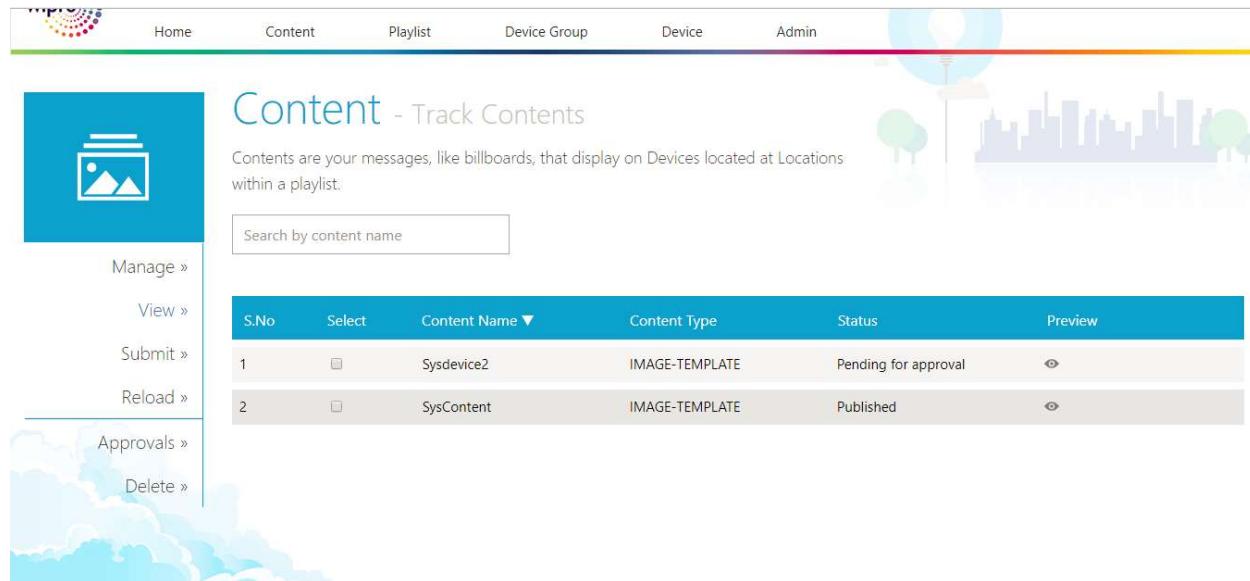
Submit »

Reload »

Approvals »

Delete »

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.



Content - Track Contents

Contents are your messages, like billboards, that display on Devices located at Locations within a playlist.

Search by content name

S.No	Select	Content Name ▼	Content Type	Status	Preview
1	<input type="checkbox"/>	Sysdevice2	IMAGE-TEMPLATE	Pending for approval	
2	<input type="checkbox"/>	SysContent	IMAGE-TEMPLATE	Published	

Manage »

View »

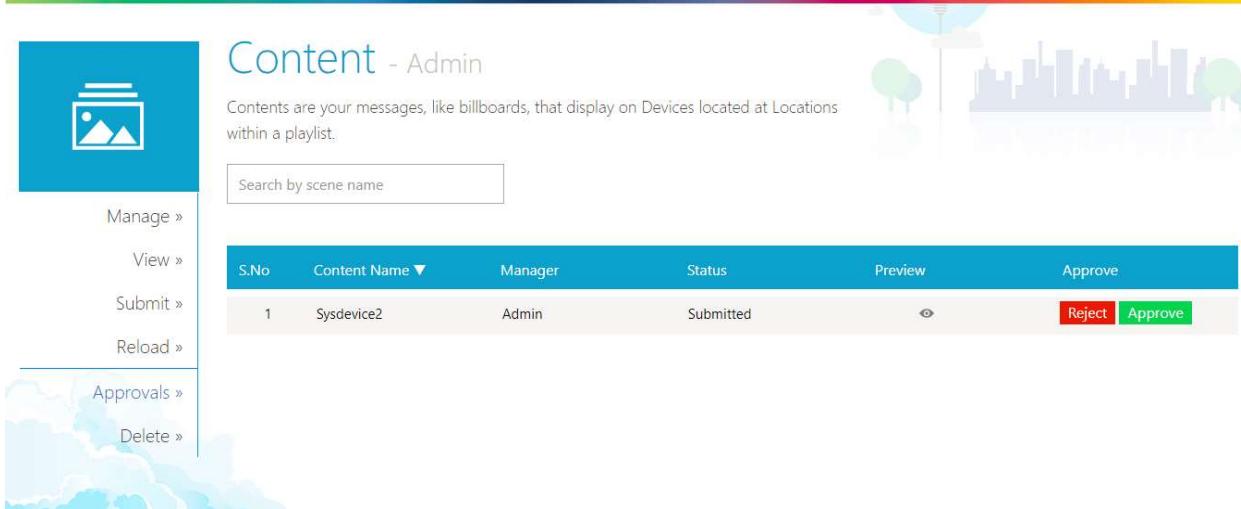
Submit »

Reload »

Approvals »

Delete »

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



Content - Admin

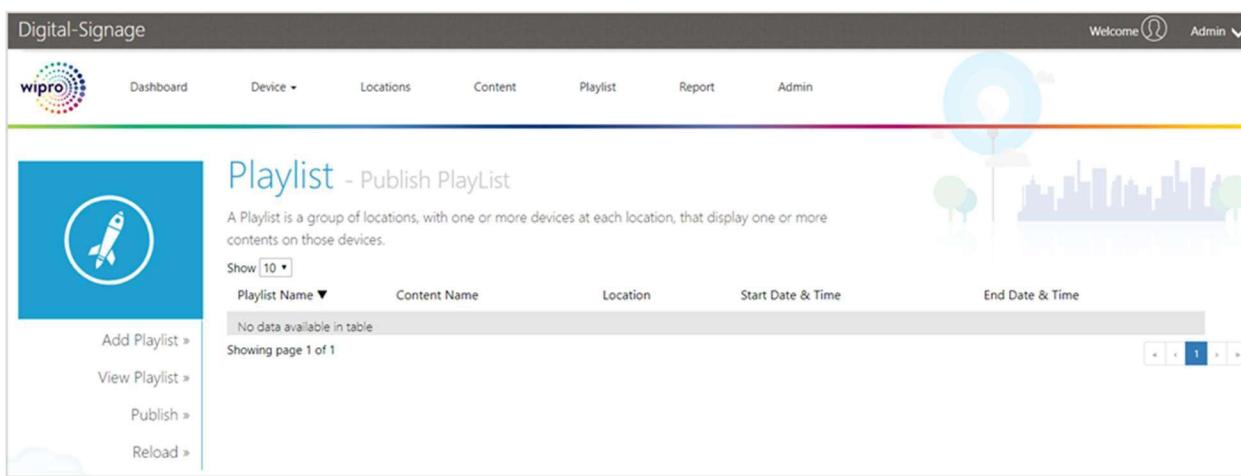
Contents are your messages, like billboards, that display on Devices located at Locations within a playlist.

Search by scene name

S.No	Content Name ▾	Manager	Status	Preview	Approve
1	Sysdevice2	Admin	Submitted		Reject Approve

Manage »
View »
Submit »
Reload »
Approvals »
Delete »

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



Digital-Signage

Welcome Admin

wipro

Dashboard Device ▾ Locations Content Playlist Report Admin

Playlist - Publish 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.

Show 10 ▾

Playlist Name ▾	Content Name	Location	Start Date & Time	End Date & Time
No data available in table				

Showing page 1 of 1

Add Playlist » View Playlist » Publish » Reload »

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



[Add Playlist »](#)
[View Playlist »](#)
[Publish »](#)
[Reload »](#)



Playlist - Add 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.

Parent Group Sub Group Devices

Parent group associated with sub group/devices are shown

Parent Group Name

Playlist Name

Start Date / End Date

Start Time / End Time

Select Contents to Preview and Publish

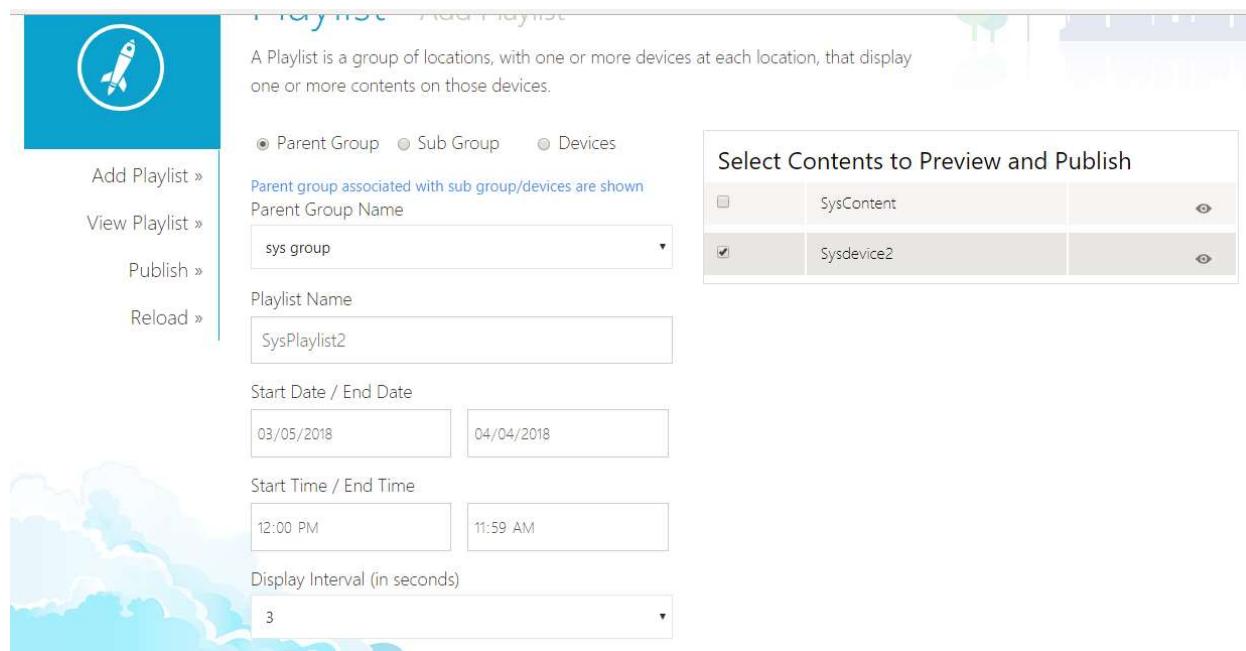
<input type="checkbox"/>	SysContent	
<input checked="" type="checkbox"/>	Sysdevice2	

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.

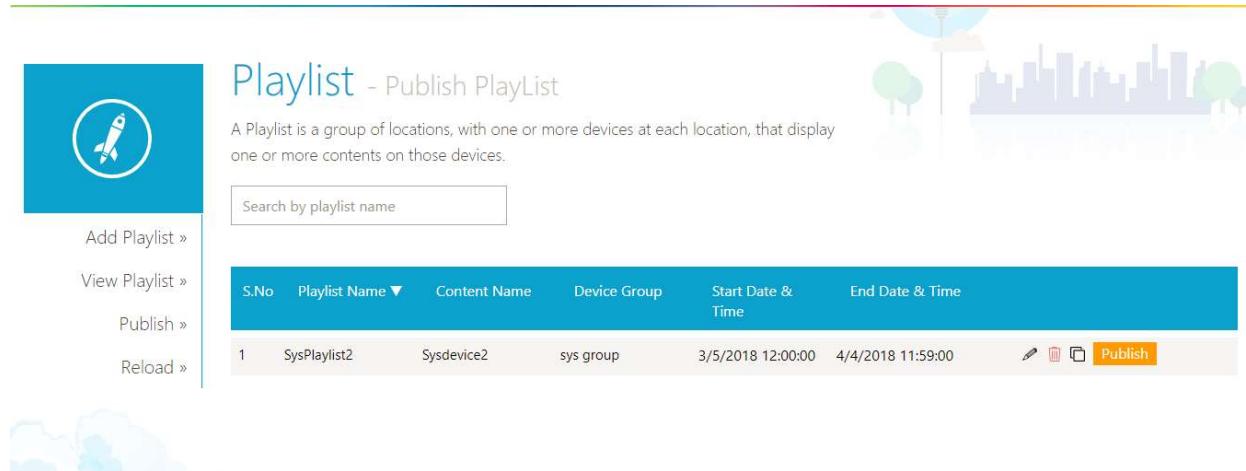
Select Contents to Preview and Publish

<input type="checkbox"/>	SysContent	
<input checked="" type="checkbox"/>	Sysdevice2	

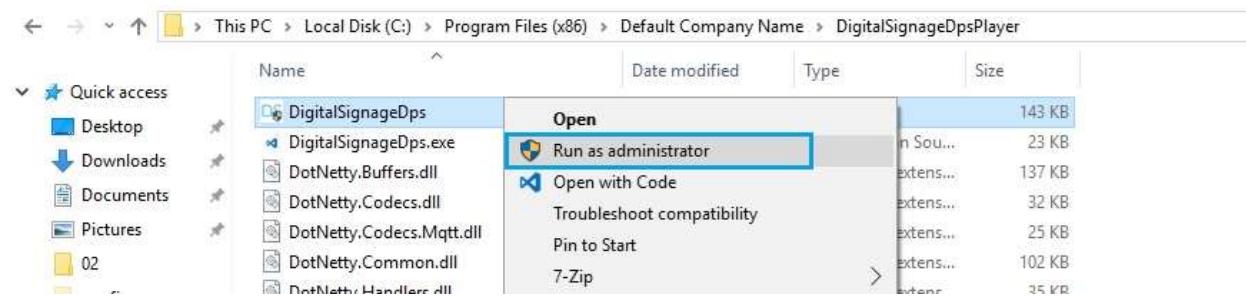
12. Enter the **Playlist Name** in the respective field.
13. Enter the **Start/End Date** and **Start/End Time** in their respective fields.
14. Set the **Display Interval** (In seconds) from the dropdown list.
15. Click **Save** button to save the Playlist is added.



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.

NewYork Classic Burger



Week 5

7th July - 2nd Sep 2017

Iceberg 190

Lorem ipsum dolor sit amet,
dignissim nibh, accumsan et ipsum
sit amet, aliquyng sim vull,



100% Iceberg Lettuce.

190

Potato Finger Chips



Sparkling Krushers 90

Lorem ipsum dolor sit amet,
dignissim nibh, accumsan et vull

Mini Leaf

Thursday, Mar 15, 2018

06 : 05

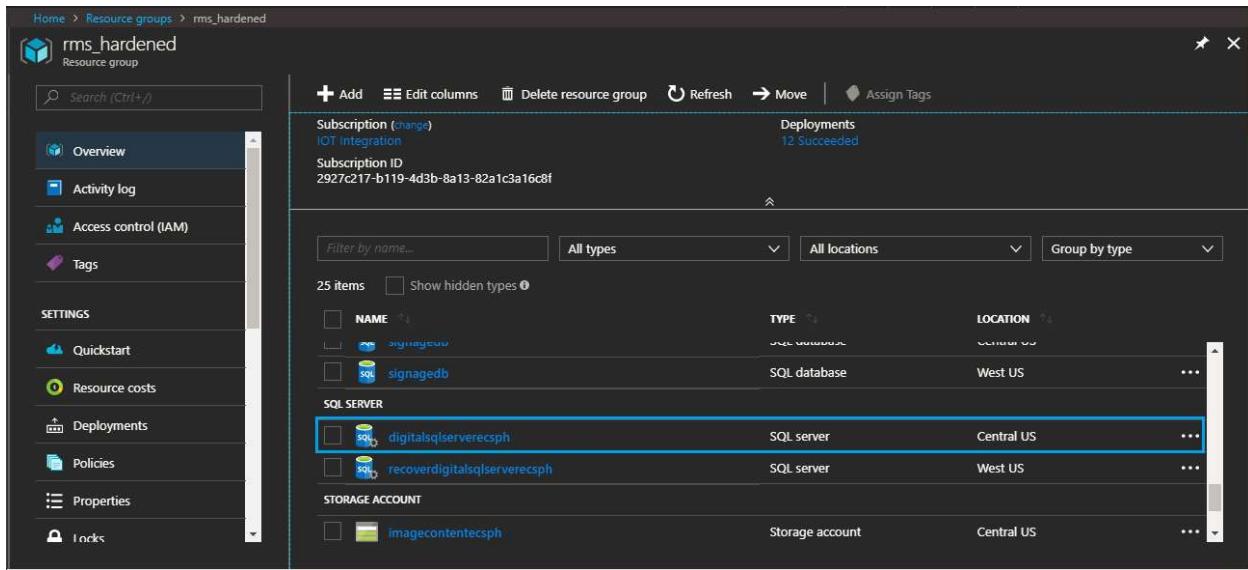


25° F

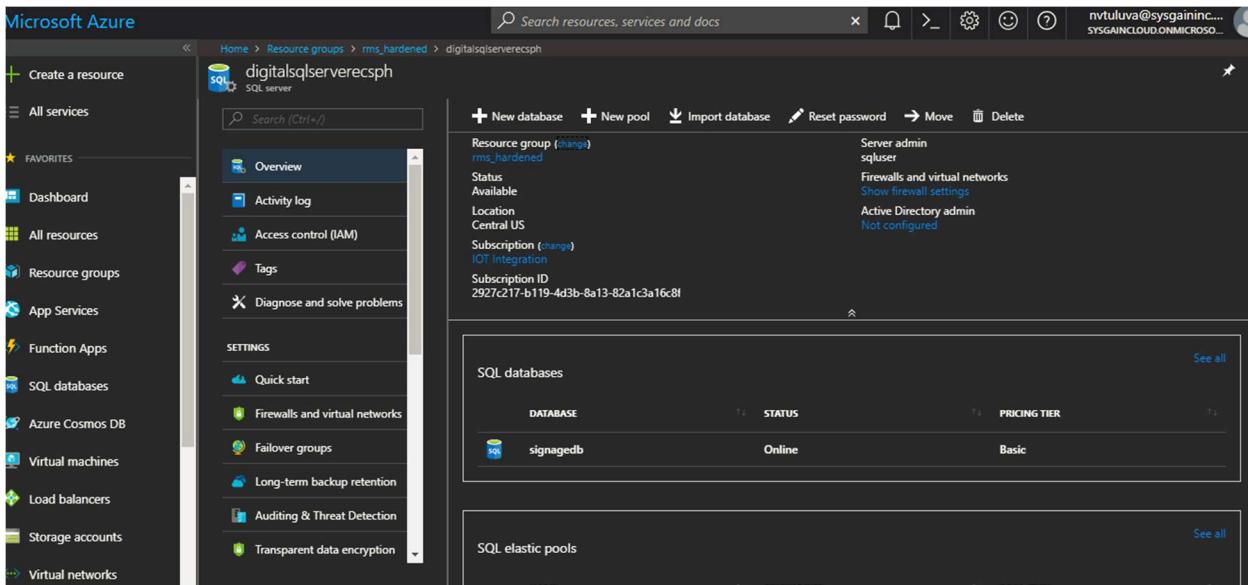


13.3.3. Geo Replication

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

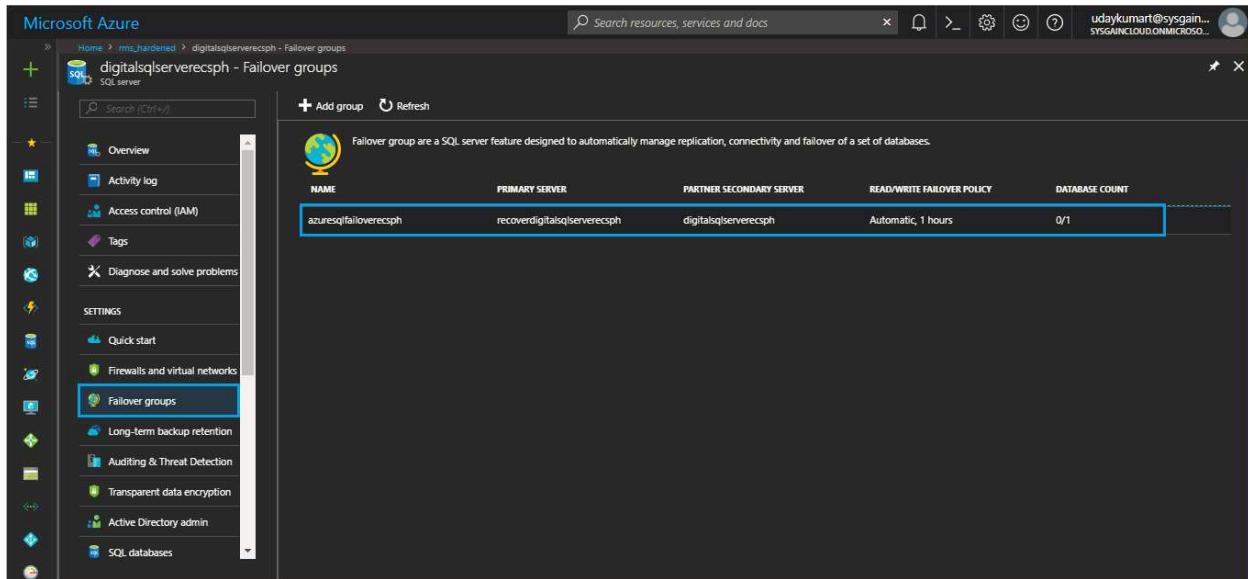


The screenshot shows the Azure portal interface for the 'rms_hardened' resource group. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Quickstart, Resource costs, Deployments, Policies, Properties, and Locks. The main content area displays a list of resources under 'Subscription' (IOT Integration) and 'Deployments' (12 Succeeded). The 'SQL SERVER' section lists three resources: 'signededb' (SQL database, Central US), 'digitalsqlserverecsph' (SQL server, Central US, highlighted with a blue border), and 'recoverdigitalsqlserverecsph' (SQL server, West US). The 'STORAGE ACCOUNT' section lists one resource: 'imagecontentecsph' (Storage account, Central US).



