Oracle® Fusion Middleware

Using Oracle WebLogic Server on Microsoft Azure IaaS (Oracle Linux x86-64)

F32844-15
October 2025

Oracle Fusion Middleware Using Oracle WebLogic Server on Microsoft Azure IaaS (Oracle Linux x86-64),

F32844-15

Contents

Preface

This preface describes the document accessibility features and conventions used in this guide —*Oracle Fusion Middleware Using WebLogic Server on Windows Azure (Oracle Linux x86-64)*.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Documentation

Refer to the following for additional information that you may need while deploying Oracle WebLogic Server on Microsoft Azure (IaaS), or post-configuration:

- To access the Oracle WebLogic Server documentation for various releases, see Oracle WebLogic Server online documentation library.
- To access the Microsoft Azure online documentation, see Azure documentation.
- To access the Microsoft documentation that supplements this document, see Oracle WebLogic Server Azure Applications.
- For information about the customer benefits, support offered, licensing information, and the partnership between Oracle Cloud and Microsoft Azure, see Oracle and Microsoft Strategic Partnership FAQ.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Get Started with Oracle WebLogic Server on Microsoft Azure IaaS

Learn about the available Oracle WebLogic Server offers on Microsoft Azure IaaS and the deployment process.

About Deploying Oracle WebLogic Server on Microsoft Azure IaaS

Oracle is committed to enabling you to embrace cloud computing by providing greater choice and flexibility in how you deploy Oracle software. In support of that commitment, Oracle has created several ready-to-deploy solution templates on Azure Marketplace that include pre-installed Oracle software.

This document provides information about the available Oracle WebLogic Server offers on Azure Marketplace, and the instructions to use these offers to install and run Oracle WebLogic Server on Microsoft Azure IaaS. These offers include single node and cluster deployments.

The offers described in this document empower you to start your business applications quickly by:

- Automatically provisioning the virtual network, storage, and Linux resources
- Installing Oracle WebLogic Server
- Setting up security with a network security group
- Load balancing with Azure Application Gateway
- Easing the Database connectivity

The offers also supports HTTP session caching with Oracle Coherence.

> **Note**
>
> Oracle WebLogic Server offers on Azure are customer managed.

When you create an Azure application based on the Oracle WebLogic Server image, you use it just as you would use it on an on-premise virtual or a physical machine. All of the configuration and management tooling are available. These applications are Bring Your Own License (BYOL), and you must have an appropriate license to run Oracle software. For more information, see:

- Oracle Fusion Middleware Licensing Information User Manual
- End User License Agreement for Oracle Products on Azure

In addition, refer to your agreement with Oracle for details on software that you are licensed to use.

Available Oracle WebLogic Server Offers

Oracle publishes several Oracle WebLogic Server offers on Azure Marketplace that can be used for single node and multi-node cluster deployments.

The following table lists the WebLogic Server offers available for deploying on Microsoft Azure (IaaS). Click on the offer to obtain it from the Azure portal. The last column **Documentation** provides links to the topics in this document which describes the process of deploying the selected offer.

> **Note**
>
> The links in the **Offer** column in the following table take you directly to the Azure Portal, where you can deploy these offers immediately. You need an Azure subscription to access the Azure Portal. If you don't have an Azure subscription, you can create a free account before you begin.
> If you are not ready to start your Azure subscription yet, you can explore the offers in the Azure Marketplace as described in Get the Required Oracle WebLogic Server Offer from Azure Marketplace.

Table 1-1 Available Oracle WebLogic Server Offers on Azure Marketplace

Offer	Type	Description	Documentation
Oracle WebLogic Server Single Node	Single node	This offer provisions a single virtual machine with pre-installed JDK and Oracle WebLogic Server without an Administration Server. It does not create a WebLogic domain.	Deploy Oracle WebLogic Server Without Administration Server on a Single Node
Oracle WebLogic Server With Admin Server	Single node	This offer provisions a single virtual machine with pre-installed JDK and Oracle WebLogic Server, along with a WebLogic domain and an Administration Server. The Administration Server is started by default, at the end of the configuration.	Deploy Oracle WebLogic Server With Administration Server on a Single Node
Oracle WebLogic Server Cluster	Cluster	This offer creates multiple virtual machines with highly available WebLogic Server cluster configuration. The Administration Server and the Managed Servers are started by default, which allow you to manage the domain.	Deploy Oracle WebLogic Server N-Node Configured Cluster
Oracle WebLogic Server Dynamic Cluster	Cluster	This offer creates multiple virtual machines with highly available, scalable, and a dynamic WebLogic Server cluster configuration. The Administration Server and the Managed Servers are started by default, which allow you to manage the domain.	Deploy Oracle WebLogic Server N-Node Dynamic Cluster

After you select an offer, use the template to choose the version of Oracle WebLogic Server, JDK, and Oracle Linux required for your deployment. To view the list of supported

combinations (for example, Oracle WebLogic Server 14.1.1.0.0 and JDK11_07 on Oracle Linux 7.6), visit the Azure Marketplace.

> **Note**
>
> These VM offers can be used on their own, separate from the Azure solutions described in this documentation. The VM offers are suitable for users who want to create a highly customized Oracle WebLogic Server on Azure experience.

Get the Required Oracle WebLogic Server Offer from Azure Marketplace

Review the available Oracle WebLogic Server single node and cluster offers and obtain them from the Azure Marketplace.

To search for and choose an Oracle WebLogic Server offer on Azure Marketplace:

1. Go to the Azure Marketplace using the following URL and log in using your Azure credentials:

   https://azuremarketplace.microsoft.com/en-us

   If you don't have an Azure account, sign up at:

   https://azure.microsoft.com/
2. In the search field at the top of the page, enter `Oracle WebLogic Server`, and click the search icon.
3. From the search results, select a version of Oracle WebLogic Server as per your requirement. This takes you to a page with links, screenshots, and videos demonstrating the capabilities of the chosen offer. Review the information available on this page.
4. When you are ready to proceed with the installation, click **Get it now**.
5. Provide the required profile information, such as **Name**, **Work email**, **Job title**, **Company**, **Country/region**, and **Phone number**.
6. Click **Continue**.
7. Perform any additional authentication actions if required, and then click **Create**. This takes you to the Azure portal.
8. Follow the deployment instructions specific to the chosen offer:
   - Deploy Oracle WebLogic Server Without Administration Server on a Single Node
   - Deploy Oracle WebLogic Server With Administration Server on a Single Node
   - Deploy Oracle WebLogic Server N-Node Configured Cluster
   - Deploy Oracle WebLogic Server N-Node Dynamic Cluster

About WebLogic Server Virtual Machine Directory Structure

The following table shows the Oracle-specific directory structure for every virtual machine that is created using the Oracle WebLogic Server image.

When referring to Oracle WebLogic Server documentation, substitute these paths for the directory variables in the documentation.

Table 1-2 WebLogic Server Virtual Machine Directories

Directory Variable	Purpose	Directory Path
`ORACLE_HOME`	Oracle home directory	`/u01/app/wls/install/oracle/middleware/oracle_home`
`WL_HOME`	WebLogic Server home directory	`/u01/app/wls/install/oracle/middleware/oracle_home/wlserver`
`JAVA_HOME`	Java home directory	`/u01/app/jdk/<jdk-version>`
`DOMAIN_HOME`	Directory where the domains you configure are created	`/u01/domains/`

How to Report Issues?

If you encounter any issue during the deployment of Oracle WebLogic Server on Microsoft Azure, or post-configuration, report it at:

https://github.com/oracle/weblogic-azure/issues

If you need more help or have a suggestion, join the public Slack channel named **oracle-weblogic**, where you can get in touch with the team. Use this channel to ask questions about the deployment process, issues encountered, or give feedback or suggestions about the features and improvements you would like to see. To join the channel, visit this site to get an invitation. The invitation email includes the details about accessing the Slack workspace. After you log in, come to `#general` and say, “hello!”.

2

Deploy Oracle WebLogic Server on a Single Node on Microsoft Azure IaaS

The offers described in this section provision a single Azure Oracle Linux virtual machine and install Oracle WebLogic Server and its dependencies on it. You can choose to deploy Oracle WebLogic Server with or without Administration Server.

Deploy Oracle WebLogic Server Without Administration Server on a Single Node

This offer provisions a single virtual machine and installs Oracle WebLogic Server on it. It neither creates a WebLogic domain nor starts the Administration Server.

