**Azure Migration with PaaS Hosting**

The following are the generalized steps to migrate the application to azure PaaS

Contents

[Introduction 2](#_Toc507166013)

[1. SSID (Source Server ID) 2](#_Toc507166014)

[2. RFS Request: 2](#_Toc507166015)

[3. RG Creation: 2](#_Toc507166016)

[4. Source Code and DB backup movement to Cloud: 2](#_Toc507166017)

[5. Security considerations 2](#_Toc507166018)

[6. PaaS web application accessible to PUBLIC 3](#_Toc507166019)

[7. Azure AD: 3](#_Toc507166020)

[8. Reply URL request 3](#_Toc507166021)

[9. Service Accounts Creation: 3](#_Toc507166022)

[10. AD Groups Creation and Addition of Members: 3](#_Toc507166023)

[11. PaaS DB restore process 3](#_Toc507166024)

[12. DB and Application Access: 4](#_Toc507166025)

[13. Internal and External DNS requests 4](#_Toc507166026)

[14. Application insights configuration 4](#_Toc507166027)

[15. Unit Test: 4](#_Toc507166028)

[16. Smoke Test: 4](#_Toc507166029)

[17. Application Security Scan: 4](#_Toc507166030)

[18. Application Security Re-Scan: 5](#_Toc507166031)

[19. Internal UAT 5](#_Toc507166032)

[20. UAT 5](#_Toc507166033)

[21. SSL request process 5](#_Toc507166034)

[22. Transition/Application Handover: 5](#_Toc507166035)

[23. CAB approval: 5](#_Toc507166036)

# Introduction

This document and steps will be followed to host the MS .Net application in azure PaaS platform.

# SSID (Source Server ID)

* 1. If we does not have a SSID for a resource planning to create in azure we need to get it before raising RFS request. It’s a pre-requisite for raising a RFS request.
  2. Take the support from infrastructure team to create the SSID, they will connect with DuPont to create it (POC - "Elizabeth H. D'Wolf" [elizabeth.h.dwolf@accenture.com](mailto:elizabeth.h.dwolf@accenture.com)).

# RFS Request:

Take to template under templates folder of below path and send the filled template to infrastructure team to raise a RFS (Request for server) demand.

<https://knowmax3.ultimatix.net/sites/dupont-reln/DRP/MergeAndSpin/Shared%20Documents/AzureDupont%20Documents/Templates/v6.0%20SpeCo%20RG%20Request.xlsx?Web=1>

# RG Creation:

* 1. Resource Group (RG) request is created after getting the approvals for the RFS, sometimes based on the demand we can initiate it parallel. The Resource Group consists of all the resources that can be used for hosting an application.
  2. Contact infrastructure team for resource creation based on the application need by considering RFS request approval. Below is the path for RG template.

<https://knowmax3.ultimatix.net/sites/dupont-reln/DRP/MergeAndSpin/Shared%20Documents/AzureDupont%20Documents/Templates/v6.0%20SpeCo%20RG%20Request.xlsx?Web=1>

# Source Code and DB backup movement to Cloud:

* 1. Need to collect the source code and DB back up from the AMS team by having proper approvals from the business owner
  2. Once the Source code is available with us, need to check-in to VSTS by organizing it to standard folder structure(like dev. and prod folders)
  3. After that we need to modify the code compatible with azure PaaS platform like updating the code with latest framework, implementing changes related to authentication... etc.
  4. DB restoration after migration it to latest versions

# Security considerations

Refrain from including any sensitive information (Passwords, Keys, certificates etc...) in VSTS and use the Azure connection\app settings property to store the sensitive information.

# PaaS web application accessible to PUBLIC

In RG request we have to mention one of the field value - Internet Accessible as “YES”, based on this Dev Ops team will spin the resources accordingly.

# Azure AD:

(Follow this step only in case the application needs Azure AD authentication)

During ARM templates preparation need to ask Dev. Ops team to enable the active directory authentication for PaaS compatible application. At application end, in the application configuration file we have to update the authentication to “None” if any other type is mentioned.