The screenshot shows the Azure portal interface for the 'digitalsqlserverecsph' SQL server within the 'rms_hardened' resource group. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Quick start, Firewalls and virtual networks, Failover groups, Long-term backup retention, Auditing & Threat Detection, and Transparent data encryption. The main content area displays resource group details (Status: Available, Location: Central US, Subscription: IOT Integration, Sub ID: 2927c217-b119-4d3b-8a13-82a1c3a16c8f) and two sections: 'SQL databases' (signededb, Online, Basic) and 'SQL elastic pools'.

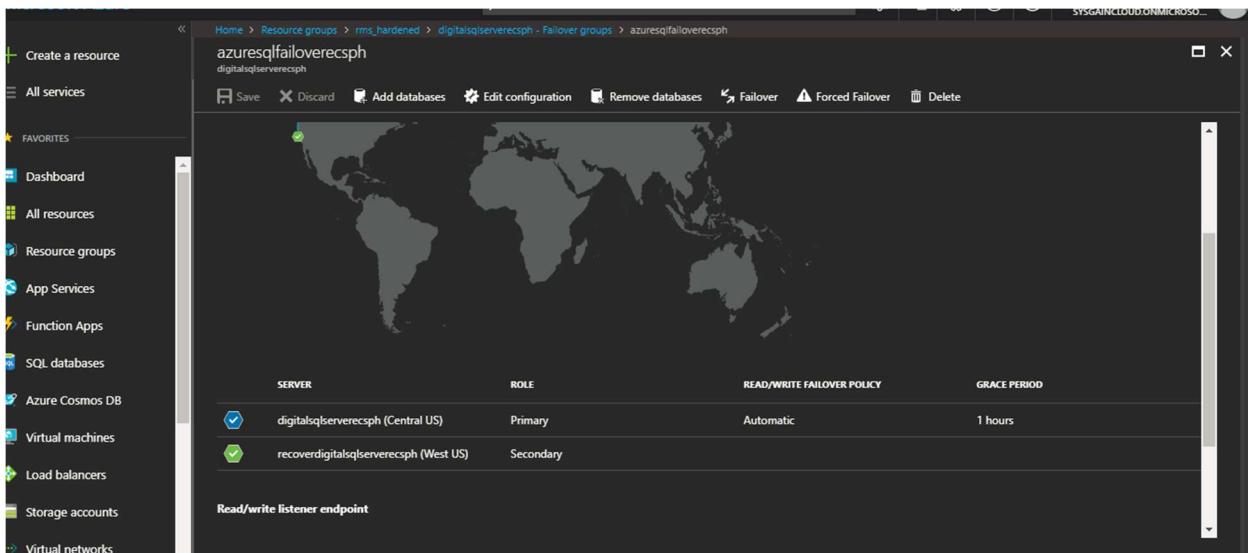
2. In the left side blade, click **Failover groups** > click **azurefailoverecsph**



The screenshot shows the Microsoft Azure portal interface for managing SQL Server failover groups. The left sidebar lists various service categories, and the main content area displays the 'Failover groups' section for the resource group 'rms_hardened'. A single failover group is listed:

NAME	PRIMARY SERVER	PARTNER SECONDARY SERVER	READ/WRITE FAILOVER POLICY	DATABASE COUNT
azuresqlfailoverrecsph	recoverdigitalsqlserverecph	digitalsqlserverecph	Automatic, 1 hours	0/1

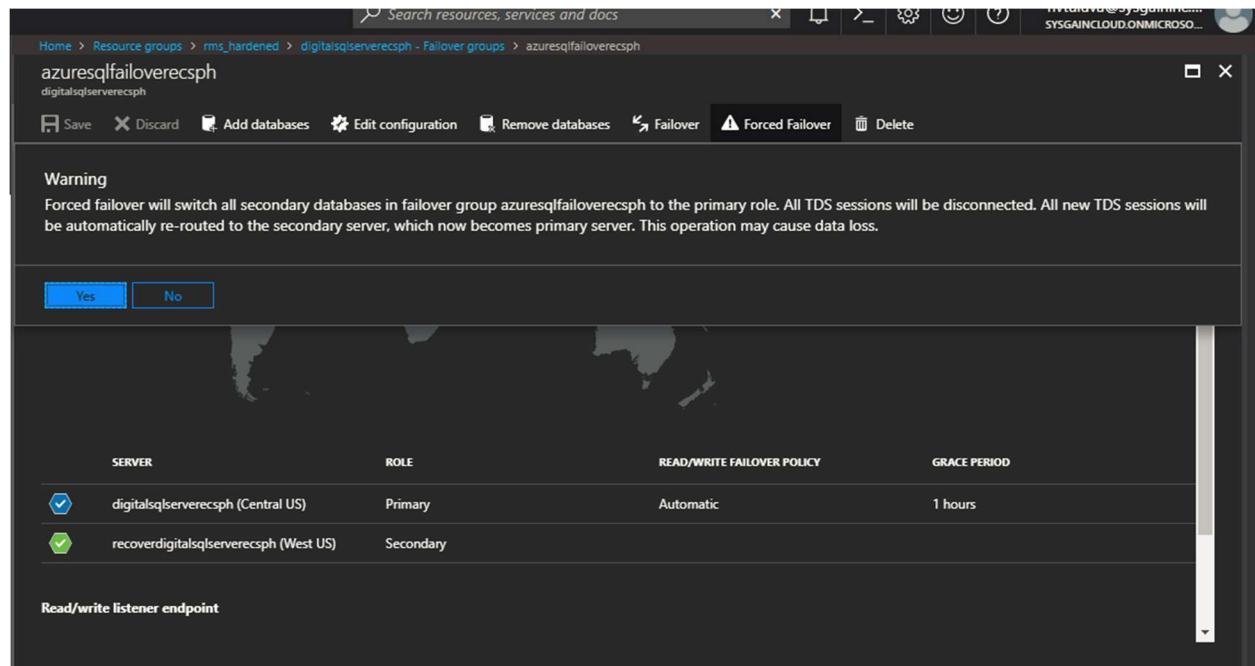
- As shown in the following figure **digitalsqlserverecph(Central US)** is primary SQL server and **recover digitalsqlserverecph (West US)** is secondary SQL server.



The screenshot shows the detailed configuration of the failover group 'azuresqlfailoverrecsph'. It displays a world map indicating the geographical locations of the primary and secondary servers. Below the map, the server roles are listed:

SERVER	ROLE	READ/WRITE FAILOVER POLICY	GRACE PERIOD
<input checked="" type="checkbox"/> digitalsqlserverecph (Central US)	Primary	Automatic	1 hours
<input checked="" type="checkbox"/> recoverdigitalsqlserverecph (West US)	Secondary		

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

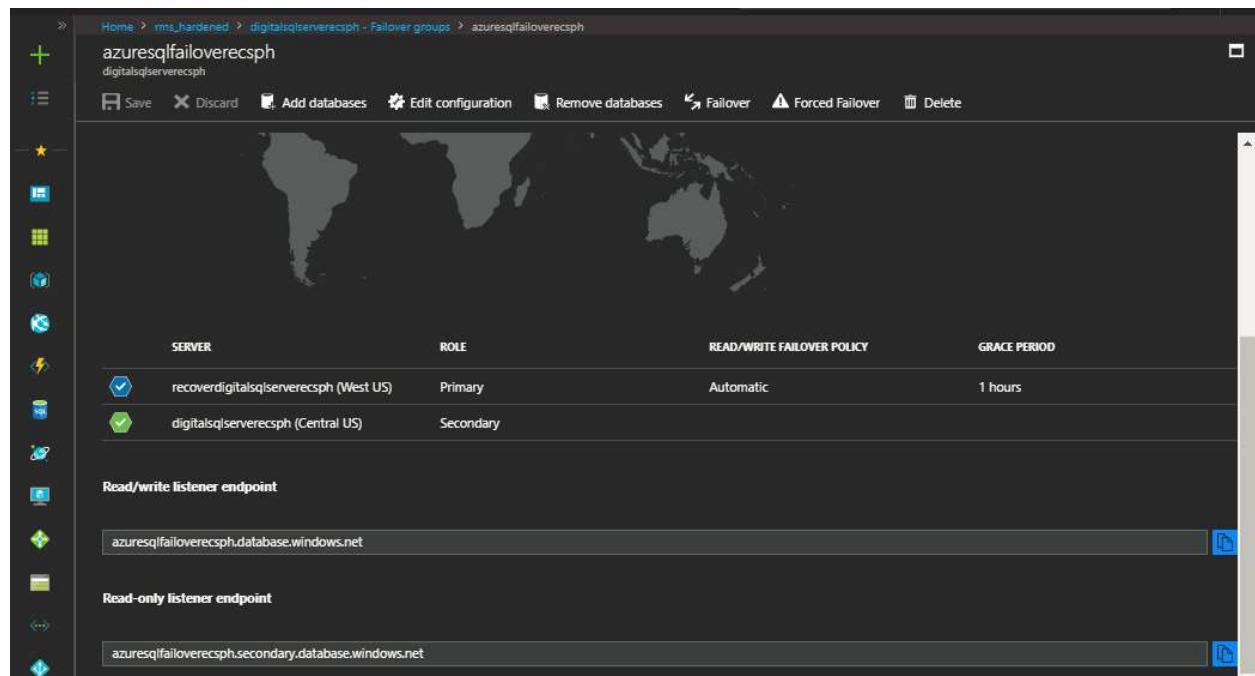


The screenshot shows the Azure portal interface for managing a failover group named 'azuresqlfailoverrecph'. A warning message at the top states: 'Forced failover will switch all secondary databases in failover group azuresqlfailoverrecph to the primary role. All TDS sessions will be disconnected. All new TDS sessions will be automatically re-routed to the secondary server, which now becomes primary server. This operation may cause data loss.' Below the warning are two buttons: 'Yes' (highlighted in blue) and 'No'. The main table displays the servers and their roles:

SERVER	ROLE	READ/WRITE FAILOVER POLICY	GRACE PERIOD
digitalsqlserverecph (Central US)	Primary	Automatic	1 hours
recoverdigitalsqlserverecph (West US)	Secondary		

Below the table, there are sections for 'Read/write listener endpoint' (containing 'azuresqlfailoverrecph.database.windows.net') and 'Read-only listener endpoint' (containing 'azuresqlfailoverrecph.secondary.database.windows.net').

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



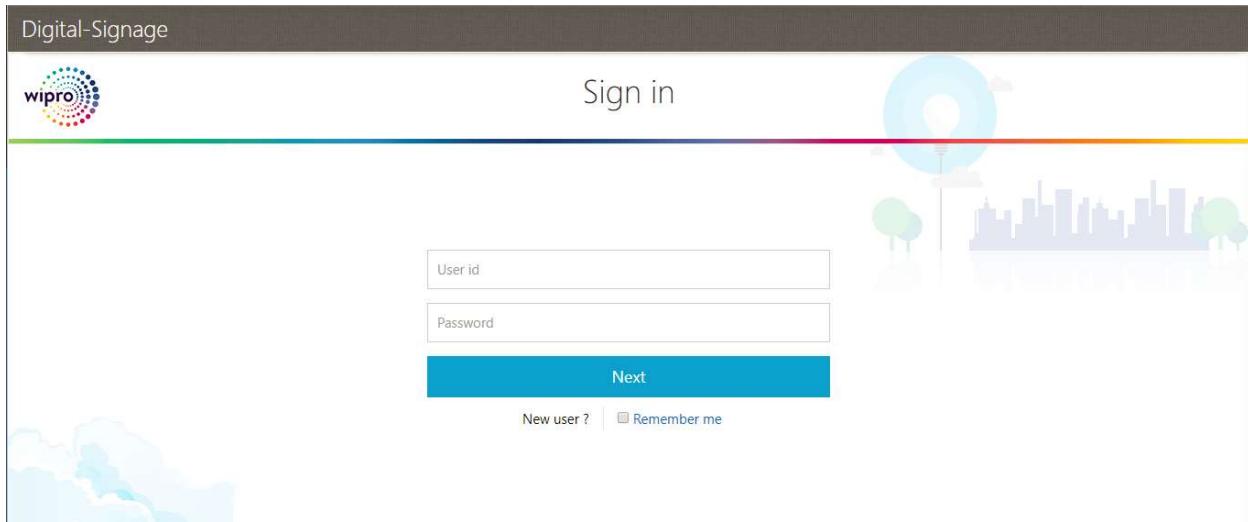
The screenshot shows the Azure portal interface for managing a failover group named 'azuresqlfailoverrecph'. The table now shows the servers and their roles after the failover:

SERVER	ROLE	READ/WRITE FAILOVER POLICY	GRACE PERIOD
recoverdigitalsqlserverecph (West US)	Primary	Automatic	1 hours
digitalsqlserverecph (Central US)	Secondary		

Below the table, there are sections for 'Read/write listener endpoint' (containing 'azuresqlfailoverrecph.database.windows.net') and 'Read-only listener endpoint' (containing 'azuresqlfailoverrecph.secondary.database.windows.net').

- Sign in to **DigitalSignage UI**

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



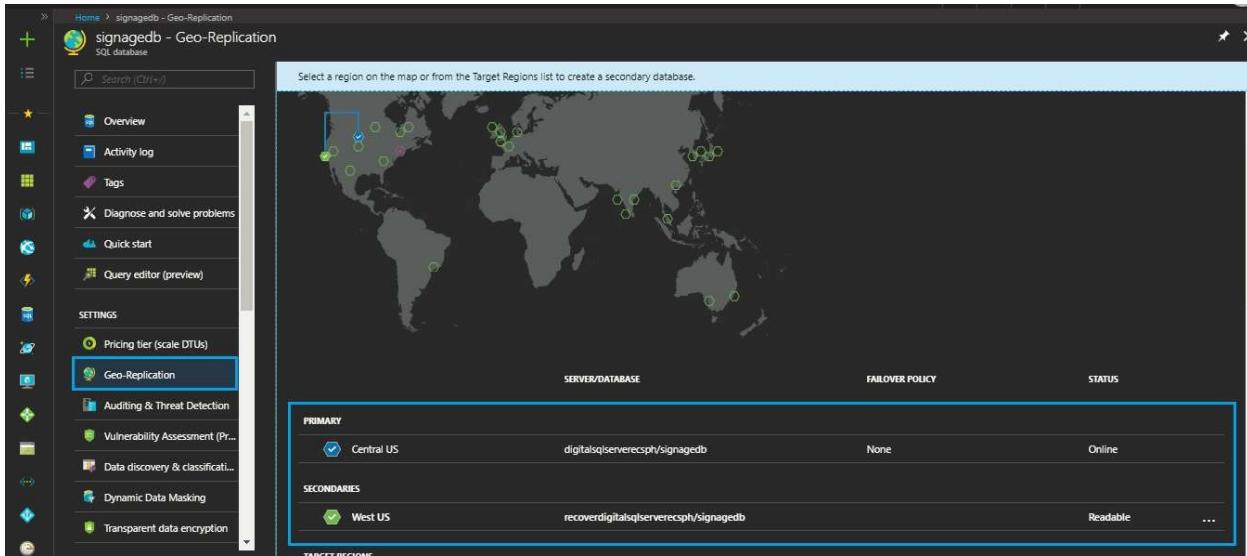
8. Once Login is successful, we can confirm that the recover digitsqlserverecsph (West US) is working as expected.

13.3.4. Database Restore

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

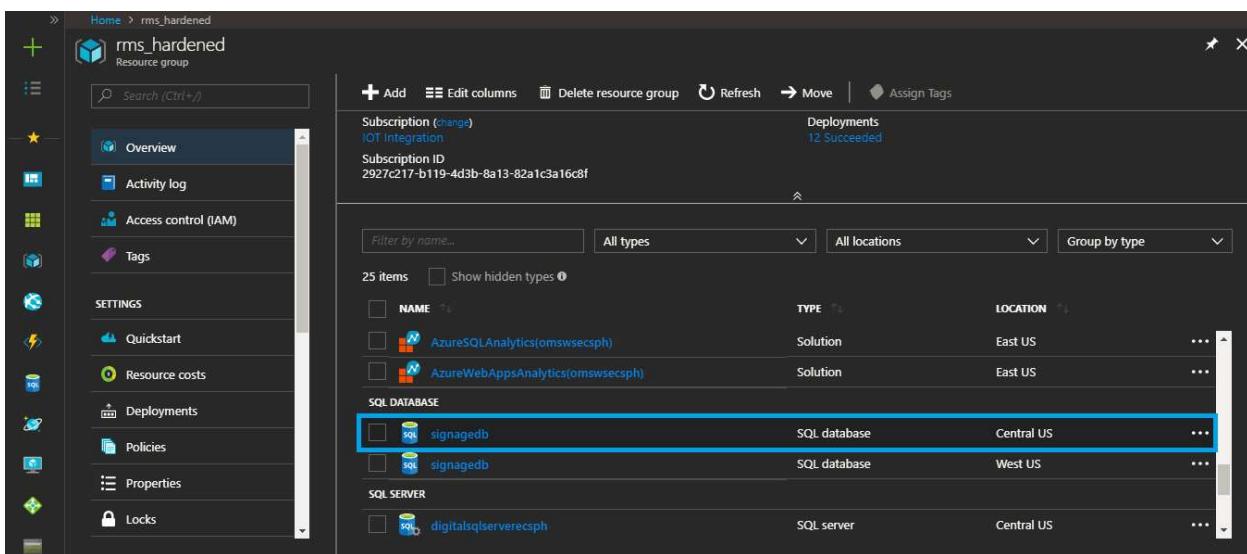
NAME	TYPE	LOCATION
AzureSQLAnalytics(omswsecph)	Solution	East US
AzureWebAppsAnalytics(omswsecph)	Solution	East US
signagedb	SQL database	Central US
signagedb	SQL database	West US

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

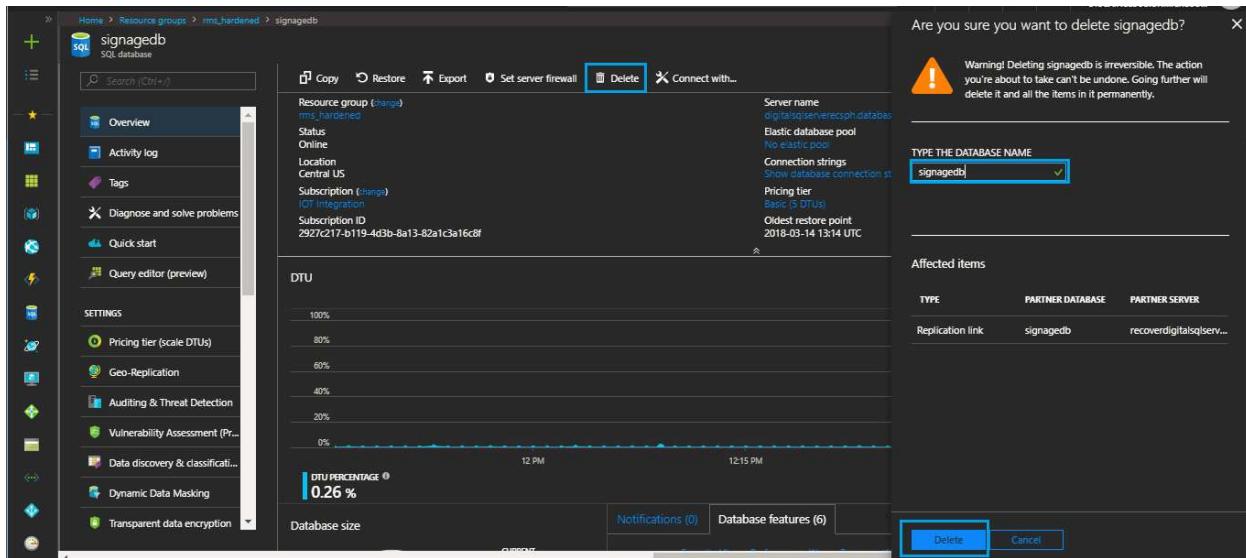


	SERVER/DATABASE	FAILOVER POLICY	STATUS
PRIMARY	Central US digitalsqlserverecsph/signagedb	None	Online
SECONDARIES	West US recoverdynamicsqlserverecsph/signagedb	Readable	...

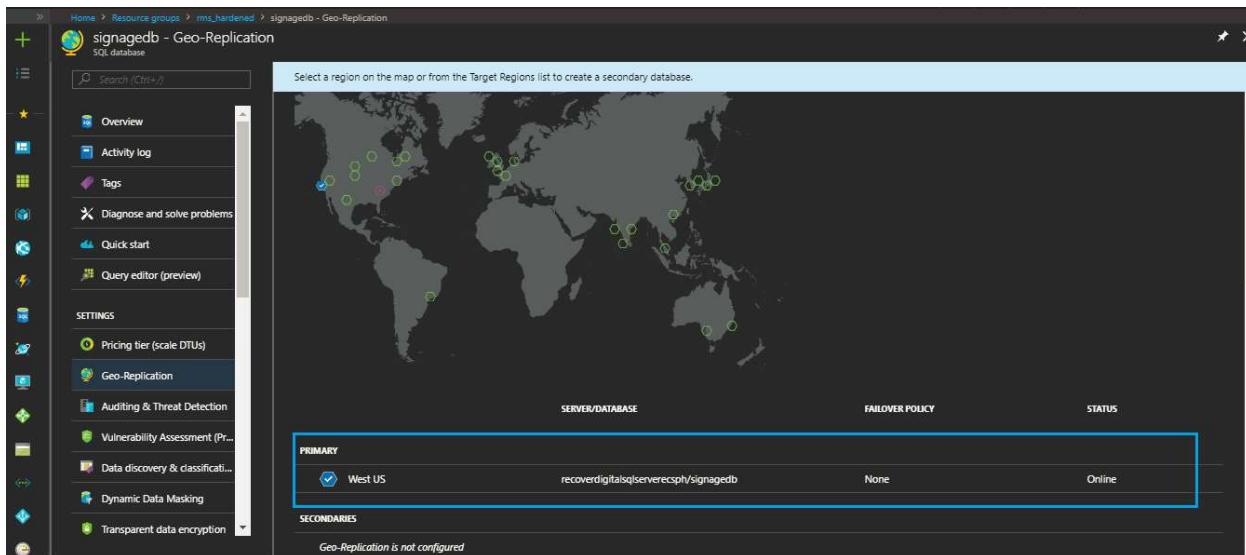
3. In the above figure **digitalsqlserverecsph/signagedb** is primary database and **recoverdynamicsqlserverecsph/signagedb** is secondary database.
4. Delete the primary database.
5. Go to **Resource group > rms_hardened**



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 **recoverdigi.../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.