> **Note**
>
> Before you proceed with the deployment process, ensure that you have obtained this offer either from the Azure Marketplace as described in Get the Required Oracle WebLogic Server Offer from Azure Marketplace, or by clicking on the offer link in Table 1-1.

The Azure portal uses a user interface concept called resource blades. They are similar to tab panels, but can cascade across the page flow.

To deploy Oracle WebLogic Server without an Administration Server on a single node, provide the required information in the following resource blades:

- Basics
- Review + create

Basics

Use the **Basics** blade to provide the basic configuration details for deploying Oracle WebLogic Server without an Administration Server. To do this, enter the values for the fields listed in Table 2-1.

Table 2-1 Fields in the Basics Blade

Section	Field	Description
Project details	**Subscription**	Select a subscription to use for the charges accrued by this offer. You must have a valid active subscription associated with the Azure account that is currently logged in. If you don't have it already, follow the steps described in Associate or add an Azure subscription to your Azure Active Directory tenant.

Table 2-1 (Cont.) Fields in the Basics Blade

Section	Field	Description
	Resource group	A resource group is a container that holds related resources for an Azure solution. The resource group includes those resources that you want to manage as a group. You decide which resources belong in a resource group based on what makes the most sense for your organization. If you have an existing resource group into which you want to deploy this solution, you can enter its name here. Alternatively, you can click the **Create new**, and enter the name so that Azure creates a new resource group before provisioning the resources. For more information about resource groups, see Azure document.
Instance details	**Region**	Select an Azure region from the drop-down list.
	Oracle WebLogic Image	Select a version of Oracle WebLogic Server and JDK that you want to deploy on a preferred version of Oracle Linux. The available options are: • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 7.6 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 7.6 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 7.6 • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 8.7 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 8.7 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 8.7 • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 9.1 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 9.1 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 9.1
	Virtual machine size	The default VM size is `1x Standard A1, 1 vcpu, 1.75 GB memory`. If you want to select a different VM size, click **Change Size**, select the size from the list (for example, A3) on the **Select a VM size** page, and click **Select**. For more information about sizing the virtual machine, see Azure documentation on Sizes.
Credentials for Virtual Machines and WebLogic	**Username for admin account of VMs**	Enter a user name for the administrator account for the virtual machine. Note this value, as you may need it when you access the virtual machine via SSH.

Table 2-1 (Cont.) Fields in the Basics Blade

Section	Field	Description
	Authentication Type	You can either use a **Password** or a **SSH Public Key** along with the username to authenticate the administrator account. If you select **Password**, you must enter the values for the following fields: • **Password**: Enter a password for the administrator account for the virtual machine. • **Confirm password**: Re-enter the password to confirm. If you select **SSH Public Key**, you must specify the value for the following fields: • **SSH public key source**: Specify the SSH public key for the administrator account for the virtual machine. • **Key pair name**: Enter a name for your SSH public key (for example, `mysshkey1`).
Optional Basic Configuration	**Accept defaults for optional configuration?**	If you want to retain the default values for the optional configuration, such as **DNS Label Prefix** and **Ports and port ranges to expose**, set the toggle button to **Yes**, and click **Next : Review + create >**. If you want to specify different values for the optional configuration, set the toggle button to **No**, and enter the following details: • **DNS Label Prefix**: Enter a value that must be added as a prefix to the Azure generated DNS name for the provisioned virtual machine. This value is combined with the **Resource group** name, the region of the resource group, and an Azure specific value. For example, if you specify `wlsmycompany` as the DNS Label Prefix, the DNS host name will be `wlsmycompany-myrg.eastus.cloudapp.azure.com`. Note that this value must start with a letter. • **Ports and port ranges to expose (N or N-N, comma separated)**: Specify the ports that you want to allow in the Azure network group protocols. Ports entered here will be exposed to the outside network. You can either specify the port numbers, or the port ranges, or a combination of both separated by comma. For example: `80,443,7001-9000` • **Cause a system assigned managed identity to be created for the VM(s).**: This option causes any VM(s) created by this deployment to be given a system assigned managed identity. Select **Yes** or **No** based on your preference. For information about the managed identities for Azure resources, including the system assigned managed identities, see What are managed identities for Azure resources?.

After you specify the required details, click **Next : Review + create >**.

Review + create

In the **Review + create** blade, review the details you provided. If you want to make changes to any of the fields, click **< previous** and update the details.

If you want to use this template to automate the deployment, download it by clicking **Download a template for automation**.

Click **Create** to create this offer. This process may take 30 to 60 minutes. For more information about the IaaS offers, see Azure documentation on IaaS.

After the deployment is complete, to access the virtual machine, refer to Access a Virtual Machine via SSH.

To create a WebLogic Server domain, see Creating WebLogic Domains Using WLST Offline in *Understanding the WebLogic Scripting Tool*.

Deploy Oracle WebLogic Server With Administration Server on a Single Node

This offer provisions a single virtual machine and installs Oracle WebLogic Server on it. It creates a WebLogic domain and starts up the WebLogic Administration Server.

> **Note**
>
> Before you proceed with the deployment process, ensure that you have obtained this offer either from the Azure Marketplace as described in Get the Required Oracle WebLogic Server Offer from Azure Marketplace, or by clicking on the offer link in Table 1-1.

The Azure portal uses a user interface concept called resource blades. They are similar to tab panels, but can cascade across the page flow.

To deploy Oracle WebLogic Server with an Administration Server on a single node, provide the required information in the following resource blades:

- Basics
- TLS/SSL Configuration
- Networking
- Database
- Review + create

Basics

Use the **Basics** blade to provide the basic configuration details for deploying Oracle WebLogic Server with an Administration Server. To do this, enter the values for the fields listed in Table 2-2.

Table 2-2 Fields in the Basics Blade

Section	Field	Description
Project details	**Subscription**	Select a subscription to use for the charges accrued by this offer. You must have a valid active subscription associated with the Azure account that is currently logged in. If you don't have it already, follow the steps described in Associate or add an Azure subscription to your Azure Active Directory tenant.
	Resource group	A resource group is a container that holds related resources for an Azure solution. The resource group includes those resources that you want to manage as a group. You decide which resources belong in a resource group based on what makes the most sense for your organization. If you have an existing resource group into which you want to deploy this solution, you can enter its name here. Alternatively, you can click the **Create new**, and enter the name so that Azure creates a new resource group before provisioning the resources. For more information about resource groups, see Azure document.
Instance details	**Region**	Select an Azure region from the drop-down list.
	Oracle WebLogic Image	Select a version of Oracle WebLogic Server and JDK that you want to deploy on a preferred version of Oracle Linux. The available options are: • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 7.6 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 7.6 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 7.6 • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 8.7 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 8.7 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 8.7 • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 9.1 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 9.1 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 9.1
	Virtual machine size	The default VM size is `1x Standard A1, 1 vcpu, 1.75 GB memory`. If you want to select a different VM size, click **Change Size**, select the size from the list (for example, A3) on the **Select a VM size** page, and click **Select**. For more information about sizing the virtual machine, see Azure documentation on Sizes.
Credentials for Virtual Machines and WebLogic	**Username for admin account of VMs**	Enter a user name for the administrator account for the virtual machine. Note this value, as you may need it when you access the virtual machine via SSH.

Table 2-2 (Cont.) Fields in the Basics Blade

Section	Field	Description
	Authentication Type	You can either use a **Password** or a **SSH Public Key** along with the username to authenticate the administrator account. If you select **Password**, you must enter the values for the following fields: • **Password**: Enter a password for the administrator account for the virtual machine. • **Confirm password**: Re-enter the password to confirm. If you select **SSH Public Key**, you must specify the value for the following fields: • **SSH public key source**: Specify the SSH public key for the administrator account for the virtual machine. • **Key pair name**: Enter a name for your SSH public key (for example, `mysshkey1`).
	Username for WebLogic Administrator	Enter a user name to access the WebLogic Administration Console which is started automatically after the provisioning. For more information about the WebLogic Administration Console, see Overview of Administration Consoles in *Understanding Oracle WebLogic Server*.
	Password for WebLogic Administrator	Enter a password to access the WebLogic Administration Console.
	Confirm password	Re-enter the password to access the WebLogic Administration Console.

