

NewgenONE OmniDocs

Configuration and Deployment Guide for Azure

Version: 11.3

Newgen Software Technologies Ltd.

This document contains propriety information of NSTL. No part of this document may be reproduced, stored, copied, or transmitted in any form or by any means of electronic, mechanical, photocopying, or otherwise, without the consent of NSTL.

Table of Contents

1	Pref	ace	4
	1.1	Revision history	4
	1.2	Intended audience	4
	1.3	Documentation feedback	4
	1.4	Third-party product information	4
2	Con	figuration of Azure Kubernetes cluster	5
	2.1	Create an Azure Kubernetes cluster	5
	2.2	Configuration of Azure container registry	15
	2.3	Configuration of ACR image scanning	20
	2.4	Create storage account	22
	2.4.1	Create a BLOB storage	22
	2.4.2	Create an Azure file share	30
	2.5	Configuration of Azure cache for Redis	32
	2.6	Configuration of application gateway ingress controller	
	2.6.1	Creation of an application gateway	36
	2.6.2		
	2.	6.2.1 Install Helm	
	2.	6.2.2 ARM authentication using a service principle	
	2.	6.2.3 Add or update Kubeconfig file	
	2.	6.2.4 Install ingress controller using Helm	
	2.7	Configuration of DNS zone	
	2.8	Run Kubectl from local machine	
	2.9	Monitor Kubernetes dashboard	54
	2.10	Azure monitor for container insights	
3	Dep	loyment of OmniDocs containers on Azure Kubernetes service	
	3.1	Prerequisites	56
	3.2	Deliverables	
	3.2.1		
	3.2.2	5	
	3.2.3		
	3.3	Changes in product's YAML files	
	3.4	Changes in application gateway Ingress YAML files	
	3.5	Changes in configuration files	
	3.5.1	•	
	3.5.2	5	
	3.5.3		
	3.5.4	AlarmMailer changes	72
	3.5.5	LDAP changes	73
	3.5.6	5	
	3.5.7		
	3.5.8	ThumbnailManager changes	80

3.5	5.9 TEM changes	81
3.5	5.10 EasySearch changes	81
3.5	5.11 WOPI changes	83
3.5	5.12 OmniScanWeb changes	86
3.6	Deployment of containers	89
3.7	Cabinet and data source creation	91
3.7	7.1 Getting started with OSA	92
3.7	7.2 Register JTS server	94
3.7	7.3 Connecting OSA to the JTS Server	96
3.7	7.4 Creating a cabinet	97
3.7	7.5 Associating a cabinet	100
3.7	7.6 Creating a data source	102
3.7	7.7 Registering a cabinet	112
3.7	7.8 Creating site and volume	113
3.8	EasySearch post-deployment changes	
3.9	OmniScanWeb: registration of cabinet	
4 Co	nfiguration of Azure DevOps release pipeline	124
4.1	Overview	
4.2	CICD pipeline architecture	
4.3	Configuration of Azure DevOps	
4.3	3.1 Configuration of release pipeline	127
4.3	3.2 Configuration of Dev stage	136
4.3	3.3 Configuration of UAT stage	
4.3	3.4 Configuration of production stage	146

1 Preface

This guide describes the deployment of OmniDocs deliverables like OmniDocs Docker containers and its required configuration files on the Azure Kubernetes Service (AKS).

1.1 Revision history

Revision Date	Description
July 2024	Initial publication

1.2 Intended audience

This guide is intended for System Administrators, developers, and any other users seeking information about the deployment of OmniDocs containers on Azure Kubernetes Services. The reader must be comfortable to understand the computer terminology.

1.3 Documentation feedback

To provide feedback or any improvement suggestions on technical documentation, you can write an email to <u>docs.feedback@newgensoft.com</u>.

To help capture your feedback effectively, request you to share the following information in your email.

- Document Name
- Version
- Chapter, Topic, or Section
- Feedback or Suggestions

1.4 Third-party product information

This guide contains third-party product information about configuring Microsoft Azure CICD Pipeline for Container Deployment on AKS Azure Kubernetes Cluster. Newgen Software Technologies Ltd does not claim any ownership on such third-party content. This information is shared in this guide only for convenience of our users and could be an excerpt from the Azure documentation. For latest information on configuring the Azure Kubernetes Cluster and Azure DevOps refer to the Azure documentation.

2 Configuration of Azure Kubernetes cluster

This section contains the steps to configure the Kubernetes Cluster on Azure.

2.1 Create an Azure Kubernetes cluster

This section explains how to create an Azure Kubernetes Cluster:

Pre-requisites:

Following are the prerequisites for Azure Kubernetes Cluster creation:

- Signed in user must have below roles:
 - At Subscription: Contributor Role
 - At Subscription: User Access Administrator
- Virtual network and subnet must be created for the Kubernetes cluster.

Before creating the Azure Kubernetes Cluster also known as AKS, you must sign in to the Azure portal at <u>https://portal.azure.com</u>.

Perform the below steps to create an Azure Kubernetes Cluster:

- 1. On the Azure portal menu or from the Home page, select Create a resource.
- 2. Select Containers and Kubernetes Service.

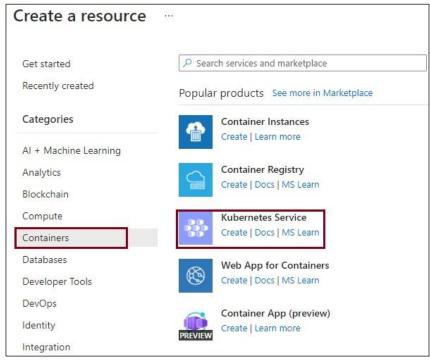


Figure 2.1

- 3. In the **Basics** tab, specify the following details on the Create Kubernetes cluster:
 - **Subscription**: Select a valid Azure subscription.
 - **Resource group**: Select or create an Azure Resource group, such as **AzureKubernetes**.
 - Kubernetes cluster name: Enter a Kubernetes cluster name such as BPMSuite-AKSCluster.
 - **Region**: Select a region into which you want to create an AKS cluster.
 - Availability zones: Usually there are three availability zones per region that allows you to spread the nodes across different physical locations for high availability. Select the availability zones as per your business requirement. [By default, select all the availability zones].
 - Kubernetes version: Select the default one that is, 1.20.9 (default).
 - **Primary node pool**: Select a VM Node size for the AKS nodes and select the number of nodes to be deployed into the AKS cluster.

NOTE:

The VM size can't be changed after the AKS cluster deployment. However, node count is adjustable.

- **Scale method**: Select the scale method as **Autoscale**. Autoscaling helps to ensure that your cluster is running efficiently with the right number of nodes for the workloads present.
- Click Next: Node Pools.

Create Kubernetes clus	ter	
Basics Node pools Authentication	n Networking Integration	s Tags Review + create
Azure Kubernetes Service (AKS) manages manage containerized applications withou operations and maintenance by provision offline. Learn more about Azure Kuberne	t container orchestration expertise. ng, upgrading, and scaling resource	
Project details		
Select a subscription to manage deployed your resources.	resources and costs. Use resource <u>c</u>	groups like folders to organize and manage all
Subscription * 🕢	Visual Studio Enterprise	\checkmark
Resource group * ()	(New) AzureKubernetes Create new	~
Cluster details		
Cluster preset configuration	to your scenario. Depending on	y choosing the preset configuration applicable the selection, values of certain fields might modify these values at any time.
Kubernetes cluster name * 🥡	BPMSuite-AKSCluster	✓
Region * 🛈	(Middle East) UAE North	\checkmark
Availability zones 🕕	None	\checkmark
	No availability zones are available View locations that support avail	e for the location you have selected. ability zones ⊡
Kubernetes version * 🔅	1.20.9 (default)	\checkmark
Primary node pool		
-	nt or test workloads, only one node nfiguration options for this node p	
Node size * (i)	Standard D8ds v4	
	8 vcpus, 32 GiB memory Standard DS2_v2 is recommend Change size	led for standard configuration.
Scale method * 🕡	Manual	
	 Autoscale Autoscaling is recommended f 	for standard configuration.
Node count range * 🛈		2
		2
Review + create < Pre-	ious Next : Node pools >	

Figure 2.2

4. On the Node pools page, keep the default options and click on the Next: Authentication>.

Create K	uberne	etes cluste	r				
Basics No	de pools	Authentication	Networking	Integrations	Tags	Review +	create
Node pools							
		primary node pool more about node p		e Basics tab, you	can also a	dd optional n	node pools to handle a
+ Add nod	le pool 📋	Delete					
Name		Mode	OS ty	pe	Node o	ount	Node size
agentpo	ol	System	Linux		2		Standard_D8ds_v
4							÷.
Enable virtua Virtual nodes a Enable virtual i	allow burstal	ble scaling backed b) serverless Azur	e Container Instar	nces. Learn	n more about	t virtual nodes 앱
Enable virtua	al machine s	scale sets					

Figure 2.3

5. On the Authentication page, keep the default options and click on the Next: Networking>.

Creat	e Kubern	etes cluster	r				
Basics	Node pools	Authentication	Networking	Integrations	Tags	Review + create	
The clust		authentication specif				nanage cloud resource ♂.	is attached to
Authenti	cation method	С) Service principa	l 🧿 System-as	signed m	anaged identity	
Authenti user may Role-bas	cation and autho	ticated. Learn more a	the Kubernetes clu bout Kubernetes			to the cluster as well a	as what the
By defau supply ye	our own keys usir	are encrypted at res	set backed by an A	Azure Key Vault. T		nal control over encryp ncryption set will be us	
Encryptic	on type	[[Default) Encryptio	n at-rest with a p	latform-n	nanaged key	\sim
Review	v + create	< Previous	Next : Ne	tworking >			



- 6. Select the Azure CNI as Network configuration and specify the following details:
 - Virtual network: Select the created VNet for this AKS cluster deployment that is, Vnet_for_AzureKubernetes.
 - **Cluster subnet:** Select the subnet into which both the nodes and containers in the cluster gets placed that is, subnet_dev (**10.0.2.0/23**).

NOTE:

This IP range 10.0.2.0/23 must be large enough to accommodate the nodes, pods, and all the Kubernetes resources that might be provisioned in your cluster.

- **Kubernetes service address range**: Specify the IP range from which you can assign Ips to the internal Kubernetes services. This range must not be connected to this virtual network, or it must not overlap with any Subnet IP ranges. For example: **10.0.0/25**.
- You can reuse this range across different AKS clusters.

• Kubernetes DNS service IP address: An IP address assigned to the Kubernetes DNS service. It must be within the Kubernetes service address range. For example: **10.0.0.10**.

NOTE:

Don't use the first IP address in your address range. The first address is used for the *10ubernetes.default.svc.cluster.local* address.

- **Docker Bridge address:** Docker bridge is not used by AKS clusters or the pods themselves, you must set this address to continue to support scenarios such as docker build within the AKS cluster. It is required to select a CIDR for the Docker bridge network address. Else, Docker picks a subnet automatically, which can conflict with other CIDRs. You must pick an address space that does not collide with the rest of the CIDRs on your networks, including the cluster's service CIDR and pod CIDR that is, **172.17.0.1/25**.
- You can reuse this range across different AKS clusters.
- Select Azure as Network policy and keep the other settings as default.
- Click Next: Integrations>.

Learn more about networking in Azure Kul	bernetes Service	
Network configuration 🕕	🔘 Kubenet	
	Azure CNI	
	The Azure CNI plugin requires an IP address from pod on a node, which can more quickly exhaust a value is set for pods per node. Consider modifying per node for each node pool on the "Node pools"	vailable IP addresses if a hig g the default values for pods
Virtual network * 🕕	VNet_for-AzureKubernetes	~
	Create new	
Cluster subnet * 🕕	subnet_dev (10.1.2.0/23)	~
	Manage subnet configuration	
Kubernetes service address range * 🕕	10.0.0/25	~
Kubernetes DNS service IP address * ①	10.0.0.10	~
Docker Bridge address * 🛈	172.17.0.1/25	~
DNS name prefix * 🕕	BPMSuite-AKSCluster-dns	Ý

Figure 2.5

7. On the Integration page, keep the default options and click the Next: Tags>.

Create Kubernetes o	luster				
Basics Node pools Authen	ication Networking	Integrations	Tags	Review + create	
Connect your AKS cluster with addit	onal services.				
Azure Container Registry					
Connect your cluster to an Azure Co create a new registry or choose one					u can
Container registry	None				\sim
Azure Monitor In addition to the CPU and memory comprehensive data on the overall p					ntion
Azure Monitor In addition to the CPU and memory	metrics included in AKS by d erformance and health of yo	our cluster. Billing is			ntion
Azure Monitor In addition to the CPU and memory comprehensive data on the overall p settings. Learn more about container perform	metrics included in AKS by d verformance and health of yo vance and health monitoring	our cluster. Billing is			ntion
Azure Monitor In addition to the CPU and memory comprehensive data on the overall p settings. Learn more about container perform Learn more about pricing	metrics included in AKS by d verformance and health of yo nance and health monitoring Enabled O D	our cluster. Billing is	is based o	n data ingestion and rete	ntion
Azure Monitor In addition to the CPU and memory comprehensive data on the overall p settings. Learn more about container perform Learn more about pricing	metrics included in AKS by d berformance and health of yo bance and health monitoring	our cluster. Billing is Disabled recommended for	is based o	n data ingestion and rete	

Figure 2.6

8. On the Tags page, keep the default options and click Next: Review + create>.

Creat	e Kubern	etes cluster	r			
Basics	Node pools	Authentication	Networking	Integrations	Tags	Review + create
Tags are	name/value pairs		ategorize resourd	ces and view cons		illing by applying the same tag to
			_		r tags will	be automatically updated.
Name	Ð		Va	alue 🛈		
			: [
Review	v + create	< Previous	Next : Re	eview + create >		

Figure 2.7

9. On the **Review + create** page, click **Create** once validation is passed.

Create Kubernetes cl	uster
✓ Validation passed	
Basics Node pools Authenti	cation Networking Integrations Tags Review + create
Basics	
Subscription	Visual Studio Enterprise
Resource group	AzureKubernetes
Region	UAE North
Kubernetes cluster name	BPMSuite-AKSCluster
Kubernetes version	1.20.9
Node pools	
Node pools	1
Enable virtual nodes	Disabled
Enable virtual machine scale sets	Enabled
Create <	Previous Next > Download a template for automation
	Figure 2.8

10. Once deployment is complete, click **Go to resource**.

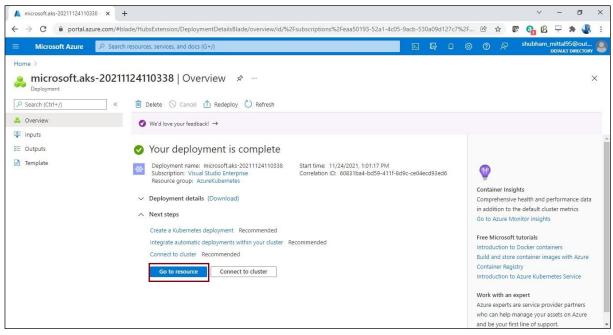


Figure 2.9

The Azure Kubernetes Cluster dashboard appears:

BPMSuite-AKSCluster - Microsoft 🗙	+				~	- 0	2
> C 🔒 portal.azure.com/#	#@shubhammittal95outlook.onmic	rosoft.com/resource/subscriptions/eaa50193-52a1	-4c05-9acb-530a09d127c7/resourc	egroups 🖻 🛧 📭	G 12 -	e 🛪 🍕	R
Microsoft Azure	rch resources, services, and docs (G+,	0	D 🖓	Q @ Q R	shubham_mi	ttal95@out	
Home > microsoft.aks-202111241103	38 >						
BPMSuite-AKSClus Kubernetes service	ster 🖈 …						×
P Search (Ctrl+/) ≪	🖉 Connect ▷ Start 🔲	Stop 📋 Delete 💍 Refresh 🔗 Give feedback					
Overview	 A Essentials 					JSON Viev	w
Activity log	Resource group : AzureKuberr	netes	Kubernetes version : 1.20	0.9			
R Access control (IAM)	Status : Succeeded (Running)	API server address : bpr	nsuite-akscluster-dns-4681c9	fb.hcp.uaenorth	1.azmk8	
Tags	Location : UAE North		Network type (plugin) : Azu	ire CNI			
Diagnose and solve problems	Subscription : Visual Studio	Enterprise	Node pools : 1 n	ode pool			
	Subscription ID : eaa50193-52	a1-4c05-9acb-530a09d127c7					
Security	Tags (Edit) : Click here to	add tags					
ubernetes resources							
Namespaces	Get started Properties	Monitoring Capabilities Recommendatio	ns Tutorials				
Workloads	Kubernetes services		Setworking				
Services and ingresses	Encryption type	Encryption at-rest with a platform-managed key	API server address	bpmsuite-akscluster-dns-			
Storage	Virtual node pools	Not enabled		4681c9fb.hcp.uaenorth.azr	nk8s.io		
	() () () () () () () () () ()		Network type (plugin)	Azure CNI			
Configuration	S Node pools		Pod CIDR	-			
ettings	Node pools	1 node pool	Service CIDR DNS service IP	10.0.0/25			
Node pools	Kubernetes versions	1.20.9 Standard D8ds v4	Docker bridge CIDR	172.17.0.1/25			

Figure 2.10

2.2 Configuration of Azure container registry

Perform the below steps to configure Azure Container Registry:

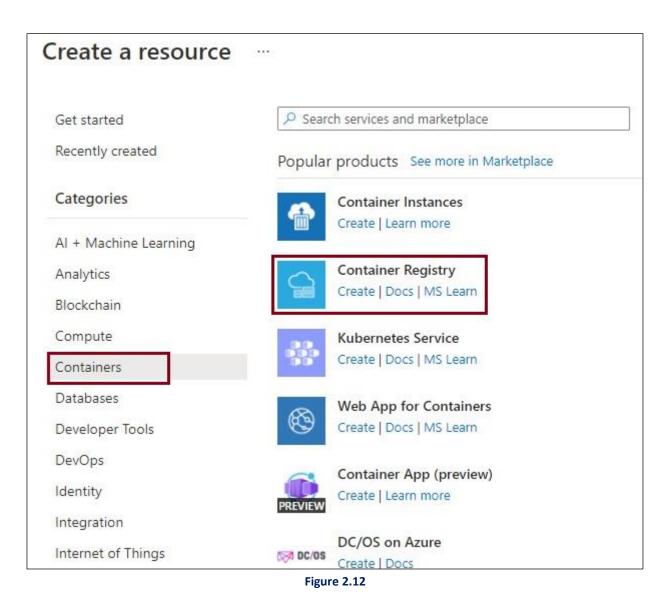
1. Sign in to the Azure Portal using the below URL:

https://portal.azure.com/

Microsoft Sign in to continue to Microsoft Azure Email, phone, or Skype No account? Create ane! Can't access your account? Sign in with a security key ③	

Figure 2.11

- 2. After a successful sign in, select Create a resource.
- 3. Select Containers and then select Container Registry.



- 4. In the **Basic** tab, specify the following details:
 - **Resource group:** Select the existing resource group or create a new resource group that is, **AzureKubernetes**.
 - **Registry name:** Specify the user-defined name that is, **newgencontainerregistry**.
 - Location: Select the location that is, UAE North, and so on.

• **SKU:** Select the SKU based on your usage as Basic, Standard, or Premium. Each SKU carry a different storage size.

For example,

SKU	Storage Limit
Basic	10 GiB
Standard	100 GiB
Premium	500 GiB or more

Project details		
Subscription *	Visual Studio Enterprise	\sim
Resource group *	AzureKubernetes	~
	Create new	
instance details		
Registry name *	newgencontainerregistry	~
		.azurecr.io
ocation *	UAE North	\checkmark
Availability zones 🕕	Enabled	
	Availability zones are enabled on premium registr support availability zones. Learn more	ies and in regions that
SKU * 🕕	Standard	~

Figure 2.13

- 5. Accept default values for the remaining settings. Then select **Review + create**. After reviewing the settings, select **Create**.
- 6. When the **Deployment succeeded** message appears, select the container registry in the portal.

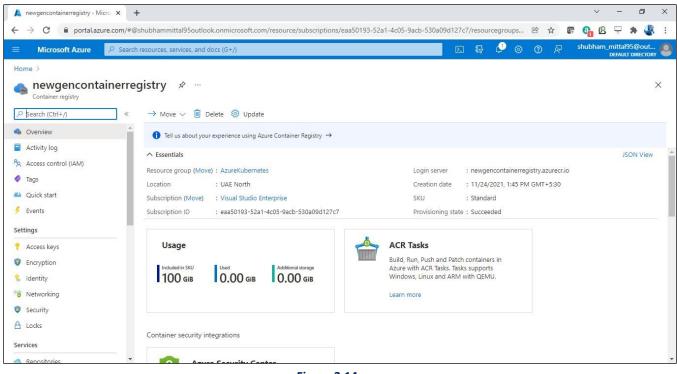


Figure 2.14

7. Click Access keys from Settings and enable Admin user.

← → C 🔒 portal.azure.c		rosoft.com/resource/subscriptions/eaa50193-52a1-4c05-9a	acb-530a09d12	27c7/re	sourceg	groups	B	☆	e (6	Ţ	* 4	R :
🗏 Microsoft Azure 🔎	9 Search resources, services, and docs (G+/)		⊾ 1	7 C	2 @	0	ম্ব	shu	ıbham	_mittal DEFAUL	95@out t directo	t
Home > newgencontainerregist	ry												
newgencontain Container registry	erregistry Access keys												×
₽ Search (Ctrl+/)	Registry name	newgencontainerregistry			D]							
Gverview	Login server	newgencontainerregistry.azurecr.io			D	1							
Activity log	Admin user ①	Enabled				-							
R Access control (IAM)													
🎙 Tags	Username	newgencontainerregistry			D								
Quick start	Name	Password		Regene	erate								
Events	password	A21832	D	C		•							
Settings	password2	Constantia ManagaMapagaMapaga SKAn	D	Ö									
📍 Access keys													
Encryption													
💲 Identity													
👌 Networking													
Security													
🖞 Locks													
services													
Repositories	-												



NOTE:

Kindly keep the **Login server**, **Username**, and **password** (or password2) as these values are required in the following steps to push or pull Docker images.

8. Use the below command to connect to the created container registry from your local machine (Where Docker Engine is already installed):

docker login <Container Registry Login server> -u <Container Registry username> -p

<Container Registry password>

For example,



Figure 2.16

9. After a successful sign in to the Container Registry, use the below command to tag and push the Docker images from your local machine to ACR (Azure Container Registry):

docker tag <image name>:<image tag> <container registry server>/<image name>:<image tag> docker push <container registry server>/<image name>:<image tag>

For Example,

docker tag ibps5serviceinstanceweb:sp2
newgencontainerregistry.azurecr.io/ibps5serviceinstanceweb:sp2
docker push newgencontainerregistry.azurecr.io/ibps5serviceinstanceweb:sp2

Where **newgencontainerregistry.azurecr.io** is the Container Registry Login server name.

NOTE:

Pushing any local Docker images to a repository is mandatory to tag that image 1st. You can also configure these commands in Jenkins to execute them automatically.

10. Use the below command to pull the Docker images from ACR to your local machine:

docker pull <container registry server>/<image name>:<image tag>

For Example,

```
docker pull
newgencontainerregistry.azurecr.io/ibps5serviceinstanceweb:latest
```

2.3 Configuration of ACR image scanning

Perform the below steps to configure ACR Image Scanning:

 Microsoft Defender for Cloud perform the ACR image scanning. Once the image scanning is configured and whenever a Docker image is pushed to the Azure Container Repository, Microsoft Defender for Cloud automatically scans that Docker image. Hence, it is mandatory to push that image in ACR to trigger the scan of an image.

NOTE:

Ensure that the Defender plan is enabled for the **Container registries**.

- 2. Go to the Microsoft Defender for Cloud page.
- 3. Click Environment settings under Management.
- 4. Click listed subscription.

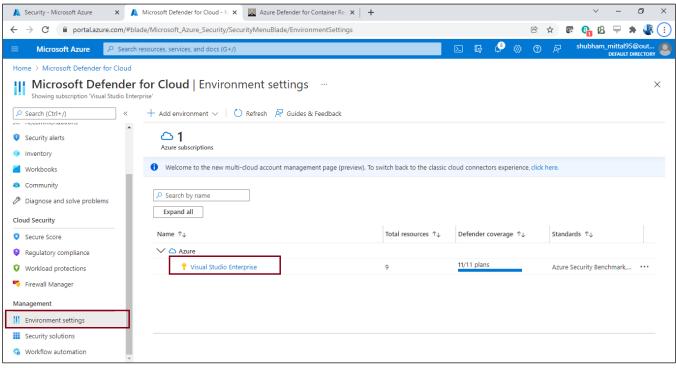


Figure 2.17

5. Enable the **Container registries** defender plan if it is not already enabled.

🙏 Security - Microsoft Azure 🛛 🗙	👗 Settings - Microsoft Azur	re 🗙 📓 Azure Defende	er for Container Re 🗙 📔 🕂		~	_	٥	×
> C 🔒 portal.azure.com/#	blade/Microsoft_Azure_S	ecurity/SecurityMenuBlade/En	wironmentSettings	₿ \$	e 🔥 🛙	, 🖵 d	•	:
Microsoft Azure 🔑 Sear	ch resources, services, and	docs (G+/)		D 🗣 🗳 🕸 🕫	shubham	_mittal95 DEFAULT D		6
lome > Microsoft Defender for Cloud	4 >							
Settings Defender Visual Studio Enterprise	r plans 🛛 …						3	×
	Save							
Settings	Servers	à	3 servers	\$15/Server/Month ()	On	Off)	
Defender plans	App Se	ervice	0 instances	\$15/Instance/Month ①	On	Off)	
 Auto provisioning 	🕺 Azure :	SQL Databases	0 servers	\$15/Server/Month (j)	On	Off)	
Email notifications	SQL se	rvers on machines	0 servers	\$15/Server/Month ① \$0.015/Core/Hour	On	Off)	
Integrations	open-:	source relational databases	0 servers	\$15/Server/Month 🕕	On	Off)	
Workflow automation	Storage	e	1 storage accounts	\$0.02/10k transactions ①	On	Off)	
Continuous export	Kuberr	ietes	16 kubernetes cores	\$2/VM core/Month ①	On	Off)	
Policy settings	Gontai	ner registries	2 container registries	\$0.29/image	On	Off)	
Security policy	🍸 Key Va	ult	0 key vaults	\$0.02/10k transactions	On	Off)	
	(i) Resour	rce Manager		\$4/1M resource management ope ①	On	Off)	
	DNS			\$0.7/1M DNS queries ①	On	Off)	



Microsoft Defender for container registries includes a vulnerability scanner to scan the images in your Azure Resource Manager-based Azure Container Registry registries.

 Provide deeper visibility into your images vulnerabilities. The integrated scanner is powered by Qualys, the industry-leading vulnerability scanning vendor.
 When issues are found – by Qualys or Defender for Cloud – you get notified in the workload protection dashboard.