# Reply URL request

Send a mail to clearing house team to get configured the reply URL’s, need to consider the DNS Name, Azure Web Application default URL. Below is the sample.

https://<<AzureWebApplicationdefaultURL>>/.auth/login/aad/callback

**Note**: Mention AD application registration name to identify the application uniquely with respect to environment to configure reply URL.

# Service Accounts Creation:

Send a request to clearing house group for creation of service accounts by following naming standards, we have to created dedicated accounts for development and production environments. Always we have to use service account to connect from application to DB specifically for SQL DB.

# AD Groups Creation and Addition of Members:

(For PaaS SQL Access)

Create Active Directory groups for SQL DB, send a request to clearing house group for creation of groups and addition of members in the respective groups, required 3-groups like READ, WRITE and ADMIN. Service account and DBA members also should be part of ADMIN groups in the respective environment. After AD groups creation and addition of members completed, with the help of dev. ops team re-run the ARM templates related to resources, this will allow AD groups to tag to SQL DB based on the RG name.

# PaaS DB restore process

Find the below link for detailed steps to get the SQL DB restored in PaaS SQL Server.

<https://knowmax3.ultimatix.net/sites/dupont-reln/DRP/MergeAndSpin/Shared%20Documents/AzureDupont%20Documents/Process%20Documents/PaaS%20SQL%20DB%20Restore%20Process%20V1.0.docx?Web=1>

# DB and Application Access:

After completion of above steps, you will be able to access the DB and application. Find the DB access process document in the below path.

<https://knowmax3.ultimatix.net/sites/dupont-reln/DRP/MergeAndSpin/Shared%20Documents/AzureDupont%20Documents/Process%20Documents/How%20to%20Connect%20to%20Database%20in%20Azure.docx?Web=1>

# Internal and External DNS requests

Finalize the DNS names based on the environment by confirming with application owner. After receiving the approval send a request to clearing house team to raise a request to create the proposed DNS names.

**Note:** For production, in case of same URL going to be used that is On-Prem, then we need to wait until cutover plan and its execution starts based on the change request.

Before sending any confirmation mail asking DNS names approval from business owner, please check their availability.

# Application insights configuration

We need to add the required dll’s to set up the application insights. After adding or downloading the dll’s from NuGet need to update the instrumentation in ApplicationInsights configuration file with <InstrumentationKey> tag. Instrumentation key could be found in azure portal under application insights section. Below is the link for more information –

<https://docs.microsoft.com/en-us/azure/application-insights/app-insights-asp-net>

# Unit Test:

As part of migration activity, developer has to perform one round of unit test to make sure all the functionality is working as expected.

# Smoke Test:

Testing team will perform one round of testing by comparing existing application behavior before moving to application security scan.

# Application Security Scan:

If we did not find any priority issues in smoke test, need to handover the application to application security scan, this scan should be allowed only development environment not in production. If required we have to give high level functionality KT to security scanning team. Once security scan is completed we will get the app scan report. Need to fix all the medium and high priority issues in app scan report.

# Application Security Re-Scan:

Code remediation for the app scan issues completed, need to send app for re-scan only for the fixed scenario not whole application. This will continue until we get sign off from the application security team.

# Internal UAT

After app scan sign off received we should plan internal UAT.

# UAT

UAT should be planned based on the internal UAT status, usually it should be done by end users or business owners of the application.

# SSL request process

Send a mail to Infra support team to raise a request for SSL, this needs to be initiate a week before the production cutover. The same certificate will be used for prod and dev.

Once installed the SSL certificate in any of the server, same can be exported and imported in any other server irrespective of environment.

# Transition/Application Handover:

Need to handover the application, database and infrastructure to respective teams-IMS, AMS and DBA.

# CAB approval:

As part of Go-Live process, we should follow CAB approval process. We have to involve AMS/IMS/DBA.