Table 2-2 (Cont.) Fields in the Basics Blade

Section	Field	Description
Optional Basic Configuration	**Accept defaults for optional configuration?**	If you want to retain the default values for the optional configuration, such as **DNS Label Prefix**, **WebLogic Domain Name**, **Virtual machine size**, and **Ports and port ranges to expose**, set the toggle button to **Yes**, and click **Next : Database >**. If you want to specify different values for the optional configuration, set the toggle button to **No**, and enter the following details: • **WebLogic Domain Name**: Enter the name of the domain that will be created by the offer. • **Enable HTTP Listen Port on WebLogic Administration Server?**: Use this option to enable the HTTP listen port on the WebLogic Administration Server. Select **Yes** or **No** based on your preference. If you disable the HTTP listen port, then the WebLogic Server Administration Console will be accessible on the HTTPS port `7002` at `https://admin-server-host:7002/console`. • **Create a system assigned managed identity to be created for the VM(s).**: This option causes any VM(s) created by this deployment to be given a system assigned managed identity. Select **Yes** or **No** based on your preference. For information about the managed identities for Azure resources, including the system assigned managed identities, see What are managed identities for Azure resources?.

After you provide the required details, click **Next : TLS/SSL Configuration >**.

TLS/SSL Configuration

The **TLS/SSL Configuration** blade enables you to configure Oracle WebLogic Server Administration Console on a secure HTTPS port, with your own TLS/SSL certificate provided by a Certifying Authority (CA).

Select **Yes** or **No** for the option **Configure WebLogic Administration Console on HTTPS (Secure) Port, with your own TLS/SSL certificate?** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Networking >**. If you select **Yes**, you can choose to provide the required configuration details by either uploading existing keystores or by using keystores stored in Azure Key Vault.

If you want to upload existing keystores, select **Upload existing KeyStores** for the option **How would you like to provide required configuration**, and enter the values for the fields listed in Table 2-3.

Table 2-3 Fields in the TLS/SSL Configuration Blade for Uploading Existing Keystores

Field	Description
Identity KeyStore Data file(.jks,.p12)	Upload an identity keystore data file by doing the following: 1. Click on the file icon. 2. Select the identity keystore file. 3. Click **Open**.
Password	Enter the passphrase for the identity keystore.
Confirm password	Re-enter the passphrase for the identity keystore.
The Identity KeyStore type (JKS,PKCS12)	Select the type of identity keystore. The supported values are JKS and PKCS12.
The alias of the server's private key within the Identity KeyStore	Enter the alias for the private key within the identity keystore.
The passphrase for the server's private key within the Identity KeyStore	Enter the passphrase for the private key within the identity keystore.
Confirm passphrase	Re-enter the passphrase for the private key.
Trust KeyStore Data file(.jks,.p12)	Upload a trust keystore data file by doing the following: 1. Click on the file icon. 2. Select the custom trust keystore file. 3. Click **Open**.
Password	Enter the passphrase for the trust keystore.
Confirm password	Re-enter the passphrase for the trust keystore.
The Trust KeyStore type (JKS,PKCS12)	Select the type of trust keystore. The supported values are JKS and PKCS12.

If you want to use keystores stored in Azure Key Vault, select **Use KeyStores stored in Azure Key Vault** for the option **How would you like to provide required configuration**, and enter the values for the fields listed in Table 2-4.

Table 2-4 Fields in the TLS/SSL Configuration Blade for Using KeyStores Stored in Azure Key Vault

Field	Description
Resource group name in current subscription containing the Key Vault	Enter the name of the Resource Group containing the Key Vault that stores the TLS/SSL certificate. An Azure Key Vault is a platform-managed secret store that can be used to safeguard secrets, keys, and TLS/SSL certificates. See About Azure Key Vault.
Name of the Azure Key Vault containing secrets for the TLS/SSL certificate	Enter the name of the Azure Key Vault that stores the secrets for the TLS/SSL certificate.
The name of the secret in the specified Key Vault whose value is the Identity KeyStore Data	Enter the name of the Azure Key Vault secret that holds the value of the identity keystore data.
The name of the secret in the specified Key Vault whose value is the passphrase for the Identity KeyStore	Enter the name of the Azure Key Vault secret that holds the value of the identity keystore passphrase.

Table 2-4 (Cont.) Fields in the TLS/SSL Configuration Blade for Using KeyStores Stored in Azure Key Vault

Field	Description
The Identity KeyStore type (JKS,PKCS12)	Select the type of identity keystore from the drop-down list. The supported values are JKS and PKCS12.
The name of the secret in the specified Key Vault whose value is the Private Key Alias	Enter the name of the Azure Key Vault secret that holds the value of the private key alias.
The name of the secret in the specified Key Vault whose value is the passphrase for the Private Key	Enter the name of the Azure Key Vault secret that holds the value of the private key passphrase.
The name of the secret in the specified Key Vault whose value is the Trust KeyStore Data	Enter the name of the Azure Key Vault secret that holds the value of the trust keystore data.
The name of the secret in the specified Key Vault whose value is the passphrase for the Trust KeyStore	Enter the name of the Azure Key Vault secret that holds the value of the trust keystore passphrase.
The Trust KeyStore type (JKS,PKCS12)	Select the type of trust keystore from the drop-down list. The supported values are JKS and PKCS12.

After you provide the required details, click **Next : Networking >**.

Networking

The **Networking** blade enables you to customize the virtual network in which the WebLogic Server created by this offer will be deployed.

Select **Yes** or **No** based on your preference. If you select **No**, the offer will create a VNET using the 10.0.0.0 address space, and you don't have to provide any details and can proceed by clicking **Next : Database >**. If you select **Yes**, you have some options to configure the networking aspects of the deployment.

First, you must decide whether or not to have the offer create a virtual network, or use an existing virtual network and subnet. There are two experiences for having the offer create a virtual network.

- Create a new virtual network with optional DNS configuration
- Select an existing virtual network

Create a new virtual network with optional DNS configuration

To have the offer create a virtual network with default settings for address space and subnet, select **(new) VirtualNetwork** from the **Virtual network** drop-down list, then select **(new) Subnet-1** from the **Subnet** drop-down list.

To customize the address space and subnet for the new virtual network, select the **Create new** link next to **Virtual network**. A sub-menu opens for further customization. For more details about what you can do with this sub-menu, see What is Azure Virtual Network?. You can specify the CIDR for the virtual network here.

Select an existing virtual network

To select an existing virtual network, select one of the virtual networks from the **Virtual network** drop-down list. The **Subnet** drop-down list allows you to select a subnet within the existing virtual network. WLS will be deployed within the selected subnet. For more advanced

configuration of the subnet, select **Manage subnet configuration**. To return to the WLS deployment experience, use the breadcrumbs navigator at the top of the Portal.

> **Note**
>
> When you select an existing virtual network, no public IP address will be created by the offer.

If you want to make the admin Graphical User Interface (GUI) accessible from the public internet, use the following steps:

1. You must associate a public IP with the admin virtual machine (VM), as described in Associate a public IP address to a virtual machine.
2. Create a Network Security Group whose inbound roles allows traffic from the expected source hosts to the admin VM on ports `7001` and `7002`. For complete guidance on Network Security Groups, see Network security groups.
3. Use the following steps to configure the Admin Server so that its **FrontendHost** is set to the public IP address:
   a. Connect to the admin VM using SSH. You may need to modify the Network Security Group inbound rules to allow this connection.
   b. Enter the `sudo su -` command and login as `root` user.
   c. Enter the `su oracle` command and switch to `Oracle` user.
   d. Execute the following command:

      ```
      /u01/app/wls/install/oracle/middleware/oracle_home/oracle_common/
      common/bin/wlst.sh
      ```

   e. Enter the following WLST commands to configure **FrontendHost**:

      ```
      connect('<weblogic username>','<weblogic password>','t3://adminVM:7001')
      edit()
      startEdit()
      cd('/Servers/admin/WebServer/admin')
      cmo.setFrontendHost('<your public ip hostname>')
      save()
      activate()
      ```

   f. To restart the Admin Server, run the command `systemctl restart wls_admin` as a `root` user.

Deny public traffic for admin server?: Use this option to deny public traffic to the WebLogic Administration Server. The default selection is **No** which makes the ports `7001` and `7002` publicly accessible. Select **Yes**, if you want these ports to be publicly inaccessible.

