

# DEPLOYMENT AND CONFIGURATION GUIDE

## TABLE OF CONTENTS

1	DEPLOYING TO PILOT ENVIRONMENT (AZURE SUBSCRIPTION) .....	2
1.1	DEPLOYMENT STEPS.....	2
1.2	POST DEPLOYMENT STEPS .....	2
1.3	Create the AD application by running the ServicePrincipal.ps1.....	3
1.4	Configure AD App:.....	5
1.5	SETTING UP THE WEB APPLICATION (BY A SERVICE ADMIN) .....	8
1.6	Install OMS Dashboards VIEWS.....	9
1.7	VERIFICATION OF DEPLOYMENT .....	13

# DEPLOYMENT AND CONFIGURATION GUIDE

## 1 DEPLOYING TO PILOT ENVIRONMENT (AZURE SUBSCRIPTION)

### 1.1 DEPLOYMENT STEPS

1. Create an Automation account with RunAs Service principal. Unfortunately ARM templates don't allow for creating AD service principals as yet, so this step is currently a manual.
  - Refer the blog <https://azure.microsoft.com/en-us/documentation/articles/automation-secconfigure-azure-runas-account/> for the steps.
  - Creation of ServicePrincipal has a propensity to fail randomly. A basic verification whether it was successfully created is **mandatory**
2. Capture the AutomationAccount name and the resourcegroup. You will need them as parameters when you 'Deploy to Azure'
3. Deploy Arm template from this location <https://github.com/AvyanConsultingCorp/azure-quickstart-templates/tree/master/azure-governancecloudwise>
4. Note the URL of the Cloudwise App Service

### 1.2 POST DEPLOYMENT STEPS

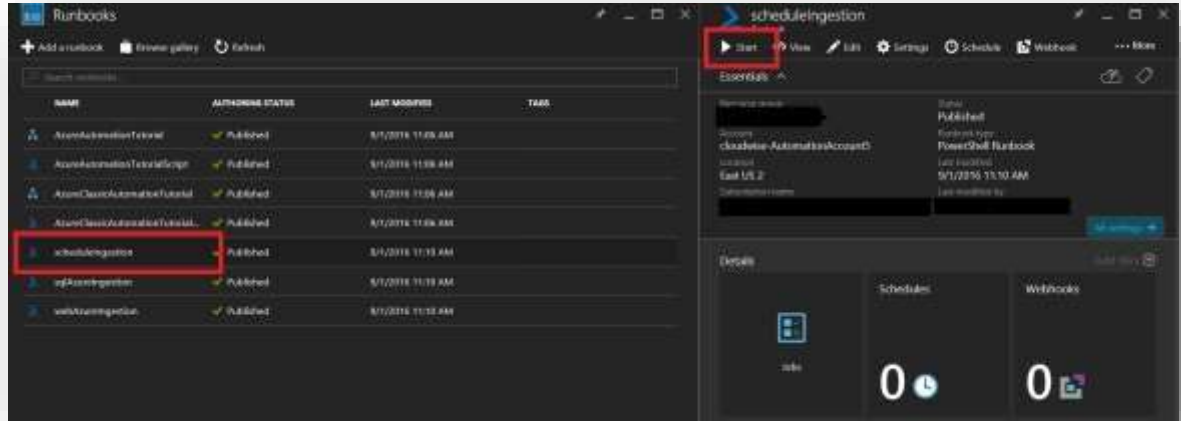
Congratulations !

You have now successfully deployed the application. You will have to do a few additional steps to have the application configured

(by a **Service Admin** only)

- Click open the scheduleIngestion runbook and click start to run the runbook. This step will kickstart the data ingestion to the OMS workspace specified.