RMS Hardening



Home > Resource groups > rms_hardened > signagedb - Geo-Replication

signagedb - Geo-Replication

SQL database

Search (Ctrl+F)

Overview

Activity log

Tags

Diagnose and solve problems

Quick start

Query editor (preview)

Pricing tier (scale DTUs)

Geo-Replication

Auditing & Threat Detection

Vulnerability Assessment (Pr...)

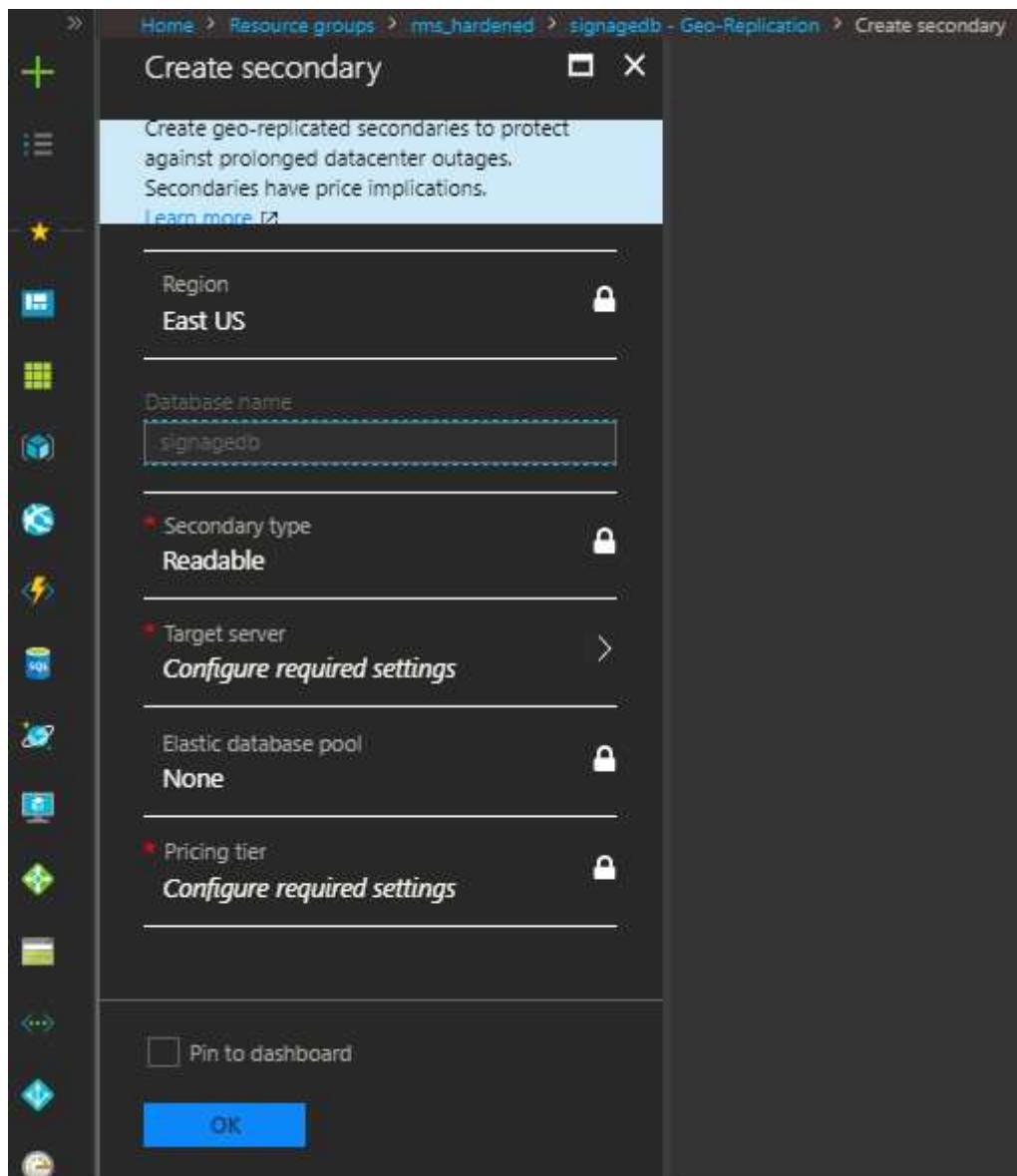
Data discovery & classificati...

Dynamic Data Masking

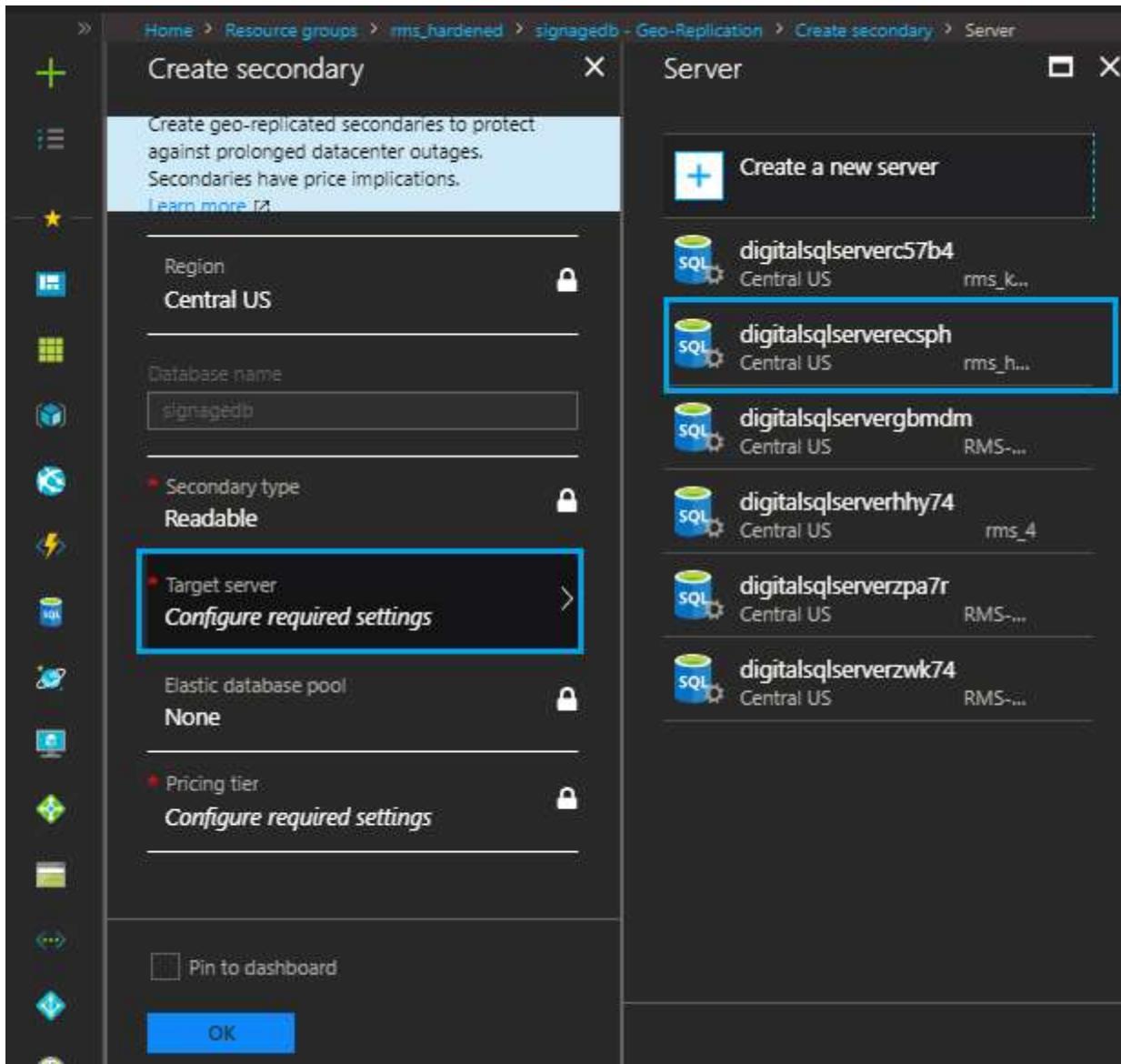
Transparent data encryption

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 recoverdigitalsqlservercph/signagedb	None	Online
SECONDARIES	Geo-Replication is not configured		
TARGET REGIONS	 East US  West US  West US 2  Central US  West Central US  South Central US  North Central US  Canada Central  South America	Recommended	



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

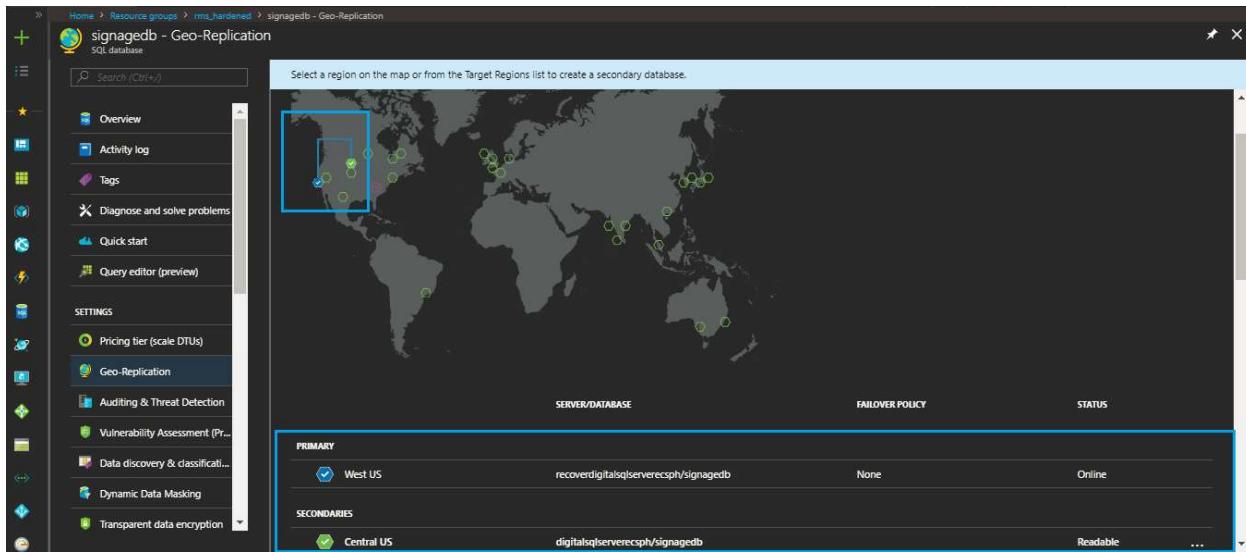


The screenshot shows the Azure portal interface for creating a secondary database. On the left, a sidebar lists various service icons. The main area has a breadcrumb navigation path: Home > Resource groups > rms_hardened > signagedb - Geo-Replication > Create secondary > Server. The title bar says "Create secondary". A callout box provides information about creating geo-replicated secondaries to protect against prolonged datacenter outages, noting that secondaries have price implications. Below this, the "Region" is set to "Central US". The "Database name" field contains "signagedb". The "Secondary type" is set to "Readable". The "Target server" section is highlighted with a blue border and contains the text "Configure required settings". Other configuration options include "Elastic database pool" (set to "None") and "Pricing tier" (with a "Configure required settings" link). At the bottom, there is a checkbox for "Pin to dashboard" and a blue "OK" button. To the right, a "Server" list displays several existing servers, each with a "Create a new server" button. One server, "digitalsqlserverecph", is highlighted with a blue border. The list includes:

- Create a new server
- digitalsqlserverc57b4 Central US rms_k...
- digitalsqlserverecph** Central US rms_h...
- digitalsqlservergbmdm Central US RMS-...
- digitalsqlserverhy74 Central US rms_4
- digitalsqlserverzpa7r Central US RMS-...
- digitalsqlserverzwk74 Central US RMS-...

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

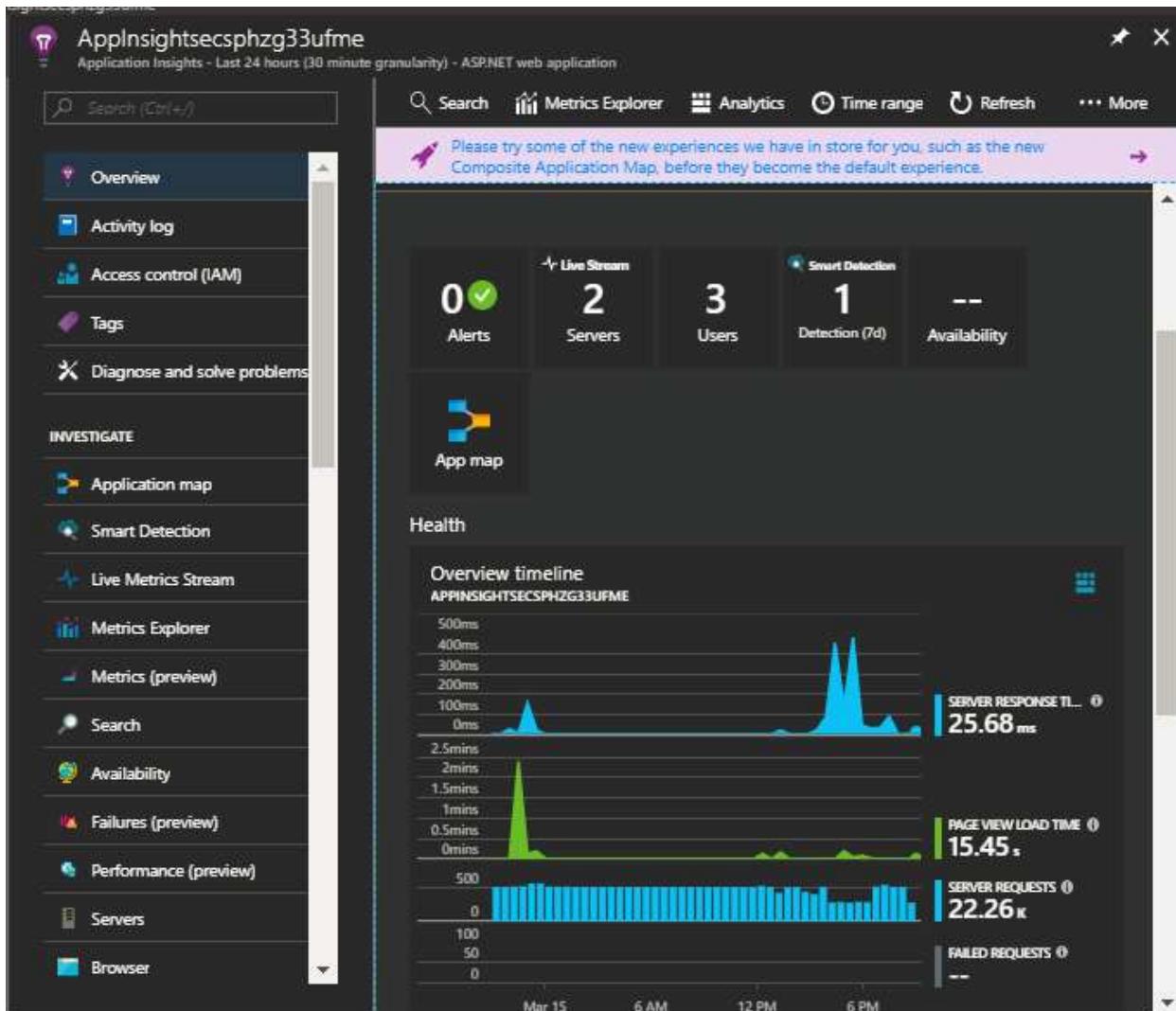
What does Application Insights monitor?

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

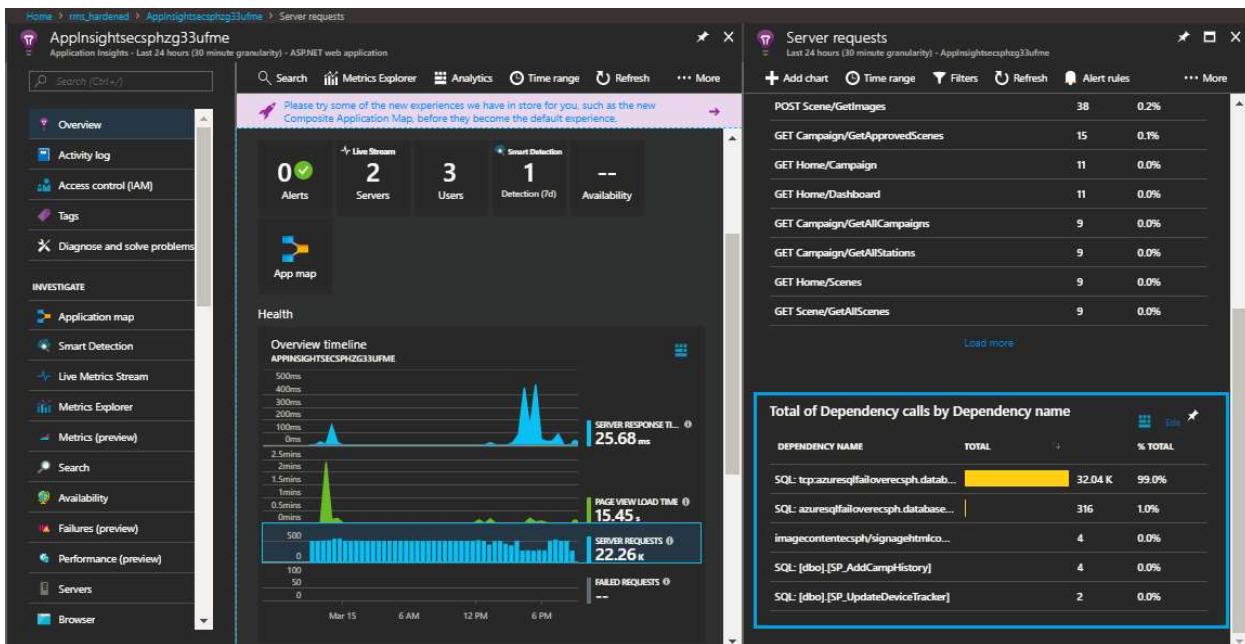
- User and session counts
- Performance counters
- Performance counters
- Host diagnostics from Docker or Azure
- Diagnostic trace logs
- Custom events and metrics

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**.

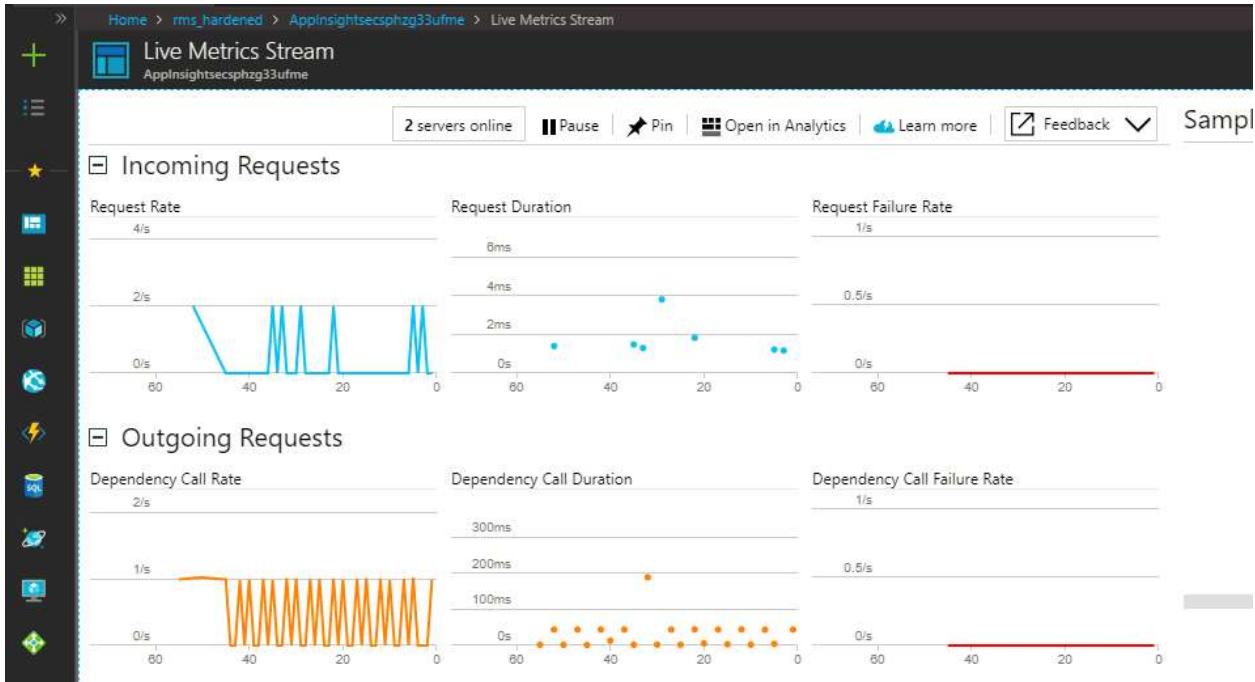


The screenshot shows the Application Insights interface for the 'rms_hardened' resource group. The left sidebar has sections like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, INVESTIGATE, Application map, Smart Detection, Live Metrics Stream, Metrics (preview), Search, Availability, Failures (preview), Performance (preview), Servers, and Browser. The main area has a 'Live Stream' summary with 0 alerts, 2 servers, 3 users, 1 detection, and 0 availability. Below it is a 'Health' section with an 'Overview timeline' chart showing SERVER RESPONSE TIME (25.68 ms) and PAGE VIEW LOAD TIME (15.45 s). A bar chart shows SERVER REQUESTS (22.26 k) and FAILED REQUESTS (0). The right side shows a table of 'Server requests' over the last 24 hours, with a total of 38 events. A callout highlights the 'Total of Dependency calls by Dependency name' table:

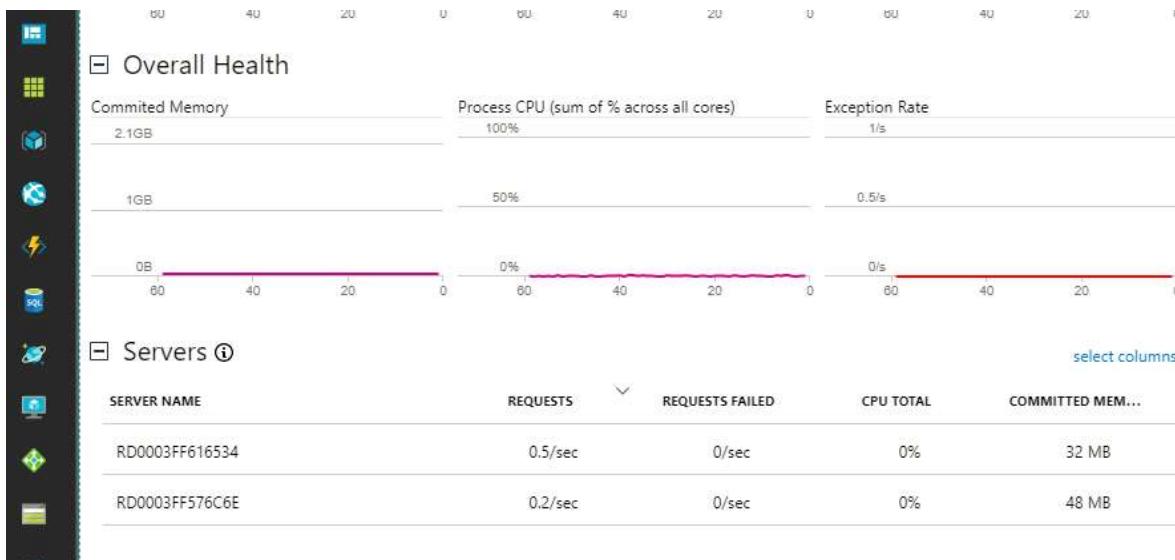
DEPENDENCY NAME	TOTAL	% TOTAL
SQL: tcp://azuresqfailovercph.database...	32.04 K	99.0%
SQL: azuresqfailovercph.database...	316	1.0%
imagecontentcph/signalehtmlco...	4	0.0%
SQL: [dbo].[SP_AddCampHistory]	4	0.0%
SQL: [dbo].[SP_UpdateDeviceTracker]	2	0.0%

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.