Configure Custom DNS Alias? : Select **Yes** or **No** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Database >**. If you select **Yes**, you must choose either to configure a custom DNS alias based on an existing Azure DNS zone, or create an Azure DNS zone and a custom DNS alias. This can be done by selecting **Yes** or **No** for the option **Use an existing Azure DNS Zone**.

> **Note**
>
> For more information about the DNS zones, see Overview of DNS zones and records.

DNS Label Prefix: Enter a value that must be added as a prefix to the Azure generated DNS name for the provisioned virtual machine. This value is combined with the **Resource group** name, the region of the resource group, and an Azure specific value. For example, if you specify `wlsmycompany` as the DNS Label Prefix, the DNS host name will be `wlsmycompany-myrg.eastus.cloudapp.azure.com`. The DNS Label Prefix must always start with a lowercase alphabet.

Ports and port ranges to expose (N or N-N, comma separated): Specify the ports that you want to allow in the Azure network group protocols. Ports entered here are exposed to the outside network.

You can either specify port numbers, port ranges, or a combination of both port numbers and ranges separated by comma. For example: `80,443,7001-9000`

If you choose to configure a custom DNS alias based on an existing Azure DNS zone, by selecting **Yes** for the option **Use an existing Azure DNS Zone**, you must specify the DNS configuration details by entering the values for the fields listed in Table 2-5.

Table 2-5 Fields in the DNS Configuration Blade

Field	Description
DNS Zone Name	Enter the DNS zone name.
Name of the resource group which contains the DNS Zone in current subscription	Enter the name of the resource group that contains the DNS zone in the current subscription.
Label for Oracle WebLogic Administration Console	Enter a label to generate a sub-domain of the Oracle WebLogic Server Administration Console. For example, if the domain is `mycompany.com` and the sub-domain is `admin`, then the WebLogic Server Administration Console URL will be `admin.mycompany.com`.
User assigned managed identity (A section; not a field.)	Click **Add** to add user assigned identities to grant resource access to the Azure resources. In the **Add user assigned managed identities** window, select the **Subscription** and the **User assigned managed identities** from the list, and click **Add**. You must add at least one user assigned identity to access Azure resources.

If you choose to create an Azure DNS zone and a custom DNS alias, by selecting **No** for the option **Use an existing Azure DNS Zone**, you must specify the values for the following fields:

- **DNS Zone Name**: Specify the DNS zone name.
- **Label for Oracle WebLogic Administration Console**: Specify a label to generate a sub-domain of the Oracle WebLogic Server Administration Console.

> **Note**
>
> In case of creating an Azure DNS zone and a custom DNS alias, you must perform the DNS domain delegation at your DNS registry post deployment. See Delegation of DNS zones with Azure DNS.

After you specify the required details, click **Next : Database >**.

Database

The **Database** blade enables you to configure Oracle WebLogic Server to connect to an existing database. Select **Yes** or **No** for the option **Connect to Database?** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Review + create >**. If you select **Yes**, you must specify the details of your database by entering the values for the fields listed in Table 2-6.

> **Note**
>
> If you want to connect Oracle WebLogic Server to a database, ensure that all necessary network access have been granted.

Table 2-6 Fields in the Database Blade

Field	Description
Choose database type	Select an existing database that you want Oracle WebLogic Server to connect to from the drop-down list. The available options are: • Azure Database for PostgreSQL • Oracle Database • Azure SQL
JNDI Name	Enter the JNDI name for your database JDBC connection.
DataSource Connection String	Enter the JDBC connection string for your database. For information about obtaining the JDBC connection string, see Obtain the JDBC Connection String for Your Database.
Global transactions protocol	Select an existing global transactions protocol from the drop-down list. The available options are: • TwoPhaseCommit • LoggingLastResource • EmulateTwoPhaseCommit • OnePhaseCommit • None
Database Username	Enter the username of your database.
Database Password	Enter the password for the database user.
Confirm password	Re-enter the database password.

After you provide the details, click **Next : Review + create >**.

Review + create

In the **Review + create** blade, review the details you provided for deploying Oracle WebLogic Server with Administration Server on a single node. If you want to make changes to any of the fields, click **< previous** or click on the respective blade and update the details.

If you want to use this template to automate the deployment, download it by clicking **Download a template for automation**.

Click **Create** to create this offer. This process may take 30 to 60 minutes. For more information about the IaaS offers, see Azure documentation on IaaS.

The WebLogic Administration Server starts automatically when the virtual machine starts.

After the provisioning is complete, the Oracle WebLogic Server Administration Console will be accessible or inaccessible depending on the options you selected in the Basics blade. Table 2-7 lists the ports on which the Administration Console will be accessible for different use cases.

Table 2-7 Ports on Which the WebLogic Server Administration Console is Accessible

Value Set for "Deny public traffic for admin server?"	Value Set for "Enable HTTP Listen Port on WebLogic Administration Server?"	WebLogic Administration Console Accessible or Inaccessible on the HTTP Port and Path `:7001/console`	WebLogic Administration Console Accessible or Inaccessible on the HTTPS Port and Path `:7002/console`
No	**Yes**	Accessible	Accessible
No	**No**	Inaccessible	Accessible
Yes	**Yes** or **No** The **Deny public traffic for admin server?** field takes a higher priority.	Inaccessible	Inaccessible

3

Deploy Oracle WebLogic Server Cluster on Microsoft Azure IaaS

The offers described in this section provision several Azure Oracle Linux virtual machines and install Oracle WebLogic Server and its required dependencies on them. These virtual machines are configured to automatically form a WebLogic Server cluster and are set to start automatically when the virtual machines start or restart.

Deploy Oracle WebLogic Server N-Node Configured Cluster

This offer creates a highly available configured cluster of Oracle WebLogic Server virtual machines.

See WebLogic Server Clustering in *Understanding Oracle WebLogic Server*.

> **Note**
>
> Before you proceed with the deployment process, ensure that you have obtained this offer either from the Azure Marketplace as described in Get the Required Oracle WebLogic Server Offer from Azure Marketplace, or by clicking on the offer link in Table 1-1.

The Azure portal uses a user interface concept called resource blades. They are similar to tab panels, but can cascade across the page flow.

To deploy an Oracle WebLogic Server configured cluster, provide the required information in the following resource blades:

- Basics
- TLS/SSL Configuration
- Azure Application Gateway
- Networking
- Database
- Coherence
- Review + create

Basics

Use the **Basics** blade to provide the basic configuration details for deploying Oracle WebLogic Server configured cluster. To do this, enter the values for the fields listed in Table 3-1.

Table 3-1 Fields in the Basics Blade

Section	Field	Description
Project details	**Subscription**	Select a subscription to use for the charges accrued by this offer. You must have a valid active subscription associated with the Azure account that is currently logged in. If you don't have it already, follow the steps described in Associate or add an Azure subscription to your Azure Active Directory tenant.
	Resource group	A resource group is a container that holds related resources for an Azure solution. The resource group includes those resources that you want to manage as a group. You decide which resources belong in a resource group based on what makes the most sense for your organization. If you have an existing resource group into which you want to deploy this solution, you can enter its name here. Alternatively, you can click the **Create new**, and enter the name so that Azure creates a new resource group before provisioning the resources. For more information about resource groups, see Azure document.
Instance details	**Region**	Select an Azure region from the drop-down list.
	Oracle WebLogic Image	Select a version of Oracle WebLogic Server and JDK that you want to deploy on a preferred version of Oracle Linux. The available options are: • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 7.6 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 7.6 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 7.6 • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 8.7 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 8.7 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 8.7 • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 9.1 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 9.1 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 9.1
	Virtual machine size	The default VM size is `1x Standard A1, 1 vcpu, 1.75 GB memory`. If you want to select a different VM size, click **Change Size**, select the size from the list (for example, A3) on the **Select a VM size** page, and click **Select**. For more information about sizing the virtual machine, see Azure documentation on Sizes.
Credentials for Virtual Machines and WebLogic	**Username for admin account of VMs**	Enter a user name for the administrator account for the virtual machine. Note this value, as you may need it when you access the virtual machine via SSH.