For example,

🙏 Security - Microsoft Azure	🗙 🙏 Vulnerabilities in	Azure Containe 🗙 🕂		v –	0 >
← → C 🔒 portal.azu	u re.com /#blade/Microsoft_A	zure_Security/SecurityMenuBlade/	26	ලි 🛧 🕼 🚱 🖵 🕽	. 🗶 :
■ Microsoft Azure	₽ Search resources, service	es, and docs (G+/)		E 🛱 🖉 🕲 🔿 🐼 shubham_mittal95	
Home > Microsoft Defender		r Registry images sl	hould be remediated (power		X
🖉 Exempt 🚫 Disable rule					
Unhealthy registries	Severity High	Total vulnerabilities 34	Vulnerabilities by severity High 5 - Vulnerabilities by severity Medium 29 - Vulnerabilities by severity	Registries with most vulnerabilities newgencicdpiepline 34	
 Arrected resources Unhealthy registries (1) 	Healthy registries (1)	Not applicable registries (0) U	Low 0		
🔎 Search container regi	stries				
Name					↑↓
newgencontainerre	gistry				
Trigger logic app	Exempt				
Was this recommenda	ntion useful? O Yes) No			

Figure 2.19

2.4 Create storage account

Perform the below to configure a storage account:

2.4.1 Create a BLOB storage

Perform the below steps to create IAM Policy and Role:

- Sign in to the Azure Portal using the below URL: <u>https://portal.azure.com/</u>
- 2. Select All services on the Azure portal menu.
- 3. Select Storage Accounts.
- 4. Click **Create** on the Storage Accounts.
- 5. On the **Basics** tab, select an active Azure subscription.
- 6. Under the Resource group field, select your desired resource group, or create a new resource group like **AzureKubernetes.**
- 7. Enter a name for your storage account like **bpmsuitestoage.**
- 8. Select a location or region in which you want to create your storage account that is, UAE North.
- 9. Select a performance tier. The default tier is Standard.
- 10. Specify how you want the storage account to replicate. The default replication option is Georedundant storage (GRS).

11. Keep the other settings as default and click **Next: Advanced>**.

Azure Blobs (objects), Azure Data	e that is highly available, secure, durable Lake Storage Gen2, Azure Files, Azure Q	
	he options you choose below. Learn mor	ueues, and Azure
	noose a new or existing resource group	to organize and
Visual Studio Enterprise		\sim
		~
ge account type, please click here.		
bpmsuitestorage		
bpmsuitestorage (Middle East) UAE North		~
(Middle East) UAE North	ded for most scenarios (general-purpose ded for scenarios that require low latenc	
(Middle East) UAE North	ded for scenarios that require low latenc	
	create the new storage account. Ch ether with other resources. Visual Studio Enterprise AzureKubernetes Create new ge account type, please click here.	Visual Studio Enterprise AzureKubernetes Create new

Figure 2.20

12. On the Advanced tab, keep the default options and click Next: Networking>.

Crea	te a stor	age accou	unt …		
Basics	Advanced	Networking	Data protection	Tags	Review + create
			namespace acc	ounis.	
Blob st	torage				
Enable	network file sys	tem v3 🕡			
			To enable NFS v v3	/3 'hierarch	ical namespace' must be enabled. Learn more about NFS
Allow c	ross-tenant rep	lication 🛈			
Access	tier 🛈		Hot: Frequent	tly accesse	d data and day-to-day usage scenarios
			Cool: Infreque	ently acces	sed data and backup scenarios
S					
Revie	ew + create		< Previous	Nex	t : Networking >
				24	

Figure 2.21

13. On the Networking tab, keep the default options and click Next: Data protection>.

Basics Advanced Networking Data protection Tags Review + create Connectivity method * Public endpoint (all networks) Public endpoint (selected networks) Private endpoint All networks will be able to access this storage account. We recommend using Private endpoint for accessing this resource privately from your network. Learn more Network routing
 Public endpoint (all networks) Public endpoint (selected networks) Private endpoint All networks will be able to access this storage account. We recommend using Private endpoint for accessing this resource privately from your network. Learn more
 Private endpoint All networks will be able to access this storage account. We recommend using Private endpoint for accessing this resource privately from your network. Learn more
 All networks will be able to access this storage account. We recommend using Private endpoint for accessing this resource privately from your network. Learn more
Private endpoint for accessing this resource privately from your network. Learn more
Network routing
Network routing
Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.
Routing preference () * (Microsoft network routing
Review + create < Previous Next : Data protection >

Figure 2.22

14. On the **Data protection** tab, keep the default options and click **Next: Tags>**.

isics	Advanced	Networking	Data protectio	on Tags	Rev	view + ci	reate			
lecov	very									
rotec	t your data from:	accidental or erro	oneous deletion o	r modification						
E	Enable point-in-t	ime restore for co	ntainers							
			ne or more contain st also be enabled.		r state.	lf point-ir	-time re:	store is	enabled, t	then versionin
- E	Enable soft delete	e for blobs								
	Soft delete enables more	s you to recover blo	bs that were previo	ously marked fo	or deleti	on, includ	ing blob	s that v	vere overv	vritten, Learn
[Days to retain de	leted blobs 🛈		7						
- E	Enable soft delete	e for containers								
	Soft delete enables	s you to recover co	ntainers that were p	reviously mark	ed for c	leletion. l	.earn mo	re		
9	Davs to retain de	leted containers	0	7						
	says to retain de									

Figure 2.23

15. On the Tags tab, keep the default options and click Next: Review + create.

Creat	te a stor	age accou	unt …				
Basics	Advanced	Networking	Data protection	Tags	Review	v + create	
			ou to categorize resour Learn more about tag		ew consc	olidated billing by applying the same tag	to
Note th	at if you create	tags and then cha	ange resource settings	on other t	abs, you	r tags will be automatically updated.	
Name	2		Value			Resource	
		\sim			\sim	All resources selected \sim	
Revie	w + create	Į.	< Previous	Next	t : Reviev	v + create >	
			Figure	2.24			

16. On the **Review + create** tab, click **Create** once validation is passed.

Creat	te a stor	age accou	unt …		
🕑 Val	lidation passed				
Basics	Advanced	Networking	Data protecti	on Tags	Review + create
Basics					
Subscript	tion		Visual Studio Er	nterprise	
Resource	Group		AzureKubernet	es	
Location			uaenorth		
Storage a	account name		bpmsuitestorag	je	
Deploym	ent model		Resource mana	ger	
Performa	ince		Standard		
Replicatio	on		Read-access ge	o-redundant	storage (RA-GRS)
Advanc	ed				
Secure tr	ansfer		Enabled		
Creat	te	< F	Previous	Next >	Download a template for automation
			Figu	re 2.25	

17. Once deployment is complete, click **Go to resource**.

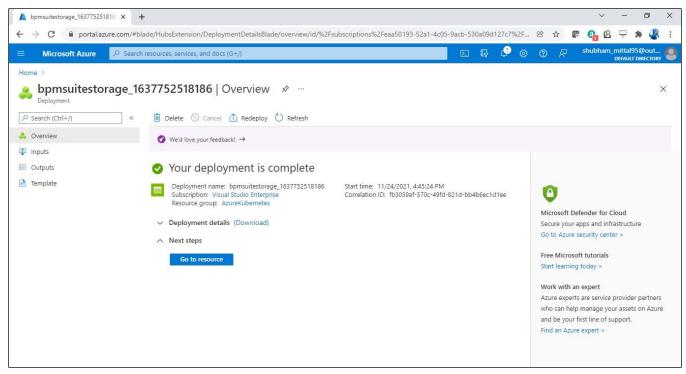


Figure 2.26

18. Click Access keys from Settings under Security + Networking.

NOTE:

Keep the **Storage account name** and **key1** (or key2) as these values are required in the following steps for the Kubernetes volume mounting.

- 19. Click **Containers** under the Data storage. The **Containers** screen appears.
- 20. Click +Container. The New Container dialog appears.
- 21. Specify the following details:
 - **Name**: Specify the unique blob storage name.
 - Public access level: Select default "Private (no anonymous access)".

22. Click Create.

👗 New container - Microsoft Azure 🗙	+			~ - 0 X
← → C	@shubhammittal95outlook.onmicrosoft.com/re	source/subscriptions/eaa50193-52a1-4c05-9acb-530a0	9d127c7/resourcegroups	ලි 🛧 🕼 🚱 🛱 🎘 🕄 :
E Microsoft Azure 🔑 Searc	h resources, services, and docs (G+/)			⑦ & shubham_mittal95@out DEFAULT DIRECTORY
Home > bpmsuitestorage				New container \times
bpmsuitestorage	Containers 🖈 …			
Search (Ctrl+/) «	+ Container 🔒 Change access level 🍃	9 Restore containers 🗸 🕐 Refresh 🗎 Delete		Name *
Cverview	Search containers by prefix			Public access level ①
Activity log	Name	Last modified	Public access level	Private (no anonymous access)
Tags	\$logs	11/24/2021, 4:45:52 PM	Private	✓ Advanced
Diagnose and solve problems				_ <u>_</u>
 Access Control (IAM) 				
 Events 				
📔 Storage browser (preview)				
Data storage				
Containers				
🛋 File shares				
🔟 Queues				
Tables				
Security + networking				Create Discard
Networking				

Figure 2.27

2.4.2 Create an Azure file share

Perform the below steps to create an Azure File Share:

- 1. Click **Overview** of the created storage account.
- 2. Click **File shares** under the Data storage. The **File shares** dialog appears.

🛕 bpmsuitestorage - Microsoft Azu 🗙	+					~	- 6	p
→ C 🔒 portal.azure.com	/#@shubhammittal95outlook.onmicroso	oft.com/resource/subscriptions/eaa50193-	2a1-4c05-9acb-530a09d127c	7/resourcegroups	r 🕁 🕝	<u>е</u> В	P *	
Microsoft Azure 🔑 Se	earch resources, services, and docs (G+/)			G 🖉 🐵	⑦ ₽	shubham	_mittal95@c DEFAULT DIREC	
Home > bpmsuitestorage_1637752	518186 >							
bpmsuitestorage	\$							×
₽ Search (Ctrl+/)	« 📲 Open in Explorer 📋 Delete	$ ightarrow$ Move \checkmark $ ightarrow$ Refresh $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	R Feedback					
Overview	Microsoft recommends upgradin	ng to the new alerts platform to ensure no interru	otions in vour alerts. Classic alerts	will be retired starting in 2	2021, Upgrade to	the new aler	ts	
Activity log	platform. Learn more		,					
Tags							JSON V	iew
Diagnose and solve problems	Resource group (move) : Azure	eKubernetes	Performance/Access t	ier : Standard/Hot				
Access Control (IAM)	Location : UAE N	North	Replication	: Read-access geo-r	redundant storag	ge (RA-GRS))	
Data migration	Primary/Secondary Location : Prima	ary: UAE North, Secondary: UAE Central	Account kind	: StorageV2 (genera	al purpose v2)			
Events	Subscription (move) : Visua	al Studio Enterprise	Provisioning state	: Succeeded				
	Subscription ID : eaa50	0193-52a1-4c05-9acb-530a09d127c7	Created	: 11/24/2021, 4:45:2	28 PM			
Storage browser (preview)	Disk state : Prima	ary: Available, Secondary: Available						
ata storage	Tags (edit) :							
Containers								
File shares	Properties Monitoring Ca	apabilities (7) Recommendations T	utorials Developer Tools					
Queues	Blob service		Security					
Tables	Hierarchical namespace	Disabled	Require secure tr	ansfer for REST API	Enabled			
	Default access tier	Hot	operations					
ecurity + networking			Storage account	kov accors	Enabled			

Figure 2.28

- 3. Click +File share. The New File share dialog appears.
- 4. Specify the following details:
 - Name: Specify the unique file share name.
 - **Tiers:** Select the 'Transaction optimized' as tier.
 - Click Create.

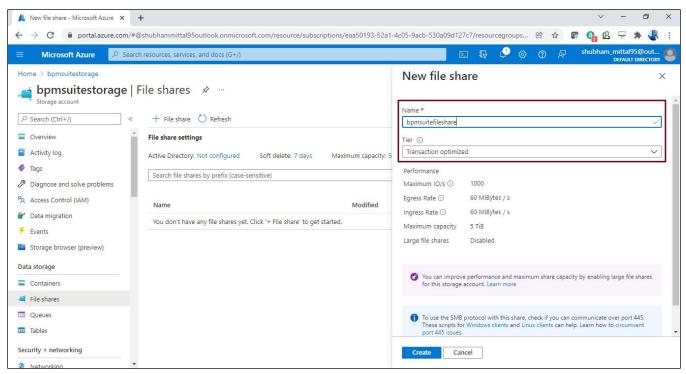


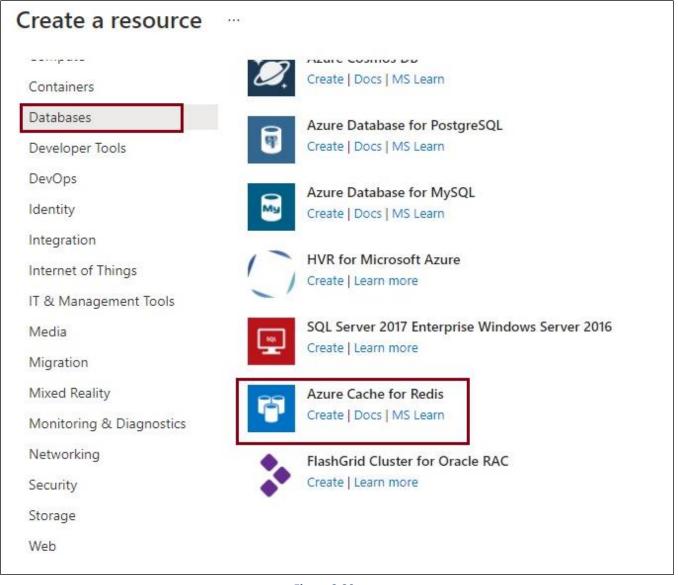
Figure 2.29

2.5 Configuration of Azure cache for Redis

Azure Cache for Redis provides fully managed open-source Redis within Azure that can be used as a distributed data or content cache. In addition, it can be used as a session store and so on along with that it provides an in-memory data store.

Perform the below steps to configure the Azure Cache for Redis:

- Sign in to the Azure Portal using the below URL: <u>https://portal.azure.com/</u>
- 2. On the Azure portal menu or from the home page, select **Create a resource**.
- 3. Select Databases.
- 4. Select Azure Cache for Redis.





- 5. Specify the following details under the **Basics** tab:
 - **Subscription**: Select a valid Azure subscription.
 - **Resource group**: select or create an Azure Resource group, such as **AzureKubernetes**.
 - **DNS name**: Enter a Redis cache DNS name such as **azrediscache**.
 - Location: Select a region into which you want to create an Azure Cache for Redis.
 - **Cache type:** Select the Redis cache service tier as per your requirement. You can select from 250 MB to 1455 GB in-memory cache.
 - Click Next: Networking>.

Basics Networking Advanced	Tags Review + create		
Azure Cache for Redis helps your applic latency, high-throughput capabilities of	ation stay responsive even as user load increases. It does so t the Redis engine. Learn more 🗗	y leveraging the low	
Project details			
Select the subscription to manage deplo your resources.	yed resources and costs. Use resource groups like folders to	organize and manage all	
Subscription *	Visual Studio Enterprise	~	
Resource group *	AzureKubernetes	~	
	Create new		
Instance Details			
DNS name *	azrediscache	~	
		.redis.cache.windows.net	
Location *	UAE North V		
Cache type (View full pricing details) *	Standard C2 (2.5 GB Cache, Replication)	~	

Figure 2.31

6. On the **Networking** tab, select the connectivity method as 'Public Endpoint' and click **Next:** Advanced>.

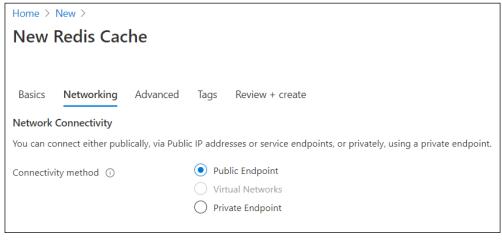


Figure 2.32

7. On the **Advanced** tab, enable the Non-TLS port, select the Redis version as 6 and click **Next:** Tags>.

New	Redis Cad	che …		
Basics	Networking	Advanced	Tags	Review + create
Non-TLS	port		🔽 Er	nable
Redis ver	sion		↓ 4● 6	



- 8. On the Tags tab, keep the default options and click Next: Review + create>.
- 9. On the Review + create tab, click Create once validation is passed.

🕦 Runnir	ng final validatio	ons				
Basics N	Vetworking	Advanced	Tags	Review + create		
Basics						
DNS name			azrediscache			
Subscription	i i		Visual	Studio Enterprise		
Resource group			AzureKubernetes			
Location			UAE North			
SKU		C2_Standard				
Advanced						
Non-TLS port			Enabled			
Redis version			б			
Redis versio	n		6			

Figure 2.34

10. Once deployment is complete, click **Go to resource**.

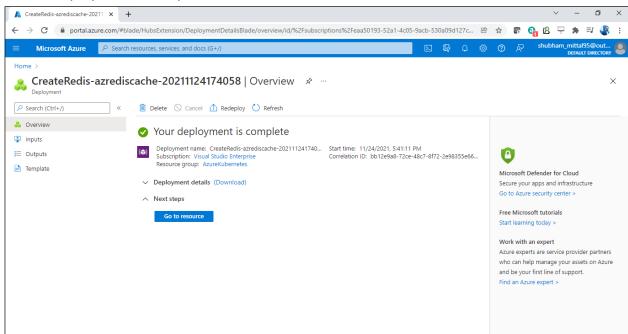


Figure 2.35

2.6 Configuration of application gateway ingress controller

This section explains how to configure Application Gateway Ingress Controller.

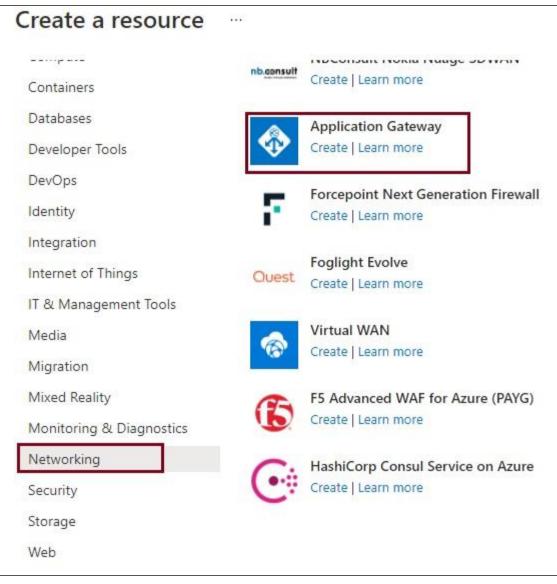
2.6.1 Creation of an application gateway

Pre-requisites:

• A subnet must be created in the same virtual network in which the Kubernetes cluster exists.

Perform the below steps to create an Application Gateway:

- 1. On the Azure portal menu or from the Home page, select **Create a resource**.
- 2. Select Networking.





- 3. Select Application Gateway. The Create application gateway screen appears.
- 4. Specify the following details under the **Basics** tab:
 - **Subscription**: Select a valid Azure subscription.
 - **Resource group**: Select or create an Azure Resource group, such as **AzureKubernetes**.
 - Application gateway name: Enter a Kubernetes cluster name such as AppGateway-AKSCluster.
 - **Region**: Select a region into which you want to create an AKS cluster that is, UAE North
 - Tier: Select Standard V2.
 - Virtual network: Select the same virtual network in which the Kubernetes cluster exists.
 - **Subnet**: Select the created subnet for the application gateway.

• Keep the other settings as default and then select the **Next: Frontends**.

Create application ga	teway	
Basics Frontends 3 B	ackends ④ Configuration ⑤ Tags ⑥ Review + create	
An application gateway is a web traffic about application gateway	load balancer that enables you to manage traffic to your web application. Learn more	e
Project details		
Select the subscription to manage depl your resources.	loyed resources and costs. Use resource groups like folders to organize and manage a	all
Subscription * 🕢	Visual Studio Enterprise 🗸	·]
Resource group * (i)	AzureKubernetes 🗸	
	Create new	
Instance details		
Application gateway name *	AppGateway-AKSCluster	/
Region *	UAE North 🗸	·]
Tier 🛈	Standard V2	•]
Enable autoscaling	• Yes • No	
Minimum instance count * 🛈	0]
Maximum instance count	10]
Availability zone 🕕	None	
HTTP2 ①	Disabled Enabled	
Configure virtual network		
Virtual network * 🕕	VNet_for-AzureKubernetes	1
	Create new	1
Subnet * 🕕	subnet_appgw (10.1.3.0/24)	1
	Manage subnet configuration	1
Previous Next : Frontends >		

Figure 2.37

5. Set the Frontend IP address type as **Public**.

6. Select **Add new** for the **Public IP address** and enter a user-defined name that is, *appgwpublicip* and then click **OK**.

Create application	gateway		
	way via its frontend IP addres	uration (5) Tags (6) Review + creat	
Frontend IP address type 🛈	Public O Pr	ivate 🔘 Both	
Public IP address	Choose public IP a Add new		~
	Add a publ Name *	appgwpublicip	
	Assignment	🔵 Dynamic 💿 Static	
	Availability zone	None	
Previous Next : Backend	is > OK	Cancel	

Figure 2.38

- 7. Select Next: Backends. The Backends tab appears.
- 8. Select **add a backend pool**. The Add a backend pool dialog appears.
- 9. Enter the following details to create an empty backend pool:
 - Name: Enter a user-defined name that is, appgwbackendpool.
 - Add backend pool without targets: Select Yes to create a backend pool with no targets.
 - Select Add to save the backend pool configuration and return to the Backends tab.

Add a backend pool Microsoft × +	~ - Ø ×
← → C	🖻 🛧 📭 🚱 🖵 🗯 🐇 :
■ Microsoft Azure P Search resources, services, and docs (G+/)	🔄 🕞 🖓 🔅 🕐 R shubham_mittal95@out 🧶
Home > Create a resource > Create application gateway ···· ✓ Basics ✓ Frontends ④ Backends ④ Configuration ⑤ Tags ⑥ Review + create A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, app services, IP addresses, or fully qualified domain names (FQDN). Add a backend pool Backend pool Backend pool No results	Add a backend pool.
Previous Next : Configuration >	Add Cancel

Figure 2.39

10. On the **Backends** tab, select **Next: Configuration.** The Configuration tab appears.

11. Select Add a routing rule in the Routing rules column. The Add a routing rule dialog appears.

12. Enter the user-defined rule name that is, routingrule1.

13. A routing rule requires a listener. On the Listener tab, enter the following details:

- Listener name: Enter a user-defined listener name that is, appgwlistener.
- Frontend IP: Select Public to select the public IP that you have created in the Frontends tab.
- Keep the other settings as default and switch to the **Backend targets** tab.

Add a routing rule - Microsoft A= × +				~	- 0 ×
← → C	1			r 🔒 🛽	🕂 🎝 🛊
■ Microsoft Azure P Search resources, services, and docs (G+/)			P @ 0 4		ittal95@out 🧶
Home > Create a resource > Create application gateway	Add a routing rule	m a given frontend IP address to one	or more backend target	s. A routing rule mus	×
✓ Basics ✓ Frontends ✓ Backends Configuration (5) Tags Create routing rules that link your frontend(s) and backend(s). You can also add more	listener and at least one backend target. Rule name * * Listener *Backend targets A listener "listens" on a specified port an gateway will apply this routing rule.	routingrule1			~
Frontends + Add a frontend IP Public: (new) appgwpublicip 💼 •••	Listener name * () Frontend IP * () Protocol () Port * () Additional settings Listener type () Error page url	appgwlistener Public HTTP HTTPS 80 Basic Multi site Yes No			S
Previous Next : Tags >	Add Cancel				

Figure 2.40

- 14. In the **Backend targets** tab, select the backend pool created in the **Backends** tab for the **Backend target**.
- 15. For the **HTTP settings**, select **Add new** to add a new HTTP setting.

Add a routing rule - Microsoft Az 🗙 🕂					~	- 0	×
← → C	1		e	8 🕁 📭	G 8	🗄 🖇	I :
■ Microsoft Azure P Search resources, services, and docs (G+/)			G 🖉 🎯 (୭ ନ		mittal95@oi default direc	
Home > Create a resource > Create application gateway	Add a routing rule						×
✓ Basics ✓ Frontends ✓ Backends Oconfiguration ③ Tags Create routing rules that link your frontend(s) and backend(s). You can also add more	Configure a routing rule to send traffic from listener and at least one backend target. Rule name * * Listener * Backend targets	routingrule1		-			<u>~</u>
Frontends + Add a frontend IP	Choose a backend pool to which this rout behavior of the routing rule. Target type Backend target * ①		direction	a set of HTTP	settings tha	t define the	~
Public: (new) appgwpublicip 💼 •••	HTTP settings ★ Path-based routing You can route traffic from this rule's listen different set of HTTP settings based on the		s based on the URL pat	n of the reque	st. You can a	ilso apply a	<u> </u>
Previous Next : Tags >	Path based rules Path Targe Add Cancel	et name HTT	IP setting name	Backend	pool		

Figure 2.41

16. In the Add an HTTP setting, enter the user-defined HTTP setting name that is,

appgwhttpsetting.

17. Keep the other settings as default and then click **Add** to return to the Add a routing rule.

Microsoft Azure P Search resources, services, and docs (G+/)		도 다 야 🖓 🖓 🖓 모 the hubham_mittal95@out.
ome > Create a resource > Create application gateway …	Add a HTTP setting	ing rules
✓ Basics ✓ Frontends ✓ Backends Oconfiguration S Tags Create routing rules that link your frontend(s) and backend(s). You can also add more Frontends + Add a frontend IP Public: (new) appgwpublicip Tore	Backend protocol Backend protocol Backend port * Additional settings Cookie-based affinity ① Connection draining ① Request time-out (seconds) * ① Override backend path ① Host name By default, Application Gateway does n	appgwhttpsetting HTTP HTTPS B0 Enable Disable Lable Disable 20 ot change the incoming HTTP host header from the client and sends the header unaltered to the
	Deckend, wultr-tenant services like App endpoint. Change these settings to ove Override with new host name Host name override	service or API management rely on a specific host header or SNI extension to resolve to the corre- rwrite the incoming HTTP host header. Ves No Pick host name from backend target Override with specific domain name e.g. contoso.com
Previous Next : Tags >		

0.

- 18. Select Add to save the routing rule in the Add a Routing and return to the Configuration tab.
- 19. Select **Next: Tags** and then click **Next: Review + create**.
- 20. Once validation is passed, select **Create**.