# DEPLOYMENT AND CONFIGURATION GUIDE



## 1.3 CREATE THE AD APPLICATION BY RUNNING THE SERVICEPRINCIPAL.PS1.

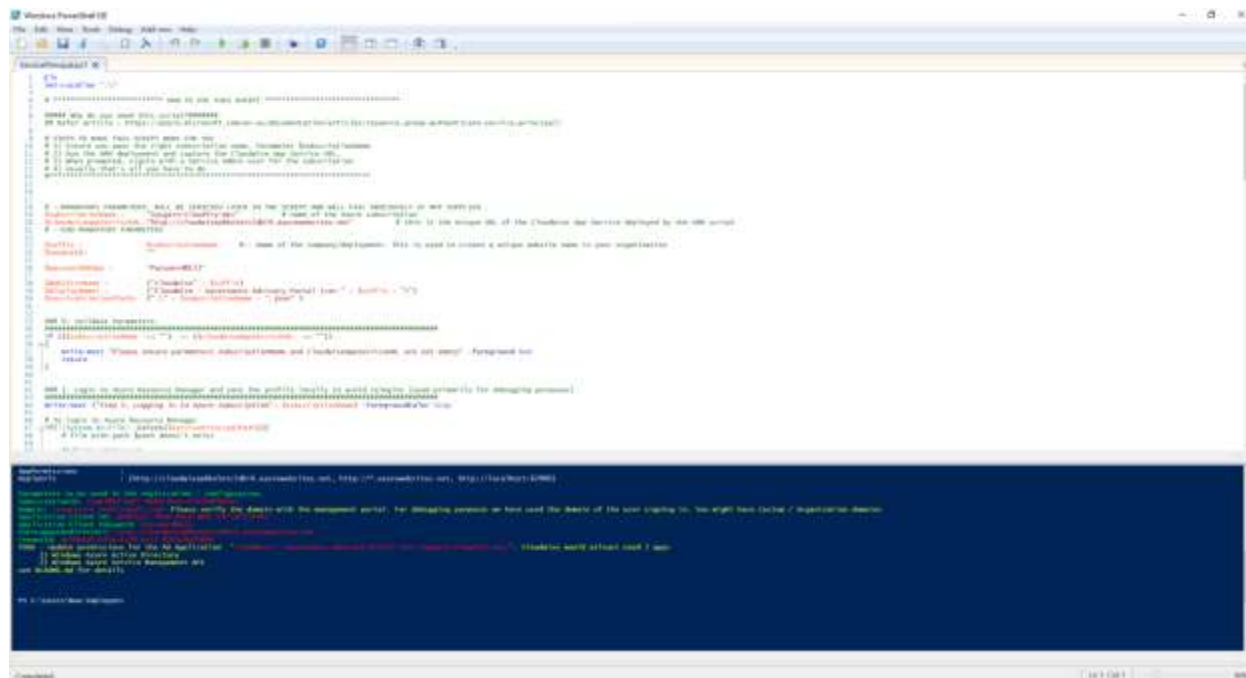
As ServicePrincipals can't yet be created in ARM json templates, one has to run this manually outside the deployment.

```
6 ##### why do you need this script?#####
7 ## Refer article - https://azure.microsoft.com/en-us/documentation/articles/resource-group-authenticate-service-principal/
8
9
10 # STEPS TO MAKE THIS SCRIPT WORK FOR YOU
11 # 1) Ensure you pass the right subscription name. Parameter $subscriptionName
12 # 2) Run the ARM deployment and capture the Cloudwise App Service URL
13 # 3) When prompted, sign in with a Service Admin user for the subscription
14 # 4) Usually that's all you have to do
15
16
17
18 # --MANDATORY PARAMETERS. WILL BE VERIFIED LATER IN THE SCRIPT AND WILL FAIL GRACIOUSLY IF NOT SUPPLIED
19 $subscriptionName = "" # name of the Azure subscription
20 $cloudwiseAppServiceURL = "" # this is the unique URL of the Cloudwise app service deployed by the ARM script
21 # --END MANDATORY PARAMETERS
22
23
```

- Edit the serviceprincipal.ps1 (in Powershell\_ise)
- You will need to supply subscriptionName and the deployed URL of the CloudWise App Service.
- Capture the output. You will need it in subsequent steps.

**PLEASE REFER TO PARAMETER DESCRIPTIONS IF YOU NEED MORE INFORMATION ON WHAT NEEDS TO BE PROVIDED AS AN INPUT.**



# DEPLOYMENT AND CONFIGURATION GUIDE



# DEPLOYMENT AND CONFIGURATION GUIDE

## 1.4 CONFIGURE AD APP:

- In Azure Portal search for Azure Active directory. Open the “App Registrations” tab
- Open the AD Application that you just created. It should start with the name “CloudWise - Governance Advisory Portal”
- Configure the following permissions in the “Required Permissions” tab
- List of Permissions

Category	Permission
Windows Service Management API	
Microsoft.Azure.ActiveDirectory	
Microsoft Graph API	Application Permissions