Table 3-1 (Cont.) Fields in the Basics Blade

Section	Field	Description
	Authentication Type	You can either use a **Password** or a **SSH Public Key** along with the username to authenticate the administrator account. If you select **Password**, you must enter the values for the following fields: • **Password**: Enter a password for the administrator account for the virtual machine. • **Confirm password**: Re-enter the password to confirm. If you select **SSH Public Key**, you must specify the value for the following fields: • **SSH public key source**: Specify the SSH public key for the administrator account for the virtual machine. • **Key pair name**: Enter a name for your SSH public key (for example, `mysshkey1`).
	Username for WebLogic Administrator	Enter a user name to access the WebLogic Administration Console which is started automatically after the provisioning. For more information about the WebLogic Administration Console, see Overview of Administration Consoles in *Understanding Oracle WebLogic Server*.
	Password for WebLogic Administrator	Enter a password to access the WebLogic Administration Console.
	Confirm password	Re-enter the password to access the WebLogic Administration Console.
	Number of VMs	Enter the number of virtual machines (VMs) you want to create, with one WebLogic Server node per VM.

Table 3-1 (Cont.) Fields in the Basics Blade

Section	Field	Description
Optional Basic Configuration	**Accept defaults for optional configuration?**	If you want to retain the default values for the optional configuration, such as **DNS Label Prefix**, **WebLogic Domain Name**, **Virtual machine size**, and **Ports and port ranges to expose**, set the toggle button to **Yes**, and click **Next : TLS/SSL Configuration >**. If you want to specify different values for the optional configuration, set the toggle button to **No**, and enter the following details: • **Managed Server prefix**: Enter a prefix for the Managed Server name. • **WebLogic Domain Name**: Enter the name of the domain that will be created by the offer. • **Enable HTTP Listen Port on WebLogic Administration Server?**: Use this option to enable the HTTP listen port on the WebLogic Administration Server. Select **Yes** or **No** based on your preference. If you disable the HTTP listen port, then the WebLogic Server Administration Console will be accessible on the HTTPS port `7002` at `https://admin-server-host:7002/console`. • **Cause a system assigned managed identity to be created for the VM(s).**: This option causes any VM(s) created by this deployment to be given a system assigned managed identity. Select **Yes** or **No** based on your preference. For information about the managed identities for Azure resources, including the system assigned managed identities, see What are managed identities for Azure resources?.

After you specify the required details, click **Next : TLS/SSL Configuration >**.

TLS/SSL Configuration

The **TLS/SSL Configuration** blade enables you to configure Oracle WebLogic Server Administration Console on a secure HTTPS port, with your own TLS/SSL certificate provided by a Certifying Authority (CA).

Select **Yes** or **No** for the option **Configure WebLogic Administration Console on HTTPS (Secure) port, with your own TLS/SSL Certificate?** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Azure Application Gateway >**. If you select **Yes**, you can choose to provide the required configuration details by either uploading existing keystores or by using keystores stored in Azure Key Vault.

If you want to upload existing keystores, select **Upload existing KeyStores** for the option **How would you like to provide required configuration**, and enter the values for the fields listed in Table 3-2.

Table 3-2 Fields in the TLS/SSL Configuration Blade for Uploading Existing Keystores

Field	Description
Identity KeyStore Data file(.jks,.p12)	Upload an identity keystore data file by doing the following: 1. Click on the file icon. 2. Navigate to the folder where the identity keystore file resides, and select the file. 3. Click **Open**.
Password	Enter the passphrase for the identity keystore.
Confirm password	Re-enter the passphrase for the identity keystore.
The Identity KeyStore type (JKS,PKCS12)	Select the type of identity keystore. The supported values are JKS and PKCS12.
The alias of the server's private key within the Identity KeyStore	Enter the alias for the private key within the identity keystore.
The passphrase for the server's private key within the Identity KeyStore	Enter the passphrase for the private key within the identity keystore.
Confirm passphrase	Re-enter the passphrase for the private key.
Trust KeyStore Data file(.jks,.p12)	Upload a custom trust keystore data file by doing the following: 1. Click on the file icon. 2. Navigate to the folder where the custom trust keystore file resides, and select the file. 3. Click **Open**.
Password	Enter the passphrase for the trust keystore.
Confirm password	Re-enter the passphrase for the trust keystore.
The Trust KeyStore type (JKS,PKCS12)	Select the type of the trust keystore. The supported values are JKS and PKCS12.

If you want to use keystores stored in Azure Key Vault, select **Use KeyStores stored in Azure Key Vault** for the option **How would you like to provide required configuration**, and enter the values for the fields listed in Table 3-3.

Table 3-3 Fields in the TLS/SSL Configuration Blade for Using Keystores Stored in Azure Key Vault

Field	Description
Resource group name in current subscription containing the Key Vault	Enter the name of the Resource Group containing the Key Vault that stores the TLS/SSL certificate. An Azure Key Vault is a platform-managed secret store that can be used to safeguard secrets, keys, and TLS/SSL certificates. See About Azure Key Vault.
Name of the Azure Key Vault containing secrets for the SSL certificate	Enter the name of the Azure Key Vault that stores the secrets for the TLS/SSL certificate.
The name of the secret in the specified Key Vault whose value is the Identity KeyStore Data	Enter the name of the Azure Key Vault secret that holds the value of the identity keystore data.

Table 3-3 (Cont.) Fields in the TLS/SSL Configuration Blade for Using Keystores Stored in Azure Key Vault

Field	Description
The name of the secret in the specified Key Vault whose value is the passphrase for the Identity KeyStore	Enter the name of the Azure Key Vault secret that holds the value of the identity keystore passphrase.
The Identity KeyStore type (JKS,PKCS12)	Select the type of identity keystore from the drop-down list. The supported values are JKS and PKCS12.
The name of the secret in the specified Key Vault whose value is the Private Key Alias	Enter the name of the Azure Key Vault secret that holds the value of the private key alias.
The name of the secret in the specified Key Vault whose value is the passphrase for the Private Key	Enter the name of the Azure Key Vault secret that holds the value of the private key passphrase.
The name of the secret in the specified Key Vault whose value is the Trust KeyStore Data	Enter the name of the Azure Key Vault secret that holds the value of the trust keystore data.
The name of the secret in the specified Key Vault whose value is the passphrase for the Trust KeyStore	Enter the name of the Azure Key Vault secret that holds the value of the trust keystore passphrase.
The Trust KeyStore type (JKS,PKCS12)	Select the type of the trust keystore from the drop-down list. The supported values are JKS and PKCS12.

After you provide the required details, click **Next : Azure Application Gateway >**.

Azure Application Gateway

The **Azure Application Gateway** blade enables you to create an Azure Application Gateway (WAF_v2 or later SKU), a public IP, and a backend pool consisting of the worker nodes for use with your WebLogic Server cluster. This Application Gateway is pre-configured with TLS termination using the provided SSL certificate and load balances across your cluster. This may also require some configuration post-deployment.

Select **Yes** or **No** for the option **Connect to Azure Application Gateway?** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Networking >**. If you select **Yes**, you must specify the details required for the Application Gateway integration by entering the values for the fields listed in Table 3-4.

> **Note**
>
> Obtaining the values for these parameters is beyond the scope of this document. For information about the same, see Tutorial: Migrate a WebLogic Server cluster to Azure with Azure Application Gateway as a load balancer.

Table 3-4 Fields in the Azure Application Gateway Blade

Field	Description
Select desired TLS/SSL certificate option	Azure Application Gateway integration requires an TLS/SSL certificate to enable the TLS/SSL termination at the gateway. Use this option to select how you want to provide the TLS/SSL certificate. If you want to upload a pre-signed TLS/SSL certificate, select **Upload a TLS/SSL certificate** and enter the values for the following fields: • **TLS/SSL certificate(.pfx)**: Upload the TLS/SSL certificate file by doing the following: 1. Click on the file icon. 2. Navigate to the folder where the TLS/SSL certificate file resides, and select the file. 3. Click **Open**. • **Password**: Enter the password for the TLS/SSL certificate. • **Confirm Password**: Re-enter the password for the TLS/SSL certificate. If you want to identify an Azure Key Vault that has the certificate and its password stored as secrets, select **Identify an Azure Key Vault** and enter the values for the following fields: • **Resource group name in current subscription containing the Key Vault**: Enter the name of the Resource Group containing the Key Vault that stores the application gateway TLS/SSL certificate and the data required for TLS/SSL termination. • **Name of the Azure Key Vault containing secrets for the certificate for TLS/SSL Termination**: Enter the name of the Azure Key Vault that stores the application gateway TLS/SSL certificate and the data required for TLS/SSL termination. • **The name of the secret in the specified Key Vault whose value is the TLS/SSL certificate data**: Enter the name of the Azure Key Vault secret that holds the value of the TLS/SSL certificate data. • **The name of the secret in the specified Key Vault whose value is the password for the TLS/SSL certificate**: Enter the name of the Azure Key Vault secret that holds the value of the TLS/SSL certificate password. If you want to generate a self-signed TLS/SSL certificate, select **Generate a self-signed certificate** and do the following: 1. Click **+ Add**. 2. In the **Add user assigned managed identity** window, select the **Subscription** and the **User assigned managed identities** from the list, and click **Add**.