Microsoft Azure P Search resources, services, and docs (G+/)				0				
Microsoft Azure 🔑	Search resources, services, and docs (G+/)		D G	P 🖗	0	shubham_	mittal95@ DEFAULT DIR	OUT
ome > Create a resource >								
reate application	gateway							×
ieute application	gaterial							
•								
Validation passed								
✓ Basics ✓ Frontends	✓ Backends ✓ Configuration ✓ Tags 6 Review + create							
Basics								
Subscription	Visual Studio Enterprise							
Subscription Resource group	Visual Studio Enterprise AzureKubernetes							
Resource group	AzureKubernetes							
Resource group Name	AzureKubernetes AppGateway-AKSCluster							
Resource group Name Region Tier	AzureKubernetes AppGateway-AKSCluster UAE North							
Resource group Name Region	AzureKubernetes AppGateway-AKSCluster UAE North Standard_v2							
Resource group Name Region Fier Enable autoscaling	AzureKubernetes AppGateway-AKSCluster UAE North Standard_v2 Enabled							
Resource group Name Region Tier Inable autoscaling Minimum instance count Maximum instance count	AzureKubernetes AppGateway-AKSCluster UAE North Standard_v2 Enabled 0							
Resource group Name Region Tier Enable autoscaling Vinimum instance count	AzureKubernetes AppGateway-AKSCluster UAE North Standard_v2 Enabled 0 10							
Resource group Name Region Tier Enable autoscaling Winimum instance count Vaximum instance count Availability zone	AzureKubernetes AppGateway-AKSCluster UAE North Standard_v2 Enabled 0 10 None							

Figure 2.43

21. Once the deployment is complete, click Go to resource.

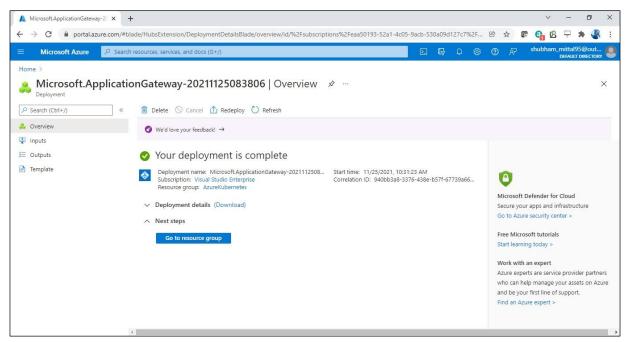


Figure 2.44

2.6.2 Installation of an application gateway ingress controller

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services. Kubernetes ingress resources are used to configure the ingress rules and routes for individual Kubernetes services. Using an ingress controller and ingress rules, a single IP address can be used to route traffic to multiple services in a Kubernetes cluster.

Pre-requisites:

- Azure Kubernetes Service must be created.
- Application Gateway must be created.

To install an Application Gateway Ingress Controller (AGIC), follow the below steps:

- Install Helm
- Azure Resource Manager Authentication using a Service Principle
- Install Ingress Controller using Helm

2.6.2.1 Install Helm

- If you use the Azure Cloud Shell<u>https://portal.azure.com/#cloudshell/</u> then the Helm CLI is already installed. To install Helm on other platforms please refer to https://helm.sh/docs/intro/install/.
- 2. Open the Azure Cloud Shell and run the following command to add the application-gateway-

kubernetes-ingress helm package.

helm repo add application-gateway-kubernetes-ingress
https://appgwingress.blob.core.windows.net/ingress-azure-helm-package/
helm repo update

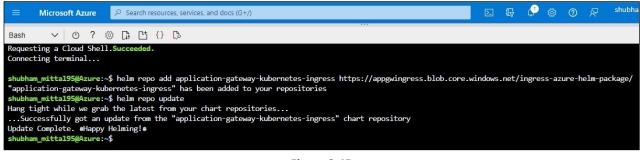


Figure 2.45

2.6.2.2 ARM authentication using a service principle

Perform the below steps for ARM Authentication using a service principle:

- 1. Application Gateway Ingress Controller (AGIC) communicates with the Kubernetes API Server and Azure Resource Manager. It requires authentication to access these APIs
- 2. Open the Azure Cloud Shell <u>https://portal.azure.com/#cloudshell/</u> and run the following command to create a service principle and encode with base64. The base64 encoding is required for the JSON blob to be saved to Kubernetes.

```
az ad sp create-for-rbac --role Contributor --sdk-auth --scopes
/subscriptions/<Subscription-id>/resourceGroups/<Resource group> | base64 -
w0
```

Where,

Subscription-id - Enter your account subscription id

Resource group - Ente the name of resource group associated with kubernetes cluster

For Example -

```
az ad sp create-for-rbac --role Contributor --sdk-auth --scopes
/subscriptions/323527f6b-535a1-406d-239b-0972646c8500c3/resourceGroups/
AzureKubernetes | base64 -w0
```

NOTE:

Keep the **base64 encoded JSON blob** as these values are required in the following steps for installing AGIC.

2.6.2.3 Add or update Kubeconfig file

Perform the below steps to add or update kubeconfig file:

- 1. Open the Azure Cloud Shell <u>https://portal.azure.com/#cloudshell/</u>.
- 2. Delete the .kube/config file (if already exists) using below command:

```
rm .kube/config
```

3. Now execute the below command to re-create .kube/config file:

```
az aks get-credentials --resource-group <ResourceGroupName> --name
<AzureEKSClusterName>
```

```
az aks get-credentials --resource-group AzureKubernetes --name BPMSuite-AKSCluster
```

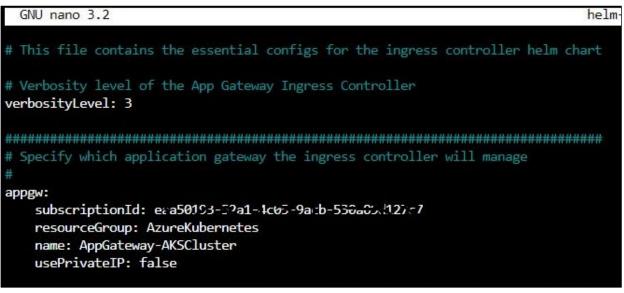
2.6.2.4 Install ingress controller using Helm

Perform the below steps to install ingress controller using Helm:

1. Open the Azure Cloud Shell <u>https://portal.azure.com/#cloudshell/</u> and run the following command to download the *helm-config.yaml* file which configures the Application Gateway Ingress Controller.

wget https://raw.githubusercontent.com/Azure/application-gateway-kubernetesingress/master/docs/examples/sample-helm-config.yaml -0 helm-config.yaml

- Edit the helm-config.yaml file and fill in the values for appgw (Application Gateway) and armAuth (ARM Authentication using Service Principle).
 nano helm-config.yaml
- Update the <subscriptionId>, <resourceGroupName>, and <applicationGatewayName> for appgw.





- 4. Comment the **armAuth** using **AAD-Pod-Identity** and uncomment the **armAuth** using **Service Principle**.
- Update the base64 encoded JSON blob created in the previous step 'ARM Authentication using a Service Principle' for secretJSON.
 For example,

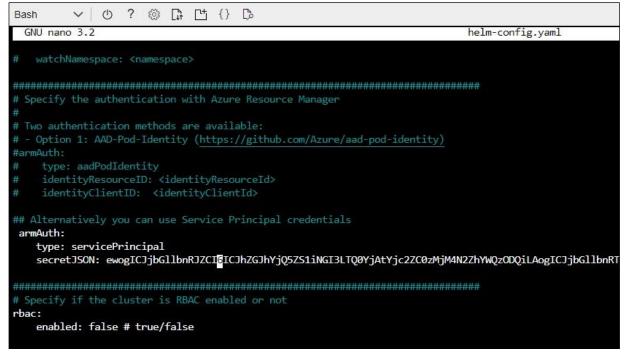


Figure 2.47

6. Specify the rbac enabled as **true** if the cluster is RBAC enabled. For example,





7. Install Helm chart **application-gateway-kubernetes-ingress** with the *helm-config.yaml* configuration from the previous step.

```
helm install ingress-azure \
  -f helm-config.yaml \
  application-gateway-kubernetes-ingress/ingress-azure \
  --version 1.4.0
```

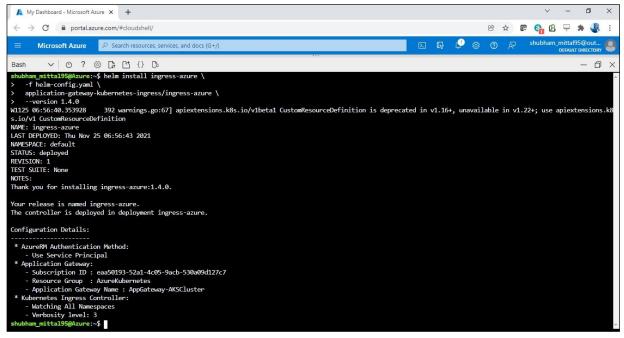


Figure 2.49

NOTE:

Use the latest version of ingress-azure. You can get the release information from the below link: <u>https://github.com/Azure/application-gateway-kubernetes-ingress/releases</u>

8. Application Gateway Ingress Controller runs as a pod in the Kubernetes cluster. You can check the running status of the AGIC pod using the below command:

Kubectl get po | grep ingress

For example,

<pre>shubham_mitta195@Azure:~\$ kubect</pre>	:l get po	grep ing	ress	
ingress-azure-649b85494b-2tthf	1/1	Running	0	10m

Figure 2.50

2.7 Configuration of DNS zone

Ingress Controller creates a Load Balancer and routes the incoming requests to the target Kubernetes services according to the host-based routing rules. Host-based routing is a capability of Ingress Controller that redirects the user requests to the right service based on the request-host header.

For example, you can set the rules as below:

- IF URL is 'ibps5serviceinstance.azure.co.in' then redirect to iBPS ServiceInstance Web container.
- IF URL is 'ibps5userinstance.azure.co.in' then redirect to the iBPS UserInstance Web container.

To support the host-based routing, you must register a custom domain and create a new RecordSet in DNS Zone for each host-path.

Perform the below steps to create a DNS Zone:

- 1. Sign in to the Azure Portal using <u>https://portal.azure.com</u>.
- 2. After a successful sign in, click Create a resource and search for the DNS Zone.

Microsoft Azure	${\cal P}$ Search resources, services, and d	ocs (G+/)
«	All services >	
+ Create a resource	New	
A Home		
📶 Dashboard	₽ DNS Zo	×
⊨ All services	DNS zone	^
★ FAVORITES		
Resource groups	Private DNS zone	
All resources	BlueCat DNS for Azure Recently created	
(Recent	AI + Machine Learning	Ubuntu Server 18.04 LTS
📀 App Services	Analytics	2 Learn more
🟆 Virtual machines (classic)	Blockchain	Web App
早 Virtual machines	Compute	Quickstarts + tutorials
🧧 SQL databases	Containers	SOL Database
Cloud services (classic)	Databases	Quickstarts + tutorials
📍 Subscriptions	Developer Tools	
Azure Active Directory	DevOps	Function App Quickstarts + tutorials
🕑 Monitor	Identity	

Figure 2.51

3. Click Create.

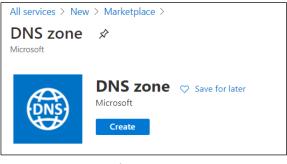


Figure 2.52

- 4. On the **Create DNS zone**, specify the following details under the **Basics** tab:
 - a. **Subscription**: Select a valid Azure subscription.
 - b. Resource group: Select or create an Azure Resource group, such as AzureKubernetes.
 - c. Name: Specify a valid DNS Zone name such as azure.co.in.
 - d. Click **Next: Tags**>.

All services > New > Marketplace	> DNS zone >	
Create DNS zone		
Basics Tags Review + create		
number of DNS records such as 'mail.co	cords for a particular domain. For example, the domain 'contoso.co ontoso.com' (for a mail server) and 'www.contoso.com' (for a web s manage your DNS records, and provides name servers that will res at you create. Learn more.	site). Azure DNS
Project details		
Subscription *	Visual Studio Enterprise with MSDN	\sim
Resource group *	AzureKubernetes	\sim
	Create new	
Instance details		
This zone is a child of an existing z	one already hosted in Azure DNS 🕕	
Name *	azure.co.in	\checkmark
Resource group location ①	Southeast Asia	\sim
Review + create Previous	Next : Tags > Download a template for automation	

Figure 2.53

- 5. On the Tags tab, keep the default options and click Next: Review + create>.
- 6. On the **Review + create** tab, click **Create** once validation is passed.

All services $>$ New $>$ Marketplace $>$ DNS zone $>$	
Create DNS zone	
() Validation passed	
Basics Tags <u>Review + create</u> Summary	
Basics Subscription Resource group Resource group location Name	Visual Studio Enterprise with MSDN AzureKubernetes southeastasia azure.co.in
Create Previous Next	Download a template for automation

Figure 2.54

7. Once deployment is complete, click **Go to resource**. The Created DNS Zone's Overview screen appears.

azure.co.in - Microsoft Azure 🗙 🗙	+					\sim	- 0	
> C 🔒 portal.azure.com/	/#@shubhammittal95outlo	ok.onmicrosoft.com/resource/subscr	iptions/eaa50193-52a1-	4c05-9acb-530a09d127c7/resou	cegroups 🖻 🕁	e 🔒 12	🖵 🗯 🌗	R
Microsoft Azure 🔑 Se	arch resources, services, and	docs (G+/)		D R	P @ 0 R	shubham_m p	ittal95@out EFAULT DIRECTO	
Home > Microsoft.DnsZone-202111	25072135882 >							
■ azure.co.in & … DNS zone								×
₽ Search (Ctrl+/)	K + Record set +	Child zone $ ightarrow$ Move $ ightarrow$ 📋 Delet	te zone 💍 Refresh					
Overview	Essentials						JSON Vie	W.
Activity log	Resource group (Mov	re) : azurekubernetes		Name server 1 : ns1-01.az	ure-dns.com.			
Access control (IAM)	Subscription (Move)	: Visual Studio Enterprise		Name server 2 : ns2-01.az	ure-dns.net.			
Tags	Subscription ID	: eaa50193-52a1-4c05-9acb-530a09	d127c7	Name server 3 : ns3-01.azi	ire-dns.org.			
				Name server 4 : ns4-01.az	ure-dns.info.			
Diagnose and solve problems	Tags (Edit)	: Click here to add tags						
iettings	A You can search for re	cord sets that have been loaded on this	nage If you don't see w	at you're looking for you can try o	rolling to allow more recor	d sets to load		
Properties	Search record sets	cord sets that have been loaded on this	page. If you don't see wi	at you re looking for, you can try st	to allow more recon	a sets to load.		
Locks	Name	Туре	TTL	Value	Alias resource type	Alias target		
Monitoring Alerts	©	NS	172800	ns1-01.azure-dns.com. ns2-01.azure-dns.net. ns3-01.azure-dns.org. ns4-01.azure-dns.info.				
Metrics				Email: azuredns-hostma Host: ns1-01.azure-dns. Refresh: 3600				
Tasks (preview)	Ø	SOA	3600	Retry: 300 Expire: 2419200 Minimum TTL: 300				



- 8. On the top of the **DNS Zone** tab, select + **Record set**.
- 9. On the **Add record set** tab, type or select the following values:
 - a. Name: Enter the user-defined name.

- b. Type: Select type as "A IPv4-address"
- c. Alias record set: Select alias as Yes.
- d. Alias type: Select the alias type as Azure resource.
- e. Choose a subscription: Select a valid Azure subscription.
- f. Azure resource: Select the Public IP Address created for the Application Gateway that is, appgwublicip.
- g. **TTL (Time To Live):** Time-to-live of the DNS request specifies how long DNS servers and clients can cache a response.

NOTE:

There is no change in the default value.

h. Click OK to save the record set.

👗 Add record set - Microsoft Azure 🗙	+				v -	- ø ×
	n/#@shubhammittal95out	look.onmicrosoft.com/resource/subscriptions	/eaa50193-52a	1-4c05-9acb-530a09d127	」 IEL 🜔 歳 の 戻 shubham_mit	
Home > Microsoft.DnsZone-20211	125072135882 >	- Child zone → Move ✓ 🔋 Delete zone ove) : azurekubernetes		Name server 1 : Name server 2 : Name server 3 : Name server 4 :		AULT DIRECTORY
Settings	Tags (Edit) You can search for	: Click here to add tags record sets that have been loaded on this page.	If you don't see v	what you're looking for, you	Azure resource Zone record set Choose a subscription *	
Properties	Search record sets	Туре	TTL	Value	Visual Studio Enterprise Azure resource *	~
Monitoring Alerts	©	NS	172800	ns1-01.azure ns2-01.azure ns3-01.azure ns4-01.azure	appgwpublicip TTL * TTL unit	~
nă Metrics Automation 그 Tasks (preview) 및 Export template	œ	SOA	3600	Email: azurec Host: ns1-01. Refresh: 3600 Retry: 300 Expire: 24192 Minimum TT Serial numbe	1 Hours	~

Figure 2.56

10. Similarly, you can add other record sets for each host-path defined in *AppGateway-IngressController.yaml* file.

🛕 azure.co.in - Microsoft Azure 🛛 🗙	+					\sim	- 0	3
+ > C 🔒 portal.azure.com	n/#@shubhammittal95outlook.on	microsoft.com/resource/subsc	riptions/eaa50193-52a1-	4c05-9acb-530a09d127c7/resourc	egroups 🖄 🕁	e 🔥 B	🖵 🛪 🌾	R
🗏 Microsoft Azure 🔑 s	earch resources, services, and docs (G+/)			🖉 🐵 🛛 🖓		mittal95@ou DEFAULT DIRECT	
Home > Microsoft.DnsZone-20211	125072135882 >							
Bazure.co.in ☆ ·· DNS zone	10							×
	« + Record set + Child	zone \rightarrow Move \checkmark 📋 Dele	ete zone 💍 Refresh					
10 0 K	Subscription ID : e	aa50193-52a1-4c05-9acb-530a0	9d127c7	Name server 3 : ns3-01.azur	e-dns.org.			
Tags				Name server 4 : ns4-01.azur	e-dns.info.			
Diagnose and solve problems	Tags (Edit) : C	lick here to add tags						
Settings	You can search for record s	ets that have been loaded on th	is page. If you don't see wi	nat you're looking for, you can try scro	olling to allow more reco	rd sets to load.		
Properties	Search record sets							
🔒 Locks	Name	Туре	TTL	Value	Alias resource type	Alias targe	t	
Monitoring				ns1-01.azure-dns.com. ns2-01.azure-dns.net.				
Alerts	Ø	NS	172800	ns3-01.azure-dns.org.				•••
Metrics				ns4-01.azure-dns.info. Email: azuredns-hostma				
Metrics				Host: ns1-01.azure-dns				
	œ	SOA	3600	Refresh: 3600 Retry: 300				
Automation	©	SOA	3600	Retry: 300 Expire: 2419200				
Automation	0	SOA	3600	Retry: 300				
Automation asks (preview) Export template	© ibps5serviceinstance	SOA	3600 3600	Retry: 300 Expire: 2419200 Minimum TTL: 300	Public IP Address	appgwpub	licip	
Automation				Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1	Public IP Address Public IP Address	appgwpub	0.5	

Figure 2.57

2.8 Run Kubectl from local machine

Before running the kubectl commands from your local machine, you must have the following prerequisites:

- kubectl: https://kubernetes.io/docs/tasks/tools/install-kubectl/
- azure-cli: <u>https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?tabs=azure-</u>cli
- Delete the .kube folder from C:\Users\<Logged-in UserName> folder if exists.
- Now execute the below command to worker node:

```
az aks get-credentials --resource-group <ResourceGroupName> --name
<AzureEKSClusterName>
```

For example,

```
az aks get-credentials --resource-group AzureKubernetes --name BPMSuite-AKSCluster
```

 Once you have run the above command to connect to the AKS cluster, you can run any kubectl commands. Here are a few examples of useful commands you can try.
 For example,

```
# List all the pods
    kubectl get pods
```

```
# List all deployments in all namespaces
kubectl get deployments --all-namespaces=true
# List all deployments in a specific namespace
# Format :kubectl get deployments --namespace <namespace-name>
kubectl get deployments --namespace kube-system
```

2.9 Monitor Kubernetes dashboard

- The Azure portal includes a Kubernetes resource view for easy access to the Kubernetes resources in your Azure Kubernetes Service (AKS) cluster.
- To see the Kubernetes resources, navigate to your AKS cluster in the Azure portal. The navigation pane on the left is used to access your resources. The resources include:
 - **Namespaces:** Displays the namespaces of your cluster. The filter at the top of the namespace list provides a quick way to filter and display your namespace resources.
 - **Workloads:** Displays information about deployments, pods, replica sets, stateful sets, daemon sets, jobs, and cron jobs deployed to your cluster.
 - Services and ingresses: Display all of your cluster's service and ingress resources.
 - **Storage:** Displays your Azure storage classes and persistent volume information.
 - **Configuration:** Displays your cluster's config maps and secrets.

BPMSuite-AKSCluster - Microsoft × +					~	- 6	9
· → C	ammittal95outlook.onmicrosoft.com/resou	urce/subscriptions/eaa50193-52a1-4c05-	9acb-530a09d127c7/reso	urceGroups 🖻	1 🗗 🖓	18 🕂 🛊	
■ Microsoft Azure P Search resource	ces, services, and docs (G+/)			0 © 0	R shubha	m_mittal95@c DEFAULT DIREC	
Home > Kubernetes services > BPMSuite-AKS	Cluster						
Kubernetes services « Default Directory	BPMSuite-AKSClus	ster Workloads					×
+ Create 🗸 🔞 Manage view 🗸 …		+ Add 🗸 📋 Delete 🖒 Refre	esh 💴 Show labels 🔗	Give feedback			
Filter for any field	😨 Overview	Deployments Pods Replica	sets Stateful sets I	Daemon sets Job	os Cron jobs		
Name ↑ 🖕	Activity log			10021			
BPMSuite-AKSCluster ····	Access control (IAM)	Filter by deployment name Enter the full deployment name	Filter by label select	132	Filter by name		~
	 Diagnose and solve problems Security 	Name	Namespace kube-system	Ready	Up-to-date	Available	
	Kubernetes resources	coredns	kube-system	⊘ 2/2	2	2	
	Namespaces Workloads	metrics-server	kube-system	☑ 1/1	1	1	
	Services and ingresses	omsagent-rs	kube-system	☑ 1/1	1	1	
	Storage	konnectivity-agent	kube-system	✓ 2/2	2	2	
		azuredefender-collector	kube-system	❷ 1/1	1	1	
	Configuration						
	Configuration Settings	< [

Figure 2.58

2.10 Azure monitor for container insights

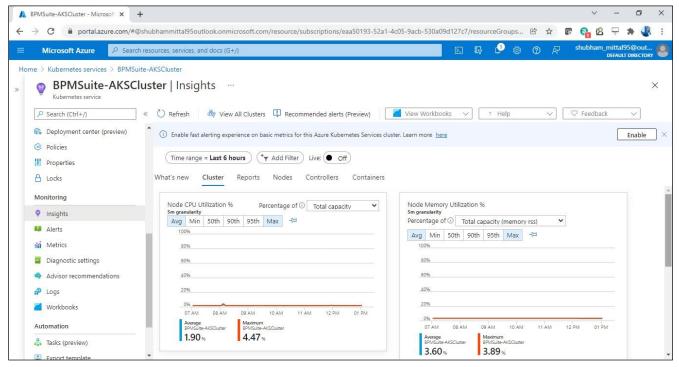
Azure Monitor for containers is a feature designed to monitor the health and performance of container workloads deployed to Azure Kubernetes service. It delivers a comprehensive monitoring experience and gives us performance visibility by collecting memory and processor metrics from controllers, nodes, and containers that are available in Kubernetes through the Metrics API. By default, Azure Monitor is enabled for container monitoring during Azure Kubernetes service creation (Under Integrations tab).

Basics Node pools Auth	entication Networking Integratio	ns Tags Review + create
Connect your AKS cluster with ad	ditional services.	
Azure Container Registry		
		oyments from a private image registry. You can
create a new registry or choose o	ne you already have. Learn more about Azu	re Container Registry 🗠
Container registry	None	~
In addition to the CPU and memo	Create new ry metrics included in AKS by default, you Il performance and health of your cluster.	
In addition to the CPU and memo comprehensive data on the overa settings. Learn more about container perfo	ry metrics included in AKS by default, you Il performance and health of your cluster. B	an enable Container Insights for more illing is based on data ingestion and retention
	ry metrics included in AKS by default, you Il performance and health of your cluster. B	
In addition to the CPU and memo comprehensive data on the overa settings. Learn more about container perfo Learn more about pricing	ry metrics included in AKS by default, you o Il performance and health of your cluster. Prmance and health monitoring	illing is based on data ingestion and retention
In addition to the CPU and memo comprehensive data on the overa settings. Learn more about container perfo Learn more about pricing	ry metrics included in AKS by default, you on Il performance and health of your cluster. Finance and health monitoring Enabled O Disabled Azure monitor is recommend	illing is based on data ingestion and retention

Figure 2.59

Perform the below steps to view the container insights:

- 1. Sign in to the Azure portal at <u>https://portal.azure.com</u>.
- 2. On the Azure portal menu or from the Home page, select All resources.
- 3. Click on the created Kubernetes service.
- 4. Click **Monitoring >> Insights**. Here are the series of tabs to monitor your AKS Cluster, Nodes, Containers, Controllers, and so on.





3 Deployment of OmniDocs containers on Azure Kubernetes service

This section describes the deployment of OmniDocs containers. Refer the below sections for procedural details.

3.1 Prerequisites

Azure Kubernetes Service must be configured, and its Worker nodes must be in Ready state.

NOTE:

Refer to the Configuration of Azure Kubernetes Cluster for the configuration of Azure Elastic Kubernetes Service.

3.2 Deliverables

Newgen has isolated the product suite into multiple Docker containers to enable the independent scalability of each Docker container. This separation is done based on the product's usability. At a broad level, Web components and EJB components are isolated for deployment in separate container instances. Web components is deployed on the underlying web server JBoss WebServer 6.0.x. EJB components is deployed on the underlying application server JBoss EAP 7.4.x. Newgen has released multiple Docker images for the different product suites along with some configuration files for data persistence, YAML files for deployment, and some documentation for end-to-end configurations and deployments.

The followings are the list of deliverables:

The Newgen delivers the following:

- Docker Images
- <u>Configuration Files</u>
- YAML Files

3.2.1 Docker images

The following Docker images are delivered for the initial product deployment:

- OmniDocs Web Components
- OmniDocs Web Service Components
- OmniDocs EJB Components
- OmniDocs Add-on Services (Wrapper, AlarmMailer, Scheduler, ThumbnailManager and LDAP)
- EasySearch (Apache Manifold only)
- Text Extraction Manager or Full-Text Search (TEM/FTS)
- OmniScan Web Components
- OmniDocs WOPI

NOTE:

These Docker images can be delivered to a private Docker repository like ACR (Azure Container Registry) or in the form of compressed files that can be shared over the FTP or similar kind of media.

3.2.2 Configuration files

Configuration files are dynamic in nature and data is written at runtime. Database details in configuration files such as *Server.xml* and *standalone.xml* are written at runtime. These types of files must be kept outside the container to persist the data. Here, Azure FileShare is used to persist configuration files.

The following configuration files are shared for OmniDocs Docker images:

- OmniDocsWeb
- OmniDocsEJB
- ODServices
- EasySearch
- TEM
- OmniScanWeb7.0
- OmniDocsWOPI

3.2.3 YAML files

YAML files stands for "YAML Ain't Markup Language". It is a human-readable object configuration file that is used to deploy and manage the objects on the Kubernetes cluster. In other words, it is a manifest file that contains the deployment descriptor of Kubernetes containers. You can execute YAML files using "kubectl apply –f <YAMLFile>" or use these files in Azure DevOps Release Pipeline to deploy the containers.