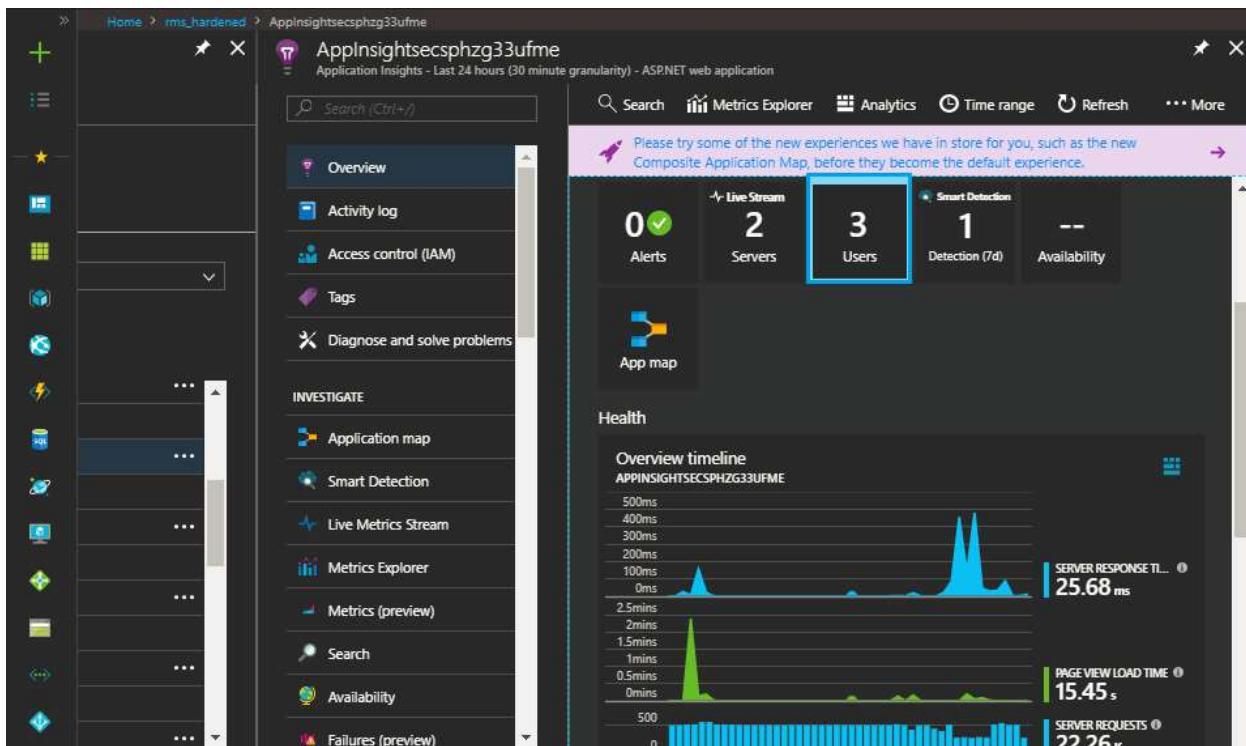


The screenshot shows the 'Live Metrics Stream' page for the 'rms_hardened' resource group. It features two main sections: 'Incoming Requests' and 'Outgoing Requests'. Under 'Incoming Requests', there are three charts: 'Request Rate' (4/s), 'Request Duration' (8ms), and 'Request Failure Rate' (1/s). The 'Request Rate' chart shows a sharp drop from 4/s to 0/s at approximately 40 seconds. The 'Request Duration' chart shows several spikes between 2ms and 4ms. The 'Request Failure Rate' chart shows a constant rate of 1/s. Under 'Outgoing Requests', there are three charts: 'Dependency Call Rate' (2/s), 'Dependency Call Duration' (300ms), and 'Dependency Call Failure Rate' (1/s). The 'Dependency Call Rate' chart shows a fluctuating rate between 0/s and 2/s. The 'Dependency Call Duration' chart shows a distribution between 100ms and 300ms. The 'Dependency Call Failure Rate' chart shows a constant rate of 0.5/s.

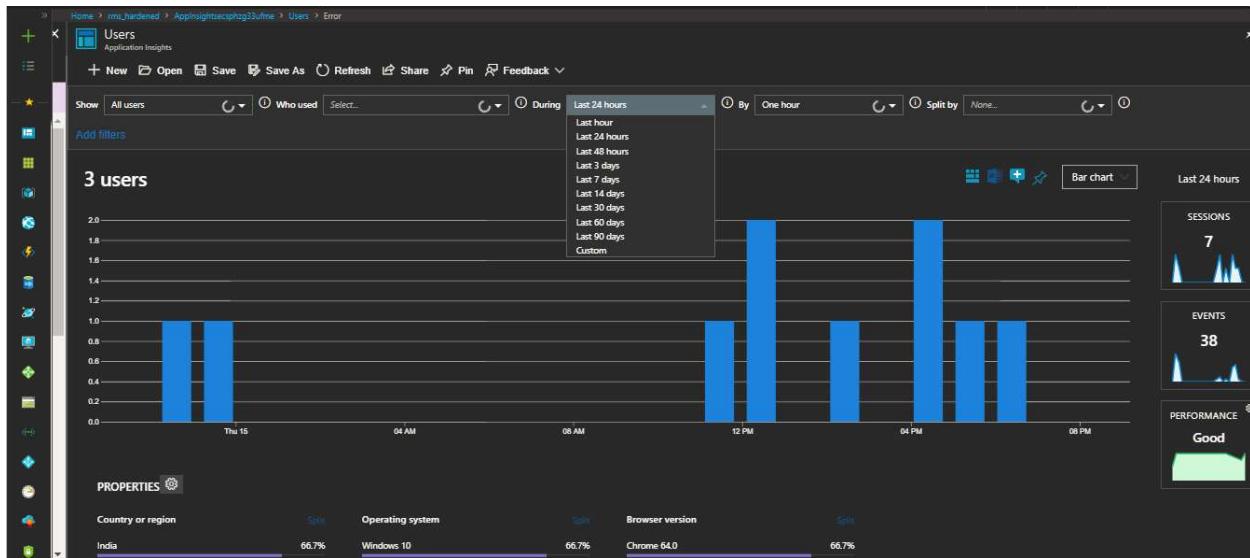


14.1.2. Users

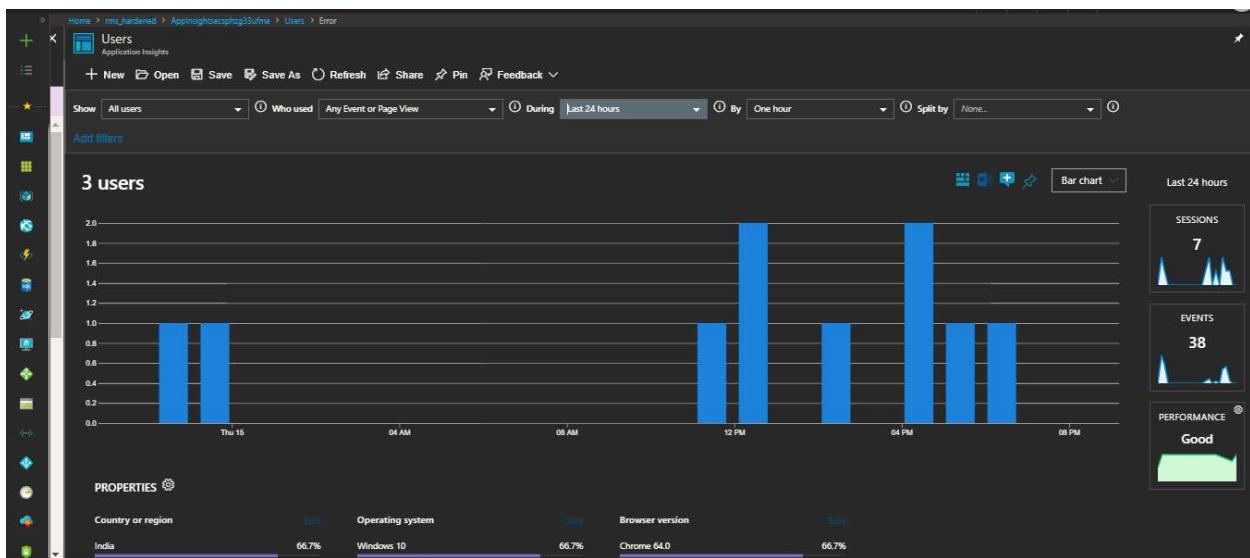
- Click **Users** to view the number of users connected to the web application and to see the number of sessions that are running in the web application.



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

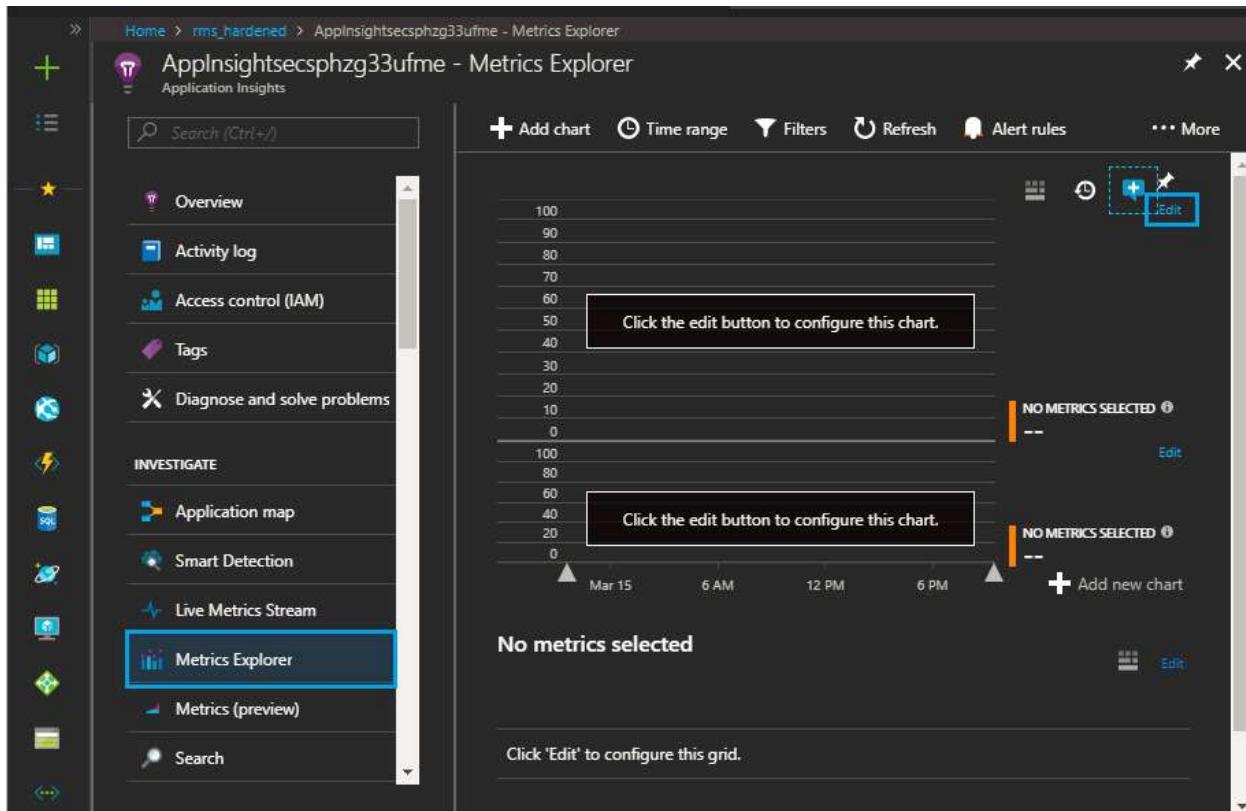


3. In this you also have other options like **Who used**, **Duration**, **By** and **split by** in to set the metrics as per your requirement.



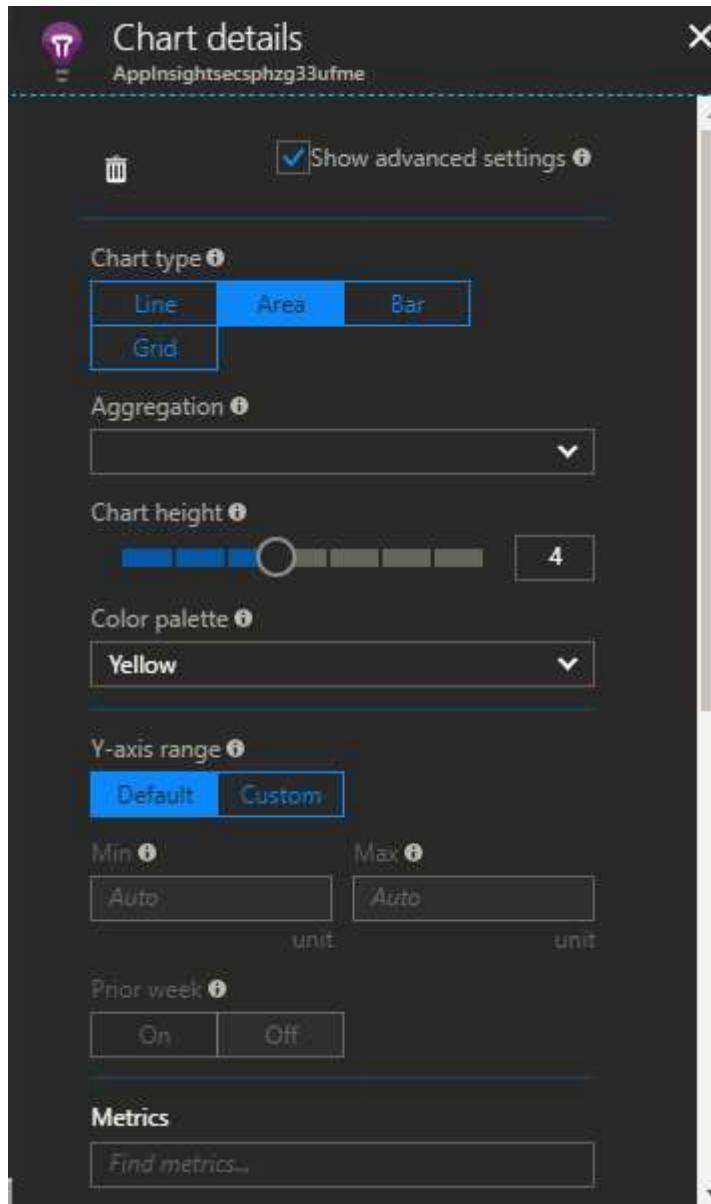
14.1.3. Metric Explorer

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.

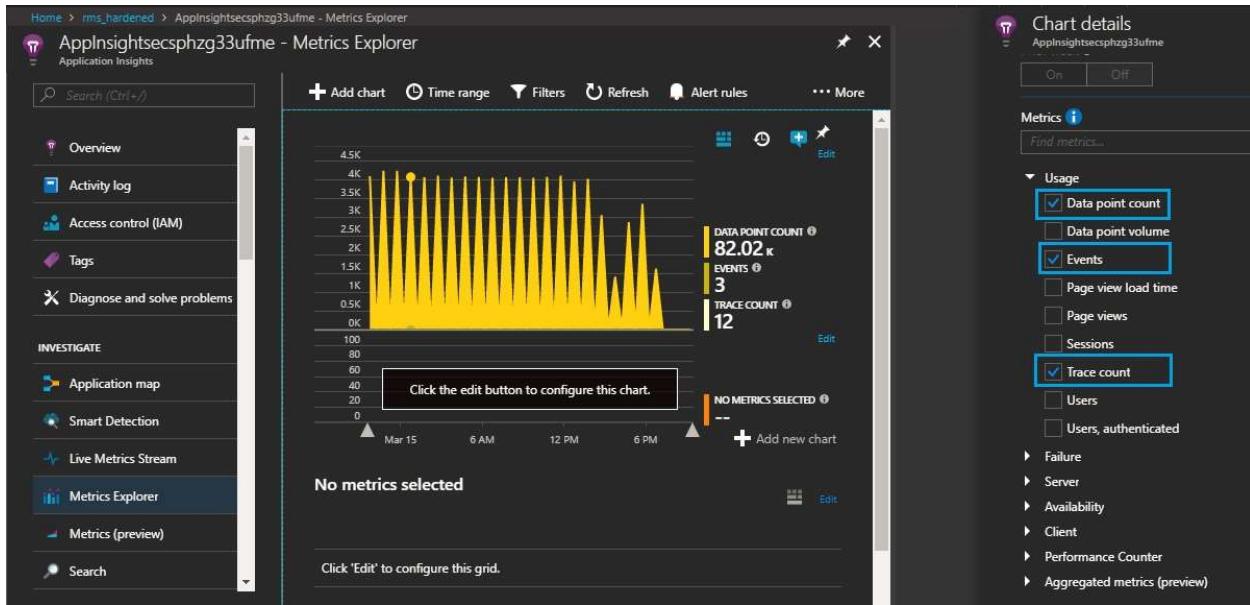


The screenshot shows the Microsoft Application Insights Metrics Explorer interface. On the left, there's a navigation sidebar with various icons and links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, INVESTIGATE, Application map, Smart Detection, Live Metrics Stream, Metrics Explorer (which is selected and highlighted in blue), Metrics (preview), and Search. The main area is titled "AppInsightsecphzg33ufme - Metrics Explorer". It features two large, empty chart containers. Each container has a "Edit" button in the top right corner. Below each chart, there's a message: "Click the edit button to configure this chart." and "NO METRICS SELECTED". At the bottom of the main area, it says "No metrics selected" and "Click 'Edit' to configure this grid."

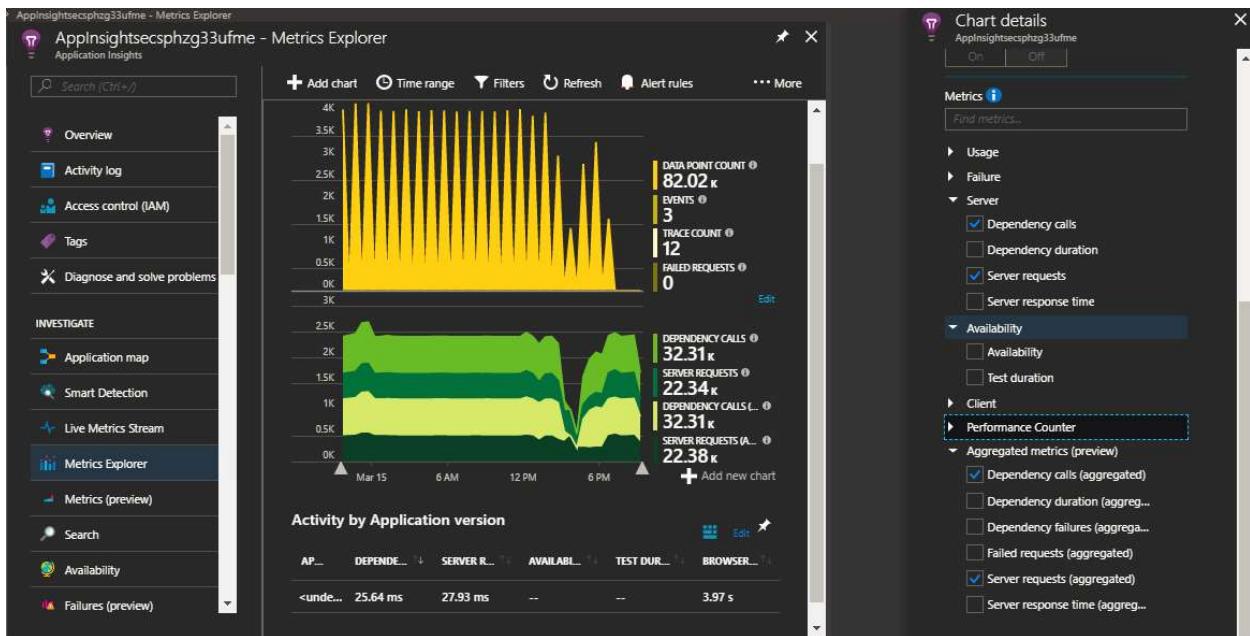
3. **Chart details** page is displayed on the right side. Set the details as per requirement.