> **Note**
>
> An Azure Key Vault is a platform-managed secret store that can be used to safeguard secrets, keys, and TLS/SSL certificates. See About Azure Key Vault.

After you specify the required details, click **Next : Networking >**.

Networking

The **Networking** blade enables you to customize the virtual network in which the WebLogic Server created by this offer will be deployed and configure a custom DNS alias for this deployment.

First, you must decide whether or not to have the offer create a virtual network, or use an existing virtual network and subnet. There are two experiences for having the offer create a virtual network.

- Create a new virtual network with optional DNS configuration
- Select an existing virtual network

Create a new virtual network with optional DNS configuration

To have the offer create a virtual network with default settings for **Virtual network**, **Subnet for WebLogic**, and **Subnet for Application Gateway**, do as follows:

- Select **(new) wls-vnet** from the **Virtual network** drop-down list.
- Select **(new) wls-subnet** from the **Subnet for WebLogic** drop-down list.
- Select **(new) appgateway-subnet** from the **Subnet for Application Gateway** drop-down list.

To customize the address space and subnet for the new virtual network, select the **Create new** link next to **Virtual network**. A sub-menu opens for further customization. For more details about what you can do with this sub-menu, see What is Azure Virtual Network?. You can specify the CIDR for the virtual network here.

Select an existing virtual network

To select an existing virtual network, select one of the virtual networks from the **Virtual network** drop-down list. The **Subnet for WebLogic** and **Subnet for Application Gateway** drop-down lists allows you to select a subnet within the existing virtual network. WLS will be deployed within the selected subnet.

> **Note**
>
> When you select an existing virtual network, no public IP address will be created by the offer.

If you want to make the admin GUI accessible from the public internet, use the following steps:

1. You must associate a public IP with the admin VM, as described in Associate a public IP address to a virtual machine.
2. Create a Network Security Group whose inbound roles allows traffic from the expected source hosts to the admin VM on ports `7001` and `7002`. For complete guidance on Network Security Groups, see Network security groups.
3. Use the following steps to configure the Admin Server so that its **FrontendHost** is set to the public IP address:
   a. Connect to the admin VM using SSH. You may need to modify the Network Security Group inbound rules to allow this connection.
   b. Enter the `sudo su -` command and login as `root` user.

c. Enter the `su oracle` command and switch to `Oracle` user.

d. Execute the following command:

```
/u01/app/wls/install/oracle/middleware/oracle_home/oracle_common/
common/bin/wlst.sh
```

e. Enter the following WLST commands to configure **FrontendHost**:

```
connect('<weblogic username>','<weblogic password>','t3://adminVM:7001')
edit()
startEdit()
cd('/Servers/admin/WebServer/admin')
cmo.setFrontendHost('<your public ip hostname>')
save()
activate()
```

f. To restart the Admin Server, run the command `systemctl restart wls_admin` as a `root` user.

Deny public traffic for admin server?: Use this option to deny public traffic to the WebLogic Administration Server. The default selection is **No** which makes the ports `7001` and `7002` publicly accessible. Select **Yes**, if you want these ports to be publicly inaccessible.

Deny public traffic for managed server?: Select **Yes** to deny public traffic to the Managed Server. This configuration for port 8002 ~ 8001 + node number has a higher priority than the **Ports and port ranges to expose (N or N-N, comma separated)** field.

Configure Custom DNS Alias? : Select **Yes** or **No** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Database >**. If you select **Yes**, you must choose either to configure a custom DNS alias based on an existing Azure DNS zone, or create an Azure DNS zone and a custom DNS alias. This can be done by selecting **Yes** or **No** for the option **Use an existing Azure DNS Zone**.

> **Note**
>
> For more information about the DNS zones, see Overview of DNS zones and records.

DNS Label Prefix: Enter a value that must be added as a prefix to the Azure generated DNS name for the provisioned virtual machine. This value is combined with the **Resource group** name, the region of the resource group, and an Azure specific value. For example, if you specify `wlsmycompany` as the DNS Label Prefix, the DNS host name will be `wlsmycompany-myrg.eastus.cloudapp.azure.com`. The DNS Label Prefix must always start with a lowercase alphabet.

Ports and port ranges to expose (N or N-N, comma separated): Specify the ports that you want to allow in the Azure network group protocols. Ports entered here are exposed to the outside network.

You can either specify port numbers, port ranges, or a combination of both port numbers and ranges separated by comma. For example: `80,443,7001-9000`.

If you choose to configure a custom DNS alias based on an existing Azure DNS zone, by selecting **Yes** for the option **Use an existing Azure DNS Zone**, you must specify the DNS configuration details by entering the values for the fields listed in Table 3-5.

Table 3-5 Fields in the DNS Configuration Blade

Field	Description
DNS Zone Name	Enter the DNS zone name.
Name of the resource group contains the DNS Zone in current subscription	Enter the name of the resource group that contains the DNS zone in the current subscription.
Label for Oracle WebLogic Administration Console	Enter a label to generate a sub-domain of the Oracle WebLogic Server Administration Console. For example, if the domain is `mycompany.com` and the sub-domain is `admin`, then the WebLogic Server Administration Console URL will be `admin.mycompany.com`.
Label for Application Gateway	This field appears if you chose to connect to the Azure Application Gateway in the **Azure Application Gateway** blade. Enter a label to generate a sub-domain of the Application Gateway.
User assigned managed identity (A section; not a field.)	Click **Add** to add user assigned identities to grant resource access to the Azure resources. In the **Add user assigned managed identities** window, select the **Subscription** and the **User assigned managed identities** from the list, and click **Add**. You must add at least one user assigned identity to access Azure resources.

If you choose to create an Azure DNS zone and a custom DNS alias, by selecting **No** for the option **Use an existing Azure DNS Zone**, you must specify the values for the following fields:

- **DNS Zone Name**
- **Label for Oracle WebLogic Administration Console**
- **Label for Application Gateway**

See Table 3-5 for the description of these fields.

> **Note**
>
> In case of creating an Azure DNS zone and a custom DNS alias, you must perform the DNS domain delegation at your DNS registry post deployment. See Delegation of DNS zones with Azure DNS.

After you specify the required details, click **Next : Database >**.

Database

The **Database** blade enables you to configure Oracle WebLogic Server to connect to an existing database. Select **Yes** or **No** for the option **Connect to Database?** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Coherence >**. If you select **Yes**, you must specify the details of your database by entering the values for the fields listed in Table 3-6.

> **Note**
>
> If you want to connect Oracle WebLogic Server to a database, ensure that all necessary network access have been granted.

Table 3-6 Fields in the Database Blade

Field	Description
Choose database type	Select an existing database that you want Oracle WebLogic Server to connect to from the drop-down list. The available options are: • Azure Database for PostgreSQL • Oracle Database • Azure SQL
JNDI Name	Enter the JNDI name for your database JDBC connection.
DataSource Connection String	Enter the JDBC connection string for your database. For information about obtaining the JDBC connection string, see Obtain the JDBC Connection String for Your Database.
Global transactions protocol	Select an existing global transactions protocol from the drop-down list. The available options are: • TwoPhaseCommit • LoggingLastResource • EmulateTwoPhaseCommit • OnePhaseCommit • None
Database Username	Enter the username of your database.
Database Password	Enter the password for the database user.
Confirm password	Re-enter the database password.

After you provide the required details, click **Next : Coherence >**.

Coherence

The **Coherence** blade enables you to deploy additional virtual machines (VMs) with Oracle Coherence*Web pre-installed and configured, for use as the HTTP session storage for web applications deployed in Oracle WebLogic Server. The Coherence cluster is configured as described in Setting Up a Coherence Cluster in *Administering Clusters for Oracle WebLogic Server*. For information about using Coherence with Oracle WebLogic Server, see Using Coherence*Web with WebLogic Server in *Administering HTTP Session Management with Oracle Coherence*Web*.