The following configuration files has shared for OmniDocs Docker images:

- OmniDocsWeb.yml
- OmniDocsWeb_Services.yml
- OmniDocsEJB.yml
- OmniDocsServices.yml
- EasySearch_ApacheOnly.yml
- TEM.yml
- OmniScanWeb7.0.yml
- OmniDocswopi.yml
- AzureFile_PV_PVC.yml
- AppGateway-IngressController.yml

Here's an example of a YAML file:





AzureFile_PV_PVC.yml file is used for Persistent Volume and Persistent Volume Claim. Persistent Volume (PV) is a storage piece in the cluster that is provisioned using Storage Classes. It contains the Azure FileShare **secretName** and **shareName** that is already created during Azure FileShare creation. It is also used to set the access permission on Azure FileShare using **mountOptions** attribute.

A PersistentVolumeClaim (PVC) is a request for storage by a user. It is similar to a Pod. Pods consume node resources and PVCs consume PV resources. Pods can request specific levels of resources (CPU and Memory). Claims can request specific size and access modes (for example, they can be mounted ReadWriteOnce, ReadOnlyMany or ReadWriteMany).

AppGateway-IngressController.yml is used for the ingress controller. An ingress controller is an object running inside the Kubernetes cluster that is used to manage the host-based routing rules. For example, you can set the host-based routing rules like if the URL is omnidocs.newgendocker.com then the ingress controller redirects the user request to OmniDocs

WEB containers. and if the URL is *omniscan.newgendocker.com* then it redirects the user request to the OmniScan WEB containers.

NOTE:

You can store the above YAML files in Azure Repo that is used by Azure DevOps Release Pipeline.

3.3 Changes in product's YAML files

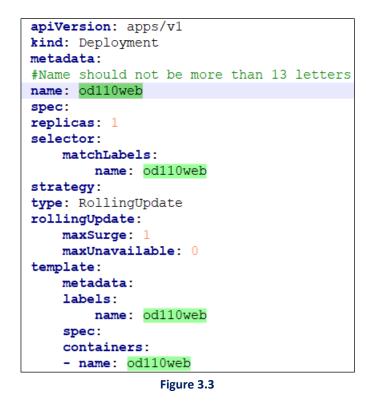
The changes in the Product's YAML Files are as follows:

• **Namespace**: In the YAML files, default namespace is given as **dev**. You can change this name as per your requirement.



Figure 3.2

 Name: In the OmniDocsWeb.yml file, od110web is given as the default name of Kubernetes objects - deployment, replicas, container, and service. You can change this name as per your requirement. While changing the name, ensure that this name is not more than 13 letters in length and must contain small letters only. For example,



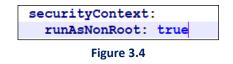
- **Replica:** In the *OmniDocsWeb.yml* file, the default replica is given as **1**. That means only one container is created after the deployment. You can increase this number as per our choice.
- Image: In the *OmniDocsWeb*.yml file, update the image location. By default, the below value is given:

image: newgencontainerregistry.azurecr.io/omnidocsll.0web:#{RELEASE.ARTIFACTS._OMNIDOCSll.0WEB.BUILDID}#

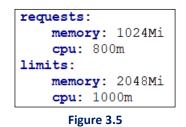
Here:

- > **newgencontainerregistry.azurecr.io** It's the name of the Azure Container Registry.
- > omnidocsweb It's the OmniDocsWeb Docker image name.
- #{RELEASE.ARTIFACTS._OMNIDOCSWEB.BUILDID}#: It's a Docker image's tag name in the form of a dynamic variable whose value gets updated at runtime using AzureDevOps Release
 Pipeline. Specify the static tag name like latest, build-number1, and so on.

• SecurityContext: In the OmniDocsWeb.yml file, SecurityContext [runAsNonRoot: true] is defined. It means the OmniDocsWeb container can never be run with root privileges. If any container tries to run with the root user, then Kubernetes stops its deployments.



 Resource Request and limit: In the OmniDocsWeb.yml file, resource request and resource limit parameters are defined. The request parameter specifies the minimum required resources to run the particular container and the limit parameter specifies the maximum resource limit that a container can use. In other words, a running container is not allowed to use more than the resource limit you set. For Example,



Here, 1000m CPU = 1 Core CPU

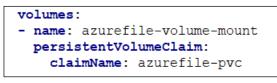
The above-specified limit is the minimum required resource to run a container. If users are increasing, then you must increase the limit range accordingly.

• VolumeMounts and Volume: Volume mounts and volumes are used to persist the data outside the container so that whenever the container terminates due to any reason our data is always persisted. In the *OmniDocsWeb.yml* file, we have persisted configuration files or folders and log files.

volumeMounts:
- name: azurefile-volume-mount
<pre>mountPath: /Newgen/jws-6.0/tomcat/bin/Newgen/NGConfig</pre>
<pre>subPath: OmniDocsll.0SPl/OmniDocsll.0Web/Newgen/NGConfig</pre>
- name: azurefile-volume-mount
<pre>mountPath: /Newgen/jws-6.0/tomcat/conf/web.xml</pre>
<pre>subPath: OmniDocsll.0SPl/OmniDocsll.0Web/web.xml</pre>
- name: azurefile-volume-mount
<pre>mountPath: /Newgen/jws-6.0/tomcat/conf/redisson.yaml</pre>
<pre>subPath: OmniDocsll.0SPl/OmniDocsll.0Web/redisson.yaml</pre>
- name: azurefile-volume-mount
<pre>mountPath: /Newgen/jws-6.0/tomcat/lib/jboss-ejb-client.properties</pre>
<pre>subPath: OmniDocsll.0SPl/OmniDocsll.0Web/jboss-ejb-client.properties</pre>
- name: azurefile-volume-mount
<pre>mountPath: /Newgen/jws-6.0/tomcat/logs</pre>
<pre>subPathExpr: OmniDocsll.0SPl/ProductLogs/odll0web-#{RELEASE.RELEASENAME}#/tomcat_logs/\$(POD_NAME)</pre>
- name: azurefile-volume-mount
<pre>mountPath: /Newgen/jws-6.0/tomcat/bin/Newgen/NGLogs</pre>
<pre>subPathExpr: OmniDocsll.0SPl/ProductLogs/odll0web-#{RELEASE.RELEASENAME}#/NGLogs/\$(POD_NAME)</pre>
- name: azurefile-volume-mount
<pre>mountPath: /Newgen/jws-6.0/tomcat/bin/Newgen/NGTemp</pre>
<pre>subPath: OmniDocsll.0SP1/ProductLogs/odl10web-#{RELEASE.RELEASENAME}#/NGTemp</pre>
- name: azurefile-volume-mount
<pre>mountPath: /Newgen/jboss-eap-7.4/bin/SystemReports</pre>
subPath: OmniDocs11.0SP1/SystemReports

Figure 3.6

In volumeMounts, **mountPath** is a path inside the container that is mounted. Here, mountPath cannot be changed as this structure is predefined in a Docker container. **subPath** works as a relative path that is appended to the attached persistent volume's shareName. **subPathExpr** is used to segregate the product logs container wise. In addition, the **name** is a user-defined name that must be matched with the name specified in volumes.



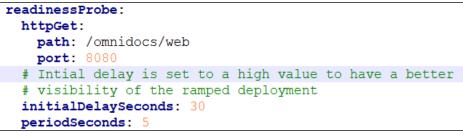


In volumes, azurefile-pvc is the persistent volume claim name.

• **Ports:** In the *OmniDocsWeb.yml* file, containerPort is specified as **8080**. That means only port 8080 is exposed outside the container and no other port is accessible from outside.

ports:	
- name: http	
containerPort:	8080
Figure 3.8	

• **ReadinessProbe:** The kubelet uses the readiness probe to know when a container is ready to start accepting traffic. Until unless the readiness probe is not succeeded, the container does not serve the user requests.





Here, until unless *ip:port/omnidocs/web* is not accessible through a browser, the container does not accept the user request.

• LivenessProbe: Docker containers have healing power, if an application running inside the container gets down due to any reason or becomes unresponsive then Kubernetes restarts the application automatically inside the container. This feature is known as LivenessProbe in Kubernetes.

For Example,

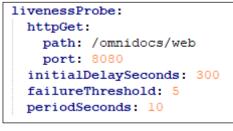


Figure 3.10

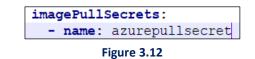
• Environment variable: In the *OmniDocsWeb.yml* file, the JAVA_OPTS parameter is defined that is used to set the heap size in the WEB container dynamically.

```
- name: JAVA_OPTS
value: "-XX:+UseContainerSupport -XX:+DisableExplicitGC -XX:InitialRAMPercentage=50.0"
```

Figure 3.11

Ensure '-**XX:MaxRAMPercentage'** is a parameter through which you can provide the available memory to use as a max heap size to JVM. In the above example, 75% of total memory is allocated as heap size.

 ImagePullSecret: ImagePullSecret is a secret value that is used to pull an image from a private container repository like Azure Container Registry.
 For example,



Execute the below command to create an ImagePullSecret: kubectl create secret docker-registry azurepullsecret --docker-server newgencontainerregistry.azurecr.io --docker-username= newgencontainerregistry --docker-password kmPF/ytffu5q6NazqvVYtJ??????

You can also create ImagePullSecret from Azure DevOps Release Pipeline.

NOTE:

You can use the above guidelines to update other YAML Files that are as follows:

- OmniDocsWeb_Services.yml
- OmniDocsEJB.yml
- OmniDocsServices.yml
- EasySearch_ApacheOnly.yml
- TEM.yml
- OmniScanWeb7.0.yml
- OmniDocswopi.yml

3.4 Changes in application gateway Ingress YAML files

Along with the product's YAML file, AppGateway Ingress Controller's YAML file **AppGateway**-**IngressController.yaml** is also shared. Using an ingress controller and ingress rules, a single IP address can be used to route traffic to multiple services in a Kubernetes cluster. The AppGateway Ingress Controller creates a Load Balancer with its external IP and routes the incoming requests to the target Kubernetes services according to the host-based routing rules. Host-based routing is a capability of Ingress Controller that redirects the user requests to the right service based on the request-host header.

For example, you can set the rules as below:

- If URL is *omnidocs.newgendocker.com*, then redirect to the OmniDocsWeb container.
- If URL is *omniscan.newgendocker.com*, then redirect to the OmniScanWeb container.

NOTE:

To support the host-based routing, register a domain and create a new RecordSet in DNS Zone for each host-path. Refer to the document <u>Configuration of Azure Kubernetes Cluster</u> to see the configuration of Application Gateway Ingress Controller and DNS Zone.

• Once Application Gateway Ingress is configured and RecordSets are created in DNS Zone, then must deploy the Ingress controller along with its ruleset using the YAML file.

```
apiVersion: networking.k8s.io/vl
cind: Ingress
netadata:
 name: appgw-ingress
 namespace: dev
 annotations:
   kubernetes.io/ingress.class: azure/application-gateway
   appgw.ingress.kubernetes.io/ssl-redirect: "true"
   appgw.ingress.kubernetes.io/request-timeout: "300"
   appgw.ingress.kubernetes.io/ssl-policy: "AppGwSSlPolicy20170401S"
spec:
 tls:
   - hosts:

    newgendocker.com

   - secretName: appgw-cert
 rules:
 - host: omnidocs.newgendocker.com
   http:
     paths:
     - path: /
       pathType: Prefix
       backend:
          service:
           name: odl10web
           port:
             number: 8080

    host: omnidocswebservices.newgendocker.com

   http:
     paths:
     - path: /
       pathType: Prefix
       backend:
          service:
            name: odll0websvc
            port:
              number: 8080
 - host: apachemanifold.newgendocker.com
```

Figure 3.13

- In *AppGateway-IngressController.yml* file, there are multiple host-based rules defined.
 - omnidocs.newgendocker.com [Specified as a record set in Route-53] If the host URL is omnidocs.newgendocker.com, then it redirects the user request to the od110web container's service which is running on port 8080. Here, od110web is the name of the OmniDocsWeb container.
 - omnidocswebservices.newgendocker.com [Specified as a record set in Route-53] If the host URL is omnidocswebservices.newgendocker.com, then it redirects the user request to the od110websvc container's service which is running on port 8080. Here, od110websvc is the name of the OmniDocs Web Service container.
 - omnidocsconsole.newgendocker.com [Specified as a record set in Route-53] If the host URL is omnidocsconsole.newgendocker.com, then it redirects the user request to the od110ejb container's service which is running on port 9990. Here, od110ejb is the name of the OmniDocsEJB container.
 - apachemanifold.newgendocker.com [Specified as a record set in Route-53] If the host URL is *apachemanifold.newgendocker.com* then it redirects the user request to the easysearch11 container's service which is running on port 8345. Here, easysearch11 is the name of the EasySearch container.
 - omniscan.newgendocker.com [Specified as a record set in Route-53] If the host URL is omniscan.newgendocker.com, then it redirects the user request to the omniscan web container's service which is running on port 8080. Here, omniscanweb is the name of the OmniScan Web container.
- In this YAML file, change the host URL, ServiceName, ServicePort, and the name **name: appgw-ingress** as required.
- In this YAML file, there is defined SSL or TLS configuration through specifying the **tls** spec along with hosts and secretName.



- You can specify the valid DNS against hosts that is, newgendocker.com.
- Before deploying the ingress controller, create a Kubernetes secret to host the certificate and private key. Execute the below command to create a Kubernetes secret:

```
kubectl create secret tls <secret-name> --key <path-to-key> --cert <path-
to-crt> -n <Namespace>
```

For example,

```
kubectl create secret tls appgw-cert --key azure.key --cert azure.crt -n
dev
```

• After making the required changes as required, deploy the Ingress controller by executing this YAML file using below command or can configure it to AzureDevOps Release Pipeline. kubectl apply -f AppGateway-IngressController.yml

NOTE:

To execute the above command, kubectl must be configured on your local server. Refer to the <u>Configuration of Azure</u> <u>Kubernetes Cluster</u> to run kubectl from your local machine.

3.5 Changes in configuration files

This section describes the changes in configuration files.

3.5.1 Prerequisites

The Prerequisites are as follows:

- All the configuration files and folders must be uploaded to the Azure FileShare defined in the YAML file *AzureFile_PV_PVC.yml*. You can upload the configuration files and folder using Azure Storage Explorer.
- The Redis Cache server is already configured.
- A valid wildcard certificate and the domain are already configured.
- SSL or TLS must be configured at the Ingress Controller or Load balancer level.

NOTE:

By default, all Docker containers are running with HTTPS protocol only. If you want to run with HTTP protocol, then some additional settings must be required. For more details, refer to the *Docker Troubleshooting Guide*.

3.5.2 OmniDocsWeb changes

The changes in OmniDocsWeb are as follows:

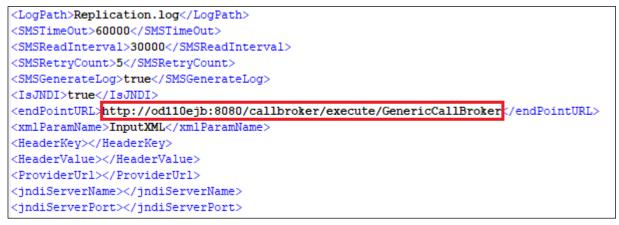
 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in NGOClientData.xml file in between the <endPointURL></endPointURL> tags located inside the OmniDocsWeb\Newgen\NGConfig\ngdbini folder at the mapped location on the Worker node.



Figure 3.15

Here, **od110ejb** is the name of the OmniDocsEJB container.

 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in IS.ini file in between the <endPointURL ></endPointURL > tags located inside the OmniDocsWeb\Newgen\NGConfig folder at the mapped location on the Worker node. For example,





• Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in *jboss-ejb-client.properties* file located inside the OmniDocsWeb folder kept inside the Azure Fileshare. For example,



Here, **od110ejb** is the name of the OmniDocsEJB container.

Update the Azure Redis cache's configuration endpoint in *redisson.yaml* file against the *singleServerConfig* or *clusterServersConfig*. If redis cache is SSL enabled then use *rediss://<endpoint url>:port* and if SSL is not enabled then use *redis://<endpoint url>:port*. This file *redisson.yaml* is located inside the OmniDocsWeb folder kept inside the Azure Fileshare.



- Figure 3.18
- Open the *web.xml* file in edit mode located inside the OmniDocsWeb folder kept inside the Azure Fileshare.

Search for filter httpHeaderSecurity and update the <param-value></param-value> tag's value with OmniDocs URL without context name against <param-name> antiClickJackingUri</param-name>.

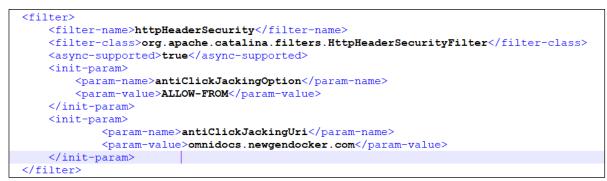


Figure 3.19

 Search for filter-class <filter-class>org.apache.catalina.filters.CorsFilter</filter-class> and update the <param-value></param-value> tag's value with OmniDocs URL with protocol against <param-name> antiClickJackingUri</param-name>.



Figure 3.20

- Open the web_svc.xml file in edit mode located inside the OmniDocsWeb folder at the mapped location on the Worker node.
- Search for filter-class "<filter-class>org.apache.catalina.filters.CorsFilter</filter-class>" and update the <param-value></param-value> tag's value with OmniDocs URL with protocol against <param-name> antiClickJackingUri</param-name>.

```
<filter>
   <filter-name>CorsFilter</filter-name>
   <filter-class>org.apache.catalina.filters.CorsFilter</filter-class>
   <init-param>
       <param-name>cors.allowed.origins</param-name>
       <param-value>https://omnidocs.bpmsoncloud.co.in</param-value>
   </init-param>
           <init-param>
                    <param-name>cors.allowed.methods</param-name>
                   <param-value>GET, POST, HEAD, OPTIONS, PUT</param-value>
            </init-param>
            <init-param>
                    <param-name>cors.allowed.headers</param-name>
                    <param-value>
                    Content-Type, X-Requested-With, accept, Origin, Access-Control-Request
                    </param-value>
            </init-param>
            <init-param>
                    <param-name>cors.exposed.headers</param-name>
                    <param-value>Access-Control-Allow-Origin</param-value>
           </init-param>
</filter>
```

Figure 3.21

3.5.3 Wrapper changes

 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in NGOClientData.xml in between the <endPointURL></endPointURL> tags file located inside the ODServices/Wrapper/ngdbini folder kept inside the Azure Fileshare.

VINIT VEISION- I.O IV	
<clientinfo></clientinfo>	
<providerurl></providerurl>	
<jndiservername></jndiservername>	
<jndiserverport></jndiserverport>	
<contextsuffix></contextsuffix>	
<wildflyusername></wildflyusername>	
<wildflypassword></wildflypassword>	
<jndicontextfactory><th>ory></th></jndicontextfactory>	ory>
	nidocs_ejb/NGOClientServiceHandlerBean!com.newgen.omni.jts.txn.NGOClientServiceHandlerHome
<adminlookupname>ejb:omnidocs_ejb/omn</adminlookupname>	idocs_ejb/NGOAdminServiceHandlerBean!com.newgen.omni.jts.txn.NGOAdminServiceHandlerHome
<pre><urlpackageprefix></urlpackageprefix></pre>	
<pre><endpointurl< pre="">http://od110ejb:8080/cal</endpointurl<></pre>	lbroker/execute/GenericCallBroker(/endPointURL>
<pre><xmlparamname>InputXML</xmlparamname></pre>	
<headerkey></headerkey>	
<headervalue></headervalue>	

Figure 3.22

Here, **od110ejb** is the name of the OmniDocsEJB container.

3.5.4 AlarmMailer changes

Prerequisite:

The cabinet is created and associated with the running containers. If the cabinet is not created, then refer to <u>Cabinet and Data Source Creation</u> section.

Make the changes in AlarmMailer that are as follows:

- Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in *IS.ini* in between the *<endPointURL></endPointURL>* tags file located inside the *ODServices* or *AlarmMailer* folder kept inside the Azure Fileshare.
 - For example,

<endPointURL>http://od110ejb:8080/callbroker/execute/GenericCallBroker</endPointURL> Here, od110ejb is the name of the OmniDocsEJB container.

 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in NGOClientData.xml in between the <endPointURL></endPointURL> tags file located inside the ODServices/AlarmMailer/ngdbini folder kept inside the Azure Fileshare. For example,

<endPointURL>http://od110ejb:8080/callbroker/execute/GenericCallBroker</endPointURL> Here, **od110ejb** is the name of the OmniDocsEJB container.

- 3. Update the below settings in the *Alarm.ini* file located inside the *ODServices/AlarmMailer* folder kept inside the Azure Fileshare.
 - Update the OmniDocs URL without context name in between the *<webservername></webservername>* tag.
 For example, *<webservername>omnidocs.newgendocker.com</webservername>* Here, *omnidocs.newgendocker.com* is the host path defined in the *AppGateway-IngressController.yml* file.
 - ii. Leave the WebServerPort as blank if OmniDocsWEB URL does not contain a port.For example, <webserverport></webserverport>
 - iii. Update the OmniDocs cabinet name in between <cabinetname></cabinetname> tag.
 For example, <cabinetname>ecmsuite</cabinetname>
 Here, ecmsuite is the OmniDocs cabinet name gets created.
 - iv. Update the OmniDocs supervisor group's user in between the <user></user> tag.
 For example, <user>supervisor</user>
 - V. Update the OmniDocs supervisor group's user password in between the
 <password></password> tag. Ensure that this password must be in an encrypted format.

For example, <password>:X-D;U:T-C;P-C;p5-C;b:d:</password>

3.5.5 LDAP changes

Prerequisite:

The cabinet is created and associated with the running containers. If the cabinet is not created, then refer to the <u>Cabinet and Data Source Creation</u> section.

The changes in LDAP are as follows: (For On_Prem Active Directory)

- Ensure that the LDAP Domain server is configured, and a private tunnel is created between the Kubernetes worker nodes and the LDAP Domain server.
- Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in *NGOClientData.xml* in between the *<endPointURL></endPointURL>* tags file located inside the *ODServices/ODAuthMgr/ngdbini* folder kept inside the Azure Fileshare. For example,

<endPointURL>http://od110ejb:8080/callbroker/execute/GenericCallBroker</endPointURL> Here, **od110ejb** is the name of the OmniDocsEJB container.

• Update the cabinet name and domain name in the Idap.ini and Hook.ini file located inside the *ODServices/ODAuthMgr* folder at the mapped location.

```
#
#Tue Nov 26 11:34:40 IST 2013
DISPort=1999
DISIPAddress=127.0.0.1
Log4j_properties_file=jtshook_log4j.properties
Encoding=UTF-8
PROTOCOL=1dap Hook.ini
LOGOUTTIME=15000
DIRECTORYSERVICE=ActiveDS
REACTUI=true
# Default domain name to add user For multidomain LDAP
DEFAULTDOMAIN=eco.com
ecmsuite=eco.com
```



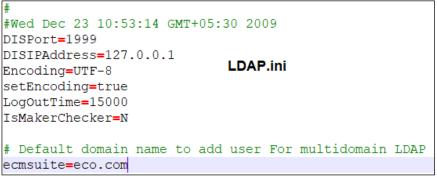


Figure 3.24

Here, **ecmsuite** is the cabinet name and *eco.com* is the domain name.

• Update the same cabinet name and domain name in the *ldap.ini* and *Hook.ini* file located inside the *OmniDocsWeb\Newgen\NGConfig* folder at the mapped location.

• Update the ODServices container's service name [Defined in respective YAML file] in *ldap.ini* and *Hook.ini* file located inside the *OmniDocsWeb\Newgen\NGConfig* folder at the mapped location.

```
*
#Tue Nov 26 11:34:40 IST 2013
DISPort=1999
DISIPAddress=odl10services
Log4j_properties_file=jtshook_log4j.properties
Encoding=UTF-8
PROTOCOL=1dap Hook.ini
LOGOUTTIME=15000
DIRECTORYSERVICE=ActiveDS
REACTUI=true
# Default domain name to add user For multidomain LDAP
DEFAULTDOMAIN=eco.com
ecmsuite=eco.com
```



```
#
#Wed Dec 23 10:53:14 GMT+05:30 2009
DISPort=1999
DISIPAddress=od110services
Encoding=UTF-8
setEncoding=true
LogOutTime=15000 Idap.ini
IsMakerChecker=N
# Default domain name to add user For multidomain LDAP
ecmsuite=eco.com
```



Here, **od110services** is the service name of the ODServices container.

 Set <Display> as true for LDAP in AdminMenuOptions.xml located inside OmniDocsWeb/Newgen/NGConfig/ngdbini/Custom/CABINETNAME folder at mapped location.

```
<SSALink>
    <LinkName>Ldap</LinkName>
    <LinkDescription>LdapDescription</LinkDescription>
    <JspName>/ldap/config.jsp</JspName>
    <Display>true</Display>
    <IconURL></IconURL>
    </SSALink>
```



The changes in LDAP are as follows: (For Azure Active Directory)

 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in *NGOClientData.xml* in between the *<endPointURL></endPointURL>* tags file located inside the *ODServices/ODAuthMgr/ngdbini* folder kept inside the Azure Fileshare. For example, *<*endPointURL>http://od110eib:8080/callbroker/execute/GenericCallBroker</endPointURL>

<endPointURL>http://od110ejb:8080/callbroker/execute/GenericCallBroker</endPointURL> Here, **od110ejb** is the name of the OmniDocsEJB container.

• Update the cabinet name, domain name, and directory service as **AzureAD** in the Hook.ini file located inside the *ODServices/ODAuthMgr* folder at the mapped location.

```
DISPort=1999
DISIPAddress=127.0.0.1
Log4j_properties_file=jtshook_log4j.properties
Encoding=UTF-8
PROTOCOL=1dap Hook.ini
LOGOUTTIME=15000
DIRECTORYSERVICE=AzureAD
REACTUI=true
# Default domain name to add user For multidomain LDAP
DEFAULTDOMAIN=eco.com
ecmsuite=eco.com
```

Figure 3.28

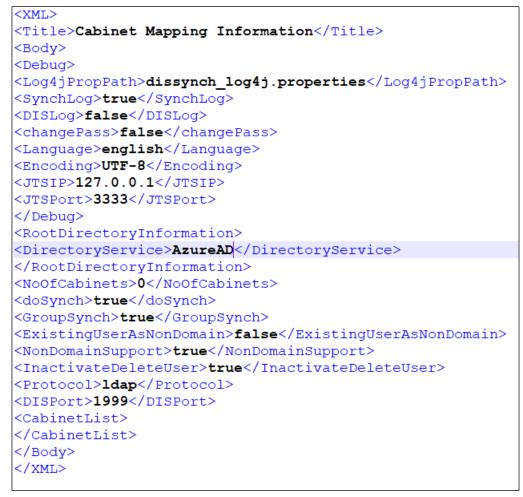
• Update the cabinet name and domain name in the *ldap.ini* file located inside the *ODServices* or *ODAuthMgr* folder at the mapped location.