# DEPLOYMENT AND CONFIGURATION GUIDE









Delegated Permissions

# DEPLOYMENT AND CONFIGURATION GUIDE

DELEGATED PERMISSIONS		REQUIRES ADMIN
<input type="checkbox"/>	Edit or delete items in all site collections	<input type="checkbox"/> No
<input type="checkbox"/>	Read and write user and shared tasks	<input type="checkbox"/> No
<input type="checkbox"/>	Read user and shared tasks	<input type="checkbox"/> No
<input type="checkbox"/>	Read and write user and shared contacts	<input type="checkbox"/> No
<input type="checkbox"/>	Read user and shared contacts	<input type="checkbox"/> No
<input type="checkbox"/>	Read and write user and shared calendars	<input type="checkbox"/> No
<input type="checkbox"/>	Read user and shared calendars	<input type="checkbox"/> No
<input type="checkbox"/>	Send mail on behalf of others	<input type="checkbox"/> No
<input type="checkbox"/>	Read and write user and shared mail	<input type="checkbox"/> No
<input type="checkbox"/>	Read user and shared mail	<input type="checkbox"/> No
<input checked="" type="checkbox"/>	Sign in and read user profile	<input type="checkbox"/> No
<input type="checkbox"/>	Read and write access to user profile	<input type="checkbox"/> No
<input checked="" type="checkbox"/>	Read all users' basic profiles	<input type="checkbox"/> No
<input checked="" type="checkbox"/>	Read all users' full profiles	<input checked="" type="checkbox"/> Yes
<input type="checkbox"/>	Read and write all users' full profiles	<input checked="" type="checkbox"/> Yes
<input checked="" type="checkbox"/>	Read all groups	<input checked="" type="checkbox"/> Yes
<input type="checkbox"/>	Read and write all groups	<input checked="" type="checkbox"/> Yes
<input checked="" type="checkbox"/>	Read directory data	<input checked="" type="checkbox"/> Yes
<input checked="" type="checkbox"/>	Read and write directory data	<input checked="" type="checkbox"/> Yes
<input checked="" type="checkbox"/>	Access directory as the signed in user	<input checked="" type="checkbox"/> Yes

# DEPLOYMENT AND CONFIGURATION GUIDE

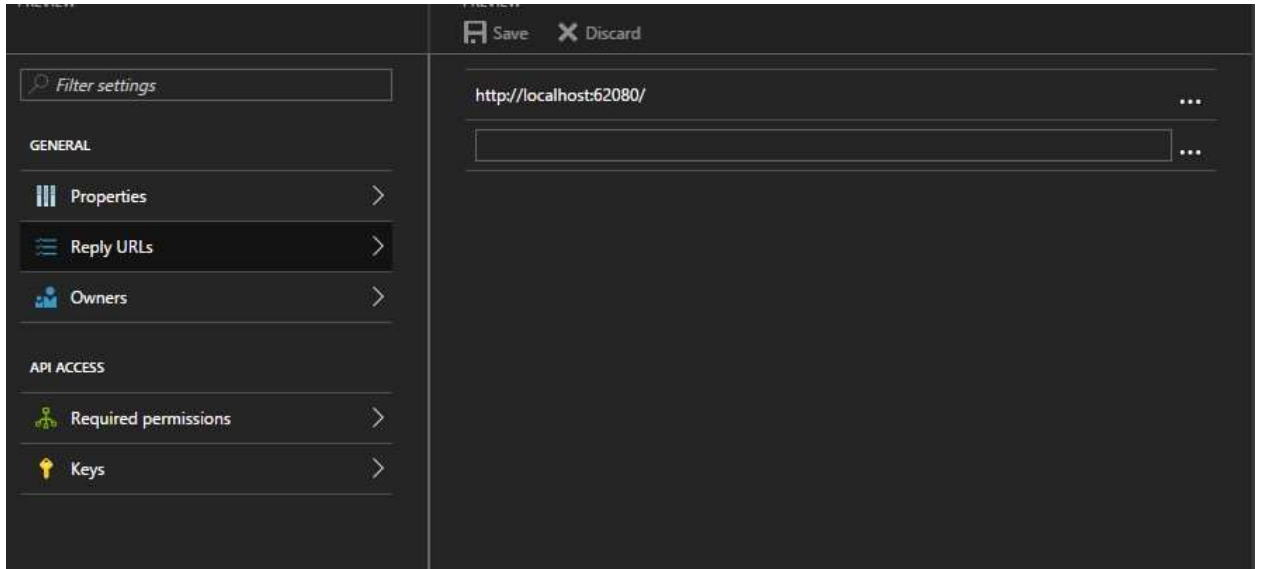
	Read items in all site collections	 No
	Sign users in	 No
	Access user's data anytime	 No
	Read users' relevant people lists (preview)	 No
	Create pages in user notebooks (preview)	 No
	Limited notebook access (preview)	 No
	Read user notebooks (preview)	 No
	Read and write user notebooks (preview)	 No
	Read all notebooks that the user can access (preview)	 No
	Read and write notebooks that the user can access (preview)	 No
	Read user tasks	 No
	Create, read, update and delete user tasks and projects (preview)	 No
	View users' email address	 No
	View users' basic profile	 No
	Read and write user mailbox settings (preview)	 No
	Read identity risk event information	 Yes

## 1.5 SETTING UP THE WEB APPLICATION (BY A SERVICE ADMIN)

1. **Ensure:** Reply url of the application is configured in the AD application. If you have done the above steps, you don't have to do this. This is just a precautionary step for operations team who deploy multiple web applications to the same AD Application.