Select **Yes** or **No** for the option **Use Coherence cache?** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Review + create >**. If you select **Yes**, you must specify the required details for Coherence integration by entering the values for the fields listed in Table 3-7.

Table 3-7 Fields in the Coherence Blade

Field	Description
Coherence virtual machine size	Select the Azure VM size for each of the servers in the Coherence cluster. The recommended size is Standard_A2_v2 or higher. To change the VM size, click **Change Size**, select the preferred size from the list in the **Select a VM size** window, and then click **Select**.
Number of Coherence cache servers	Enter the number of VMs in the Coherence cluster.

Table 3-7 (Cont.) Fields in the Coherence Blade

Field	Description
Coherence Web Local Storage enabled	Use this to enable or disable the local storage for the Coherence*Web cluster tier. Select **Yes** or **No** based on your preference. For information about the Coherence cluster member storage settings, see Configure Coherence Cluster Member Storage Settings in *Administering Clusters for Oracle WebLogic Server*

Click **Next : Review + create >** to continue.

Review + create

In the **Review + create** blade, review the details you provided for deploying an Oracle WebLogic Server configured cluster. If you want to make changes to any of the fields, click **< previous** or click on the respective blade and update the details.

If you want to use this template to automate the deployment, download it by clicking **Download a template for automation**.

Click **Create** to create this offer. This process may take 30 to 60 minutes. For more information about the IaaS offers, see Azure documentation on IaaS.

The WebLogic Administration Server starts automatically when the virtual machine starts.

After the provisioning is complete, the Oracle WebLogic Server Administration Console will be accessible or inaccessible depending on the options you selected in the Basics blade. Table 3-8 lists the ports on which the Administration Console will be accessible for different use cases.

Table 3-8 Ports on Which the WebLogic Server Administration Console is Accessible

Value Set for "Deny public traffic for admin server?"	Value Set for "Enable HTTP Listen Port on WebLogic Administration Server?"	WebLogic Administration Console Accessible or Inaccessible on the HTTP Port and Path `:7001/console`	WebLogic Administration Console Accessible or Inaccessible on the HTTPS Port and Path `:7002/console`
No	**Yes**	Accessible	Accessible
No	**No**	Inaccessible	Accessible
Yes	**Yes** or **No** The **Deny public traffic for admin server?** field takes a higher priority.	Inaccessible	Inaccessible

The HTTPS TLS/SSL certificate management is not handled by the offer and must be configured after installation. For more information about configuring certificates and keystores, see Configuring Keystores in *Administering Security for Oracle WebLogic Server*.

Deploy Oracle WebLogic Server N-Node Dynamic Cluster

This offer creates a highly available and a scalable dynamic cluster of Oracle WebLogic Server virtual machines.

For more information about Oracle WebLogic Server dynamic clustering, see Overview in *Configuring Elasticity in Dynamic Clusters for Oracle WebLogic Server*.

> **Note**
>
> Before you proceed with the deployment process, ensure that you have obtained this offer either from the Azure Marketplace as described in Get the Required Oracle WebLogic Server Offer from Azure Marketplace, or by clicking on the offer link provided in Table 1-1.

The Azure portal uses a user interface concept called resource blades. They are similar to tab panels, but can cascade across the page flow.

To deploy an Oracle WebLogic Server dynamic cluster, provide the required information in the following resource blades:

- Basics
- TLS/SSL Configuration
- Oracle HTTP Server Load Balancer
- Networking
- Database
- Coherence
- Review + create

Basics

Use the **Basics** blade to provide the basic configuration details for deploying an Oracle WebLogic Server dynamic cluster. To do this, enter the values for the fields listed in Table 3-9.

Table 3-9 Fields in the Basics Blade

Section	Field	Description
Project details	**Subscription**	Select a subscription to use for the charges accrued by this offer. You must have a valid active subscription associated with the Azure account that is currently logged in. If you don't have it already, follow the steps described in Associate or add an Azure subscription to your Azure Active Directory tenant.

Table 3-9 (Cont.) Fields in the Basics Blade

Section	Field	Description
	Resource group	A resource group is a container that holds related resources for an Azure solution. The resource group includes those resources that you want to manage as a group. You decide which resources belong in a resource group based on what makes the most sense for your organization. If you have an existing resource group into which you want to deploy this solution, you can enter its name here. Alternatively, you can click the **Create new**, and enter the name so that Azure creates a new resource group before provisioning the resources. For more information about resource groups, see Azure document.
Instance details	**Region**	Select an Azure region from the drop-down list.
	Oracle WebLogic Image	Select a version of Oracle WebLogic Server and JDK that you want to deploy on a preferred version of Oracle Linux. The available options are: • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 7.6 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 7.6 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 7.6 • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 8.7 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 8.7 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 8.7 • WebLogic Server 12.2.1.4.0 and JDK8 on Oracle Linux 9.1 • WebLogic Server 14.1.1.0.0 and JDK8 on Oracle Linux 9.1 • WebLogic Server 14.1.1.0.0 and JDK11 on Oracle Linux 9.1
	Virtual machine size	The default VM size is `1x Standard A1, 1 vcpu, 1.75 GB memory`. If you want to select a different VM size, click **Change Size**, select the size from the list (for example, A3) on the **Select a VM size** page, and click **Select**. For more information about sizing the virtual machine, see Azure documentation on Sizes.
Credentials for Virtual Machines and WebLogic	**Username for admin account of VMs**	Enter a user name for the administrator account for the virtual machine. Note this value, as you may need it when you access the virtual machine via SSH.

Table 3-9 (Cont.) Fields in the Basics Blade

Section	Field	Description
	Authentication Type	You can either use a **Password** or a **SSH Public Key** along with the username to authenticate the administrator account. If you select **Password**, you must enter the values for the following fields: • **Password**: Enter a password for the administrator account for the virtual machine. • **Confirm password**: Re-enter the password to confirm. If you select **SSH Public Key**, you must specify the value for the following fields: • **SSH public key source**: Specify the SSH public key for the administrator account for the virtual machine. • **Key pair name**: Enter a name for your SSH public key (for example, `mysshkey1`).
	Username for WebLogic Administrator	Enter a user name to access the WebLogic Administration Console which is started automatically after the provisioning. For more information about the WebLogic Administration Console, see Overview of Administration Consoles in *Understanding Oracle WebLogic Server*.
	Password for WebLogic Administrator	Enter a password to access the WebLogic Administration Console.
	Confirm password	Re-enter the password to access the WebLogic Administration Console.
	Initial Dynamic Cluster Size	Specify the initial number of Managed Servers that you want to configure in the dynamic cluster.
	Maximum Dynamic Cluster Size	Specify the maximum number of Managed Servers that you want to configure in the dynamic cluster.

Table 3-9 (Cont.) Fields in the Basics Blade

Section	Field	Description
Optional Basic Configuration	**Accept defaults for optional configuration?**	If you want to retain the default values for the optional configuration, such as **DNS Label Prefix**, **WebLogic Domain Name**, **Virtual machine size**, and **Ports and port ranges to expose**, set the toggle button to **Yes**, and click **Next : TLS/SSL Configuration >**. If you want to specify different values for the optional configuration, set the toggle button to **No**, and enter the following details: • **Managed Server prefix**: Enter a prefix for the Managed Server name. • **WebLogic Domain Name**: Enter the name of the domain that will be created by the offer. • **Enable HTTP Listen Port on WebLogic Administration Server?**: Use this option to enable the HTTP listen port on the WebLogic Administration Server. Select **Yes** or **No** based on your preference. If you disable the HTTP listen port, then the WebLogic Server Administration Console will be accessible on the HTTPS port `7002` at `https://admin-server-host:7002/console`. • **Cause a system assigned managed identity to be created for the VM(s).**: This option causes any VM(s) created by this deployment to be given a system assigned managed identity. Select **Yes** or **No** based on your preference. For information about the managed identities for Azure resources, including the system assigned managed identities, see What are managed identities for Azure resources?.

After you provide the required details, click **Next : TLS/SSL Configuration >**.

TLS/SSL Configuration

The **TLS/SSL Configuration** blade enables you to configure Oracle WebLogic Server Administration Console on a secure HTTPS port, with your own TLS/SSL certificate provided by a Certifying Authority (CA).