#
#Wed Dec 23 10:53:14 GMT+05:30 2009
DISPort=1999
DISIPAddress=127.0.0.1
Encoding=UTF-8 LDAP.ini
setEncoding=true
LogOutTime=15000
IsMakerChecker=N
Default domain name to add user For multidomain LDAP
ecmsuite=eco.com

Figure 3.29

Here, **ecmsuite** is the cabinet name and *eco.com* is the domain name.

• Update the directory service as **AzureAD** in the DIS.xml file located inside the **ODServices** or **ODAuthMgr** folder at the mapped location.





- Update the same cabinet name and domain name in the *ldap.ini* and *Hook.ini* file located inside the **OmniDocsWeb\Newgen\NGConfig** folder at the mapped location.
- Update the ODServices container's service name [Defined in respective YAML file] in Idap.ini and Hook.ini file located inside the **OmniDocsWeb\Newgen\NGConfig** folder at the mapped location.
- Update the directory service as **AzureAD** in Hook.ini and config.ini located inside the **OmniDocsWeb\Newgen\NGConfig** folder at the mapped location.

```
DISPort=1999

DISIPAddress=odll0services

Log4j_properties_file=jtshook_log4j.properties

Encoding=UTF-8

PROTOCOL=1dap

LOGOUTTIME=15000

DIRECTORYSERVICE=AzureAD

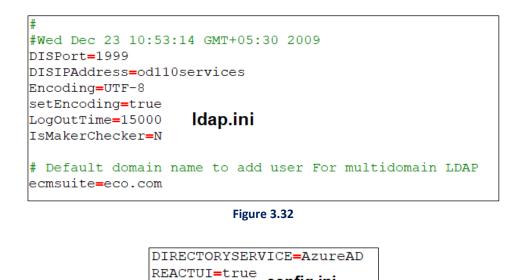
REACTUI=true

# Default domain name to add user For multidomain LDAP

DEFAULTDOMAIN=eco.com

ecmsuite=eco.com
```







config.ini

Here, **od110services** is the service name of the ODServices container.

 Set <Display> as true for Idap in AdminMenuOptions.xml located inside OmniDocsWeb/Newgen/NGConfig/ngdbini/Custom/CABINETNAME folder at mapped location. For example,

```
<SSALink>
<LinkName>Ldap</LinkName>
<LinkDescription>LdapDescription</LinkDescription>
<JspName>/ldap/config.jsp</JspName>
<Display>true</Display>
<IconURL></IconURL>
</SSALink>
```



3.5.6 SSO changes

Prerequisite:

The cabinet is created and associated with the running containers. If the cabinet is not created, then refer to <u>Cabinet and Data Source Creation</u> section.

The changes in SSO are as follows:

- Update the <*Host-Path URL of OmniDocsWeb container>* at the place of *ibps5aurora.newgendocker.com* in *mapping.xml* file located inside the *OmniDocsWeb/Newgen/NGConfig/ngdbini/SSOConFig* folder.
- Update the **CabinetName** in *mapping.xml* file located inside the *OmniDocsWeb/Newgen/NGConfig/ngdbini/SSOConFig* folder.
- Configure the CabinetName=DomainName in *sso.ini* file located inside the *OmniDocsWeb/Newgen/NGConfig/ngdbini/SSOConFig* folder.
- ecmsuite=eco.com

3.5.7 Scheduler changes

Prerequisite:

The cabinet is created and associated with the running containers. If the cabinet is not created, then refer to <u>Cabinet and Data Source Creation</u> section.

The changes in Scheduler are as follows:

 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in IS.ini in between the <endPointURL></endPointURL> tags file located inside the ODServices or Scheduler folder kept inside the Azure Fileshare.

For example,

<endPointURL>http://od110ejb:8080/callbroker/execute/GenericCallBroker</endPointURL> Here, **od110ejb** is the name of the OmniDocsEJB container.

 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in NGOClientData.xml in between the <endPointURL></endPointURL> tags file located inside the ODServices/Scheduler/ngdbini folder kept inside the Azure Fileshare. For example,

<endPointURL>http://od110ejb:8080/callbroker/execute/GenericCallBroker</endPointURL> Here, od110ejb is the name of the OmniDocsEJB container.

- Update the ODServices container's service name [Defined in respective YAML file] in *SchedulerConf.ini* file located at **ODServices** or **Scheduler** folder at the mapped location. For example: **schedulerIpAddress=od110services**
- Update the ODServices container's service name [Defined in respective YAML file] in eworkstyle.ini file located at

OmniDocsWeb/Newgen/NGConfig/ngdbini/Custom/<CABINETNAME> folder at mapped location.

For example: schedularLocation=od110services

3.5.8 ThumbnailManager changes

Prerequisite:

The cabinet is created and associated with the running containers. If the cabinet is not created, then refer to <u>Cabinet and Data Source Creation</u> section.

The changes in ThumbnailManager are as follows:

 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in IS.ini in between the <endPointURL></endPointURL> tags file located inside the ODServices or ThumbnailManager folder kept inside the Azure Fileshare. For example,

<endPointURL>http://od110ejb:8080/callbroker/execute/GenericCallBroker</endPointURL> Here, od110ejb is the name of the OmniDocsEJB container.

 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in NGOClientData.xml in between the <endPointURL></endPointURL> tags file located inside the ODServices/ThumbnailManager/ngdbini folder kept inside the Azure Fileshare. For example,

<endPointURL>http://od110ejb:8080/callbroker/execute/GenericCallBroker</endPointURL> Here, **od110ejb** is the name of the OmniDocsEJB container.

• Update the cabinet name, supervisor group's user name, and password in *ThumnailConfig.xml* located inside the **ODServices** or **ThumbnailManager** folder at the mapped location on the Worker node.

```
<cabinets><cabinet><cabinetname>ecmsuite</cabinetname><jtsip>127.0.0.1
</jtsip><jtsport>3333</jtsport><user>supervisor</user><password>:X-D;U:T-C;P-C;p5-C;b:
</password><BatchSize>10</BatchSize><priority>1</priority><encoding>UTF-8
</encoding></cabinet></cabinets>
```

Figure 3.35

3.5.9 TEM changes

Prerequisite:

The cabinet is created and associated with the running containers. If the cabinet is not created, then refer to <u>Cabinet and Data Source Creation</u> section.

The changes in TEM are as follows:

 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in IS.ini and NGOClientData.xml in between the <endPointURL></endPointURL> tags file located inside the TEM folder kept inside the Azure Fileshare. For example,

<endPointURL>http://od110ejb:8080/callbroker/execute/GenericCallBroker</endPointURL>

- Here, **od110ejb** is the name of the OmniDocsEJB container.
- Update the cabinet name in filename FTSServer-CABINETNAME-1.properties. For example: FTSServer-**ecmsuite**-1.properties [ecmsuite is the cabinet name].
- Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in FTSServerecmsuite-1.properties renamed earlier.
- Update the OmniDocs supervisor group's user name.
- Update the OmniDocs supervisor group's user password. Ensure this password must be in an encrypted format.

```
ServerAddress=od110ejb
SiteId=1
UserName=supervisor
Password=:X-D;U:T-C;P-C;p5-C;b:d:
PollTime=10
OCRPath=tesseract
DocumentCount=1000
Language=eng
SleepTime=15
```



3.5.10 EasySearch changes

Prerequisite:

The cabinet is created and associated with the running containers. If the cabinet is not created, then refer to <u>Cabinet and Data Source Creation</u> section.

The changes in EasySearch (Apache Manifold only) are as follows:

- Update the Database details in the *ESconfig.ini* file located inside the *EasySearch**ESConfigurator**conf* folder kept inside the Azure Fileshare.
 - ESClusterName=CABINETNAME_cluster
 - OdDBIPAddress=DBIP
 - OdDBPort=DBPORT
 - OdCabinetName=CABINETNAME
 - OdDBUserName=DBUSER
 - OdDBPassword=DBPASSWORD in encrypted format
 - OdDBType=sqlserver | oracle | postgres

```
ESServerTCPPort=9300
ESServerHttpPort=9200
ESProtocol=http
ESClusterName=ecmsuite_cluster
OdDBIPAddress=omnidocs-aurorards-db-instance-1-restore
OdDBPort=5432
OdCabinetName=ecmsuite
OdDBUserName=postgres
OdDBUserName=postgres
OdDBPassword=:X-D;Y-D;L-C;N-C;VSJ-C;4T-C;r
OdDBType=postgres
MCFIPAddress=127.0.0.1
```



- Update AppToBeConfigured=ApacheManifold in the *ESconfig.ini* file located inside the *EasySearch\ESConfigurator\conf* folder kept inside the Azure Fileshare
- Update the cabinet name in the **CrawlerConfig.xml** file located inside the **EasySearch\apachemanifoldcf-2.25\example** folder kept inside the Azure Fileshare.
- Update the OmniDocs supervisor group's user name.
- Update the OmniDocs supervisor group's user password. Ensure this password must be in an encrypted format.

```
(cabinets>)
<jtsip>127.0.0.1</jtsip>
<jtsport>3333</jtsport>
<StopPhraseFlag>N</StopPhraseFlag>
<StopPhrases>
<StopPhrase>Newgen Software Technologies</StopPhrase>
<StopPhrase>omnidocs</StopPhrase>
</StopPhrases>
<Pages>ALL</Pages>
<KeyVault>false</KeyVault>
<isAuthEnabled>N</isAuthEnabled>
<cabinet>
<cabinetname>odazure24nov</cabinetname>
<user>supervisor</user>
<password>:X-D;Y-D;L-C;N-C;VSJ-C;4T-C;r</password>
<ESEnabled>N</ESEnabled>
</cabinet>
</cabinets>
```

Figure 3.38

- Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in *NGOClientData.xml* and *RMClientData.xml* in between the <*endPointURL></endPointURL>* tags file located inside the EasySearch/apache-manifoldcf-2.25/example/Newgen/NGConfig/ngdbini folder kept inside the Azure Fileshare.
- Update the EnableEasySearch=Y in the *eworkstyle.ini* file located inside the *OmniDocsWeb\Newgen\NGConfig\ngdbini\Custom\CABINET_NAME* folder kept inside the Azure Fileshare.





3.5.11 WOPI changes

 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in NGOClientData.xml file in between the <endPointURL></endPointURL> tags located inside the OmniDocs_WOPI\Newgen\NGConfig\ngdbini folder at the mapped location on the Worker node.



Figure 3.40

Here, **od110ejb** is the name of the OmniDocsEJB container.

 Update the OmniDocsEJB container name [Defined in OmniDocsEJB.yml file] in IS.ini file in between the <endPointURL ></endPointURL > tags located inside the OmniDocs_WOPI\Newgen\NGConfig folder at the mapped location on the Worker node. For example,

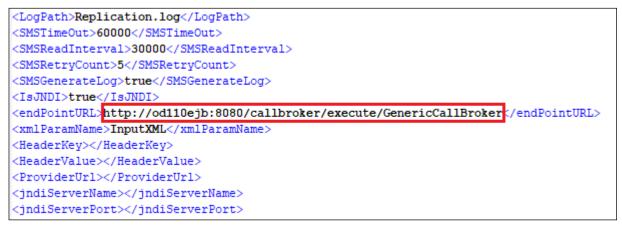


Figure 3.41

 Update the WOPI_SOURCE, OMNIDOCS_REDIRECTURL and CABINETNAME in WOPIConfiguration.ini file located inside the OmniDocs_WOPI\Newgen\NGConfig\AddInsConfig folder at the mapped location on the Worker node.



Figure 3.42

Where,

https://wopi.newgendocker.com is host URL of WOPI container. <u>https://omnidocs11alpine.newgendocker.com</u> is Host URL of Omnidocs WEB container. **odpostgres15dec** is cabinet name.

- Open the *web.xml* file in edit mode located inside the *OmniDocs_WOPI* folder at the mapped location on the Worker node.
- Search for filter-class <filter-class>org.apache.catalina.filters.CorsFilter</filter-class> and update the <param-value></param-value> tag's value with OmniDocs URL against <paramname> antiClickJackingUri</param-name> and * against <paramname>cors.allowed.origins</param-name>

<filter></filter>
<filter-name>httpHeaderSecurity</filter-name>
<filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
<async-supported>true</async-supported>
<pre><init-param></init-param></pre>
<param-name>antiClickJackingOption</param-name>
<pre><param-value>ALLOW-PROM</param-value></pre>
<init-param></init-param>
<pre><pre>aram-name>antiClickJackingUri</pre>/param-name></pre>
<pre><param-value>omnidocs11alpine2.newgendocker.com</param-value></pre>
<pre><filter></filter></pre>
<filter-name>CorsFilter</filter-name>
<filter-class>org.apache.catalina.filters.CorsFilter</filter-class>
<init-param></init-param>
<pre><pre>cors.allowed.origins</pre>/param-name></pre>
<pre><pre><rpre></rpre></pre></pre>
<init-param></init-param>
<pre><param-name>cors.allowed.methods</param-name></pre>
<pre><pre><pre><pre><pre><pre><pre><pre></pre></pre></pre></pre></pre></pre></pre></pre>
<init-param></init-param>
<pre><param-name>cors.allowed.headers</param-name></pre>
<pre><pre><pre><pre><pre><pre><pre><pre></pre></pre></pre></pre></pre></pre></pre></pre>

Figure 3.43

• Add the *CSPHeaderAllowedDomains* tag in the *eworkstyle.ini* file located inside the *OmniDocsWeb/Newgen/NGConfig/ngdbini/odwebini* folder at the mapped location on the Worker node.

- Add the WOPIOfficeExtensionSuppport and WOPIOfficeExtensionSuppportURL tag in the eworkstyle.ini file located inside the OmniDocsWeb/Newgen/NGConfig/ngdbini/Custom/CABINET_NAME folder at the mapped location on the Worker node.
 - WOPIOfficeExtensionSupport = doc, docx, DOCX, DOC, xls, xlsx, XLSX, XLS, ppt, pptx, PPTX, PPT, wopitest, WOPITEST, wopitestx, and WOPITESTX
 - WOPIOfficeExtensionSupportURL = https://wopi.newgendocker.com

3.5.12 OmniScanWeb changes

Perform the below steps to register the cabinet in OmniScanWeb:

 Open the OmniScanWeb using the following URL: *http://<Host-Path URL of OmniScanWeb container>/omniscanweb* For example, <u>https://omniscan.newgendocker.com/omniscanweb</u>

2. Click **Register New Cabinet** link on the OmniScan Web login screen.

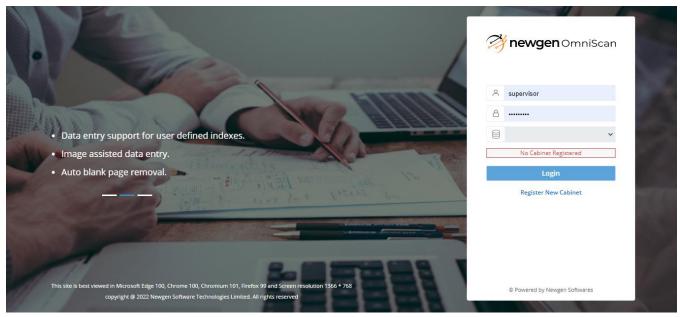


Figure 3.44

 Specify the Server URL as given below: http://<Host-Path URL of OmniDocsWeb container>/NGServlet/servlet/ExternalServlet For example,

https://omnidocs.newgendocker.com/NGServlet/Servlet/ExternalServlet

4. Specify the **OmniDocs EJB** container name for AppServer IP or Server URL, 8080 for AppServer Port, and JBOSSEAP for AppServer Type.

← Login	Register Cabinet
1 Connect	: 2 Register
Server URL	
https://omnid	locs11alpine.newgendocker.com/NGServlet/servlet/ExternalS
AppServer IP	
od110ejb	
AppServer Port	
8080	
AppServer Type	2
JBOSSEAP	~
	Connect
	Prewgen OmniScan
	© Powered by Newgen Softwares

Figure 3.45

5. Click **Connect**.

6. Select the **Cabinet Name**, **Site ID**, and **Volume ID** from the list.

← Login Register Cabinet	
Connect 2 Register	
Cabinet Name	
odpostgres19nov	~
Site ID	
odpostgres19novsite	~
Volume ID	
odpostgres19novvol	~
Register	
💏 newgen Omnis	ican
© Powered by Newgen Softwares	

Figure 3.46

7. Click Register.

Man /	newgen OmniScan
	은 supervisor
	A
Automated bulk scanning.	🗧 odpostgres19nov 🗸
Creation of document types for segregation.	Login
Definition of data classes with fields.	Register New Cabinet
Cabinet odpostgres19nov has been successfully registered in OmniDocs. Chrome 100, Chromium 101, Firefox 99 and Screen resolution 1366 + 768	D Powered by Newgen Softwares

Figure 3.47

The registered cabinet appears in the **Cabinet Name** list on the login screen. Now you can log into OmniScan Web.

NOTE:

Ensure that the **OmniScan_Template_Repository** folder is already created in OmniDocs before logging into OmniScan Web.

3.6 Deployment of containers

Perform the below steps to deploy the containers:

 Deploy the containers on Azure Kubernetes Service from your local machine by executing the below command or you can deploy them using Azure DevOps Release Pipeline. However, it recommends deploying the containers using Azure DevOps for better traceability.
 kubectl apply -f <YAML_File>

For example,

kubectl apply -f OmniDocsWeb.yml

NOTE:

- To execute the above command, kubectl must be configured on your local server. Refer to the <u>Configuration</u> <u>of Azure Kubernetes cluster</u> section to run kubectl from your local machine.
- To deploy the containers using Azure DevOps Release Pipeline, Azure DevOps must be configured. Refer to the <u>Configuration of Azure DevOps Release Pipeline</u> section.
- In Azure DevOps Pipeline, a separate Release pipeline is created for each Docker image like OmniDocsWeb, OmniDocsWebService, OmniDocsEJB, OmniDocsServices, EasySearch, TEM, and OmniScanWeb7.0.

For Example,

Services V		Q Search for service	es, features, marketplace products, and docs	[Alt+S]	🔷 omnidocs @ ngdev 🔻 🛛 Mumb	ai 🔻 Support	•
Developer Tools X CodePipeline	Develop	er Tools > CodePipe	line > Pipelines				
Source • CodeCommit	Pip	elines Info	C & Notify	View history Release change	Delete pipeline Create pipe	line	
Artifacts CodeArtifact	٩				< 1 >	0	
 Build • CodeBuild 		Name	Most recent execution	Latest source revisions	Last executed		
Deploy • CodeDeploy		OmniDocs101Se rvices-DevStage	⊘ Succeeded	Source – 7fb6f314: ok AWS-ECR-Registry – sha256:1:	9 days ago		
 Pipeline CodePipeline Getting started 		TEM101- DevStage	⊘ Succeeded	Source – 7fb6f314: ok AWS-ECR-Registry – sha256:d:	9 days ago		
Pipelines		OmniDocs101EJ B-DevStage	⊘ Succeeded	Source – 7fb6f314: ok AWS-ECR-Registry – sha256:5:	9 days ago		
Settings		OmniDocs101W eb-DevStage	⊘ Succeeded	AWS-ECR-Registry – sha256:9: Source – 7fb6f314: ok	9 days ago		
Q. Go to resource		OmniScanWeb5 0-DevStage	⊘ Succeeded	AWS-ECR-Registry – sha256:8: Source – 7fb6f314: ok	10 days ago		
Feedback		EasySearch101- DevStage	⊘ Succeeded	AWS-ECR-Registry – sha256:b: Source – 7fb6f314: ok	9 days ago		
		OmniDocs101W eb-ProdStage	⊘ Succeeded	AWS-ECR-Registry – sha256:d: Source – 7fb6f314: ok	14 days ago		
		OmniDocs101W eb-UATStage	⊘ Succeeded	Source - 7fb6f314: ok	9 days ago		

Figure 3.48

- Trigger the Release Pipeline to deploy the required Docker containers.
- Once the deployment is done, deployed containers can be visible from the Kubernetes Dashboard. Refer to the <u>Configuration of Azure Kubernetes cluster</u> to configure the Kubernetes Dashboard.

🛞 kubernetes		Q Search							+	۰	e
Cluster	Pods									÷ .	
Cluster Roles Namespaces	Name 个	Namespace	Labels	Node	Status	Restarts	CPU Usage (cores)	Memory Usage (bytes)	Age		
Nodes Persistent Volumes	easysearch101-5d9	f8d6458-ns8j9 default	app: easysearch101 pod-template-hash: 5d9f8d6458	ip-10-0-2-168.ap- south- 1.compute.interna	Running	0			.1.3.days	:	:
Storage Classes	ibps5siejb-55f5594	96-f5rt9 default	app: ibps5slejb pod-template-hash: 55f559496	Ip-10-0-2-168.ap- south- 1.compute.interna	Running	0		-	a.month		:
amespace efault 👻	ibps5siweb-698f8d	fc96-bcw2d default	app: ibps5siweb pod-template-hash: 698f8dfc96	ip-10-0-1-186.ap- south- 1.compute.interna	Running	0	-	-	.7.days	1	:
verview	ibps5siweb-698f8d	fc96-sltvm default	app: ibps5siweb pod-template-hash: 698f8dfc96	ip-10-0-2-168.ap- south- 1.compute.interna	Running	0			a.montb	ļ	:
orkloads Cron Jobs	ondeserver-8d547b	845-75ck5 default	app: nodeserver pod-template-hash: 8d547b845	ip-10-0-2-168.ap- south- 1.compute.interna	Running	0		-	2.days	1	:
Daemon Sets Deployments Jobs	od101ejb-58658d48	34d-nt8fk default	app: od101ejb pod-template-hash: 58658d484d	ip-10-0-1-186.ap- south- 1.compute.interna	Running	0			a.month	1	:
Pods Replica Sets	od101services-648	f6bbff6-lgdm7 default	app: od101services pod-template-hash: 648f6bbff6	ip-10-0-2-168.ap- south- 1.compute.interna	Running	0			38.seconds	1	:
Replication Controllers Stateful Sets	od101web-65786d4	dcc-5fgpn default	app: od101web pod-template-hash: 65786d4dcc	ip-10-0-1-186.ap- south- 1.compute.interna	Running	0			23.days		:
iscovery and Load Balancing	omsejb-559555dd8	c-nkc9j default	app: omsejb pod-template-bash: 559555dd8c	ip-10-0-1-186.ap- south-	Running	0		-	.19.days	ł	:



• Update the container's replica set from **1** (default value) to any other number in YAML files, then that number of containers is listed in Kubernetes Dashboard.

- In any case to restart the container then there are two options either redeploy the container from Azure DevOps Release Pipeline which launches the new container by following up the rolling update feature of Kubernetes or execute the restart command from Kubernetes' pod's shell.
- The restart command is different for each container. For example,

Container Name	Restart Command
OmniDocsWeb,	restartjws.sh
OmniDocsWebService	Testal gws.sh
OmniDocsEJB	restartjboss.sh
OmniDocsServices	restartalarm.sh, restartauthmgr.sh, restartscheduler.sh, restartthumbnail.sh,
Ommoocsservices	restartwrapper.sh
EasySearch	restartapache.sh
TEM	restarttem.sh
OmniScanWeb7.0	restartjws.sh
OmniDocsWOPI	restartjws.sh

 Once the EasySearch11 container is deployed, execute the below command in Kubernetes pod's shell for the 1st time to configure the Apache Manifold jobs. After that in subsequent deployments, this execution is not required. runESConfigurator.sh

3.7 Cabinet and data source creation

Prerequisites:

- OmniDocsWeb, OmniDocsEJB, and OmniDocsServices are already deployed.
- ALB Ingress Controller is already configured and deployed using the *AppGateway*-*IngressController.yml* file.
- Azure BLOB Storage is already created to store the PN files. PN files are encrypted files that contain all the added, uploaded, and scanned documents by Newgen products.

Once the above prerequisites are fulfilled, refer the below sections to create the Cabinet and Data Source.

- <u>Getting started with OSA</u>
- <u>Register JTS Server</u>
- <u>Connecting OSA to the JTS Server</u>
- Creating a Cabinet
- Associating the Cabinet
- Creating a Data Source

- <u>Registration of the Cabinet</u>
- <u>Creating Site and Volume</u>

3.7.1 Getting started with OSA

Perform the below steps to start the OSA:

- Since the container is a CLI-based deployment you can't launch any GUI-based application inside the container. But you must use the OSA to create a cabinet that is a GUI-based application. In such a case, deploy OSA to some GUI-based machine either on a local server or on an EC2 instance. Also, add an inbound rule in the Kubernetes worker node's security group to allow OSA to communicate with the OmniDocs Services container deployed on that worker node.
- 2. Once OSA is deployed on a machine, navigate to the OSA folder on that machine and double click on RunAdmin.bat (For Windows) or RunAdmin.sh (For Linux) to start OSA.
- 3. When the application is launched. The Login dialog appears.

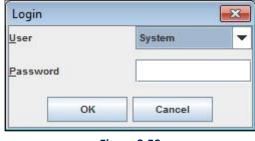


Figure 3.50

- 4. Select the user as **System** and specify the password as **system**.
- 5. Click **OK** to log in. After the successful login, the OSA screen appears displaying the list of registered services.

@ OmniDocs Service Adn	ninistration				i n a		×
Server Help							
- 🖳 Servers	Services						
	Select Service	e <all></all>	-				
		Server		Location			Sta
	Start	Stop	<u>R</u> egister	Unregister	Connect	Dis	connect
	4						•
Status							
Initialization Complete							Ready

Figure 3.51

3.7.2 Register JTS server

Perform the below steps to register the JTS Server:

1. To register the JTS server, click **Register** button. The **Register New Server** dialog appears.

Register New Se	erver		
Enter the details	5		
Server Type	JTS		-
IP Address			
Admin Port			
	ок	Cancel	



- 2. Select the JTS and specify the public IP address of the Kubernetes Worker node on which the OmniDocsServices (Wrapper, AlarmMailer, THN, and so on) container is deployed. For example, suppose there are two worker nodes in the Kubernetes cluster and after deploying the OmniDocsServices container, it gets deployed to the 1st worker node then specify the IP address of the 1st worker node. But in a case, 2 replicas are deployed on the OmniDocsServices container, one on each worker node, in that case, specify the IP address of any worker node.
- 3. Specify the Admin port of Wrapper service running inside the OmniDocsServices container. Since Wrapper is running inside the container with Admin port 9996 but that Admin port cannot be accessed directly. Kubernetes generates a random port (aka NodePort) for each port running inside the container that is exposed outside the container for public use. To get this NodePort either from Kubernetes Dashboard or by executing the below command from your local machine:

```
kubectl get svc <OmniDocsServices container name>
For example,
```

C:\WINDOWS\system	n32\cmd.exe			_		×
C:\Users\vivek NAME od101services	_kumar>kube TYPE NodePort	ctl get svc od10 CLUSTER-IP 172.20.43.136	1services EXTERNAL-IP <none></none>	PORT(S) 3333:30846/TCP_9996:31370/TCP_1999:31477/TCP	AGE 3h49i	m
C:\Users\vivek	_kumar>_					

Figure 3.53

Here, **Wrapper Admin port 9990** is exposed outside the container and Kubernetes has generated a random port **31370** as a NodePort. This NodePort keeps changing whenever you redeploy the container.

erver		×
5		
JTS		-
35.154.27.	245	
31370		
ОК	Cancel	
	JTS 35.154.27.3 31370	JTS 35.154.27.245 31370

Figure 3.54

4. Click **OK** to register the JTS Server.

3.7.3 Connecting OSA to the JTS Server

Perform the below steps to connect the OSA to the JTS Server:

1. Once the JTS Server is registered, it is displayed in the list in a disconnected state.

- 🖳 Servers	Services			
	Select Servic	e <all></all>	•	
		Server	Location	S
	JTS		35.154.27.245 : 31370	Disconnected
	Start	Stop	<u>R</u> egister <u>U</u> nregister	<u>Connect</u> Disconnect
	L			

Figure 3.55

- 2. Select the registered JTS Server and click **Connect**. Once JTS is connected, the **Manage** button gets enabled.
- 3. Click **Manage** button, after clicking on the Manage button, an entry of the connected JTS server along with its IP Address is displayed on the upper-left panel in the repository view.
- 4. Select the JTS from the repository view. The list of already created and associated cabinets, appears.