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.



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

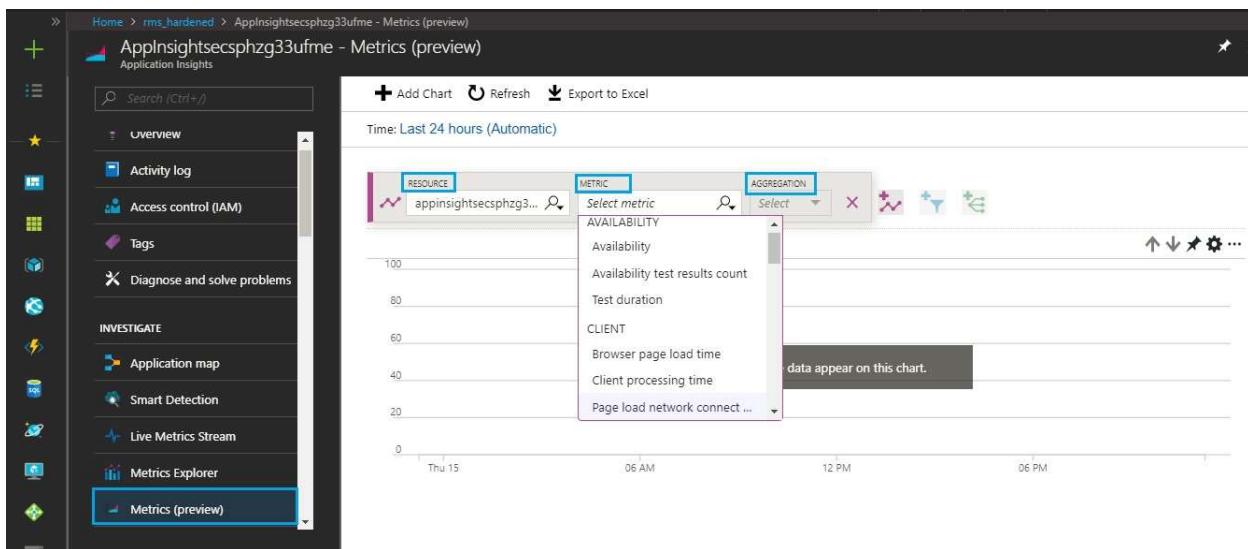


- To check the logs, click the required chart for which you want to see the logs of each request as shown in the following figure.

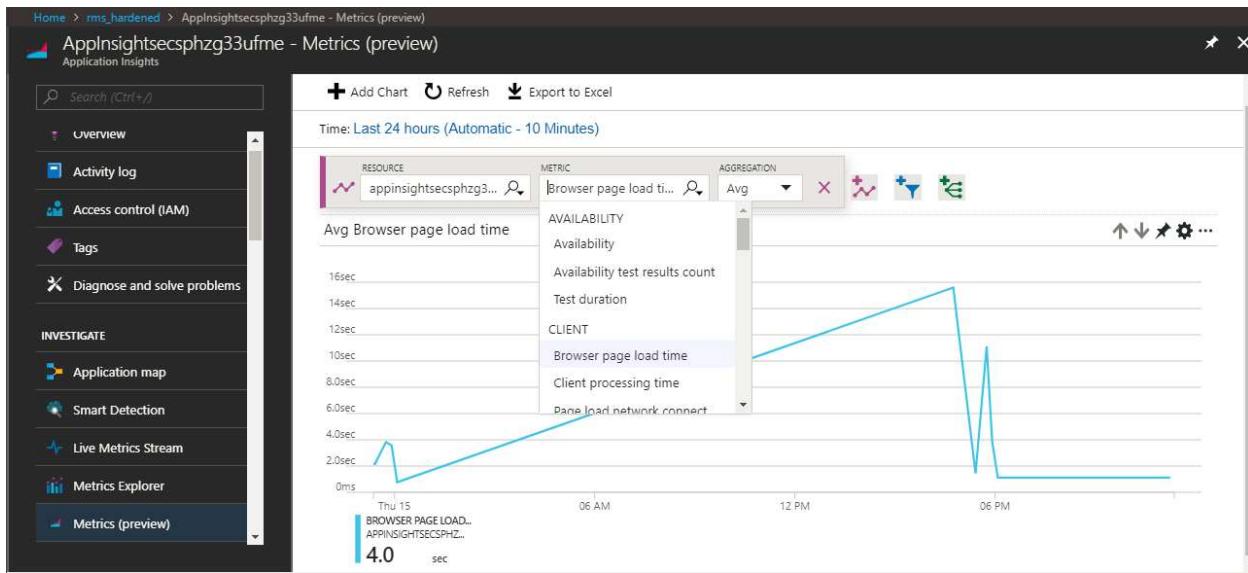


14.1.4. Metric preview

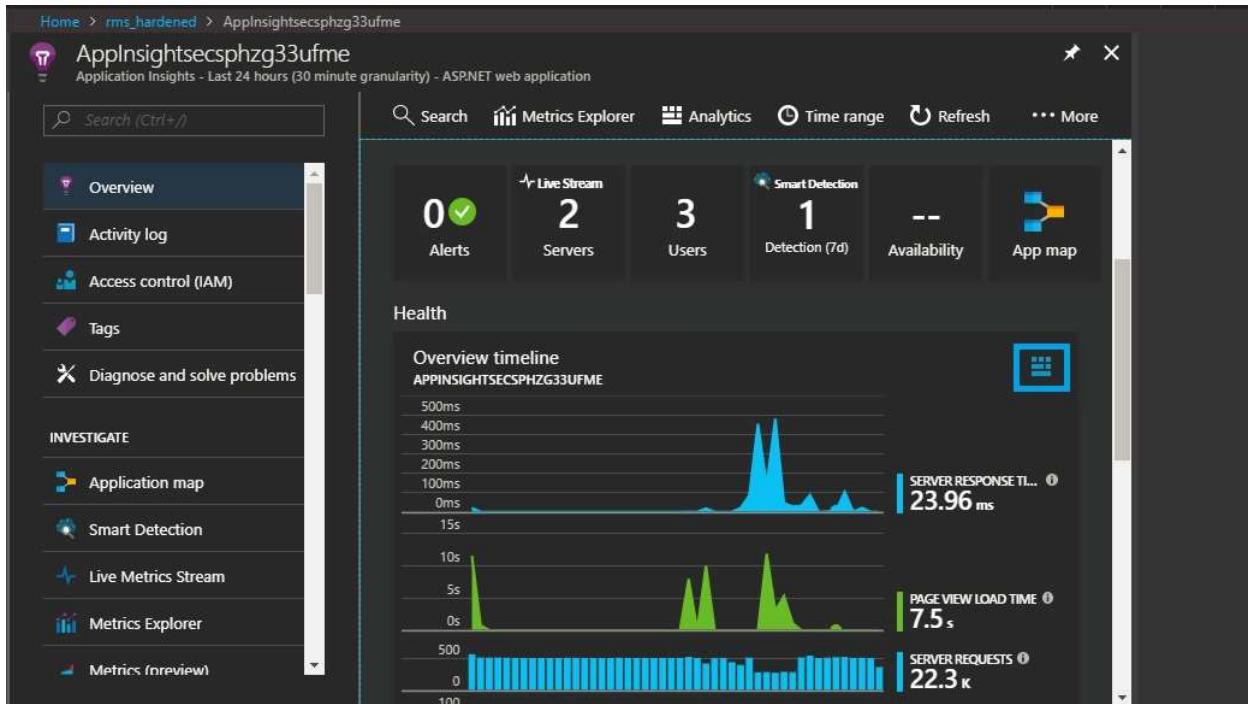
1. Select **Metric Explorer** from the left menu.
2. Select the resource from the drop-down list, select the metric and the aggregation as per requirement.



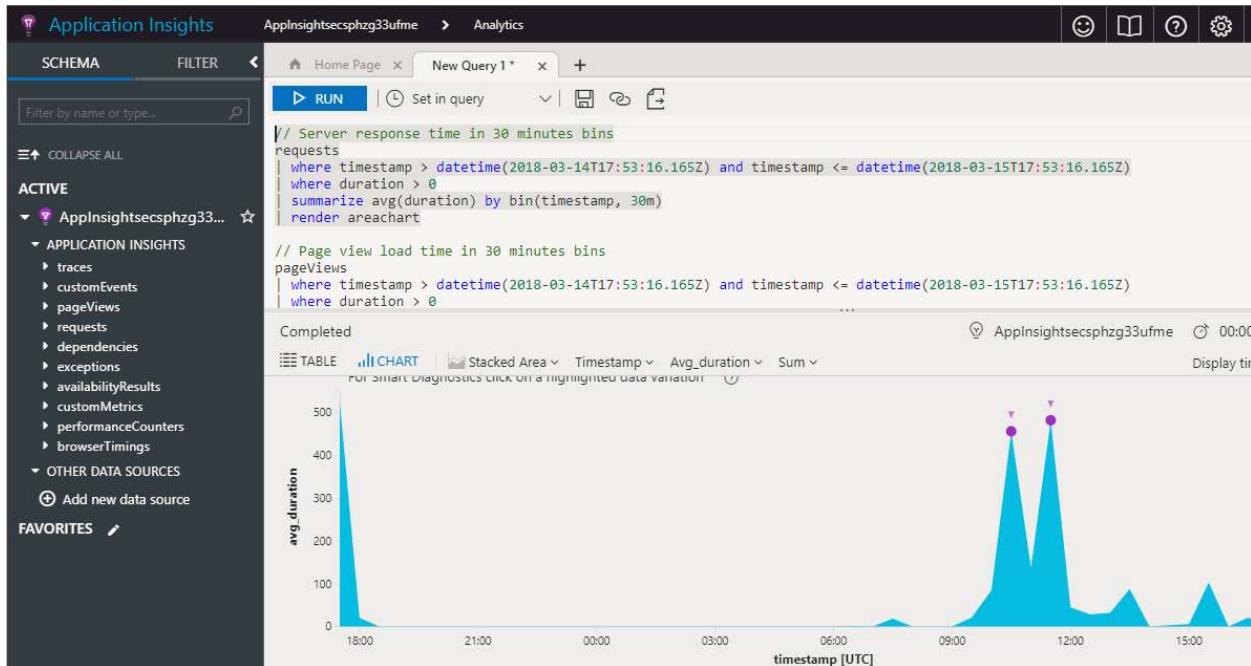
3. The graph is displayed as per the selected metric and aggregation.



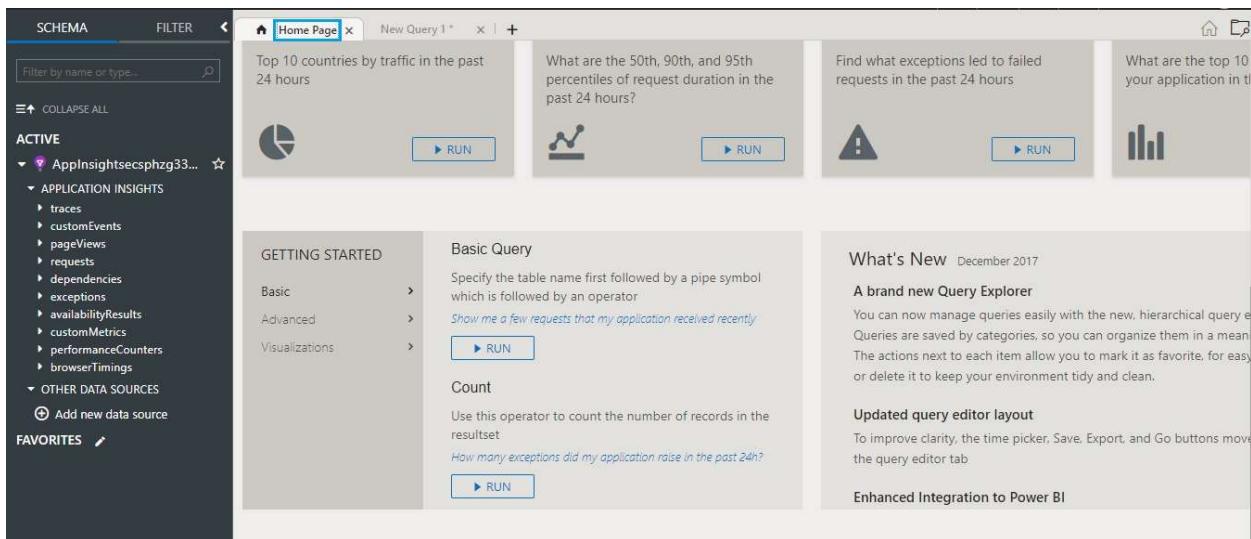
4. User can use the **Usage Customized Query** to view the metrics.
5. Click the icon on the top right corner of the **Overview timeline** section as shown in the following figure.



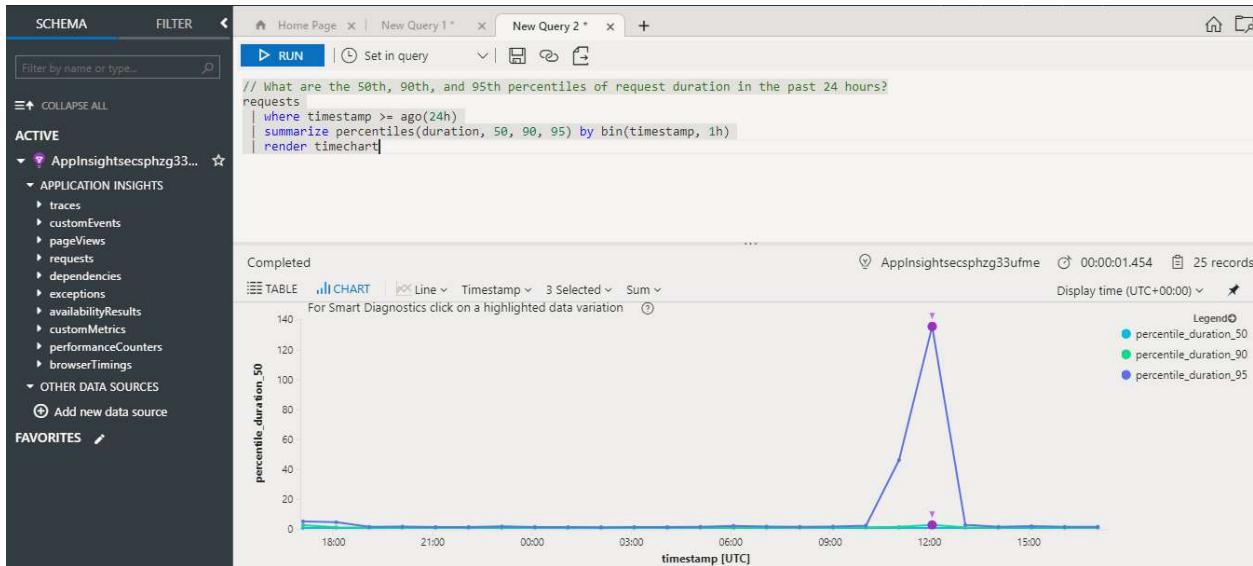
6. A new tab with some default queries & chart for the same are displayed as shown in the following figure.



- 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.

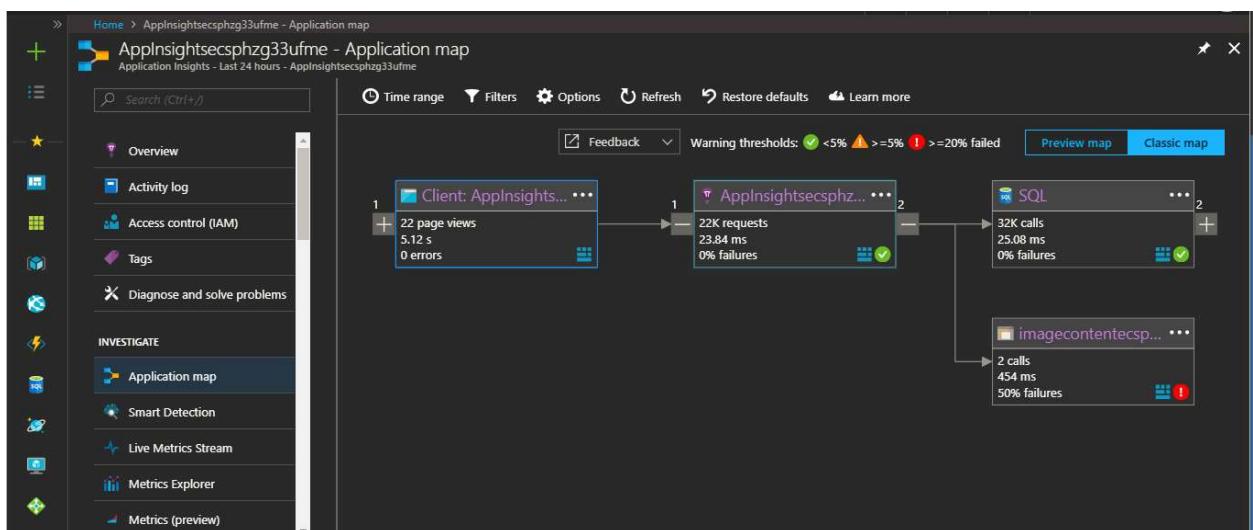


- Click **RUN** in the Performance section to display default queries & charts.

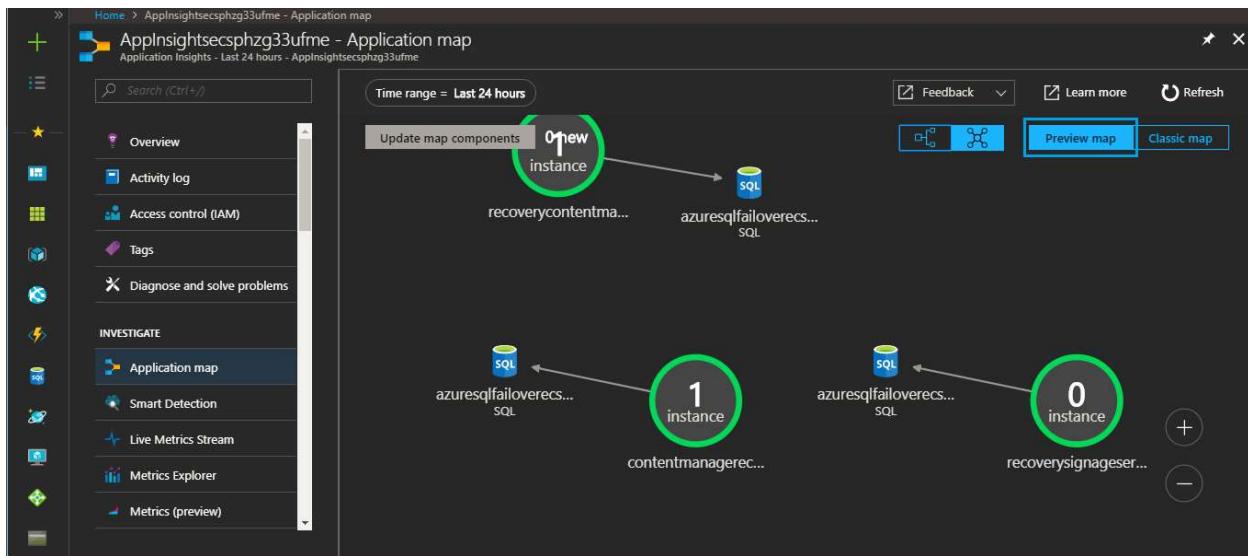


14.1.5. Application Map

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.

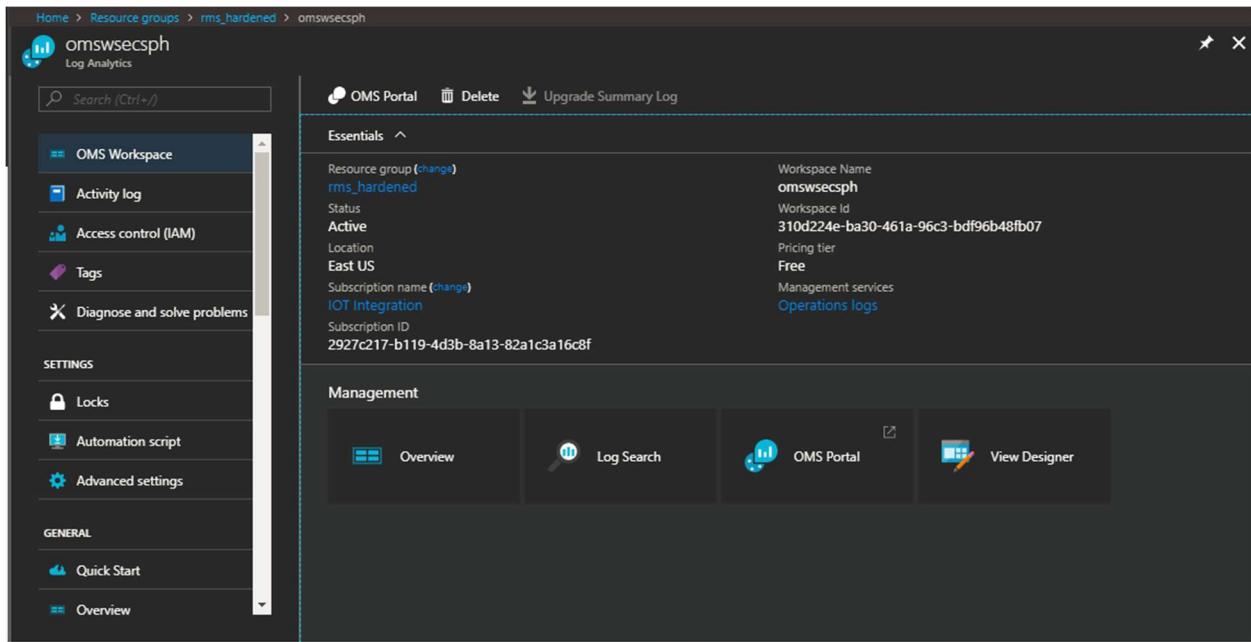
OMS are helpful to monitor SQL Database, Web Apps and Other Azure Components

In this Deployment we are using below two solutions.