# DEPLOYMENT AND CONFIGURATION GUIDE



2. Open Portal and then you get an initial screen where you need to put subscription id, Client Application ID and Client secret and then press submit.
3. After submit you will be redirect to AD login page where you need to input your active directory url and then press GO.
4. After this you need to input your LiveID credentials and after successfully login you will be redirect to Rule page where you can see all rules and submit rules.

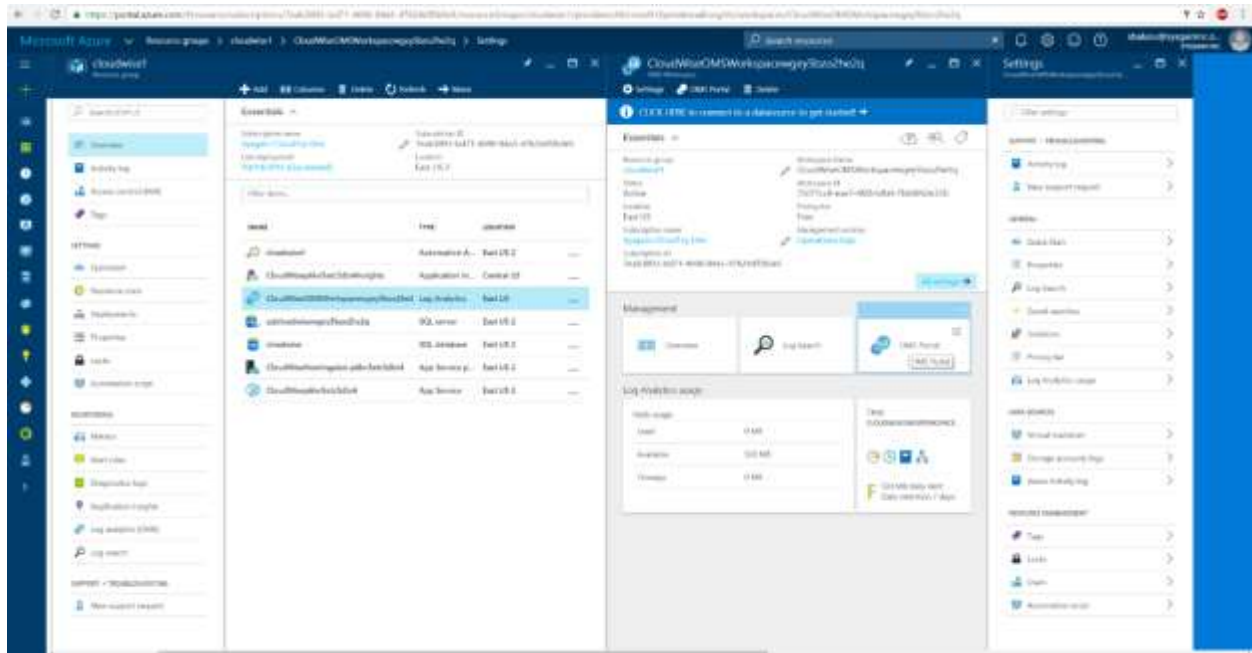
## 1.6 INSTALL OMS DASHBOARDS VIEWS.

This is currently a manual process as ARM json deploys do not yet support creation of OMS views.