Server JTS Help					
♀	Server Information IP Addres Encoding Log Z Transaction Connect	-	SocketTimeou	Log Count 10	Adn <u>B</u> at
	Cabinet Transaction Pool CabinetName	MinDBConnections	MaxDBConnections	0.11-0	
	CabinetName	10 MinDBConnections		CabinetType Both Document Database and Ima	mssal
	ecmsuite17july	10	and the second se	Both Document Database and Ima	and the second
	Cabinet Operations				
	a constraint and a second second	Compile SP Property	Test Delete Unlock	Enable Trace Upgrade	leLicense
	Associate Dissociate	Complear Property			

Figure 3.56

3.7.4 Creating a cabinet

Perform the below steps to create a cabinet:

For MSSQL:

1. Click **Create**. The Create Cabinet dialog appears.

Create Cabinet (35.154.27.2	45 : 31370)	X
Cabinet Type		
O Document datab	ase 🔘 Image Server database 💿 Both	
Database Type		
MSSQL / Amazon	RDS Oracle O Postgres O Azure	
MSSQL Information		
Device Size (M	IB) 5 Log Size (MB) 5	
Cabinet information		
Cabinet Name		1
Server Name		j
<u>U</u> ser name]
Password		
Database Path	.mdf	1
CD Key		
Security <u>L</u> evel	Object Level	
Password Algorithm	PC1	
	Enable <u>F</u> TS	
Status		
	OK Cancel	

Figure 3.57

- 2. Select the cabinet type that needs to be created from the Cabinet Type area. The Cabinet can be a **Document database**, an **Image server database**, or both.
- 3. Select the database option from the Database Type section.
- 4. Specify the initial database size in the **Device Size** textbox and specify the initial log size in the **Log Size** textbox. Else, continue with the default values.
- 5. Specify the following cabinet information:
 - Specify the cabinet name in the **Cabinet Name** textbox.
 - Specify the server name (name of the machine where the MS SQL server is running) in the **Server I.P.** textbox.
 - Specify the username in the **User name** textbox.
 - Specify the password in the **Password** textbox.

- Specify the CD key in the **CD Key** textbox.
- Select the **Enable FTS** checkbox.

NOTE:

In the case of MSSQL if the Database port is not equal to 1433 (Default port) update the database port in the *DatabaseDriver.xml* file located inside the OmniDocsEjb/ngdbini folder kept inside the Azure FileShare before creating the cabinet.

Create Cabinet (35.154.27.2	45:31370)
Cabinet Type	
O Document datab	ase 🔾 Image Server database 💿 Both
Database Type	
MSSQL / Amazon	RDS <u>O</u> racle <u>O</u> Postgres <u>O</u> Azure
MSSQL Information	
Device Size (N	1B) 5 Log Size (MB) 5
Cabinet information	
C <u>a</u> binet Name	ecmsuite
Server Name	10.0.1.43
<u>U</u> ser name	applogin
Pass <u>w</u> ord	•••••
Database Path	ecmsuite.mdf
CD Key	38GQI0YDOyA0iokFMtD~q8old6izYz0v6ek1M
Security Level	Object Level 💌
Password Algorithm	PC1 💌
	Enable FTS
Status	
	OK Cancel

Figure 3.58

6. Click **OK** to create the cabinet. The Cabinet created successfully dialog appears.



Figure 3.59

3.7.5 Associating a cabinet

Perform the below steps to associate the cabinet:

For MSSQL:

- 1. Click **Stop** to enable the Associate button.
- 2. Click Associate. The Associate a Cabinet dialog appears with the following tabs:
 - i. Database tab: Select the database type.
 - ii. **Cabinet properties tab:** Specify the cabinet details that you have specified during cabinet creation.

Database Cabinet p	roperties	Connection	
		d the server name where and password for acces	
Cabinet Name	ecms	uite	
Map this cabinet to			
Document databa	se	🖌 Image Server datab	ase
Server Name	10.0.1	.43	
Us <u>e</u> r name	applo	gin	
Password	*****		

Figure 3.60

iii. **Connection tab:** Specify the **maximum** and the **minimum** number of connections that the JTS should maintain with the database, specify the **query time** out for the selected cabinet in the Query timeout text box and specify the **refresh interval** time for connection.

ociate a C	abinet (35.154.27.24	5:31370)		
Database	Cabinet properties	Connection		
	e number of database inet. Also specify the o			t
Ma <u>x</u> imu	im connection	25		
Minimu	m connection	10		
Query ti	imeout	0	second(s)	
Refresh	Interval	60	Minutes	

Figure 3.61

3. Click **Done** to associate the selected cabinet. Once the cabinet is associated successfully, it appears with the list.

Ø OmniDocs Service Adminis	tration			- 0	×
Server JTS Help					
9 🖳 Servers	Server Information				
P I JTS (35.154.27.245 : 3 ↓ ↓ Locks ↓ ↓ Users	Encodin	s 35.154.27.245 g UTF-8 🕶		erverP <u>o</u> rt 3333 put(mins) 30	Adr <u>B</u> al
	Log	tion 🗹 Xml 🖌 Error 🗌 Sock	Error Log Size (MB) 10	Log Count 10	
		Start	Stop Disconnect E	Ediț. <u>C</u> reate	
	Cabinet Transaction Pool CabinetName	MinDBConnections	MaxDBConnections	CabinetType	
	ecmsuitesql	10	25	Both Document Database and Ima	. mssql
	ecmsuite17july	10	10	Both Document Database and Ima	
	ecmsuite	10	25	Both Document Database and Ima	-
	Cabinet Operations Associate Dissociate	Compile SP Property	Test Delete Unloc	k Enable <u>T</u> race Upgrad	de <u>L</u> icense
< II F	1				•
Status Associate Cabinet successful	Jacob				Ready

Figure 3.62

3.7.6 Creating a data source

Perform the below steps to create the data source:

For MSSQL:

- Open the<Host-Path URL of OmniDocsEJB container> like http://ecmsuiteconsole.newgendocker.com.in as defined in the AppGateway-IngressController.yml file. It automatically redirects to the JBoss EAP 7.4 Admin console.
- 2. Enter the newgen as username and password system123# respectively to login to the Admin console. After a successful login, the Red Hat JBoss Enterprise Application Platform screen appears.

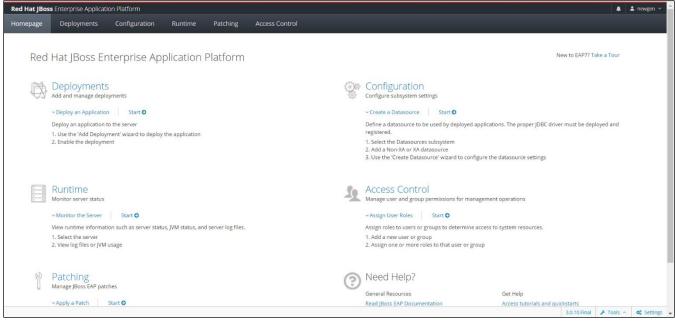


Figure 3.63

- 3. Go to the **Subsystems** in the Configuration tab.
- 4. Go to the Datasources & Drivers. Then, click Datasources.

Homepage Deployments	Configuration Runtime Patc	hing Access Control		
Configuration	Subsystem (29)	Datasources & Drivers	Datasource @- C Datacou	irces
Subsystems 2 > Interfaces > Socket Bindings > Paths System Properties	Fiter by: name or subtitle Batch Jieret Core Management Datasources & Drivers Deployment Scanners Discovery EE EJB IO Infinispan JCA JMX	Datasources O >	Filter by: nome, xa, _/disabled Add Datasource 5 Ø ExampleDS • Non-XA Ø ecmsuite17july • Xa data	I types of resources are referred to as datasources and XA datasources are used for applications which do not use ions, or applications which use transactions with a single database. sources are used by applications whose transactions are distributed nultiple databases. XA datasources introduce additional overhead.

Figure 3.64

- 5. Click Plus + icon and select Add Datasource. The Add Datasource dialog appears.
- 6. For MSSQL Database Server, select **Microsoft SQLServer** and click **Next**.

Add Datasource					×
Choose Template	Attributes	JDBC Driver	Connection	Test Connection	Review
Choose one of the prede	fined templates to quic	kly add a datasource or cho	pose "Custom" to specify	your own settings.	
 Custom 		2		, ,	
○ H2					
O PostgreSQL					
MySQL					
 Oracle 					
 Microsoft SQLServer 					
O IBM DB2					
 Sybase 					
				Cancel	< Back Next >

Figure 3.65

- 7. Provide a DataSource Name and JNDI Name.
 - Name: Enter the OmniDocs cabinet name that is cabinet name.
 - JNDI Name: java:/same as OmniDocs cabinet name
- 8. Click Next.

Add Datasource					×
Choose Template Attri	2 2	JDBC Driver	Connection	Test Connection	Review
Help Name *	ecmsuite				
JNDI Name *	java:/ecm	suite elds are marked with *			
	Required fi	elds are marked with *			
				Cancel	< Back Next >

Figure 3.66

- 9. Select JDBC Driver Name.
- 10. For MSSQL, select sqljdbc42.jar.
- 11. Clear Drive Module Name and Driver Class Name textboxes.
- 12. Click Next.

Add Datasource					×
Choose Template	Attributes	JDBC Driver	Connection	Test Connection	Review
Help					
Driver Nam	sqljdbc4	2.jar			~
Driver Module Na	me				
Driver Class Na	me				
	Required	fields are marked with *			
				Cancel	< Back Next >

Figure 3.67

13. Provide the following Connection Setting details and click Next:

- Connection URL: jdbc:sqlserver://MSSQL_Server_IP:MSSQL_Server_Port;databaseName=CABINET_NAME
- UserName: Enter the SQL Server User Name
- **Password:** Enter the SQL Server Password
- Security Domain: Keep this blank.

Add Datasource				×
Choose Template Attrib	-	Connection	Test Connection	Review
Help				
Connection URL	jdbc:sqlserver://10.0.1.43:1522;dat	abaseName=ecmsuite		
User Name	applogin			Ð
Password	·······			۲
Security Domain				۲
			Cancel	< Back Next >

Figure 3.68

14. Click Next on the Test Connection page.

Add Datasource					;	×
Choose Template	Attributes	JDBC Driver	Connection	Test Connection	Review	
On this page you can te	st the connection of your	datasource.				
Please note that testing	the connection changes	the semantics of this wiza	rd:			
 If you go back are bindings once the If you cancel the 	nd change settings, this v e datasource has been c wizard, the datasource v		ed datasource. Please no s might require a reload ill be created after finish		name and JNDI	
				Cancel	< Back Next >	>

Figure 3.69

15. Click **Finish.** After the creation of the datasource, a success message appears.

Add Datasource					×	
	butes	JDBC Driver	Connection	Test Connection	Review	
Help						
Name	ecmsuite					
JNDI Name	java:/ecmsuite					
Connection URL	jdbc:sqlserver://10.0.1.43:1522;databaseName=ecmsuite					
Driver Name	sqljdbc42.jar					
User Name	••••• •					
Password		۲				
				Cancel	< Back Finish	

Figure 3.70

16. Click View Datasource to view the created datasource. The created datasource appears in the list of Datasource.

Add Datasource					×
Choose Template	Attributes	JDBC Driver	Connection	Test Connection	Review
		•	$\mathbf{\tilde{O}}$		
		Operation	Successful		
		Datasource ecmsuite	successfully added.		
		View Dat	asource		
				Cancel	< Back Close
<u></u>				Cancer	Close

Figure 3.71

- 17. Click **View** against the datasource. A screen appears with the attributes of the datasource appears.
- 18. Click Edit link.

Red Hat JBoss Enterprise Application Platform	C Reload Required	🧟 🛔 newgen 🗸
«Back / Configuration -> Subsystems / Subsystem -> Datasourc Drivers -> / Datasource & Drivers -> Datasource -> Datasource -> ecmsuite ->		# C
ecmsuite (enabled)		
C DT COTCC (C DT CONTROLOGY)		
Attributes Connection Pool Security Credential Reference Validation Timeouts Statements / Tracking		
✓ Edit [™] DiReset [™] Help		
Datasource Class com.microsoft.sqlserver.jdbc.SQLServerDataSource		
Driver Class		
Driver Name sql/dbc42.jar		
JNDI Name java/ecmsuite		
Statistics Enabled false		
	3.0.10.Final 🖌	Tools ^ Of Settings

Figure 3.72

19. Clear the **Datasource Class** textbox and click **Save**.

Red Hat JBoss Enterprise Application Platform	ී Reload Re	equired 🦧 🌲 newgen 🗸
« Back $\ / \ $ Configuration \Rightarrow Subsystems $\ / \ $ Subsystem \Rightarrow Datasourc Drivers $\ \sim$	/ Datasources & Drivers ⇒ Datasources / Datasource ⇒ ecrnsuite ∨	# 6
CCMSUITE (enabled) A JDBC data-source configuration Attributes Connection Pool Security Credential Reference Validation	Tanut T. Statement / Tanking	
Connection Pool Security Credential Reference Validation Validation	imevus statemens navang	
Datasource Class		
Driver Class		
Driver Name • sqljdbc42.jar		
JNDI Name		
Statistics Enabled % OFF		
Required fields are marke	id with *	
	Can	cel Save
	3.0.10.Final	🖌 Tools \land 🛛 😋 Settings

Figure 3.73

- 20. After that restart the OmniDocsEJB container.
- 21. Once the OmniDocsEJB container is restarted, open the JBossEAP Admin console once again.
- 22. Go to the **Subsystems** in the Configuration tab.
- 23. Go to the Datasources & Drivers. Then, click Datasources.

Select the created data source and click **Test connection** from the dropdown list. On the successful data connection, a success message appears.

Red Hat jBoss Enterprise Application Platform 🤇 🕈 La newgen 🗸												
Homepage Deployments Configuration Runtime Patching Access Control												
Configuration			Subsystem (29)	Dataso	ources &	Drivers		Datasouro	e	⊕ ∽ <i>2</i>	ecmsuite	
Subsystems	0	>	Fiter by: name or subtitle	Datasou	urces	4	>	Filter by: nar	ne, xa,/disal	oled, deployment	Datasource	
Interfaces	- -	>	Batch JBeret	JDBC Dr	lvers		>	⊘ Exampl	eDS		O The datasource	ecmsuite is enabled. Disable
Socket Bindings		>	Core Management					🕑 ecmsul	e Disable	View ~		
Paths			Datasources & Drivers 3 >					🕝 ecmsui	Test Conner Remove	tion (5)	Main Attributes	java:/ecmsuite
System Properties			Deployment Scanners					🕑 ecmsui		_	Driver Name:	sqljdbc42.jar
5,500,000,000			Discovery								Connection URL:	jdbc:sqlserver://10.0.1.43:1522;databaseName=ecm
			EE								Enabled:	true
			EJB								Statistics Enabled:	false
			ю									
			Infinispan >									
			JCA									
			JMX									
	3.0.10.Final / Tools ~ of settings											

Red Hat JBoss Enterprise Applicat				🦨 👗 newge
Homepage Deployments	Configuration Runtime Pate	ching Access Control		
onfiguration	Subsystem (29)	Datasources & Drivers	Datasource 🕑 🗸 😂	ecms
ubsystems	Fiter by: name or subtitle	Datasources >	Filter by: name, xa,/disabled, deployment	Datasource
nterfaces	Batch JBeret	IDBC Drivers >	⊘ ExampleDS	The datasource ecmsuite is enabled. Disable
ocket Bindings	Core Management		⊘ ecmsuite enabled View ∽	
	Datasources & Drivers >		⊘ ecmsuite17july	Main Attributes
aths	Deployment Scanners		⊘ ecmsuitesql	JNDI Name: java:/ecmsuite
ystem Properties				Driver Name: sqljdbc42.jar
	Discovery			Connection URL: Jdbc:sqlserver://10.0.1.43:1522;databaseName=ecm
	EE			Enabled: true
	EJB			Statistics Enabled: false
	ю			
	Infinispan >			
	JCA			
	JMX			

Figure 3.75

24. Add the below connection pool setting and idle-connection-timeout setting inside the created DataSource in *standalone.xml* file located inside the **OmniDocsEjb** or **configuration** folder kept inside the Azure FileShare.

For example,

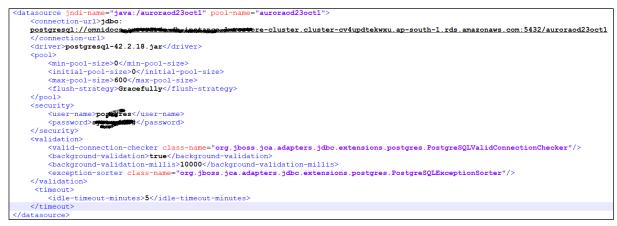


Figure 3.76

25. Restart the **OmniDocsEJB** container once again.

3.7.7 Registering a cabinet

Perform the below steps to register a cabinet:

 Register the cabinet for OmniDocs Admin using the following URL: http://<Host-Path URL of OmniDocsWeb container>/omnidocs/admin/main/registration/registration.jsp For example, http://ecmsuite.newgendocker.com /omnidocs/admin/main/registration/registration.jsp

Omi Docs"	
	Registration
	Cabinet List
	Select Cabinet 🗸
	Site List
	Select Site ~
	Username
	supervisor2
	Password
	Register as ○ Admin ○ Web ● Both
	Cancel Register

Figure 3.77

All the created cabinets get auto populated in the **Cabinet List** dropdown list.

- 2. Select the required cabinet, select the associated site, and specify the Username and Password.
- 3. Select the Register as **Both** and click **Register.** After successful registration, a confirmation message appears.

Omn Docs'		
		Cabinet Registration Successful
	Registration Cabinet List auroraod23oct1 ~ Site List auroraod23oct1site ~	
	Username supervisor Password	
	Register as Admin O Web Both Cancel Register	

Figure 3.78

3.7.8 Creating site and volume

Perform the below steps to create site and volume:

 Login to the OmniDocs Admin using the following URL: http://<Host-Path URL of OmniDocsWeb container>/omnidocs/admin For example, http://ecmsuite.newgendocker.com/omnidocs/admin

Highly Scalable Architecture	Control Content Management (ECM) platform enables end-to-end management of large volume of documents and digital content, right from capture to doposition. It samelessi integrates with other enterprise applications to manage unstructured content and enables digital transformation of your organization.
	Login UserName Password ecmsulte Remember Me
	Login Forgot Password?
	NEWGEN

Figure 3.79

2. After a successful login, click Sites link under Administration.

🔘 NEWGEN	OmniDocs ADMIN DES	ктор			0
Administrati	on	Configure		Personalize	
 Cabinet Details Applications Folders Users Groups Roles 	DataClasses Global Indexes Keywords Sites Volumes Manage Audit Logs	OmniProcess Web API	Search Dashboard	Repository View	Landing Page Configuration Tool Bar Multilingual Definition
Management Report Management License Management	tt • Service Management • Trash Management				

Figure 3.80

3. Click +Add. The Add Site dialog appears.

Add Site	×
SMS Site	Site*
Hadoop Site	
Amazon S3 Site	Site Address*
HCP Site	
MS Azure Site	Port No*
	Cancel Save

Figure 3.81

- 4. Click Amazon S3 Site.
- 5. Specify the user-defined site name, **Access Key**, and **Secret Key** that have rights to the S3 bucket.
- 6. Click Save.

Add Site	×
SMS Site	Site*
Hadoop Site	auroraod23oct1site
Amazon S3 Site	Role Based
HCP Site	Region*
MS Azure Site	
	Access Key*
	AKIAJENJGPC2TBE3W5EA
	Secret Key*
	•••••
	Cancel Save

Figure 3.82

The added Site appears under Sites in the left pane.

	NEWGEN	OmniDocs	ADMIN DESKTOP		0
رم Administration	1 Home > Ad	Iministration- Sites	5		
o	Sites	+ Add	auroraod23oct1site		
OmniProcess •	auroraod23oct1si	te			
Search				Site* auroraod23oct1site	
A Personalize				Role Based*	
Dashboard				Region*	
<u>়</u> Management				Access Key* AKIAJENJGPC2TBE3W5EA	7
				Secret Key*	
					Modify



7. Go back to the **Home** page.

🔘 NEWGEN	OmniDocs ADMIN DESI	ктор		0				
Administratio	on	Configure	2	Personalize				
 Cabinet Details Applications Folders Users Groups Roles 	DataClasses Global Indexes Keywords Sites Volumes Manage Audit Logs	OmniProcess Web API	Search Dashboard	Repository View	Landing Page Configuration Tool Bar Multilingual Definition			
Managemen Report Management	t • Service Management							
License Management	Trash Management							

Figure 3.84

8. Select Volumes. The Volumes screen appears.

N	NEWGEN	OmniDocs	ADMIN DESKTOP				0
⊑o Administration	🛈 Home >	Administration- Volu	mes				
٥	Volumes	+ Add	Name your new volume here*				
OmniProcess ① Search				Home Site	select a site	~	
WebAPI				Default Path*	select a path	~	
C Personalize				Volume Block Size (MB)	50	~	
Dashboard				Encryption	No Encryption O Default 256-bit	○ Custom Encryption	
 Management				Encryption Class Name			
				Replication Type	Immediate	~	
			Delete				Add

Figure 3.85

9. Specify the following details:

- Home Site: Select the newly created Site name.
- Default Path: Select the S3 bucket in which you want to store PN files.
- Volume Name: Specify the user-defined volume name.

10. Click Add.

N	NEWGEN	OmniDocs	ADMIN DESKTOP				0
Lo Administration	1 Home >	Administration- Volu	imes				
OmniProcess	Volumes	+ Add	auroraod23oct1vol				Run Compaction Replicate
Search Search WebAPI Personalize Dashboard Q Management				Home Site Default Path* Volume Block Size (MB) Encryption Encryption Class Name	auroraod23oct1site SMS:od10devnew 50 No Encryption O Default 256-bit	Custom Encryption	
			â Delete	Replication Type	Immediate	v	Add

Figure 3.86

The added volume appears under Image Volumes in the left panel.

N	NEWGEN	OmniDocs	ADMIN DESKTOP
_o Administration	🔟 Home $>$ Adm	inistration- Volu	imes
Ø	Volumes	+ Add	auroraod23oct1vol
OmniProcess (+) Search	auroraod23oct1vol		
API WebAPI			



11. Go back to the **Home** screen.

🔘 NEWGEN	OmniDocs ADMIN DE	SKTOP		(D 🚺
2 Administrat	tion	Configure		Personalize	
Cabinet Details Applications Folders Users Groups Roles	 DataClasses Global Indexes Keywords Sites Volumes Manage Audit Logs 	OmniProcess Web API	Search Dashboard	Color and Accessibility The Color and Accessibility The Repository View Tool Bar Custom Operations Multilingual Definition	
💪 Manageme					
Report Management License Management	Service Management Trash Management				

Figure 3.88

12. Click Cabinet Details.

- 13. Select the added volume from the **Default Image Volume** using the dropdown
- 14. Click **Save**. The Site and Volume are now created successfully.

() N	EWGEN OmniDocs ADMIN DESKTOP		0		
Lo Administration	1 Home > Administration- Cabinet Details				
ø	Cabinet Details			2	Q L
OmniProcess ① Search	Cabinet Name auroraod23oct1	Cabinet Type postgres	Created Date and Time 08/11/2020 04:46		
WebAPI O Personalize	Inherit Ownership	Remove the Rights of Supervisor (Rights once removed will not be restored again)	Separate User/ Group Privileges (Once enabled, can't be disabled)		
Dashboard Oashboard Management	Cnce enabled, can't be disabled)	Enable Data Security Functionality (Once enabled, can't be disabled)	Enable User Access Report		
	Key Management Service None	Default Imaging Volume auroraod23oct1vol	Auto Versioning		
	Enable Two Factor Authentication	Two Factor Authentication Class Name	Enable Multilingual		
				Cancel	Save

Figure 3.89

15. Log in to the OmniDocs Web using the below URL to start. http://<Host-Path URL of OmniDocsWeb container>/omnidocs/web For example: http://ecmsuite.newgendocker.com/omnidocs/web

3.8 EasySearch post-deployment changes

Perform the below steps to do EasySearch post-deployment changes:

 Login to the ApacheManifold Admin using the following URL: <Host-Path URL of ApacheManifold>/mcf-crawler-ui/login.jsp For example,

http://ecmsuiteapache.newgendocker.com/mcf-crawler-ui/login.jsp



Figure 3.90

- 2. Log in with the following credentials:
 - User ID: admin
 - Password: admin
- 3. After a successful login, click **Jobs** tree showing in the left panel.
- 4. Click Status and Job Management. The below job list appears:
 - <CABINET_NAME>_Document
 - <CABINET_NAME>_Folder
- 5. Start both the jobs.
- 6. Once both the jobs started, the Job's status appears as **Running.**

Apache ManifoldCF™	■ Document Ingestion							
	Status of Jobs							
亘 Outputs 〈	1 data	Name		Start Time				
🔒 Authorities 🛛 <	Action		Status		End Time	Documents	Active	Processed
🛓 Repositories 🛛 <	► Restart 💉 Restart minimal 🔲 Pause 🔲 Abort	ecmsuite_Document	Running	7/29/20 5:07:54 PM		1	1	1
Jobs	Restart 🖍 Restart minimal 🔢 Pause 🔲 Abort	ecmsuite_Folder	Running	7/30/20 11:34:17 AM		1	1	1
	C Refresh							
List all Jobs Status and Job Management								
Status Reports <								
3 History Reports <								
3 History Reports <								
3 History Reports <								
3 History Reports <								
D History Reports <								
D History Reports <								
3 History Reports <								

Figure 3.91

3.9 OmniScanWeb: registration of cabinet

Perform the below steps to register the cabinet in OmniScanWeb:

 Open the OmniScanWeb using the following URL: *http://<Host-Path URL of OmniScanWeb container>/omniscanweb* For example,
 https://cmniscanweb.

https://omniscan.newgendocker.com/omniscanweb

2. Click Register New Cabinet link on the OmniScan Web login screen.

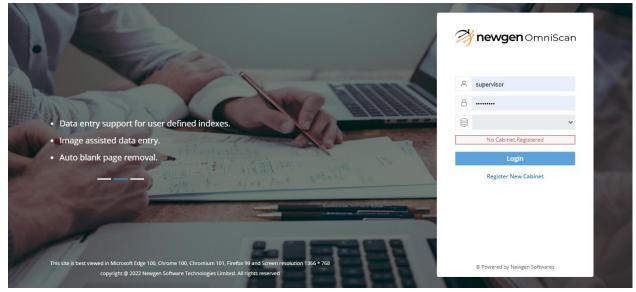


Figure 3.92

 Specify the Server URL as given below: *http://<Host-Path URL of OmniDocsWeb container>/NGServlet/servlet/ExternalServlet* For example,

https://omnidocs.newgendocker.com/NGServlet/servlet/ExternalServlet

4. Specify the **OmniDocs EJB** container name for AppServer IP or Server URL, 8080 for AppServer Port, and JBOSSEAP for AppServer Type.