- Azure SQL Analytics
- Azure Web Apps Analytics

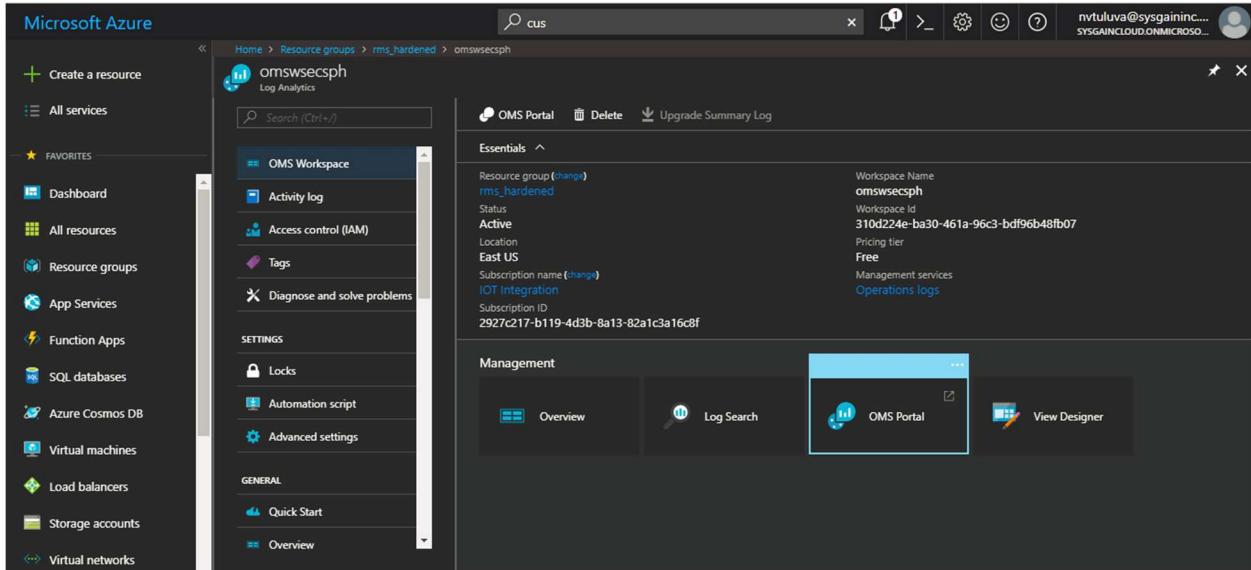
1. Go to **Azure portal > Resource group > Deployments > Microsoft.Template**. Get the **OMS Portal URL** from the **Outputs** section as shown in the following figure.

RMS Hardening



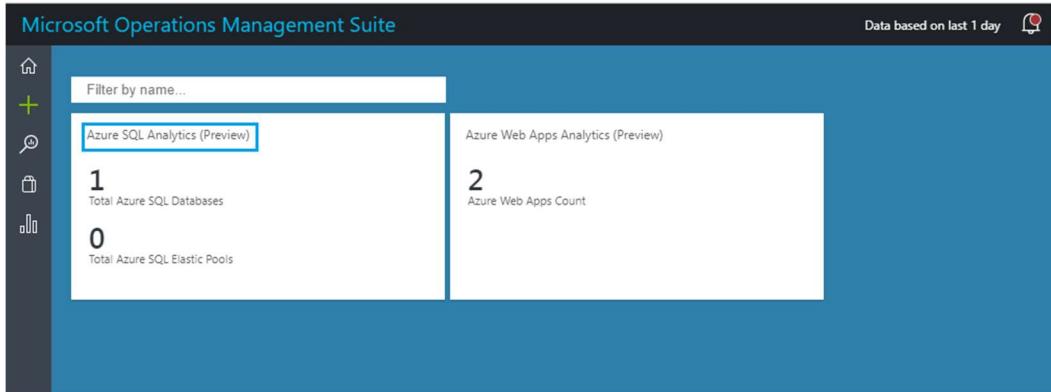
The screenshot shows the Azure portal interface for an OMS workspace named 'omswsecsth'. The 'Essentials' section displays basic information such as Resource group ('rms_hardened'), Status ('Active'), Location ('East US'), and Subscription name ('IOT Integration'). The 'Management' section includes links for Overview, Log Search, OMS Portal, and View Designer. The 'OMS Portal' link is highlighted with a blue box.

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



This screenshot is identical to the one above, showing the Azure portal for the 'omswsecsth' workspace. The 'OMS Portal' button is again highlighted with a blue box.

- 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

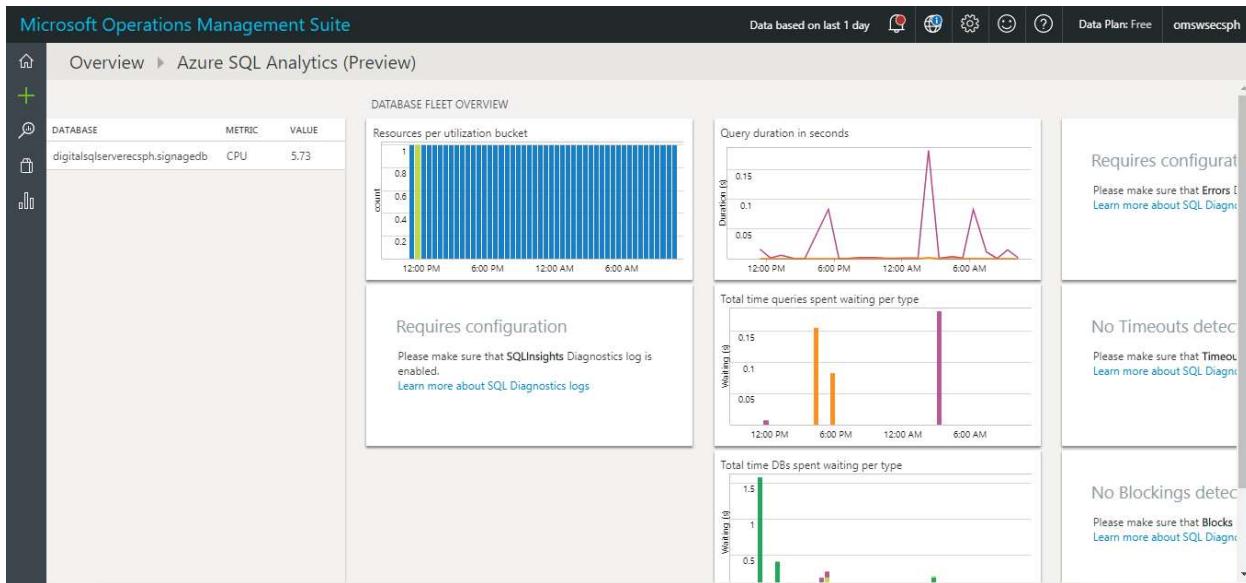
Azure SQL Analytics solution in Azure Log Analytics collects and visualizes important SQL Azure performance metrics.

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.

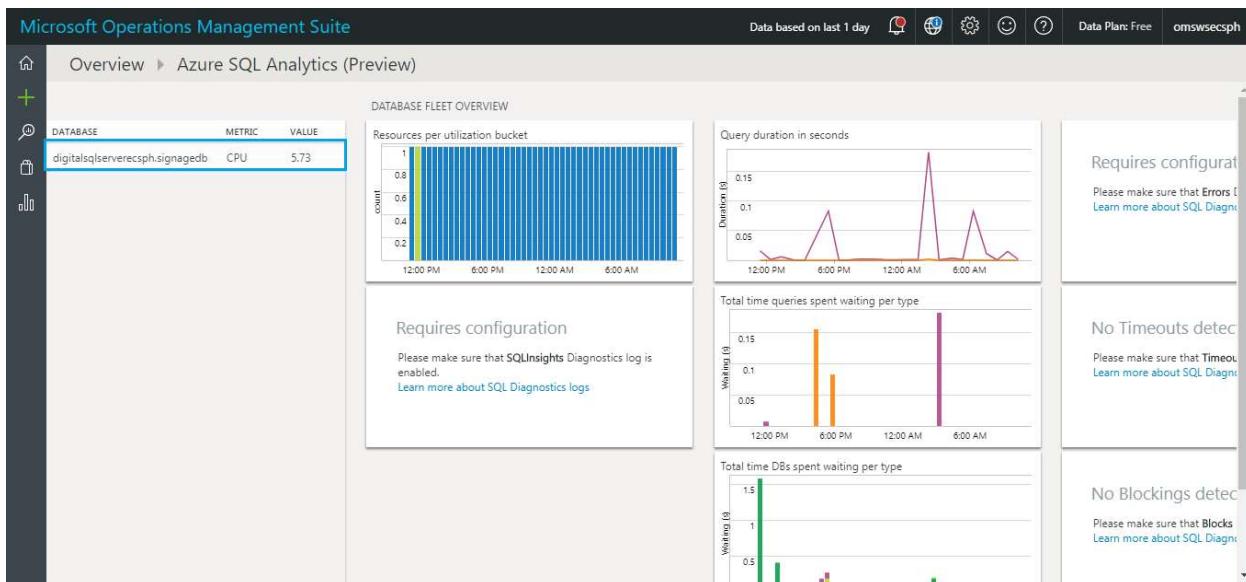
Using this solution, we can find out below metrics:

- 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.



Microsoft Operations Management Suite

Overview ▶ Azure SQL Analytics (Preview) ▶ Database

Data based on last 1 day | 🔔 | 🌐 | ⚙️ | 😊 | ? | Data Plan: Free | omswsecph

RESOURCE INFO

- Subscription name: 2927c217-b119-4d3b-8a13-82a1c3a16c8f
- Server name: digitalsqlserverecspf
- Database name: signagedb

INSIGHTS SUMMARY

Requires configuration
Please make sure that **SQLInsights** Diagnostics log is enabled.
[Learn more about SQL Diagnostics logs](#)

QUERIES

View full insights report

CHART: Query time (s) vs Time (12:00 PM, 6:00 PM, 12:00 AM, 6:00 AM)

CHART: Query wait (s) vs Time (12:00 PM, 6:00 PM, 12:00 AM, 6:00 AM)

QUERY	METRIC	MAX (s)	Avg (s)	Dominant Wait	Max (s)	Avg (s)	Execs
0x8E1CD77DC2F5...	Duration	0.18	0	CPU	0.18	0	16163
0x987B8E9C4742...	Duration	0.08	0.04	BUFFERIO	0.08	0.04	2
0x388887E6006D...	Duration	0.02	0	CPU	0.01	0	40
0xC824056576DF...	Duration	0.02	0		0	0	124
0x7C53C732068FF3...	Duration	0	0		0	0	2
0xA2130AA67E36...	Duration	0	0		0	0	22
0x2737776D43F...	Duration	0	0		0	0	1
0xABD89E08357...	Duration	0	0		0	0	31
0xBD7BB7487C56...	Duration	0	0		0	0	62
0xN1388997A0869	Duration	0	0		0	0	1

Microsoft Operations Management Suite

Overview ▶ Azure SQL Analytics (Preview) ▶ Database

Data based on last 1 day | 🔔 | 🌐 | ⚙️ | 😊 | ? | Data Plan: Free | omswsecph

DATABASE WAITS

CHART: No Waits (s) vs Time (12:00 PM, 6:00 PM, 12:00 AM, 6:00 AM)

WAIT TYPE	TOTAL (s)
SOS_SCHEDULER_YIELD	2.37
WRITELOG	0.32
PAGEIOLATCH_SH	0.24
MEMORY_ALLOCATION_EXT	0.01
PAGELATCH_SH	0
PAGELATCH_EX	0
RESERVED_MEMORY_ALLOCATION_EXT	0

EVENTS

No data detected
Please make sure that data Diagnostics log is enabled.
[Learn more about SQL Diagnostics logs](#)

TIME	EVENT
Currently no data is available. Please check if proper Diagnostics settings logs are enabled.	

DATABASE METRICS

CHART: DTU% vs Time (12:00 PM, 6:00 PM, 12:00 AM, 6:00 AM)

CHART: Session% vs Time (12:00 PM, 6:00 PM, 12:00 AM, 6:00 AM)

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:

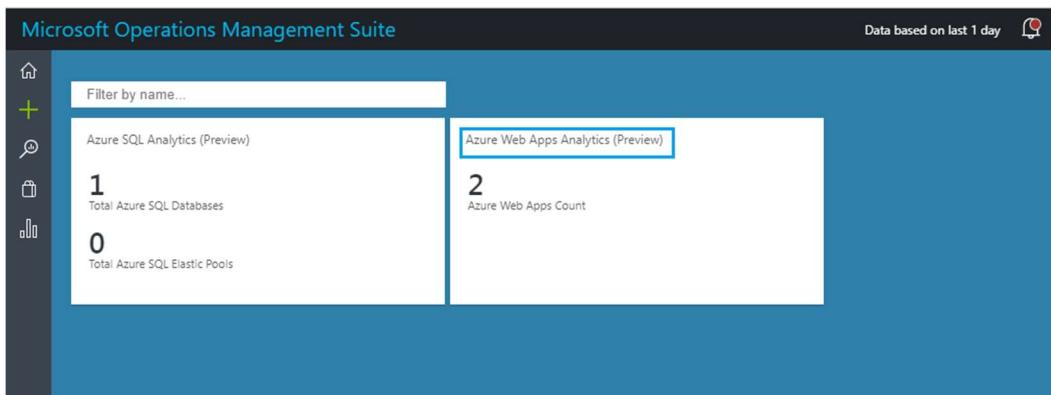
- Top Web Apps with the highest response time
- Number of requests across your Web Apps, including successful and failed requests
- Top Web Apps with highest incoming and outgoing traffic

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

Azure Web Apps metrics like

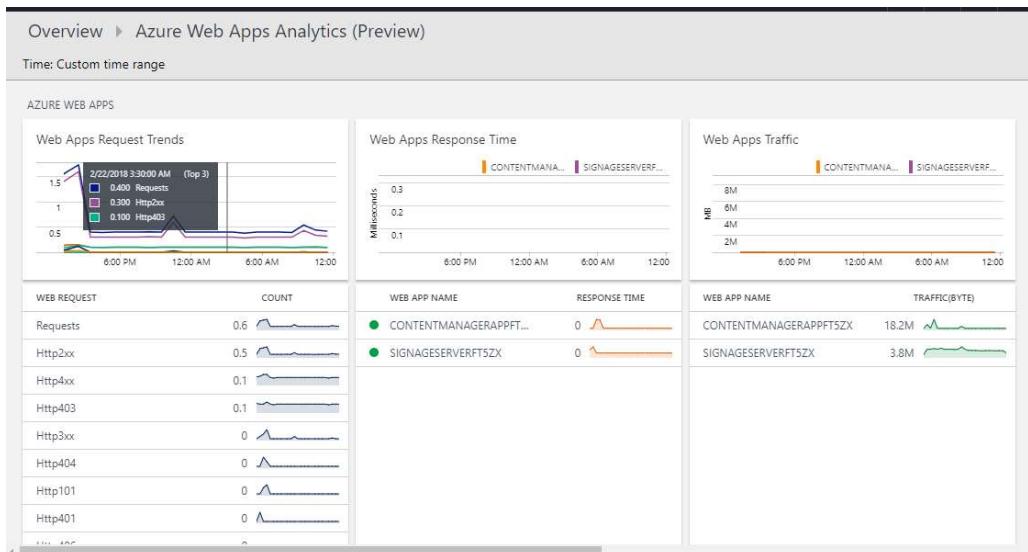
- Average Memory Working Set
- Average Response Time
- Bytes Received/Sent
- CPU Time
- Requests
- Memory Working Set
- Httpxxx

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

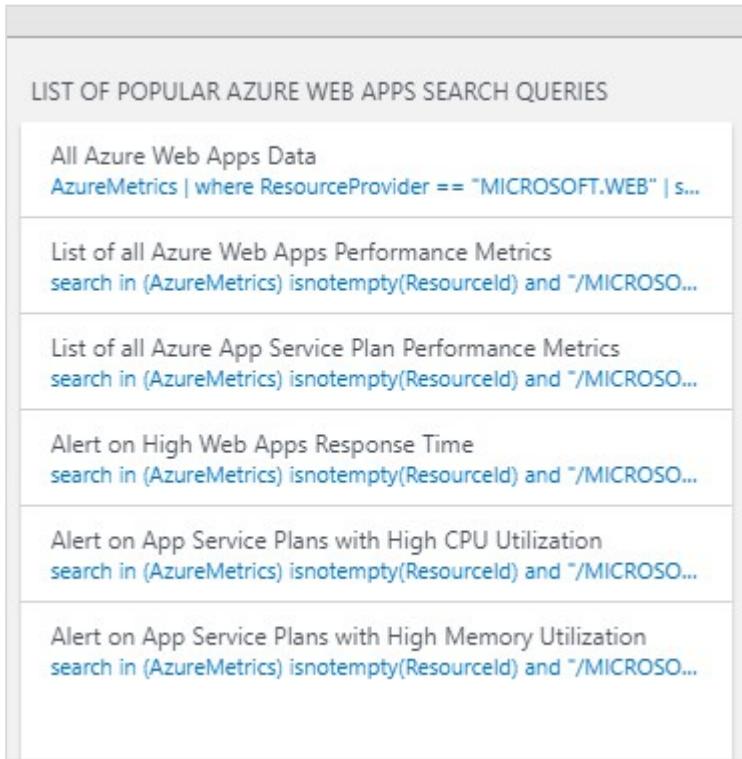


The screenshot shows the Microsoft Operations Management Suite dashboard. On the left, there's a sidebar with icons for Home, Add, Filter by name..., Azure SQL Analytics (Preview), and Azure Web Apps Analytics (Preview). The main area has two cards: '1 Total Azure SQL Databases' and '2 Azure Web Apps Count'. The 'Azure Web Apps Count' card is highlighted with a blue border.

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.



The screenshot shows a list of search queries under the heading "LIST OF POPULAR AZURE WEB APPS SEARCH QUERIES". The queries are:

- All Azure Web Apps Data
[AzureMetrics | where ResourceProvider == "MICROSOFT.WEB" | s...](#)
- List of all Azure Web Apps Performance Metrics
[search in \(AzureMetrics\) isnotempty\(ResourceId\) and "/MICROSO...](#)
- List of all Azure App Service Plan Performance Metrics
[search in \(AzureMetrics\) isnotempty\(ResourceId\) and "/MICROSO...](#)
- Alert on High Web Apps Response Time
[search in \(AzureMetrics\) isnotempty\(ResourceId\) and "/MICROSO...](#)
- Alert on App Service Plans with High CPU Utilization
[search in \(AzureMetrics\) isnotempty\(ResourceId\) and "/MICROSO...](#)
- Alert on App Service Plans with High Memory Utilization
[search in \(AzureMetrics\) isnotempty\(ResourceId\) and "/MICROSO...](#)

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.