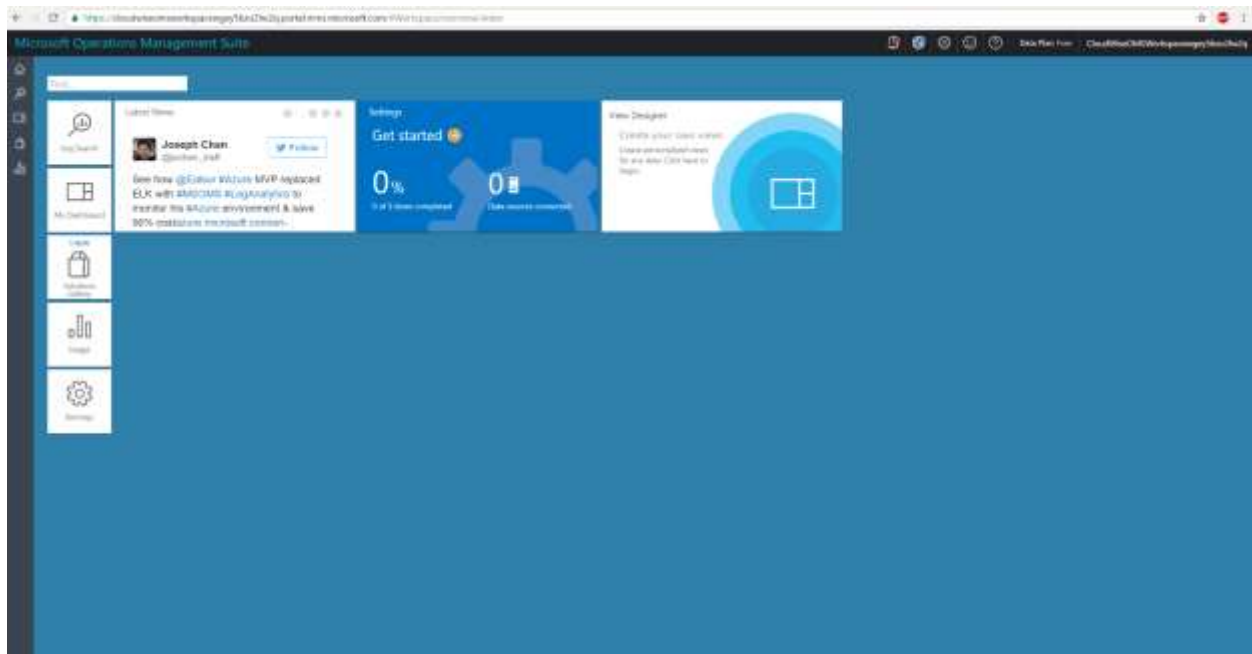
(By a ServiceAdmin/Contributor role)