Image: Connet Image: Connet Server URL https://omnidocs11alpine.newgendocker.com/NGServlet/servlet/Externals/ ApServer IP Image: Connet Mode: Connet Image: Connet Image: Connet Image: Connet <th>← Login</th> <th>Register Cabinet</th>	← Login	Register Cabinet
https://omnidocs11alpine.newgendocker.com/NGServlet/servlet/ExternalSi AppServer IP od110ejb AppServer Port 8080 AppServer Type JBOSSEAP Connect	1 Connect	2 Register
AppServer IP od110ejb AppServer Port 8080 AppServer Type JBOSSEAP Connect Connect	Server URL	
od110ejb AppServer Port 8080 AppServer Type JBOSSEAP Connect	https://omnidoc	s11alpine.newgendocker.com/NGServlet/servlet/ExternalS
AppServer Port 8080 AppServer Type JBOSSEAP Connect	AppServer IP	
8080 AppServer Type JBOSSEAP V Connect	od110ejb	
AppServer Type JBOSSEAP ✓ Connect	AppServer Port	
JBOSSEAP Connect	8080	
Connect	AppServer Type	
inewgen OmniScan	JBOSSEAP	~
		Connect
© Powered by Newgen Softwares		inewgen OmniScan
		© Powered by Newgen Softwares

Figure 3.93

- 5. Click Connect.
- 6. Select the **Cabinet Name**, **Site ID**, and **Volume ID** from the list.

← Login Register Cabinet
Connect 2 Register
Cabinet Name
odpostgres19nov 🗸
Site ID
odpostgres19novsite 🗸
Volume ID
odpostgres19novvol
Register
🎢 newgen OmniScan
© Powered by Newgen Softwares

Figure 3.94

7. Click Register.

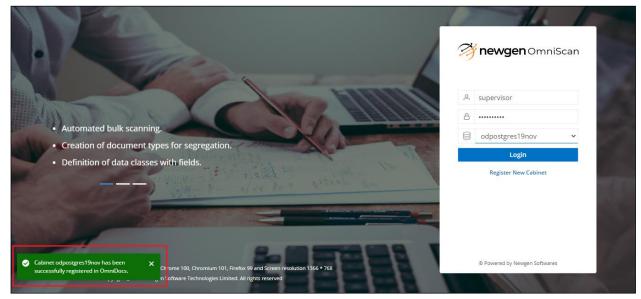


Figure 3.95

The registered cabinet appears in the **Cabinet Name** list on the login screen. Now you can log into OmniScan Web.

NOTE:

Ensure that the **OmniScan_Template_Repository** folder is already created in OmniDocs before logging into OmniScan Web.

4 Configuration of Azure DevOps release pipeline

This chapter describes the configuration of Azure DevOps Release Pipeline. Refer the below sections for procedural details.

4.1 Overview

The Build Pipeline and Release Pipeline are separated into two parts. Build Pipeline is done through the Jenkins server which can be installed on an on-premises machine or a cloud machine. Using the Azure DevOps Release Pipeline cloud service, you can manage the Release pipeline. In this architecture, three stages are created that is, Dev, UAT, and Production and in each stage, deployment is quite different. You can have some more stages depending on the requirements. This guide describes the configuration of the Azure DevOps Release Pipeline for container deployment on Azure Kubernetes Service (AKS).

4.2 CICD pipeline architecture

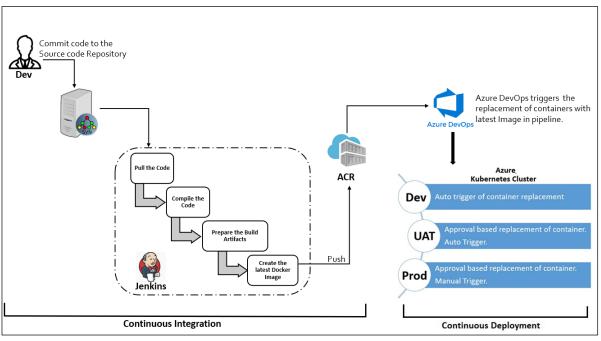


Figure 4.1

- 1. The Newgen representative builds the product's base Docker images on the company's onpremises servers using Jenkins.
- 2. As soon as the Dev team commits the code to the source code repository, the Jenkins pipeline gets triggered. It pulls the code then compiles them and prepares the build artifacts as well as creates Docker images and pushes the newly created Docker images to the Azure Container Registry.
- 3. As soon as any Docker image is pushed to the Azure Container Registry, Azure DevOps Release Pipeline triggers the deployment to the Dev environment. Here, you can configure the performance testing as well as security testing of the application. In Addition, you can perform manual testing as required.
- 4. UAT and Production deployments are based on approval and are available on-demand. To deploy to the UAT environment, you need to trigger the UAT deployment. Upon deployment trigger, an approval mail is sent to the project manager or the concerned team. As soon as the project manager approves the go-ahead, UAT deployment gets started automatically.
- 5. Production deployment is also based on approval, but it is multi-level approval. To deploy a production environment, you require the approval of all stakeholders, and the production environment doesn't get triggered automatically on receiving all the approvals. A manual intervention mail is sent to the engineer who is supposed to deploy to production with a checklist. During deployment, all the checklist points get verified before performing the

production deployment. In case any point of the checklist is not covered, then deployment to the production gets rejected.

4.3 Configuration of Azure DevOps

Perform the below steps to configure Azure DevOps:

- 1. Sign in to the Azure DevOps portal at https://azure.microsoft.com/en-in/services/devops/
- 2. After a successful sign in, click **New Project** to create a new project.

😋 Projects - Home 🛛 🗙	+				~	1	<u>~</u>	ð	×
← → C	vekkumar0906/		¢	☆	en al la	ß	Ţ	* 4	R :
C Azure DevOps		Create new project						×	
vivekkumar0906	vivekkumar0906	Project name *							
New organization	Projects My work items My pull requests	BPMSuite_Containers]~
		Description							
	vivek_kumar	view the project. Certain acces	ate people you is to will be this project	able to	ij			۲	
		\checkmark Advanced							i I
					c	ance	el 🛛	Creat	
Organization settings									

Figure 4.2

- 3. Specify the Project name, and Description.
- 4. Select the **Visibility** as **Private** and create the Azure DevOps Release Pipeline for different Docker Images.

4.3.1 Configuration of release pipeline

This section explains how to create Release Pipeline.

NOTE:

Refer the following steps to configure the Release Pipeline for the Docker Images.

- OmniDocsWeb
- OmniDocsWeb_Services
- OmniDocsEJB
- OmniDocsServices
- EasySearch
- TEM
- OmniScanWeb7.0
- OmniDocsWOPI

Perform the below steps to create Release Pipeline:

1. After project creation, the project summary screen appears. Hover over the **Repos** and select **Files**.

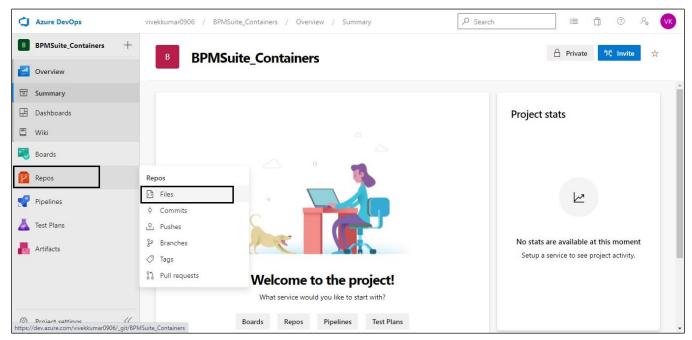


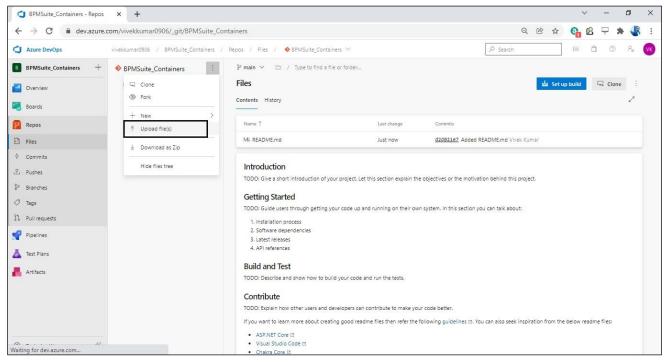
Figure 4.3

2. Click Initialize.

😋 Files - Repos	x +					~	-	٥	×
\leftrightarrow \rightarrow C \cong dev.azure.	com/vivekkumar0906/_git/BPMSuite_Containers		Q	œ ☆	e,	ß	Ţ	•	:
Azure DevOps	vivekkumar0906 / BPMSuite_Containers / Repos / Files / 🕎 BPMSuite_Containers 🗠	, P Search] /=	Ô	0	,P ₀	VK
BPMSuite_Containers +	BPMSuite_Containers is empty. Add some code!								
Overview	Charles and the	Pies Pies							
💐 Boards	Clone to your computer								
Repos	HTTPS SSH https://weekumar0906@dev.azure.com//weekumar0906/BPMSuite, D OR 🖵 Clone in VS Code 🗸								
Files	Generate Git Credentials								
¢ Commits	O Having problems authenticating in Git? Be sure to get the latest version Git for Windows or our plugins for Intellü, Eclipse, Android Studio or Windows command line.								
Pushes									
^{ရွှိစု} Branches	Push an existing repository from command line								
🖉 Tags	HTTPS SSH								
វិរិ Pull requests	git remote add origin https://vivekkumar0906@dev.azure.com/vivekkumar0906/BPMSuite_Containers/_git/								
Pipelines									_
👗 Test Plans	Import a repository								
Artifacts	Import								
	Initialize &main branch with a README or gitignore								
	Add a README Add a .gitignore: None V Initialize								
Waiting for web.vortex.data.microsoft	com								-

Figure 4.4

3. Click **More actions** and then select the **Upload file(s)**.





4. Browse or drag and drop all the YAML files that have shared and then select **Commit**.

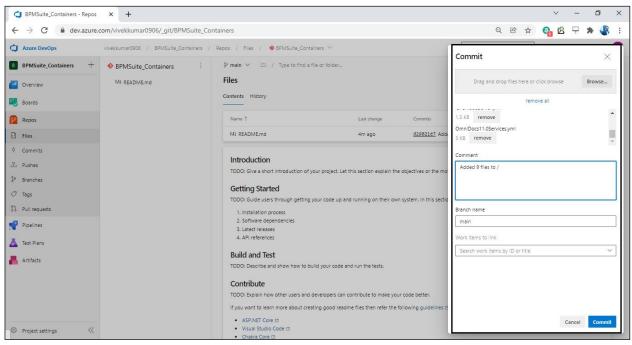


Figure 4.6

5. Hover over to the **Pipelines** in the left panel and select **Releases**.

Dependence - Repos	× +				\sim	-	٥	×
← → C 🌘 dev.azure.	com/vivekkumar0906/_git/BPMSuite_Co	ntainers?path=%2F&version=GBmain		Q 🖻 🕁	G 8		• 4	R
Azure DevOps	vivekkumar0906 / BPMSuite_Containers /	Repos / Files / 🚸 BPMSuite_Containers 🗠		✓ Search	i≡ (0	ρ,	V
B BPMSuite_Containers +	• BPMSuite_Containers	🖇 main 🗸 🗈 / Type to find a file or folde	Tao -					
Overview	D: AppGateway-IngressControlle	Files		👪 Set	up build	Clon	e :	Ē
🜷 Boards	AzureFile_PV_PVC.yml IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Contents History					2	
<u>2</u> Repos	BPS5.0ServiceInstanceEJB.yml	Committed			Create a	pull reques	t ×	
🖸 Files	D IBPS5.0ServiceInstanceWeb.yml							
¢ Commits	D. iBPS5.0UserInstanceEJB.yml	Name †	Last change	Commits				
Pushes	: iBPS5.0UserInstanceWeb.yml	C. AppGateway-ingressController.yml	Just now	808f4f52 Added 9 files to / Vivek Kumar				
စို ^စ Branches	BPSNodeServer.yml	AzureFile_PV_PVC.yml	Just now	808f4f52 Added 9 files to / Vivek Kumar				
🖉 Tags	C: OmniDocs11.0Services.yml	D IBPS5.0Portal.yml	Just now	808f4f52 Added 9 files to / Vivek Kumar				
🖁 Pull requests	MI README.md	BPS5.0ServiceInstanceEJB.yml	Just now	808f4f52 Added 9 files to / Vivek Kumar				
Pipelines	Pipelines	D iBPS5.0ServiceInstanceWeb.yml	Just now	808f4f52 Added 9 files to / Vivek Kumar				
	🖬 Pipelines	D, iBPS5.0UserinstanceEJB.yml	Just now	808f4f52 Added 9 files to / Vivek Kumar				
Test Plans	요. Environments	D: IBPS5.0UserInstanceWeb.yml	Just now	808f4f52 Added 9 files to / Vivek Kumar				
Artifacts	🖉 Releases	D. IBPSNodeServer.yml	Just now	808f4f52 Added 9 files to / Vivek Kumar				
	Library	C). OmniDocs11.0Services.yml	Just now	808f4f52 Added 9 files to / Vivek Kumar				
	 Task groups Deployment groups 	MI README.md	5m ago	d2d021e7 Added README.md Vivek Kumar			_	
ttps://dev.azure.com/vivekkumar090	6/BPMSuite_Containers/_release	Introduction TODO: Give a short introduction of your project	. Let this section explain th	e objectives or the motivation behind this project.				



- 6. Click New Pipeline button. Select a template dialog appears.
- 7. Select the **Deploy to a Kubernetes cluster** template.

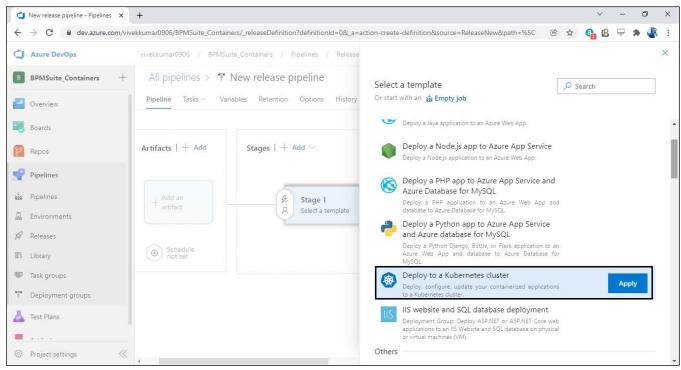
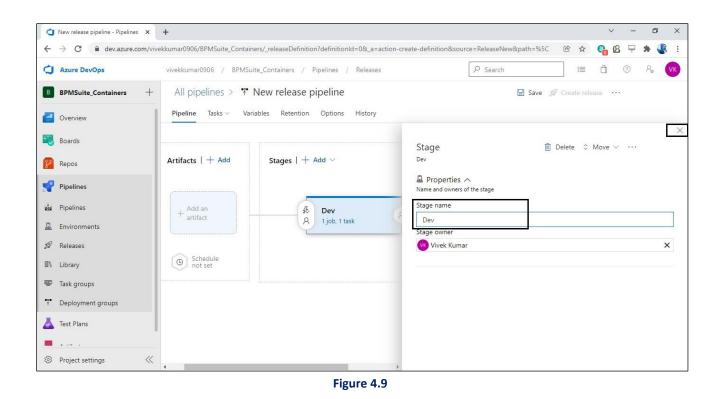


Figure 4.8

- 8. Click Apply. The Stage panel appears.
- 9. Specify the **Stage name** and click **close** icon to close the dialog.



10. Enter the unique name for your pipeline and click **Save**.

🔾 New release pipeline - Pipelines	× Settings - Service connections (i	≅ × +				~	-	٥	×
\leftrightarrow \rightarrow C \bigcirc dev.azure.com	n/vivekkumar0906/BPMSuite_Contai	ners/_releaseDefinition?definitionId=0&_a=action	create-definition&source=ReleaseNew&path=	2 6	☆ (a 12	Ŧ	* 🌗	R :
Azure DevOps	vivekkumar0906 / BPMSuite_Con	tainers / Pipelines / Releases	♀ Search		1	Ô	0	20	VK
B BPMSuite_Containers +	All pipelines > 👎 iBPS	-ServiceInstance-Web	🔚 Save 🚀	Create rel	ease 🗐	∃ View r	eleases		
Overview	Pipeline Tasks Variables	Retention Options History							
Boards									
😢 Repos	Artifacts $ +$ Add	Stages $+$ Add \vee							
Pipelines									
uta Pipelines	+ Add an artifact	& Dev 8							
Environments		A 1 job, 1 task							
🔊 Releases									
III Library	Schedule not set								
Task groups									
*** Deployment groups									
👗 Test Plans									
Artifacts									
Project settings									



11. Specify **Comment** and click **OK** on the **Save** dialog.

Save		>
Folder *		
\		\sim
Comment Rename the pipeline name		
	ОК	Cancel



- 12. Click Add an artifact. The Add an artifact dialog appears.
- 13. Click **Azure Container Registry** under the **Source** type.
- 14. Select the **Service connection** which authenticates the Azure Container Registry.
- 15. In case Service connection is not created, follow the below steps to create Service connection:

Configuration of Service connection for Azure Container Registry:

- Click Manage link. The Create service connection page appears in a new tab.
- Click **Create service connection**. The New service connection dialog appears.
- Select Azure Resource Manager as the connection type and click Next.
- Select Service principle (automatic) as the Authentication method.
- Specify the following parameters:
 - Subscription as Scope level.
 - Select an existing **Azure subscription**.
 - Select the **Resource Group** in which Azure Container Registry is created.
 - (Optional) Specify the Service connection name and Description.
 - Select the checkbox Grant access permission to all pipelines.
- Click **Save**. Once the service connection is created, it appears in the list.

New Azure service connection		\times
Azure Resource Manager using service principal (au	tomatic)	
Scope level		
 Subscription 		
O Management Group		
 Machine Learning Workspace 		
Subscription		
HIVR (b8233ce3-0bae-46c4-a9ca-24d7b6a6e914)		~
Resource group		
AzureKubernetes		~
Service connection name		
Service connection name ACR_Connection1		
Service connection name ACR_Connection1 Description (optional) ACR_Connection1 for container registry		
Service connection name ACR_Connection1 Description (optional) ACR_Connection1 for container registry		
Description (optional) ACR_Connection1 for container registry Security	Back	Save

Figure 4.12

- 16. If the **Service connection** is already created, then select the created service connection.
- 17. Select **Resource Group** from the list in which Azure Container Registry is created.
- 18. Select the created Azure Container Registry.
- 19. Select a Docker image for example, **ibps5serviceinstanceweb** as a **Repository**.
- 20. Select Latest as the Default version. Leave the Source alias with its default value and click Add.

iBPS5-ServiceInstance-Web - Pip 🗙	< +				~	-	٥	×
← → C 🔒 dev.azure.com/	/vivekkumar0906/BPMSuite_Conta	iners/_releaseDefinition?definitionId=2&_a=env	onments-editor-preview	Q 🖻 🕁	G 18	₽	* 🖑	:
Azure DevOps	vivekkumar0906 / BPMSuite_Co	ntainers / Pipelines / Releases						×
B BPMSuite_Containers +	All pipelines > 👎 iBPS	5-ServiceInstance-Web						
Overview	Pipeline Tasks - Variables	Retention Options History	<u>@</u>					
Boards			Jenkins					
Repos	Artifacts $ +$ Add	Stages I $+$ Add \sim	Show less Service connection * Manage @					
Pipelines			ACR_Connection1			~	U	
ula Pipelines	*	B Dev	Resource Group *					
A Environments	Add an artifact	A 1 job, 1 task	AzureKubernetes				~	
Ø Releases	~		Azure Container Registry *				~	
III\ Library	Schedule not set		Repository * ①					
🐨 Task groups			ibps5serviceinstanceweb				\sim	
Deployment groups			Default version * ①					
📥 Test Plans			Latest				\sim	
Artifacts			Source alias * ①					
			_ibps5serviceinstanceweb					
Project settings			Add					

Figure 4.13

21. Once the artifact is added, it appears in the **Artifacts**. Click **Continuous deployment trigger** icon. The **Continuous deployment trigger** dialog appears.

👌 iBPS5-ServiceInstance-Web - Pip 🗙	+			~	-	٥	×
← → C 🔒 dev.azure.com/	vivekkumar0906/BPMSuite_Containers/_releaseDefinition?definitionId=2&_a=environments-editor-preview	Q	₿ ☆	G B	Ţ	* 🎚	1
Azure DevOps	vivekkumar0906 / BPMSuite_Containers / Pipelines / Releases	,₽ Search	i	= ô	0	<i>P</i> .	VK
B BPMSuite_Containers +	All pipelines > 🚏 iBPS5-ServiceInstance-Web	🔚 Save 💋 Cr	eate release	View	releases		
Cverview	Pipeline Tasks V Variables Retention Options History						
Boards							
😰 Repos	Artifacts + Add Stages + Add V						
Pipelines							
👪 Pipelines	iborStanidainsta						
🚊 Environments	neweb A 1job, 1 task						
🖉 Releases							
UN Library	Schedule not set						
📟 Task groups							
Teployment groups							
👗 Test Plans							
Artifacts							
Project settings							

Figure 4.14

22. Enable the **Trigger** and specify the **Tag filter**.

For example,

^latest\$ - trigger the release only if the tag is "latest"

v1\.[0-9] - trigger the release for tags like "v1.23", "beta-v1.3-test"

iBPS5-ServiceInstance-Web - Pip X	+	~	-	٥	х
← → C 🔒 dev.azure.com/	vivekkumar0906/BPMSuite_Containers/_releaseDefinition?definitionId=2&_a=environme	nts-editor-preview Q 🖻 🖈 🚱 🖄	P	* 4	B =
C Azure DevOps	vivekkumar0906 / BPMSuite_Containers / Pipelines / Releases	,⊅ Search i≡	3	P _a	VK
B BPMSuite_Containers +	All pipelines > 🚏 iBPS5-ServiceInstance-Web	🗟 Save 🕫 Create release 🔳 View r	releases		
Overview	Pipeline Tasks Variables Retention Options History				
Boards Repos	Artifacts + Add Stages + Add ~	Continuous deployment trigger Azure Container Repository, JppsSienviceinstanceweb			×
	Ber R Dev JepsSeeniceinsta neeweb R 1 job, 1 task	Creates a release every time an image is pushed to the selected repository. Tag Filter O			
👗 Test Plans					
Project settings	4	,			

Figure 4.15

- 23. Click Close icon to close the Continuous deployment trigger dialog.
- 24. Click Save.
- 25. Click Add an artifact. The Add an artifact dialog appears.
- 26. Click Azure Repos under the Source type.
- 27. Select the **project**, **Source (repository)** and default branch **main.** Also, keep the other settings as default.

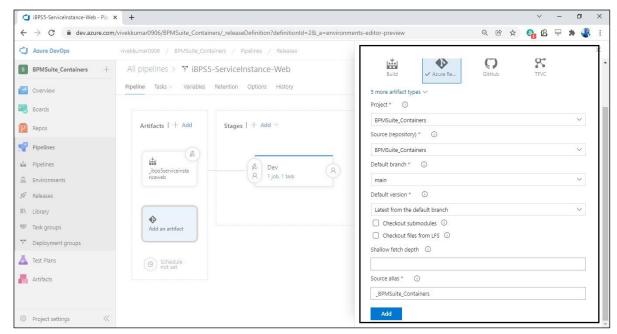


Figure 4.16

- 28. Click Add then Save.
- 29. Configure three stages: Dev, UAT, and Production, and on each stage deployment process is different. You can have some more stages depending on the requirements.

4.3.2 Configuration of Dev stage

Perform the below steps to configure the Dev Stage:

1. Click View stage tasks.

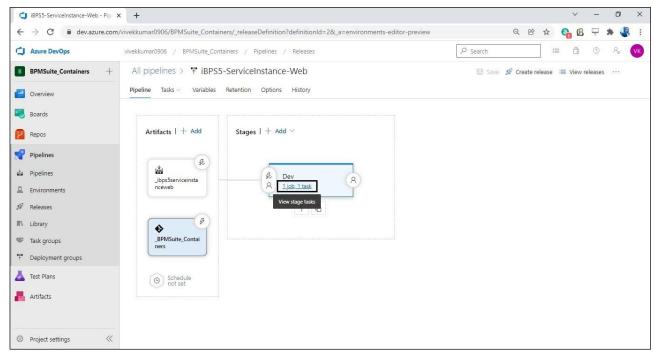


Figure 4.17

2. Click Agent Job and then select ubuntu as the Agent Specification.

iBPS5-ServiceInstance-Web - Pip 🗙	+				~	_	٥	×
← → C 🔒 dev.azure.com/	vivekkumar0906/BPMSuite_Containers/_releaseDefinition?definitionId=2&_a=definition	finition-tasks&environmentId=2	QB	\$ Q	ß	Ţ	*	8 8
Azure DevOps	vivekkumar0906 / BPMSuite_Containers / Pipelines / Releases	✓ Search] !≡	Ô	0	<i>P</i> o	VK
B BPMSuite_Containers +	All pipelines > 🔻 iBPS5-ServiceInstance-Web	🗟 Save	🚀 Create re	lease 🔚	View re	eases		
Overview	Pipeline Tasks - Variables Retention Options History							
Boards	Dev	Agent job 🕕				Û	Remov	re
😢 Repos	Agent job ■ Run on agent +	Display name *						
Pipelines		Agent job						
📩 Pipelines	Wubecti P Kubecti	Agent selection \land						-
Environments		Agent pool 🕕 Pool information Manage 🗠						
🖉 Releases		Azure Pipelines				2	U	
IIN Library		Agent Specification *						
📟 Task groups		ubuntu-20.04					\sim	
T Deployment groups		Demands ①						
Last Plans		Name	Condition		Val	ue		
Artifacts		+ Add						
		Execution plan						
Project settings		Parallelism 🕕						+

Figure 4.18

3. Click Add a task to Agent Job + icon and search for the Replace Tokens and add them.

NOTE:

Ensure **Replace Tokens** task must be the 1st task under the Agent Job.

