Addendum 1 to Open edX Deployment Guide

Table of Contents

Based on feedback from partners and our own testing, we have made the following changes to deployment guide and process

1. Deployment status emails configurations:

We have worked on this issue and verified that Office 365 emails and gmail smtp settings are working now. Please follow the following guidance for configuring the email to receive deployment notifications.

Third-Party SMTP Relay - Gmail & O365

During the STAMP deployment, we allow users to provide an SMTP relay that will allow them to relay deployment notification and other system emails to the cluster administrative user(s). It has come to attention that this doesn't work well with third-party email providers like Google or Outlook/O365. Therefore, we have made additional updates to support two providers: Gmail & O365.

There are five (5) deployment email parameters (see STEP 3 above):

- – this is any address or distribution list where you'd like all notification emails will be sent
- – this is the SMTP server fully qualified address
- – this is the communication port on the SMTP server specified above
- – this is the user name to authenticate with on the SMTP server specified above

- – this is the corresponding password for authentication

Server Settings

O365 Settings

The SmtpServer & SmtpServerPort details for O365 can be found here:

https://support.office.com/en-us/article/POP-and-IMAP-settings-for-Outlook-Office-365-for-business-7fc677eb-2491-4cbc-8153-8e7113525f6c

(see the “POP and IMAP settings for Office 365 for business email” section)

The SmtpServer & SmtpServerPort details for GMAIL can be found here:

https://support.google.com/a/answer/176600?hl=en

(see the “Use the Gmail SMTP Server” section)

User Credentials

The is typically the email address of the account with SMTP relay access. This applies to both Gmail and O365.

:

for O365, this is the password of the account with SMTP relay access.

for Gmail, this is an application password (see more details below)

Gmail Settings

If you are using Gmail, the password for the email address you are using for SmtpAuthenticationUser will not work. You must instead create and use an App Password that is associated with the email address. Creating this application password has a pre-requisite: your account must have 2-Step Verification enabled. Here’s how to configure your account:

Enable 2-Step Verification (pre-requisite): https://support.google.com/accounts/answer/185839?hl=en

Create an App Password: https://support.google.com/accounts/answer/185833?hl=en (see the “How to generate an App password” section)

Examples

O365: I have an office 365 account oxa-admin@contoso.com. To login to this account, I use the following password: 123@contoso_com. I'd however like to send all notifications to oxanotifications@contoso.com which is a distribution list to my engineering team.

My OXA deployment email parameters would be:

Gmail: I have a Gmail account oxa-admin-team1@gmail.com. To login to this account, I use the following password: 123@contoso_com. I want to send all notifications to oxanotifications-team1@gmail.com. I also need a separate App password which I generated as eekqiutsqrvliube under my "oxa-admin-team1@gmail.com" account.

My OXA deployment email parameters would be:

2. Core quota limits have exceeded

Message=Operation results in exceeding quota limits of Core. Maximum allowed: 10, Current in use: 5, Additional requested: 12.

This error typically is shown if your subscription doesn't have capacity support enough cores. You should file a ticket with Azure to increase more VM Capacity (cores) to your subscription.

3. How to access the VMs after deployment

Accessing the VMs is done via SSH. There is only one entry point and that is the jumpbox.

It is assumed you have logged into the azure portal (portal.azure.com) and selected your target azure subscription.

Here's how to proceed:

1. From the azure portal, click on resource groups icon and select the resource group you created as part of the bootstrap. It will be the name of your cluster ([Cluster Name] deployment variable).
2. From within the list of resources, search for "**jb**".
3. The search should return a list of resources associated with your jumpbox.
4. Click on the resource named "[**Cluster Name**]**-jb-ip**" and copy the value of its DNS Name.
5. From your bash console type the following:
    a. **ssh [the admin user name from your parameters.json file @[domain name of your jumpbox] -i [path to your ssh private key that was generated in Step 2.3.2]**
6. This should log you into the jumpbox

Once you have access to the jump box, all other servers will be available via the private network. If you'd like to access a specific machine, do the following:

- From the azure portal, click on resource groups icon and select the resource group you created as part of the bootstrap. It will be the name of your cluster ([Cluster Name] deployment variable).
- From within the list of resources, search for "**vnet**".
- The search should return the Virtual Network Resource named "[Cluster Name]-vnet"
- Click on the Virtual Network Resource. It should list all network interfaces (NICs) associated with all resources connected to your virtual network. These are private ip addresses. For the lms/cms frontend, the resource will be named like **"[Cluster Name]-vmss-[deploymentVersionId from your parameters.json file]"**

- Once you determine which NIC you'd like to connect to, do the following:
    - **ssh [IP Address]**

      where [**IP Address**] is the private ip address of the NIC associated with server you'd like to connect to.

4. I am seeing degrading status on the VMs in the Azure portal

This typically means something went wrong with the deployment. The only way to know the details of error is to have correct email configuration where you will see notifications and details of failed deployments. Please see #1 item in this document on configuring emails correctly

5. Where do I specify the service passwords?

We have added an additional parameter to command line section 3.2.3 to specify the service account password. Please make sure that this password doesn't have any non-alpha numeric characters. Mongo

DB has some restrictions. The default password we used earlier has been changed to take this into account.

[Enlistment Root]\oxa-tools\scripts\Deploy-OxaStamp.ps1 -AzureSubscriptionName [Subscription Name] -ResourceGroupName [Cluster Name] -Location "central us" -TargetPath "[Enlistment Root]\oxa-tools\config\stamp\default" -AadWebClientId <AAD web client ID from Azure> -AadWebClientAppKey <AAD web client app key from Azure> -AadTenantId <AAD tenant id> -KeyVaultDeploymentArmTemplateFile "[Enlistment Root]\oxa-tools\templates\stamp\stamp-keyvault.json" -FullDeploymentParametersFile "[Enlistment Root]\oxa-tools\config\stamp\default\parameters.json" -FullDeploymentArmTemplateFile "[Enlistment Root]\oxa-tools\templates\stamp\stamp-v2.json" -ClusterAdministratorEmailAddress [Your Email Address] -SmtpServer <SMTP server name> -SmtpServerPort <SMTP server port> -SmtpAuthenticationUser <SMTP auth user> -SmtpAuthenticationUserPassword <SMTP auth user password> -ServiceAccountPassword <Service Account Password>