1. Open the resource group and click on the OMS Portal link. This will open the OMS portal in a different window

# DEPLOYMENT AND CONFIGURATION GUIDE

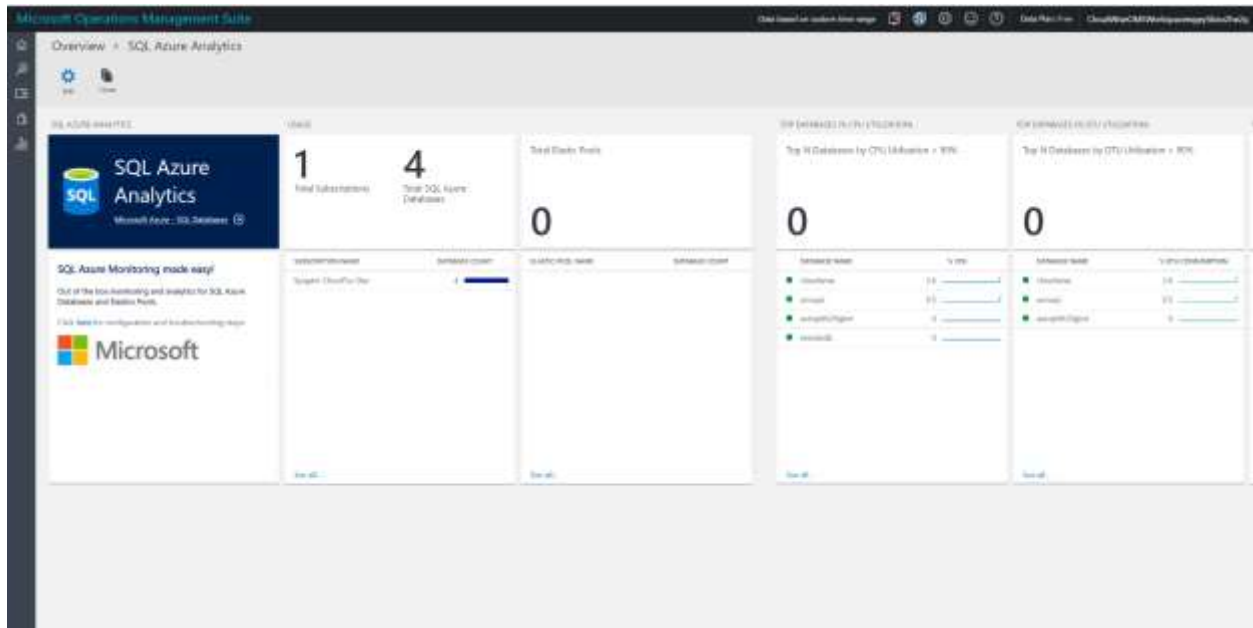
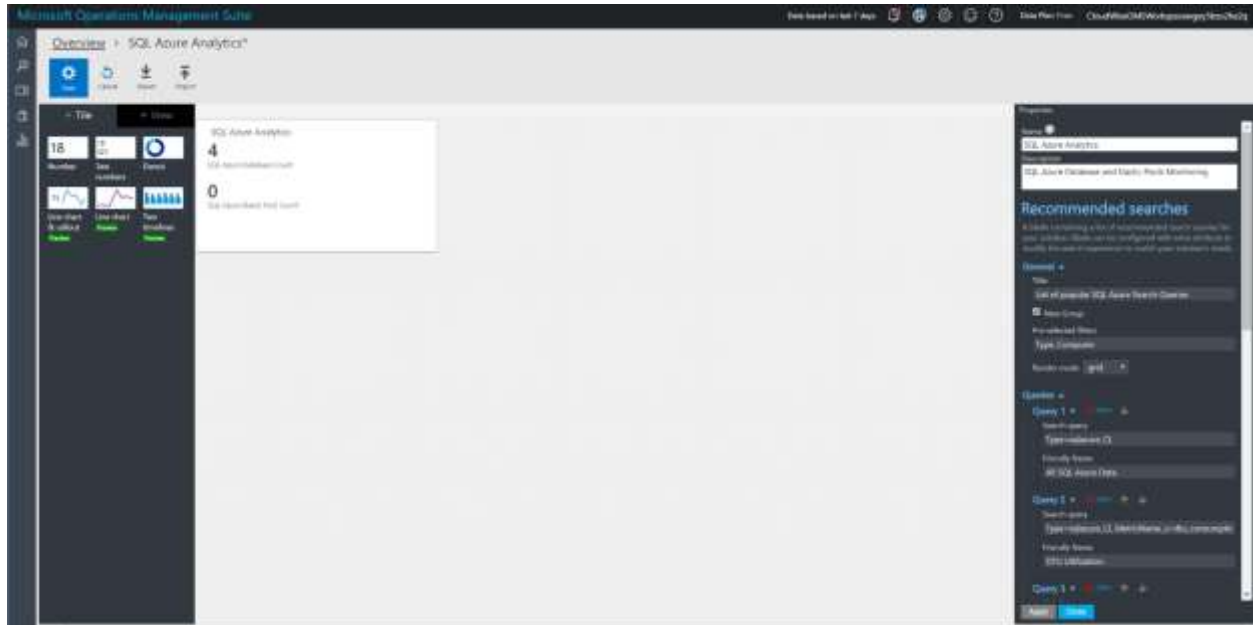