👌 iBPS5-ServiceInstance-Web - Pip	× +					\sim	-	٥	×
← → C 🔒 dev.azure.com	m/vivekkumar0906/BPMSuite_Containers/_releaseDefinition?definitionId	d=2&_a=definition-tasks&environmentId=2		QE	☆	G 2	Ţ	* 4	8 E
Azure DevOps	vivekkumar0906 / BPMSuite_Containers / Pipelines / Releases		₽ Search] 18	i õ	0	2	VK
B BPMSuite_Containers +	All pipelines > 🚏 iBPS5-ServiceInstance-Web		🗟 Save	🔗 Create r	elease	View	release	5	
Cverview	Pipeline Tasks - Variables Retention Options History								
Boards	Dev Deployment process	Replace Tokens ①			ũ	View YAI	ML 🗎	Remove	2
💡 Repos	Agent job ≣ Run on agent	+ Task version 4.* ~							
Pipelines	#O# Replace tokens in **/*.config	O iii Display name *							
🛍 Pipelines	var d Replace Tokens	Replace tokens in **/*.config							
A Environments	with the second	Root directory (1)							
🖉 Releases									1
III\ Library		Target files * ①							. 1
Task groups		**/*.config							
Deployment groups		Files encoding * ①							A
👗 Test Plans		auto						~	7
Artifacts		Token pattern *							
		#{ }#						~	
		🕑 Write unicode BOM 🛈							
Project settings		Escape values type 🕕							-

Figure 4.19

- 4. Click Browse Root Directory icon under the Replace Token settings.
- 5. Select appropriate YAML file (for example, *iBPS5.0ServiceInstanceWeb.yml*).
- 6. Copy the content of the **Root directory** and paste it to the **Target files** textbox.
- 7. Leave the other settings as default and click **Save.**

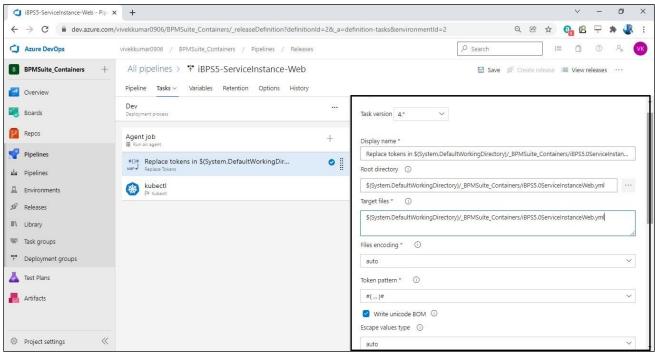


Figure 4.20

- 8. Click Kubectl task under the Agent Job.
- 9. Select Task version **1** and specify the **Display name**.
- 10. Select Kubernetes Service Connection as the Service connection type.
- 11. Select **Kubernetes service connection** which authenticates kubectl to interact with the Kubernetes cluster.
- 12. If **Kubernetes service connection** is not created, then follow the below step to create Kubernetes service connection.
- 13. Configuration of Kubernetes service connection.
 - Click Manage link. The Service connections page appears in a new tab.
 - Click **New service connection** or **Create service connection**. The New service connection dialog appears.
 - Select Kubernetes and click Next. The New Kubernetes service connection dialog appears.
 - Select KubeConfig as an Authentication method.
 - Copy the content of *KubeConfig* file.

NOTE:

```
You can get the KubeConfig file by executing below command:
az aks get-credentials --resource-group <ResourceGroupName> --name
<AzureEKSClusterName>
For example,
az aks get-credentials --resource-group AzureKubernetes --name BPMSuite-
AKSCluster
```

- Select an existing Azure Kubernetes cluster for example, BPMSuite_AKSCluster
- Specify the Service connection name and Description.
- Select the checkbox **Grant access permission to all pipelines** and click **Verify** and **Save**. Once the Service connection is created, it appears in the list.

INCW RUDEITIELES SEI	vice connection	<
KubeConfig		
 Service Account 		
 Azure Subscription 		
KubeConfig		
apiVersion: v1		
clusters:		
- cluster: certificate-authority-data	<i></i>	
Copy and paste the contents of your		
Cluster context (optional)		_
BPMSuite_EKSCluster	~	1
Verify		
Details		
Details Service connection name		
15-5.55/17-2		
Service connection name		
Service connection name Kubernetes_Connecton1		
Service connection name Kubernetes_Connecton1 Description (optional)		
Service connection name Kubernetes_Connecton1 Description (optional) Kubernetes_Connecton1	to all pipelines	
Service connection name Kubernetes_Connecton1 Description (optional) Kubernetes_Connecton1 Security	to all pipelines Back Verify and save	

Figure 4.21

- 14. If Kubernetes service connection is already created, then select the created connection.
- 15. Select the Namespace, that is, dev.
- 16. Select Apply command using the Command dropdown.

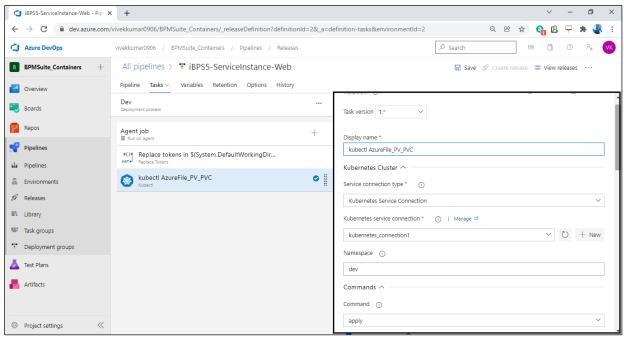


Figure 4.22

- 17. Select the checkbox Use configuration.
- 18. Select the radio button **File path**.
- 19. Browse the *AzureFile_PV_PVC.yml* file path from the **Azure Repos**.

iBPS5-ServiceInstance-Web - Pip	< +	v – Ø	×
\leftrightarrow \rightarrow C \cong dev.azure.com	/vivekkumar0906/BPMSuite_Containers/_releaseDefinition?definition1	nld=2&_a=definition-tasks&environmentId=2 🔍 🖄 🖈 🚱 🗜 🌲 🐇	:
Azure DevOps	vivekkumar0906 / BPMSuite_Containers / Pipelines / Releases	🔎 Search 🕮 🗂 🔿 🗞	VK
BPMSuite_Containers +	All pipelines > 🚏 iBPS5-ServiceInstance-Web	🗟 Save 🖋 Create release 🗮 View releases 💠	
Overview	Pipeline Tasks Variables Retention Options History		
Boards	Dev Deployment process	Command ()	•
😢 Repos	Agent job	+ Use configuration ①	
Pipelines	■ Run on agent #0# Replace tokens in \$(System.DefaultWorkingDir	Configuration type ①	
👪 Pipelines	van + Replace Tokens	File path Inline configuration	
🚊 Environments	kubectl AzureFile_PV_PVC	File path * ①	
🔊 Releases		\$(System.DefaultWorkingDirectory)/_BPMSuite_Containers/AzureFile_PV_PVC.yml	
III Library		Arguments ①	
🖤 Task groups			1
T Deployment groups			
👗 Test Plans		Secrets ^	
Artifacts		Type of secret *	
		dockerRegistry ~	
		Container registry type * ①	
Project settings		Azure Container Registry	+

Figure 4.23

- 20. Expand the **Advanced** tree structure.
- 21. Select the Check for latest version checkbox.
- 22. Right click added kubectl task and select **Clone task(s)**.

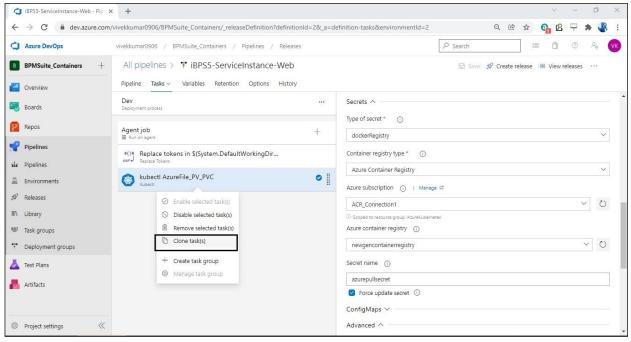


Figure 4.24

- 23. Change the **Display name** of newly cloned task.
- 24. Browse the *yml* file (for example, **iBPS5.0ServiceInstanceWeb.yml**) path from the **Azure Repos**.

iBPS5-ServiceInstance-Web - Pip	× +			× -	- 6	7	×
\leftrightarrow \rightarrow C $\stackrel{\bullet}{\bullet}$ dev.azure.com	/vivekkumar0906/BPMSuite_Containers/_releaseDefinition?definition	d=2&_a=definition-tasks&enviro	nmentid=2 🔍 🖄 🖨 🚱	<u>ß</u>	*		:
Azure DevOps	vivekkumar0906 / BPMSuite_Containers / Pipelines / Releases		Ø Search i≣	1 0	2	•	VK
B BPMSuite_Containers +	All pipelines > 👎 iBPS5-ServiceInstance-Web		🗟 Save 🦸 Create release 🗮 V	ew relea:	ses ····		
Overview	Pipeline Tasks - Variables Retention Options History						
Boards	Dev	Kubernetes Servic	e Connection			~	^
Boards	Deployment process	Kubernetes service o	connection * 🕕 Manage 🗠				
P Repos	Agent job	+ kubernetes_conne	ection1	0	+ N	New	
Pipelines	*Ot Replace tokens in \$(System.DefaultWorkingDir	Namespace 🕕					
Pipelines	van Replace Tokens	dev					
A Environments	kubectl AzureFile_PV_PVC	Commands ^					
🔊 Releases	kubectl iBPS5.0ServiceInstanceWeb	Command ()					
III Library	W Kubecti	apply				\sim	
🐨 Task groups		🕑 Use configurati	on ①				
Deployment groups		Configuration type	0				
👗 Test Plans		File path) Inline configuration				4
Artifacts		File path * 🕡					
		\$(System.DefaultV	VorkingDirectory)/_BPMSuite_Containers/iBPS5.0ServiceInstar	ceWeb.yr	nl		
		Arguments 🕦					
Project settings							

Figure 4.25

- 25. Expand the Secrets tree structure.
- 26. Select dockerRegistry as a Type of secret.
- 27. Select Azure Container Registry (ACR) as a Container registry type.
- 28. Select the created Azure service connection for ACR.
- 29. Select the created Azure container registry.
- 30. Specify the secret name such as azurepullsecret.
- 31. Select the Force update secret checkbox.

Azure DevOps	amitgaur0360 / amitgaur / Pipelines / Releases		🔎 Search 📰 🗇 🔗 🗛
A amitgaur +	All pipelines > 🚏 iBPS5-ServiceInstance-Web		🔚 Save 💋 Create release \cdots
Overview	Pipeline Tasks V Variables Retention Options History		
🕄 Boards	Dev Deployment process		Type of secret * ()
😢 Repos	Agent job	+	Container registry type * (i)
Pipelines	Run on agent Of Replace tokens in \$(System.DefaultWorkingDir		Azure Container Registry
🕍 Pipelines	var Replace Tokens		Azure subscription 🕦 Manage 🗠
🚊 Environments	Kubecti AzureFile_PV_PVC.yml		DevopsGen (14410144 e005 4505 (144 9507 244 9507 244) V
🖉 Releases	kubectl iBPS5-ServiceInstance-Web	⊘ ∥	Scoped to subscription 'DevopsGen' Azure container registry
01 Library			
🖭 Task groups			k8snonprdcidevacr V 🕐
Deployment groups			Secret name
👗 Test Plans			azurepullsecret Force update secret
			ConfigMaps ~
🖄 Project settings 🛛 📈			Connginaps v

Figure 4.26

- 32. Right click cloned kubectl task and Select Clone task(s).
- 33. You can change the **Display name** of newly cloned task.
- 34. Browse the *AppGateway-IngressController.yml* file path from the **Azure Repos**.

iBPS5-ServiceInstance-Web - Pip	+		v -	٥	×
← → C 🔒 dev.azure.com,	/vivekkumar0906/BPMSuite_Containers/_releaseDefinition?definition1	ld=28La=de	efinition-tasks&environmentId=2 🔍 🔍 🖄 🛱 😰 📮	* 🔇	:
Azure DevOps	vivekkumar0906 / BPMSuite_Containers / Pipelines / Releases		🔎 Search 💷 🗇 🗇	P.	VK
B BPMSuite_Containers +	All pipelines > 🚏 iBPS5-ServiceInstance-Web		🗟 Save 🦸 Create release 🗯 View release		
Overview	Pipeline Tasks		kubernetes connection1 V O	+ New	
Boards	Dev Deployment process		Namespace ()	1 den	-
😢 Repos	Agent job	+	dev		
Pipelines	■ Run on agent #0# Replace tokens in \$(System.DefaultWorkingDir		Commands ^		2
uta Pipelines	van el Replace Tokens		Command ①		
Environments	kubectl AzureFile_PV_PVC		apply	~	
🖉 Releases	kubectl iBPS5.0ServiceInstanceWeb		✓ Use configuration ①		
III Library			Configuration type ①		
📟 Task groups	Kubecti AppGateWay-IngressController	•	File path Inline configuration		_
T Deployment groups			File path * 🕥	Browse File	path
👗 Test Plans			\$(System.DefaultWorkingDirectory)/_BPMSuite_Containers/AppGateway- IngressController.yml		
📕 Artifacts			Arguments		. 1
Project settings			Secrets V		-



35. Click **Save**. Now, as soon as any Docker Image is pushed to the Azure container registry with the tag name **sp2**, Azure DevOps trigger the deployment to the **Dev Stage**.

4.3.3 Configuration of UAT stage

Perform the below steps to configure the UAT Stage:

- 1. UAT deployments are approval based and they are available on-demand. Once you are ready to deploy to the UAT environment, you just need to trigger the UAT deployment. When you trigger that deployment, an approval mail is sent to the project manager or the concerned team. As soon as the approval is provided for the go-ahead, the UAT deployment starts automatically.
- 2. Go to the **Pipeline** tab of the Release Pipeline for which **Dev stage** is configured (for example, **iBPS5-ServiceInstance-Web**).
- 3. Select Dev stage and click Clone icon. A cloned Stage gets created.

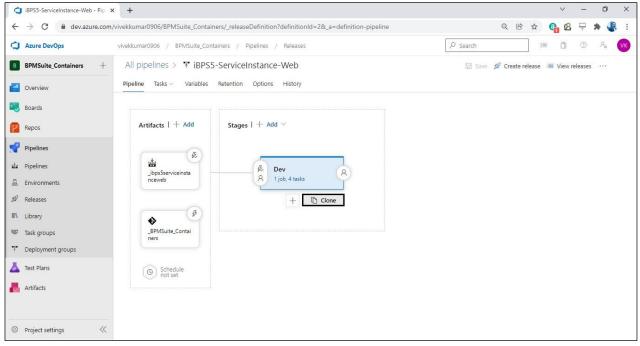
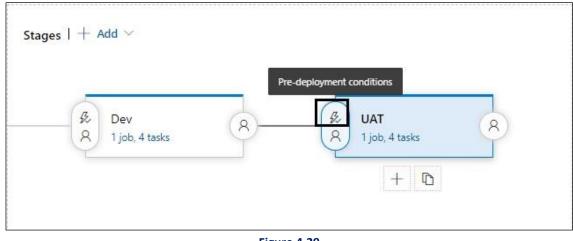


Figure 4.28

- 4. Specify the name of the cloned stage as **UAT** in the **Stage** panel.
- 5. Click **Pre-deployment conditions** icon of the UAT stage. The Pre-deployment conditions panel appears.





- 6. Select the Manual Only under the Triggers section.
- 7. As soon as the trigger type is changed from After **stage** to **Manual Only**, the UAT stage appears in parallel to Dev Stage instead of a series.

iBPS5-ServiceInstance-Web - Pip	× +		v – Ø
← → C 🔒 dev.azure.com	n/vivekkumar0906/BPMSuite_Cont	ainers/_releaseDefinition?definitionId=2&_a=def	inition-pipeline Q 🖄 🙀 🚱 🐺 🌲 🍕
Azure DevOps	vivekkumar0906 / BPMSuite_C	ontainers / Pipelines / Releases	,∕2 Search ﷺ @ ⑦ 옷
B BPMSuite_Containers +	All pipelines > 🌾 iBP	S5-ServiceInstance-Web	🖬 Save 🖋 Create release 🗮 View releases 🛛 \cdots
Overview	Pipeline Tasks Variable	s Retention Options History	
Boards			Pre-deployment conditions
Repos	Artifacts + Add	Stages $+$ Add \vee	UAT
Pipelines	(F)		ổo Triggers ∧ Define the trigger that will start deployment to this stage
a Pipelines	jbps5seniceinsta nceweb	Select trigger ①	
Environments			
P Releases	(3)		After After Manual release stage only
N Library ₱ Task groups	BPMSuite_Contai		
 Deployment groups 	ners UAT 8	A Pre-deployment approvals	
Test Plans	Schedule		Select the users who can approve or reject deployments to this stage
Artifacts	not set		→] Gates Define gates to evaluate before the deployment. Learn more
Project settings			d ^g Deployment queue settings ∨ Define behavior when multiple releases are queued for deployment



- 8. In the Pre-deployment conditions panel, enable the **Pre-deployment approvals**.
- 9. Select the list of users or groups who can approve or reject the deployment to this stage.
- 10. You can select users or groups by typing their names.
- 11. Select the **The user requesting a release or deployment should not approve it** checkbox in Approval policies.

- 12. Click **Close icon** to close the Pre-deployment conditions panel.
- 13. Click **Save** to save the changes.

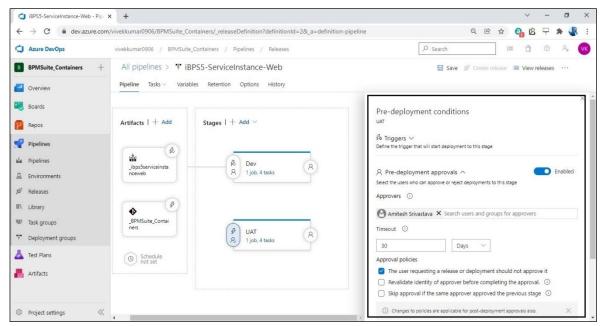


Figure 4.31

14. Click **View stage tasks** link of the UAT stage. Also, make the required changes in the UAT stage's tasks as per your requirements.

For example, you can make the following changes in the below tasks:

• **Kubectl Task:** Kubernetes service connection, Kubectl command, changes in YAML files, and so on.

4.3.4 Configuration of production stage

Production deployment is also based on approval, but it is multi-level approval. To deploy a production environment, you require the approval of all stakeholders, and the production environment doesn't get triggered automatically on receiving all the approvals. A manual intervention mail is sent to the engineer who is supposed to deploy to production with a checklist. During deployment, all the checklist points get verified before performing the production deployment. In case any point of the checklist is not covered, then deployment to the production gets rejected.

Perform the below steps to configure the Production Stage:

- 1. Go to the **Pipeline** tab of the Release Pipeline (for example, **iBPS5-ServiceInstance-Web**) for which **Dev and UAT stages** are just configured.
- 2. Select the **UAT stage** and click **Clone** icon. A cloned Stage gets created.

0	iBPS5-ServiceInstance-Web - Pip	< +			~	-	٥	×
÷	→ C	/vivekkumar0906/BPMSuite_Contain	ners/_releaseDefinition?definitionId=2&_a=definition-pipeline		G 12	₽ ;	* 🖑	:
¢	Azure DevOps	vivekkumar0906 / BPMSuite_Con	ainers / Pipelines / Releases	,	0	0	۶,	VK
в	BPMSuite_Containers +	All pipelines > 👎 iBPS	-ServiceInstance-Web	🗟 Save 🔗 Create release	View n	eleases		
	Overview	Pipeline Tasks ~ Variables	IBPS5-ServiceInstance-Web					
-	Boards							
2	Repos	${\it Artifacts 1+ Add}$	Stages $+$ Add \vee					
P	Pipelines	(B)						
and a	Pipelines	ibps5serviceinsta	& Dev 8					
묘	Environments	nceweb	A 1 job, 4 tasks					
\$	Releases							
11	Library	\$						
	Task groups	_BPMSuite_Contai						
• ••	Deployment groups		Ø UAT R R 1 job, 4 tasks R					
∡	Test Plans	Schedule not set	+ Clone					
	Artifacts							
	Project settings 《							



- 3. Specify the name of the cloned stage as **Production** in the **Stage** panel.
- 4. Click **Pre-deployment conditions** icon of the Production stage. The Pre-deployment conditions dialog appears.
- 5. Select Manual Only option under the Triggers section.
- 6. As soon the trigger type is changed from **After stage** to **Manual Only**, the Production stage appears in parallel to Dev and UAT stages instead of a series.

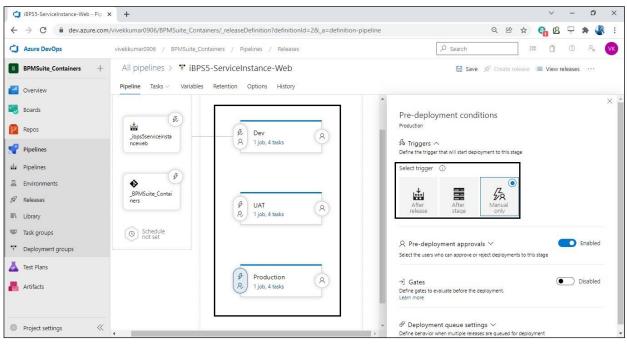


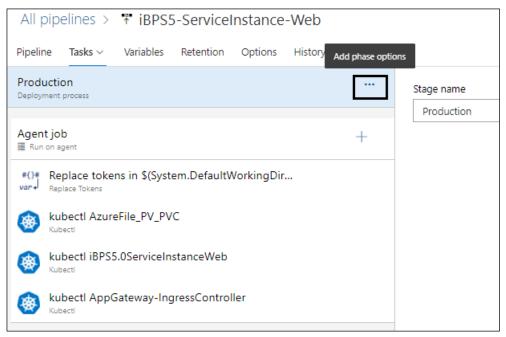
Figure 4.33

- 7. In the **Pre-deployment conditions** panel, select the list of users or stakeholders whose approval is required for the deployment to the Production stage.
- 8. Select **Any Order** as an **Approval order**. It indicates that approval of all Stakeholders is required (in any order).
- 9. Select **The user requesting a release or deployment should not approve it checkbox** in the select policies.
- 10. Click Close icon to close the Pre-deployment conditions panel.
- 11. Click **Save** to save the changes.

対 iBPS5-ServiceInstance-Web - Pip 🗙	< +		✓ - 0 >			
\leftrightarrow \rightarrow C \cong dev.azure.com/	/vivekkumar0906/BPMSuite_Containers	/_releaseDefinition?definitionId=2&_a=definiti	on-pipeline Q 🖻 🕁 🚱 🖓 🌸			
Azure DevOps	vivekkumar0906 / BPMSuite_Containe	ers / Pipelines / Releases	🔎 Search 📁 🗇 🗞 🚺			
B BPMSuite_Containers +	All pipelines > ₹ iBPS5-S	erviceInstance-Web	🗟 Save 🖋 Create release 🔚 View releases \cdots			
Cverview	Pipeline Tasks Variables Re	etention Options History				
Noards	(F)		5 Triggers ✓ Define the trigger that will start deployment to this stage			
P Repos	_ibps5serviceinsta	& Dev 8				
Pipelines	nceweb	A 1 job, 4 tasks	R Pre-deployment approvals Select the users who can approve or reject deployments to this stage			
u Pipelines	<i>(g</i>)	Approvers ①				
A Environments	BPMSuite_Contai		🚱 Amitesh Srivastava 🗙 🚱 Sanjeev Kumar 🗙			
🖉 Releases	ners	JUAT 8	Search users and groups for approvers			
III Library		R 1 job, 4 tasks	Approval order Any order Any order Any one user			
📟 Task groups	Schedule not set					
Teployment groups			Timeout 🛈			
👗 Test Plans			30 Days V			
Artifacts		Production R 1 job, 4 tasks R	Approval policies The user requesting a release or deployment should not approve it			
		Y	Revalidate identity of approver before completing the approval.			
			Skip approval if the same approver approved the previous stage ①			
Project settings	•		,			

Figure 4.34

- 12. Click View stage tasks link to the Production stage.
- 13. Click Add phase options icon in the Tasks tab.





14. Select the Add an agentless job.

15. Move Agentless job above the Agent Job in the Tasks tab.

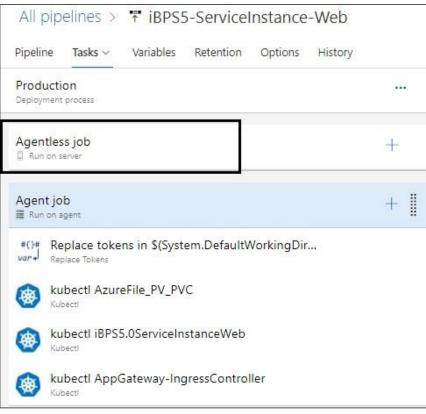


Figure 4.36

- 16. Click Add a task to Agentless job icon.
- 17. Add a **Manual intervention** task.

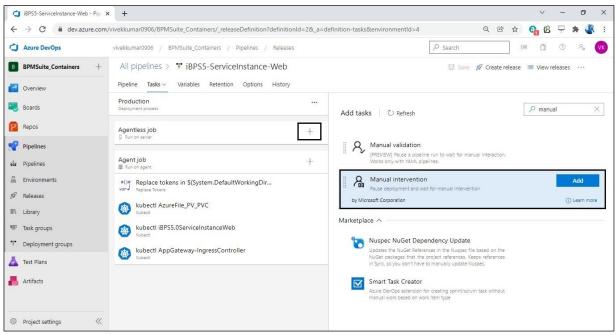


Figure 4.37

- 18. Click added task Manual intervention.
- 19. Specify the checklist points that need to execute before deploying to the production stage. **For example:**

Before deploying to the Production, ensure that the below checklists are completed:

- All Major and Catastrophic bugs must be fixed.
- The latest images must be thoroughly tested on the Dev and UAT stages.
- Approval has taken from all stakeholders.
- Deployment downtime has taken from the client.
- 20. Select the user or group that are supposed to deploy to the production. A manual intervention mail with the above-mentioned checklist is sent to the engineer who is supposed to deploy to production with a checklist. During deployment, all the checklist points get verified before performing the production deployment. In case any point of the checklist is not covered, then deployment to the production gets rejected.

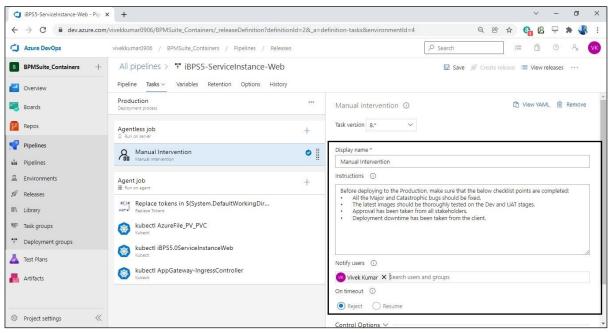


Figure 4.38

- 21. Make the other required changes in the Production stage's tasks as per your requirements. For example, you can make the following changes in the below tasks:
 - **Kubectl Task:** Kubernetes service connection, Kubectl command, changes in YAML files, and so on.

NOTE:

Refer the above steps to configure the Release Pipeline of other Docker Images.