Microsoft Operations Management Suite

Log Search

Favorites History Analytics

Show legacy language converter

Usage | where IsBillable == true | summarize count() by DataType

return all Usage records pipe results filter billable records pipe results count the records per DataType

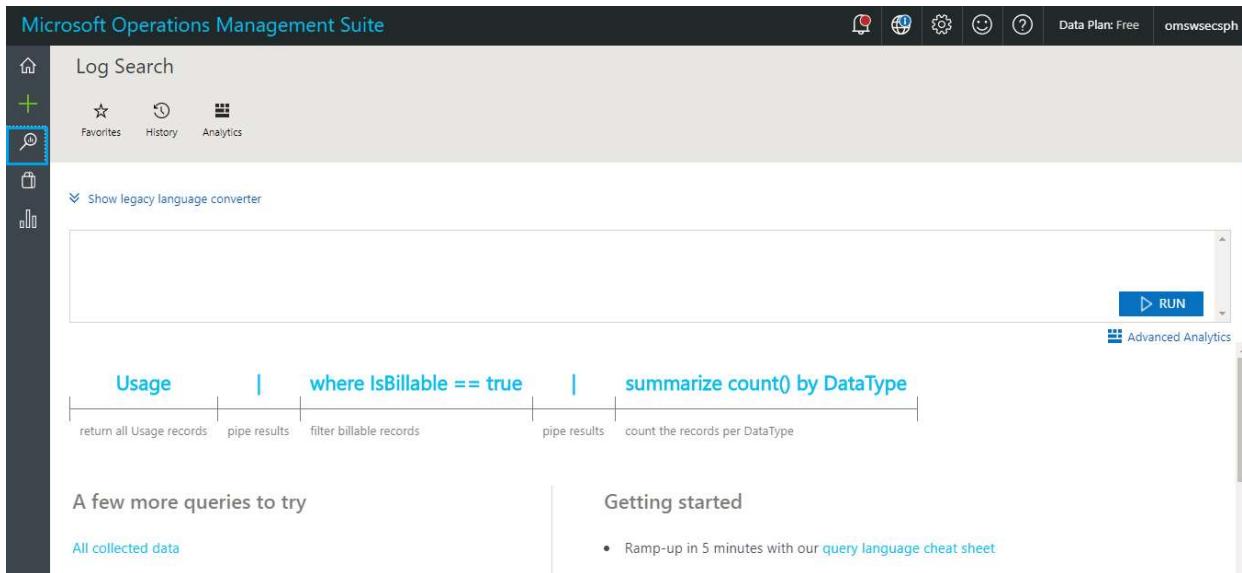
A few more queries to try

All collected data

Getting started

- Ramp-up in 5 minutes with our [query language cheat sheet](#)

RUN Advanced Analytics



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

Microsoft Operations Management Suite

Log Search

Favorites History Analytics

Show legacy language converter

search *

RUN Advanced Analytics

Search History



Microsoft Operations Management Suite

Log Search

Export PowerBI Alert Save Favorites History Analytics

Data based on last 1 day 1 bar = 1hr

11:30:00 AM Mar 15, 2018 3:30:00 AM Mar 16, 2018

TYPE (3)

AzureMetrics	212K
AzureDiagnostics	190
Usage	54

+Add

search *

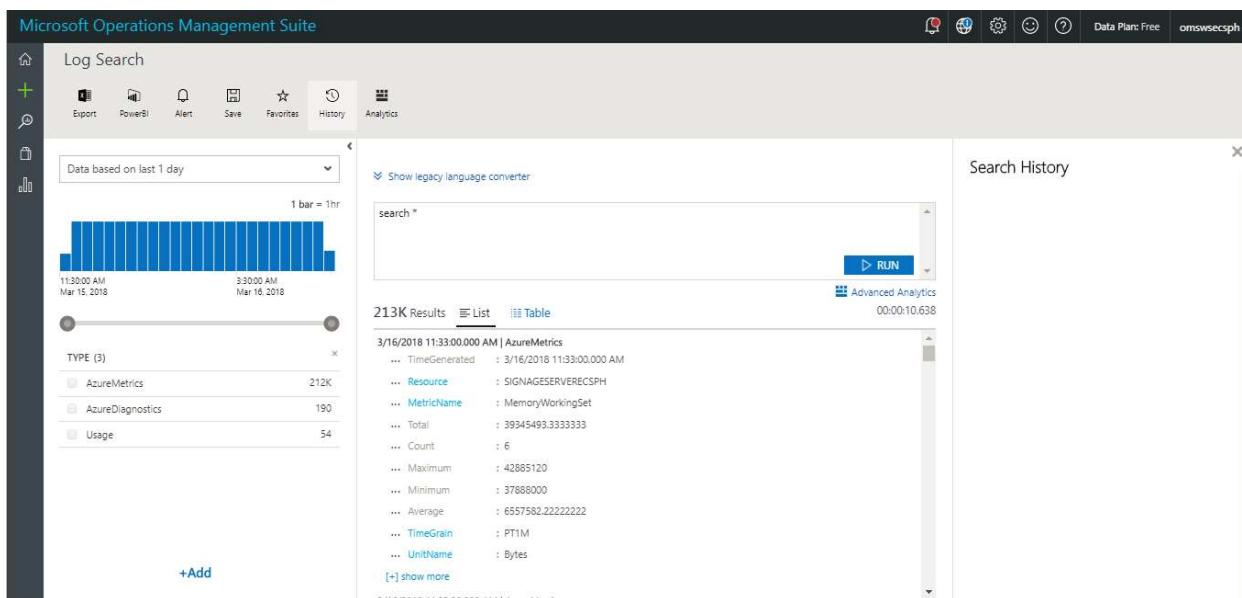
213K Results List Table

3/16/2018 11:33:00.000 AM | AzureMetrics

- TimeGenerated : 3/16/2018 11:33:00.000 AM
- Resource : SIGNAGESERVERECPSPH
- MetricName : MemoryWorkingSet
- Total : 39345493.3333333
- Count : 6
- Maximum : 42885120
- Minimum : 37888000
- Average : 6557582.22222222
- TimeGrain : PT1M
- UnitName : Bytes

[+] show more

Search History



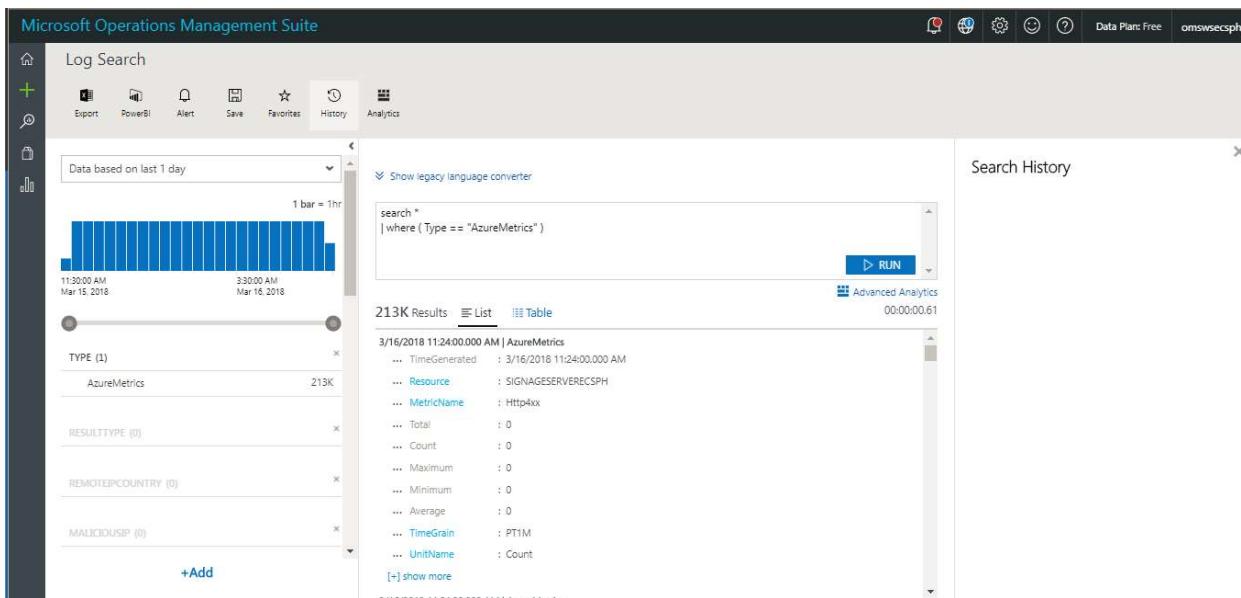
14.2.4. IoT HUB

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.

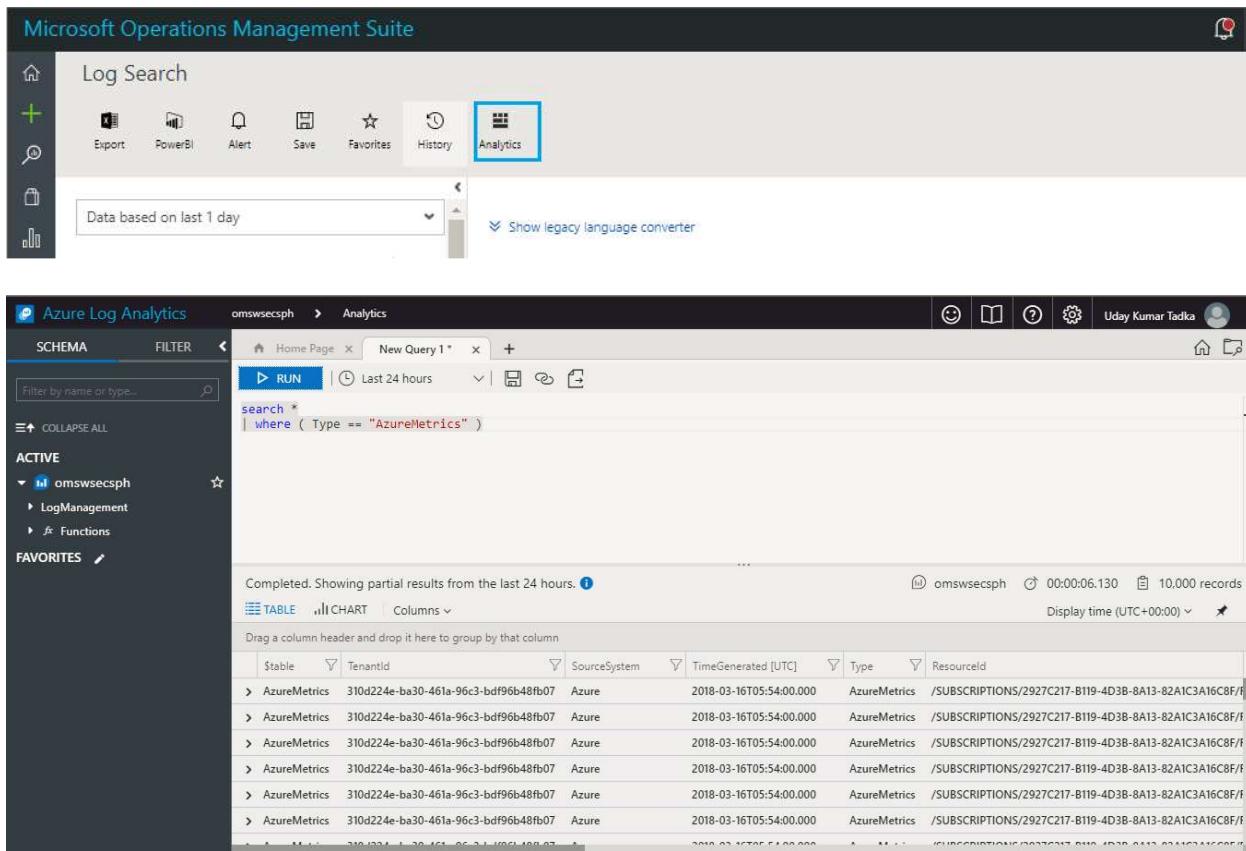


The screenshot shows the Microsoft Operations Management Suite Log Search interface. On the left, there's a histogram visualization for 'AzureMetrics' data over the last day. Below it are several filter panels: 'TYPE (1)' set to 'AzureMetrics', 'RESULTTYPE (0)', 'REMOTEIPCOUNTRY (0)', and 'MALICIOUSIP (0)'. On the right, a search bar contains the query: 'search * | where (Type == "AzureMetrics")'. Below the search bar is a table titled '213K Results' showing log entries. One entry is expanded to show details: '3/16/2018 11:24:00.000 AM | AzureMetrics ... TimeGenerated : 3/16/2018 11:24:00.000 AM ... Resource : SIGNAGESERVERECSPH ... MetricName : Http4xx ... Total : 0 ... Count : 0 ... Maximum : 0 ... Minimum : 0 ... Average : 0 ... TimeGrain : PT1M ... UnitName : Count'. The interface also includes a 'RUN' button and a 'Search History' section.

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.



The screenshot shows the Microsoft Operations Management Suite (OMS) Log Search interface. At the top, there's a navigation bar with 'Microsoft Operations Management Suite' and a bell icon. Below it is a toolbar with icons for 'Log Search' (highlighted), 'Export', 'PowerBI', 'Alert', 'Save', 'Favorites', 'History', and 'Analytics' (highlighted). A dropdown menu shows 'Data based on last 1 day'. The main area displays 'Azure Log Analytics' results for the schema 'omswsecph'. The query is set to 'Last 24 hours' and is defined as:

```
search *
| where ( Type == "AzureMetrics" )
```

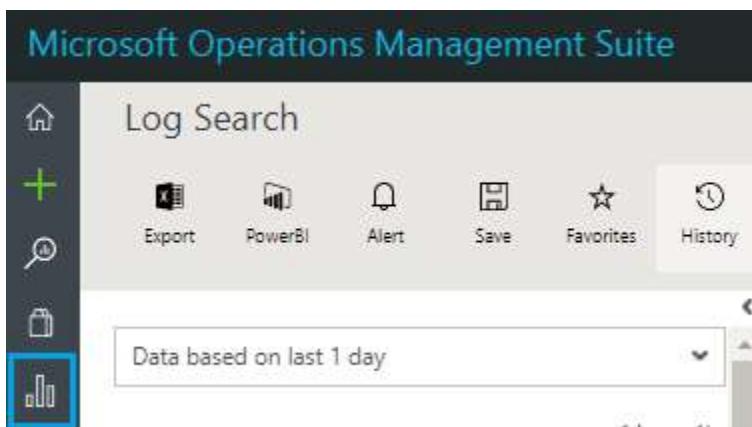
The results table shows 10,000 records from the last 24 hours. The columns include:

Stable	TenantId	SourceSystem	TimeGenerated [UTC]	Type	ResourceId
>	310d224e-ba30-461a-96c3-bdf96b48fb07	Azure	2018-03-16T05:54:00.000	AzureMetrics	/SUBSCRIPTIONS/2927C217-B119-4D3B-8A13-82A1C3A16C8F/F
>	310d224e-ba30-461a-96c3-bdf96b48fb07	Azure	2018-03-16T05:54:00.000	AzureMetrics	/SUBSCRIPTIONS/2927C217-B119-4D3B-8A13-82A1C3A16C8F/F
>	310d224e-ba30-461a-96c3-bdf96b48fb07	Azure	2018-03-16T05:54:00.000	AzureMetrics	/SUBSCRIPTIONS/2927C217-B119-4D3B-8A13-82A1C3A16C8F/F
>	310d224e-ba30-461a-96c3-bdf96b48fb07	Azure	2018-03-16T05:54:00.000	AzureMetrics	/SUBSCRIPTIONS/2927C217-B119-4D3B-8A13-82A1C3A16C8F/F
>	310d224e-ba30-461a-96c3-bdf96b48fb07	Azure	2018-03-16T05:54:00.000	AzureMetrics	/SUBSCRIPTIONS/2927C217-B119-4D3B-8A13-82A1C3A16C8F/F
>	310d224e-ba30-461a-96c3-bdf96b48fb07	Azure	2018-03-16T05:54:00.000	AzureMetrics	/SUBSCRIPTIONS/2927C217-B119-4D3B-8A13-82A1C3A16C8F/F
>	310d224e-ba30-461a-96c3-bdf96b48fb07	Azure	2018-03-16T05:54:00.000	AzureMetrics	/SUBSCRIPTIONS/2927C217-B119-4D3B-8A13-82A1C3A16C8F/F
>	310d224e-ba30-461a-96c3-bdf96b48fb07	Azure	2018-03-16T05:54:00.000	AzureMetrics	/SUBSCRIPTIONS/2927C217-B119-4D3B-8A13-82A1C3A16C8F/F
>	310d224e-ba30-461a-96c3-bdf96b48fb07	Azure	2018-03-16T05:54:00.000	AzureMetrics	/SUBSCRIPTIONS/2927C217-B119-4D3B-8A13-82A1C3A16C8F/F
>	310d224e-ba30-461a-96c3-bdf96b48fb07	Azure	2018-03-16T05:54:00.000	AzureMetrics	/SUBSCRIPTIONS/2927C217-B119-4D3B-8A13-82A1C3A16C8F/F

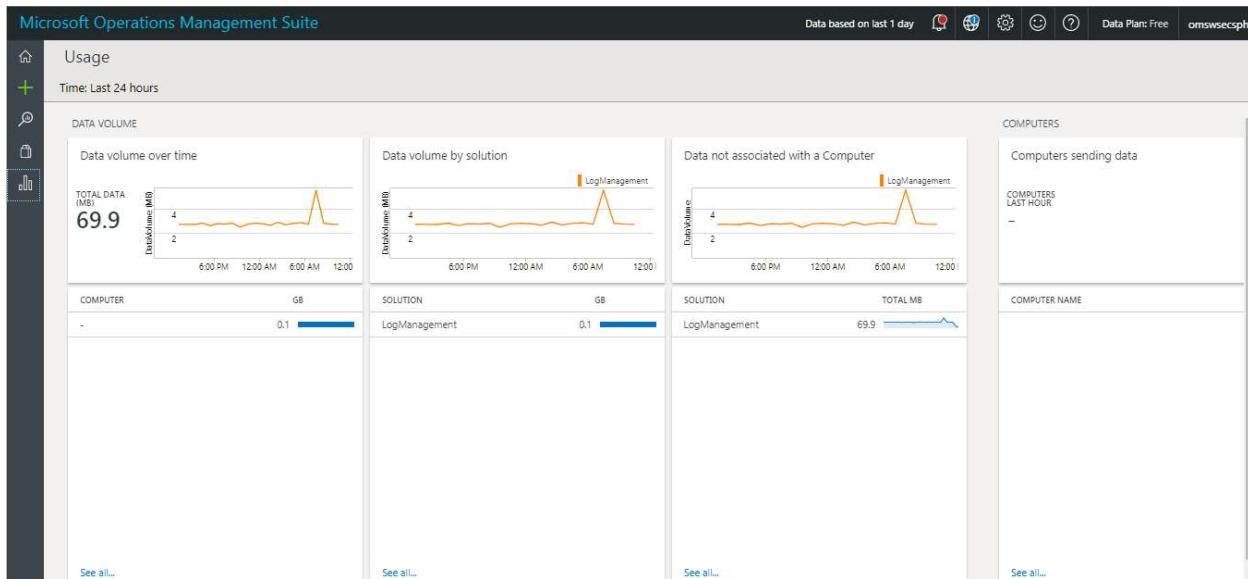
14.2.6. Usage Page

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.



The screenshot shows the Microsoft Operations Management Suite (OMS) Log Search interface. At the top, there's a navigation bar with 'Microsoft Operations Management Suite' and a bell icon. Below it is a toolbar with icons for 'Log Search' (highlighted), 'Export', 'PowerBI', 'Alert', 'Save', 'Favorites', and 'History'. A dropdown menu shows 'Data based on last 1 day'. The 'Analytics' icon in the toolbar is also highlighted.



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:

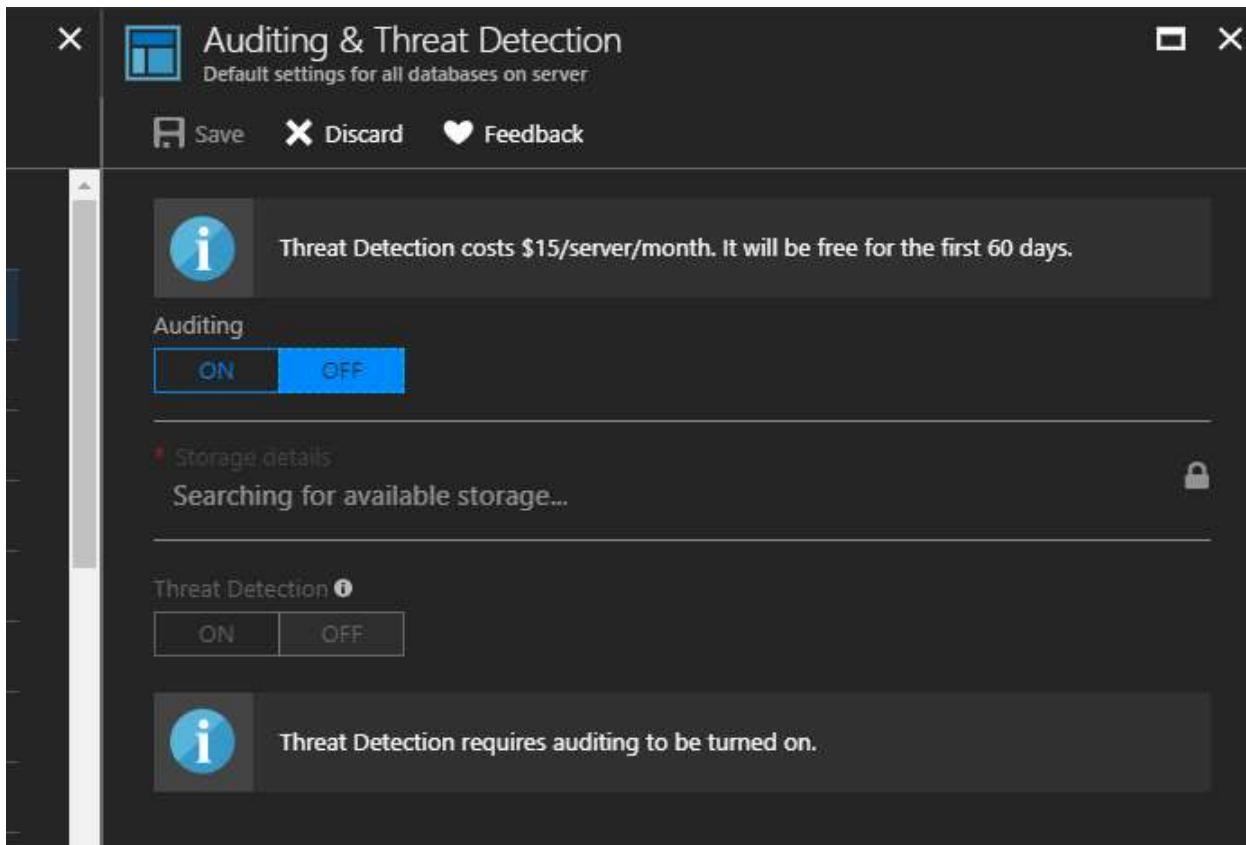
1. Click **Enable auditing and threat detection on SQL servers** as shown in the following figure.

Filter				
Add a Next Generation Firewall	3 endpoints	Open	!	High
Enable Network Security Groups on subnets	2 subnets	Open	!	High
Enable Auditing & Threat detection on SQL servers	7 SQL servers	Open	!	High
Enable Auditing & Threat detection on SQL databases	9 SQL databases	Open	!	High
Apply disk encryption	3 virtual machines	Open	!	High
Restrict access through Internet facing endpoint	3 virtual machines	Open	▲	Medium
Add a vulnerability assessment solution	3 virtual machines	Open	▲	Medium
Reboot after system updates	dataAggServer	Open	▲	Medium
Provide security contact details	1 subscription	Open	▲	Medium
Remediate security configurations	1 computer	Open	i	Low

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

SQL SERVER	STATE	SEVERITY	...
digitalsqlserverh3zqr	Open	! High	...
emssqlsrv	Open	! High	...
recoverdigitalsqlserverh3zqr	Open	! High	...
sqlserverh7o4564fywcuu	Open	! High	...
sqlserverog5u6	Open	! High	...
sqlserverogcovu5npohju	Open	! High	...
sqlserversi7xp	Open	! High	...
digitalsqlserverboqtf	Resolved	● High	...
digitalsqlserverdzlxk	Resolved	● High	...