2. Click on the View Designer



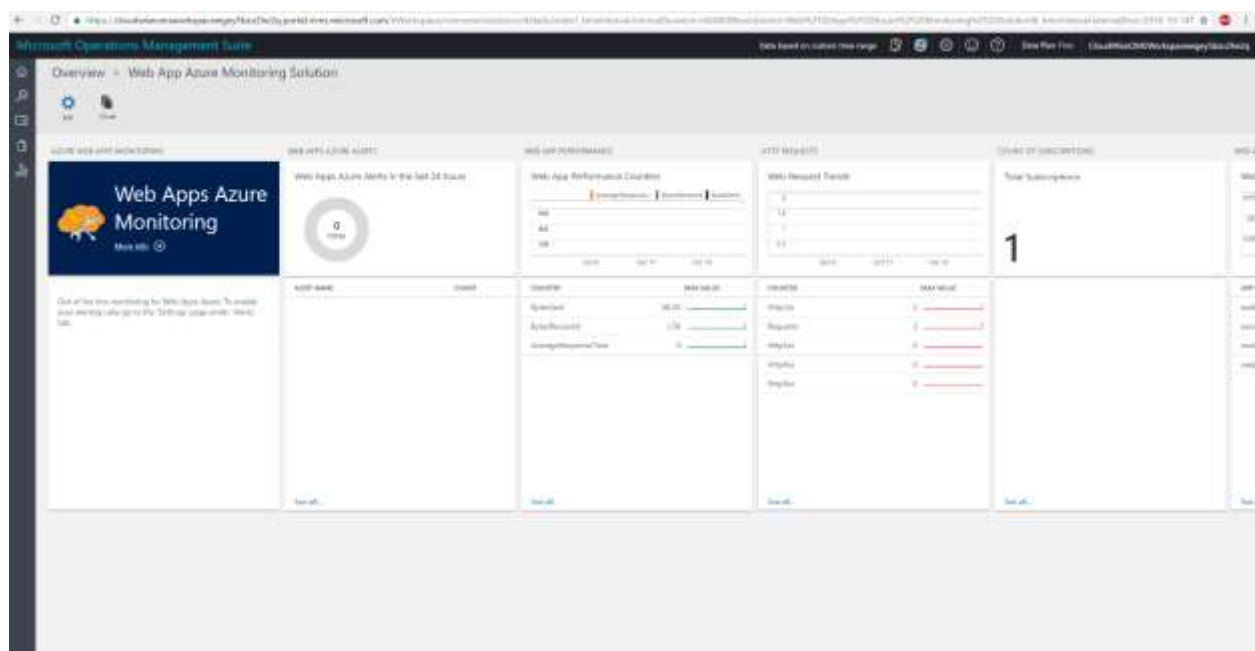
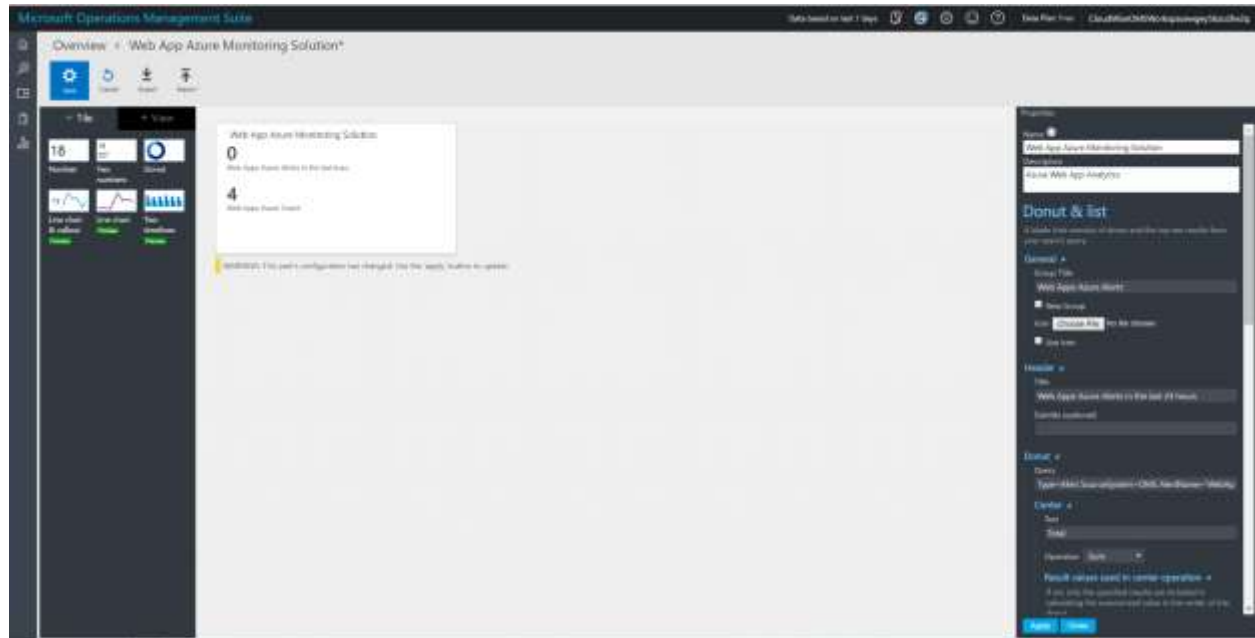
3. Import SQL DB view by clicking on the Import button and browsing to the file (OMSAzureDashboards\OMSSQLDBAzureMonitoringSolution.omsview)

# DEPLOYMENT AND CONFIGURATION GUIDE



4. Repeat the same step for the Web App Monitoring dashboard. Import view OMSAzureDashboards\OMSWebAppAzureMonitoringSolution.omsview

# DEPLOYMENT AND CONFIGURATION GUIDE



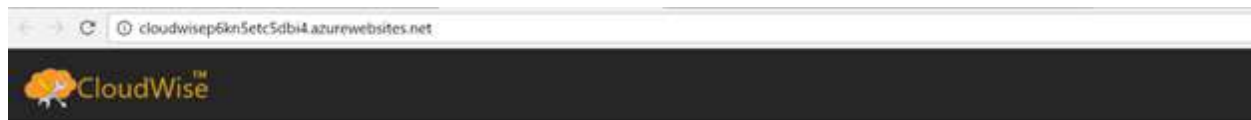
# DEPLOYMENT AND CONFIGURATION GUIDE

## 1.7 VERIFICATION OF DEPLOYMENT

### 1. Application Verification

- Login to the Azure portal
- Navigate to the App Service URL

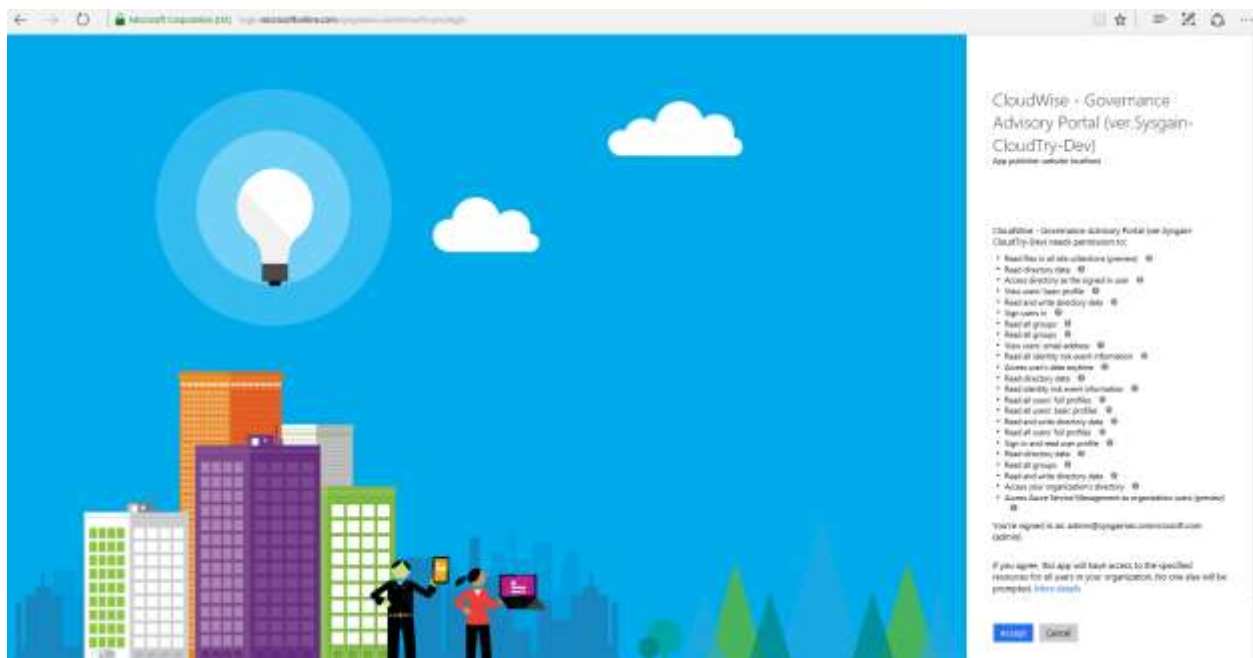
You should be able to see the following screen



### SUBSCRIPTION REGISTRATION SETTINGS

Subscription Id	<input type="text" value="REDACTED"/>
Current Offer	Pay-As-You-Go
Application Client Id	<input type="text" value="REDACTED"/>
Application Password	<input type="password" value="REDACTED"/>
Notification Email IDs	<input type="text" value="REDACTED"/>
<input type="button" value="Submit"/>	

Subsequent steps should lead you to a signin (**please signin with a ServiceAdmin Credential**)



# DEPLOYMENT AND CONFIGURATION GUIDE

CloudWave

Outbound | Rules Settings | Subscription Settings

Hi! admin@company.com | Sign out

GOVERNANCE RULES

Please configure the rules that need to be prioritized for frequent runs. By default all available rules for your license configuration are selected.

STANDARD RULES

select

Rule Name

☐

Are you on a cost-effective subscription?

☐

Do you have a target deployment for staging and testing rules that is not limited self?

☐

Are your dev/test environments configured for auto-deployment?

ADVANCED RULES (1/1/2021 / 2021/01/01)

select

Rule Name

☐

Have you configured Application / availability settings before deployment?

☐

Are you running any of them?

☐

Is your deployment architecture protected by Azure IAM (e.g. most rules) standard?

☐

Have you configured your monitoring agent?

☐

Are you configuring logging and/or alerting?

☐

Do you have auto-scaling configured that triggers on the basis of time or last 10 days?

ADDITIONAL RULES

select

Rule Name

☐

Are you using the latest auto-control (MPC) configuration?

Submit