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?

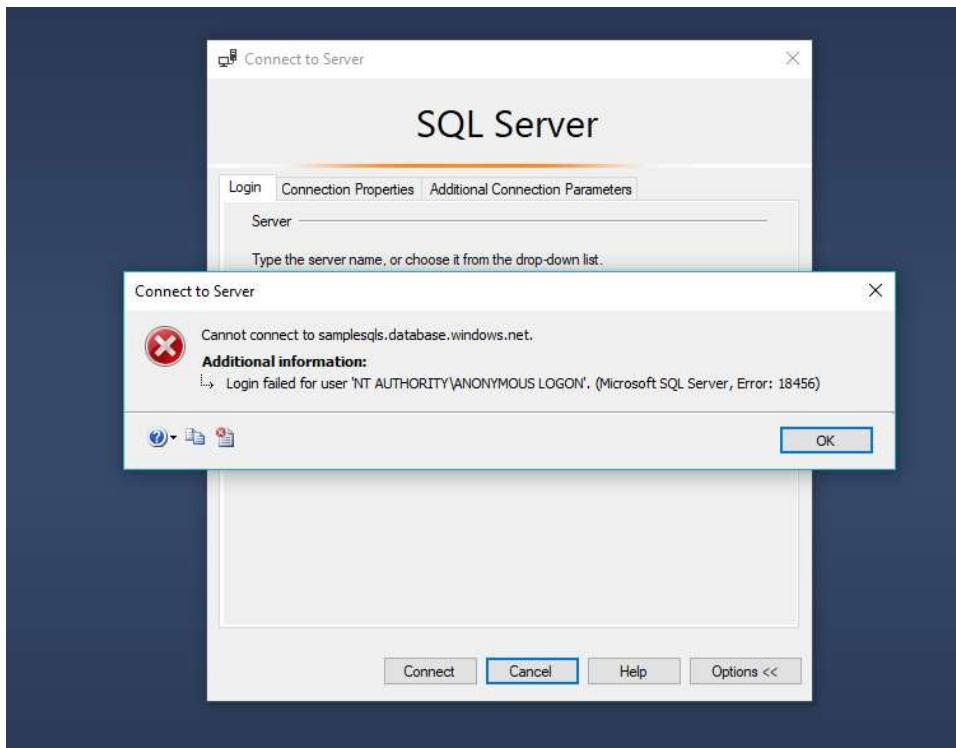
A security policy defines the desired configuration of your workloads and helps ensure compliance with company or regulatory security requirements. In Azure Security Center, you can

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:

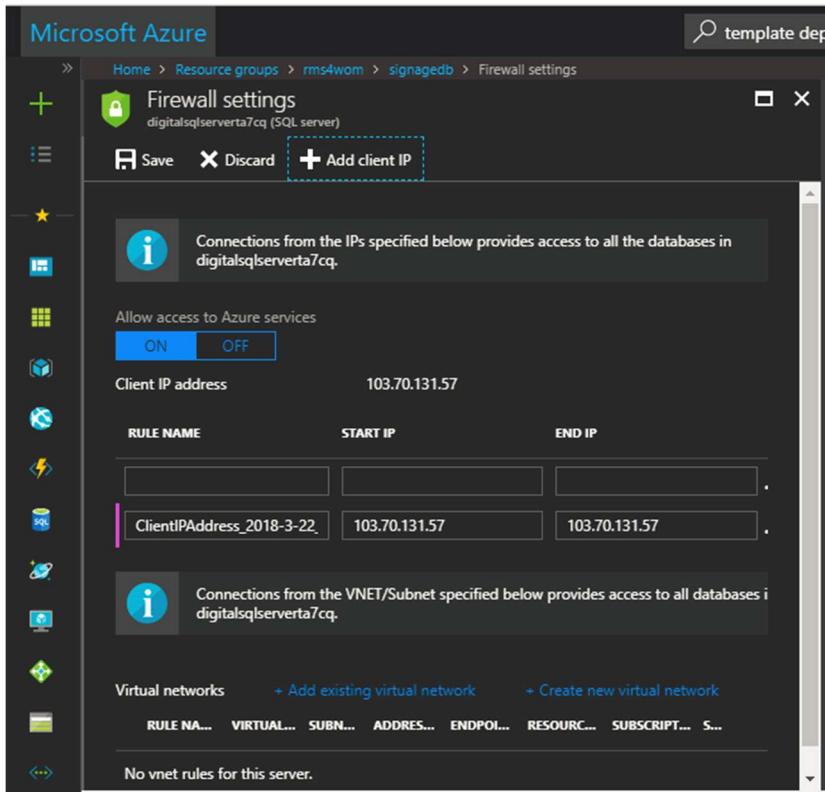
- Data collection
- Security policy
- Email notifications
- Pricing tier

16. Access SQL Database using Active Directory



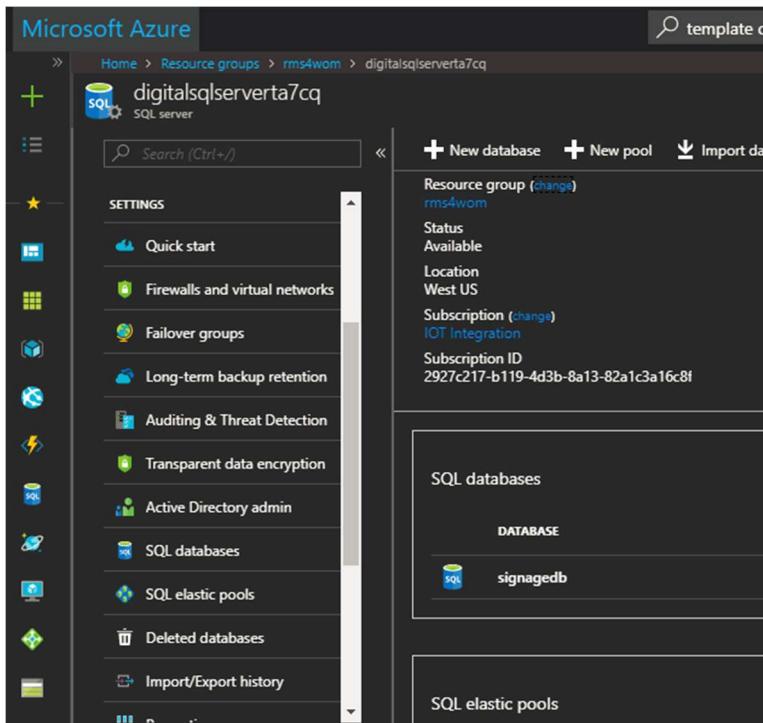
To Enable Firewall settings:

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.



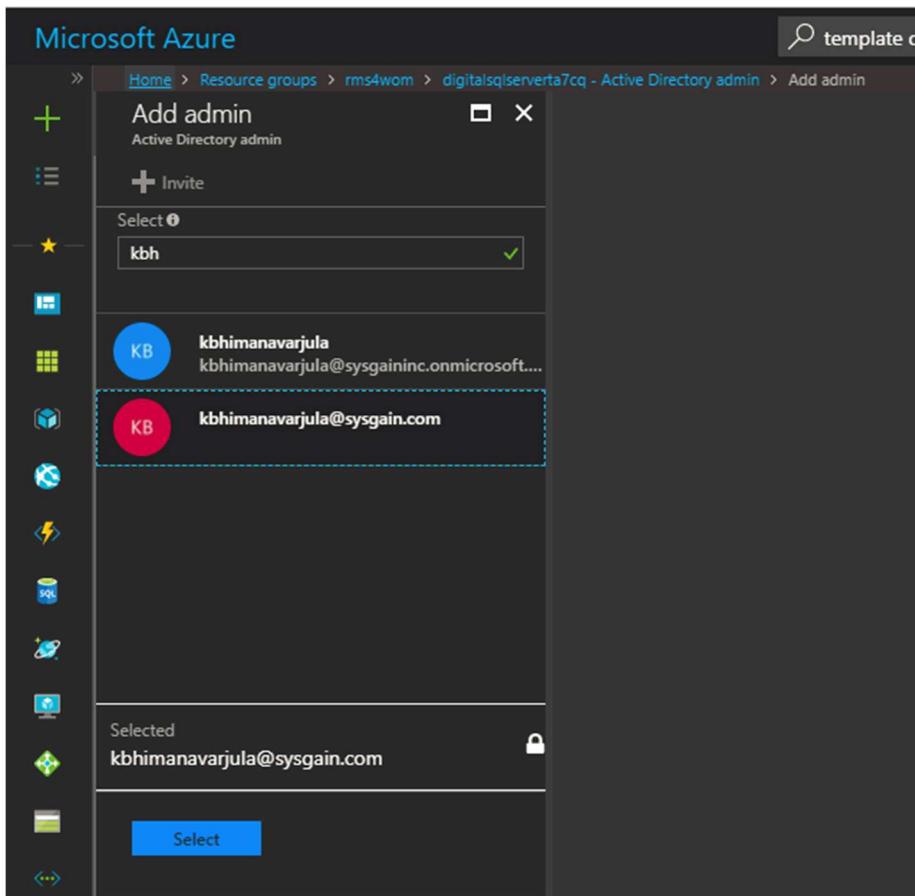
2. Select your **Sql Server** from the **Azure Portal** and click **Active Directory Admin**

RMS Hardening

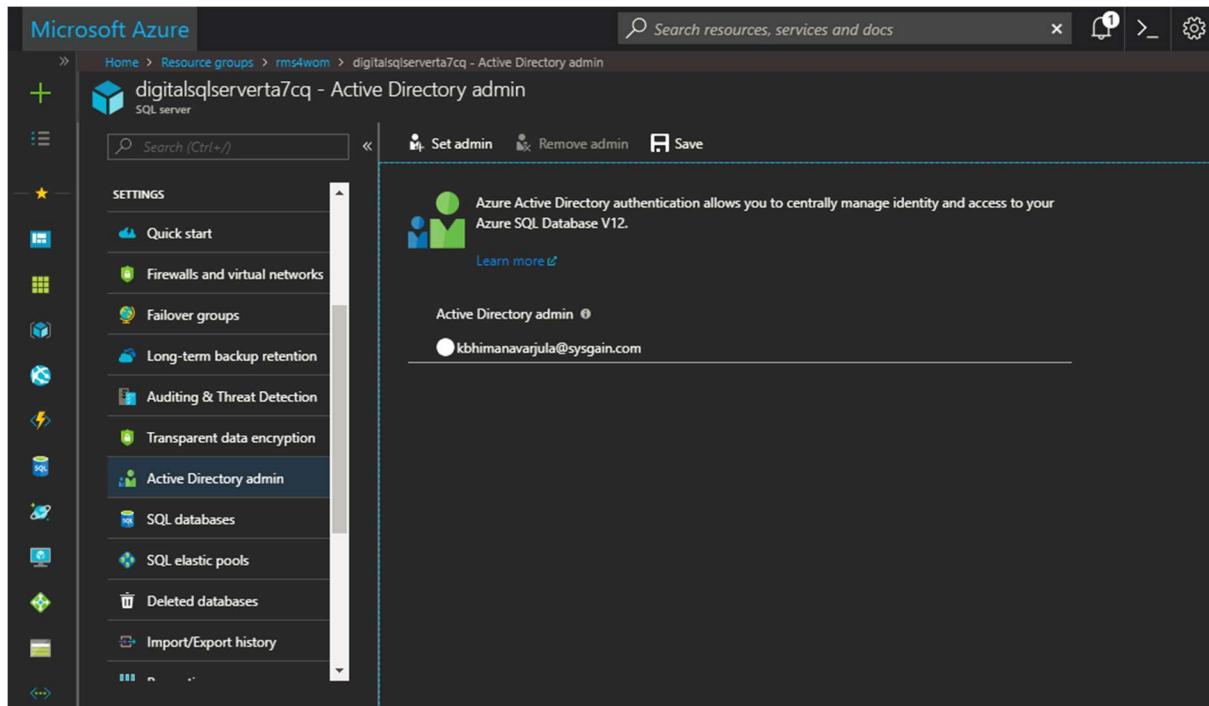


The screenshot shows the Microsoft Azure portal interface for managing a SQL server named 'digitalsqlserverta7cq'. The left sidebar lists various service icons. The main content area displays the 'SETTINGS' section for the resource group 'rms4wom'. It includes details like 'Status: Available', 'Location: West US', and 'Subscription: IOT Integration'. Under the 'SQL databases' section, there is one database listed: 'signagedb'. Other sections visible include 'Firewalls and virtual networks', 'Failover groups', 'Long-term backup retention', 'Auditing & Threat Detection', 'Transparent data encryption', 'Active Directory admin', 'SQL databases', 'SQL elastic pools', and 'Deleted databases'.

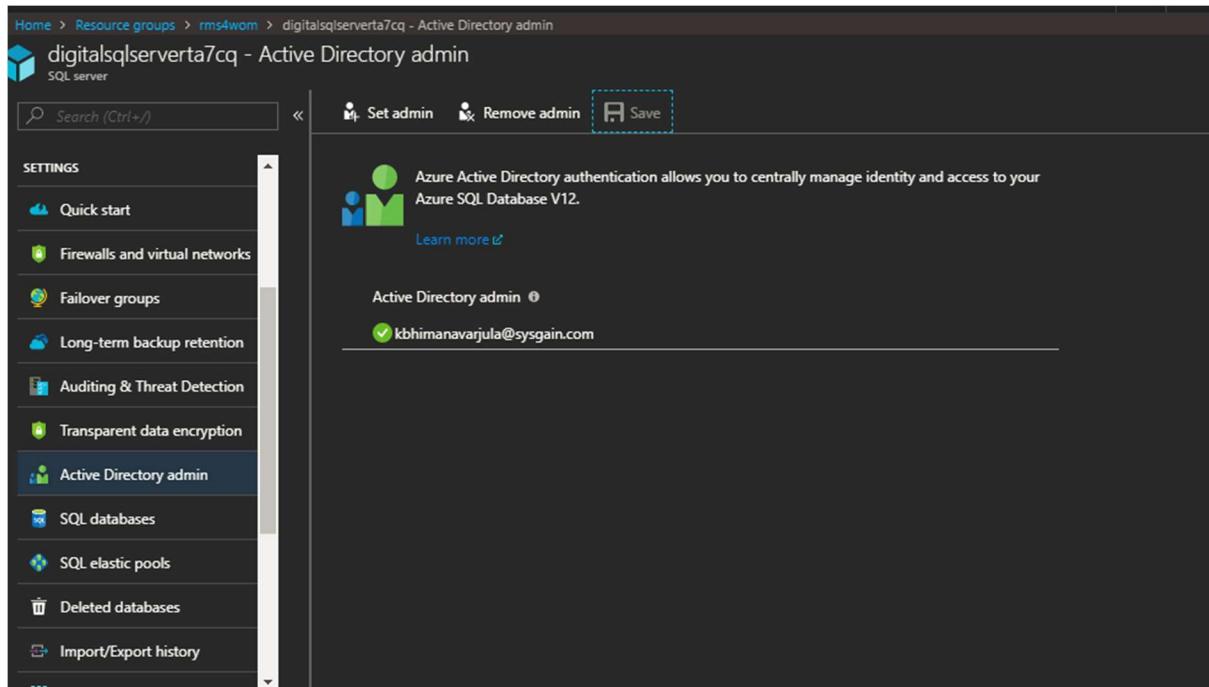
3. Select the **Admin Id** as shown in the following figure and click **Set Admin** and **Save**



The screenshot shows the 'Add admin' dialog in the Microsoft Azure portal. The user has selected the 'Active Directory admin' option. In the 'Select' input field, the name 'kbh' is typed, and a dropdown list shows two entries: 'kbhimanavarjula' and 'kbhimanavarjula@sysgaininc.onmicrosoft.com'. The second entry is highlighted with a red circle containing 'KB'. Below the list, the 'Selected' section shows 'kbhimanavarjula@sysgain.com' with a lock icon. At the bottom, there is a blue 'Select' button.

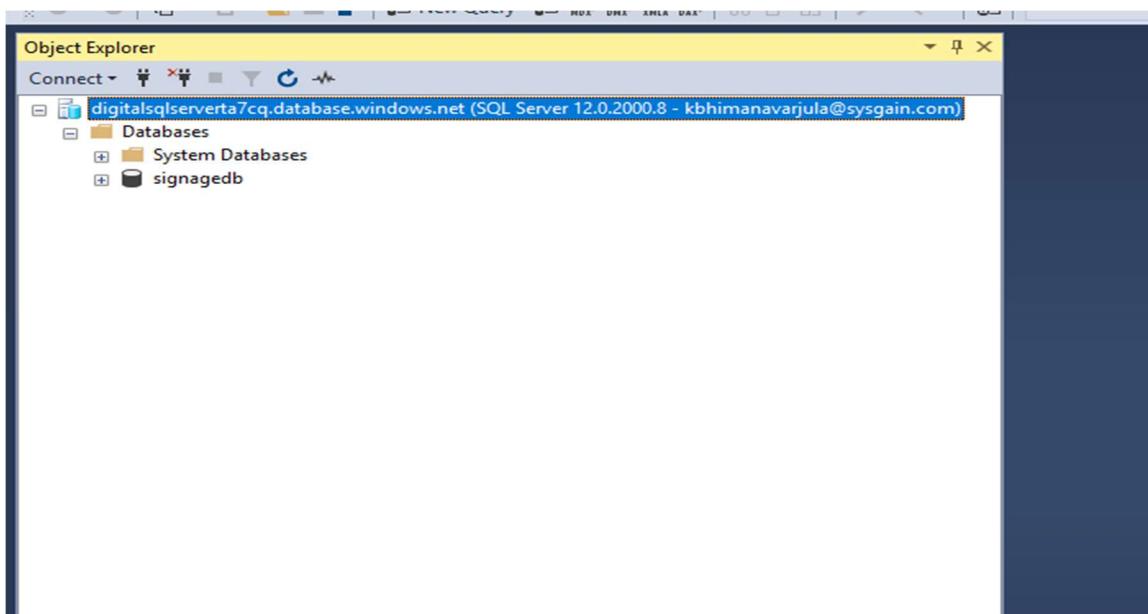
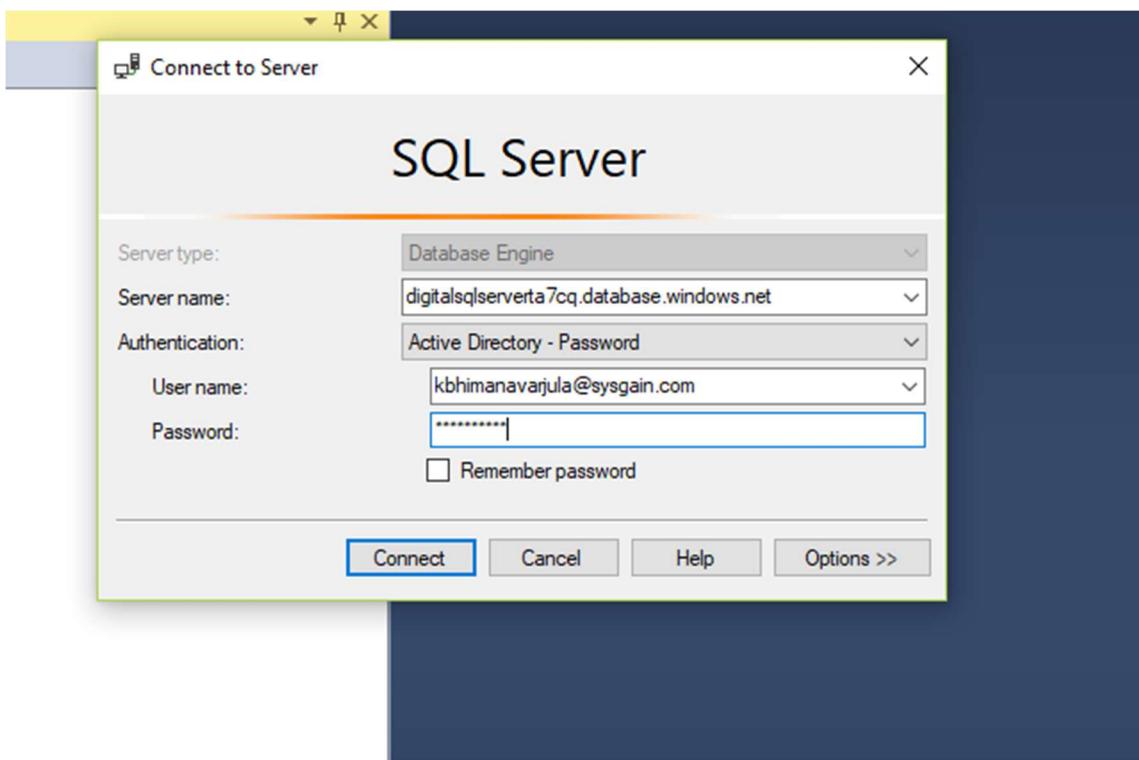


The screenshot shows the Microsoft Azure portal interface. The left sidebar lists various service icons. The main content area shows a resource named "digitalsqlserverta7cq - Active Directory admin". The "SETTINGS" menu on the left has several options: Quick start, Firewalls and virtual networks, Failover groups, Long-term backup retention, Auditing & Threat Detection, Transparent data encryption, Active Directory admin (which is selected and highlighted in blue), SQL databases, SQL elastic pools, Deleted databases, and Import/Export history. At the top right, there are buttons for "Set admin", "Remove admin", and "Save". Below the "Active Directory admin" section, it says "Azure Active Directory authentication allows you to centrally manage identity and access to your Azure SQL Database V12." and provides a "Learn more" link. A user email "kbhimanavarjula@sysgain.com" is listed as an Active Directory admin.



This screenshot is identical to the one above, showing the Microsoft Azure portal interface for managing the Active Directory admin settings of a SQL server. The "Active Directory admin" section is highlighted, and the "Save" button is visible. The user "kbhimanavarjula@sysgain.com" is listed as an Active Directory admin with a green checkmark next to their name.

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