Select **Yes** or **No** for the option **Configure WebLogic Administration Console on HTTPS (Secure) Port, with your own TLS/SSL Certificate?** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Oracle HTTP Server Load Balancer >**. If you select **Yes**, you can choose to provide the required configuration details by either uploading existing keystores or by using keystores stored in Azure Key Vault.

If you want to upload existing keystores, select **Upload existing KeyStores** for the option **How would you like to provide required configuration**, and enter the values for the fields listed in Table 3-10.

Table 3-10 Fields in the TLS/SSL Configuration Blade for Uploading Existing Keystores

Field	Description
Identity KeyStore Data file(.jks,.p12)	Upload an identity keystore data file by doing the following: 1. Click on the file icon. 2. Navigate to the folder where the identity keystore file resides, and select the file. 3. Click **Open**.
Password	Enter the passphrase for the identity keystore.
Confirm password	Re-enter the passphrase for the identity keystore.
The Identity KeyStore type (JKS,PKCS12)	Select the type of identity keystore. The supported values are JKS and PKCS12.
The alias of the server's private key within the Identity KeyStore	Enter the alias for the private key within the identity keystore.
The passphrase for the server's private key within the Identity KeyStore	Enter the passphrase for the private key within the identity keystore.
Confirm passphrase	Re-enter the passphrase for the private key.
Trust KeyStore Data file(.jks,.p12)	Upload a trust keystore data file by doing the following: 1. Click on the file icon. 2. Navigate to the folder where the custom trust keystore file resides, and select the file. 3. Click **Open**.
Password	Enter the passphrase for the trust keystore.
Confirm password	Re-enter the passphrase for the trust keystore.
The Trust KeyStore type (JKS,PKCS12)	Select the type of the trust keystore. The supported values are JKS and PKCS12.

If you want to use keystores stored in Azure Key Vault, select **Use KeyStores stored in Azure Key Vault** for the option **How would you like to provide required configuration**, and enter the values for the fields listed in Table 3-11.

Table 3-11 Fields in the TLS/SSL Configuration Blade for Using Keystores Stored in Azure Key Vault

Field	Description
Resource group name in current subscription containing the Key Vault	Enter the name of the Resource Group containing the Key Vault that stores the TLS/SSL certificate. An Azure Key Vault is a platform-managed secret store that can be used to safeguard secrets, keys, and TLS/SSL certificates. See About Azure Key Vault.
Name of the Azure Key Vault containing secrets for the TLS/SSL certificate	Enter the name of the Azure Key Vault that stores the secrets for the TLS/SSL certificate.
The name of the secret in the specified Key Vault whose value is the Identity KeyStore Data	Enter the name of the Azure Key Vault secret that holds the value of the identity keystore data.

Table 3-11 (Cont.) Fields in the TLS/SSL Configuration Blade for Using Keystores Stored in Azure Key Vault

Field	Description
The name of the secret in the specified Key Vault whose value is the passphrase for the Identity KeyStore	Enter the name of the Azure Key Vault secret that holds the value of the identity keystore passphrase.
The Identity KeyStore type (JKS,PKCS12)	Select the type of identity keystore from the drop-down list. The supported values are JKS and PKCS12.
The name of the secret in the specified Key Vault whose value is the Private Key Alias	Enter the name of the Azure Key Vault secret that holds the value of the private key alias.
The name of the secret in the specified Key Vault whose value is the passphrase for the Private Key	Enter the name of the Azure Key Vault secret that holds the value of the private key passphrase.
The name of the secret in the specified Key Vault whose value is the Trust KeyStore Data	Enter the name of the Azure Key Vault secret that holds the value of the trust keystore data.
The name of the secret in the specified Key Vault whose value is the passphrase for the Trust KeyStore	Enter the name of the Azure Key Vault secret that holds the value of the trust keystore passphrase.
The Trust KeyStore type (JKS,PKCS12)	Select the type of the trust keystore from the drop-down list. The supported values are JKS and PKCS12.

After you provide the required details, click **Next : Oracle HTTP Server Load Balancer >**.

Oracle HTTP Server Load Balancer

The **Oracle HTTP Server Load Balancer** blade enables you to provision an Oracle HTTP Server, set up a public IP, and configure it with WebLogic Server cluster address.

Select **Yes** or **No** for the option **Connect to Oracle HTTP Server?** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Networking >**. If you select **Yes**, you must specify the Oracle HTTP Server configuration details by entering the values for the fields described in Table 3-12.

Table 3-12 Fields in the Oracle HTTP Server Load Balancer Blade

Field	Description
Oracle HTTP Server image	Select an image with your preferred versions of Oracle HTTP Server, JDK, and Oracle Linux. The available options are: • OHS 12.2.1.4.0 and JDK8 on Oracle Linux 7.3 • OHS 12.2.1.4.0 and JDK8 on Oracle Linux 7.4 • OHS 12.2.1.4.0 and JDK8 on Oracle Linux 7.6
Oracle HTTP Server Domain name	Enter the domain name for Oracle HTTP Server.
Oracle HTTP Server Component name	Enter the name for the Oracle HTTP Server component.
Oracle HTTP Server NodeManager username	Enter the username for the Oracle HTTP Server Node Manager.
Oracle HTTP Server NodeManager Password	Enter the password for Oracle HTTP Server Node Manager.

Table 3-12 (Cont.) Fields in the Oracle HTTP Server Load Balancer Blade

Field	Description
Confirm password	Re-enter the password for Oracle HTTP Server Node Manager.
Oracle HTTP Server HTTP Port	Enter the HTTP port for Oracle HTTP Server.
Oracle HTTP Server HTTPS Port	Enter the HTTPS port for Oracle HTTP Server.
Oracle Vault Password	Enter the password to configure TLS/SSL store Oracle Vault.
Confirm password	Re-enter the password to configure TLS/SSL store Oracle Vault.

You can choose to provide the details required for configuring TLS/SSL in WebLogic Server by either uploading existing keystores or by using the keystores stored in Azure Key Vault. Select a preferred option for **How would you like to provide required configuration**, and enter the values for the fields described in Table 3-13.

Table 3-13 Fields in the Oracle HTTP Server Load Balancer Blade for TLS/SSL Configuration Settings

Option	Field	Description
Upload existing KeyStores	**TLS/SSL certificate Data file(.jks,.p12)**	Upload an existing keystore file for TLS/SSL configuration by doing the following: 1. Click on the file icon. 2. Select the keystore file (JKS or PKCS12 format). 3. Click **Open**.
	Password	Enter the password for the TLS/SSL certificate.
	Confirm password	Re-enter the password for the TLS/SSL certificate.
	Type of the certificate format(JKS,PKCS12)	Select the type of the certificate format from the drop-down list. The supported certificate formats are JKS and PKCS12.
Use KeyStores stored in Azure Key Vault	**Certificate Type**	Select the type of the certificate format from the drop-down list. The supported certificate formats are JKS and PKCS12.
	Resource group name in current subscription containing the Key Vault	Enter the name of the Resource Group containing the Key Vault that stores the TLS/SSL certificate and the data required for TLS/SSL termination. An Azure Key Vault is a platform-managed secret store that can be used to safeguard secrets, keys, and TLS/SSL certificates. See About Azure Key Vault.
	Name of the Azure Key Vault containing secrets for the certificate for TLS/SSL Termination	Enter the name of the Azure Key Vault that stores the secrets for the TLS/SSL certificate and the data required for TLS/SSL termination.
	The name of the secret in the specified Key Vault whose value is the TLS/SSL certificate Data	Enter the name of the Azure Key Vault secret that holds the value of the TLS/SSL certificate data.

Table 3-13 (Cont.) Fields in the Oracle HTTP Server Load Balancer Blade for TLS/SSL Configuration Settings

Option	Field	Description
	The name of the secret in the specified Key Vault whose value is the password for the TLS/SSL certificate	Enter the name of the Azure Key Vault secret that holds the value of the TLS/SSL certificate password.

After you specify the required details, click **Next : Networking >**.

Networking

The **Networking** blade enables you to customize the virtual network in which the WebLogic Server created by this offer will be deployed and configure a custom DNS alias for this deployment.

Deny public traffic for admin server?: Use this option to deny public traffic to the WebLogic Administration Server. The default selection is **No** which makes the ports `7001` and `7002` publicly accessible. Select **Yes**, if you want these ports to be publicly inaccessible.

Deny public traffic for managed server?: Select **Yes** to deny public traffic to the Managed Server. This configuration for port 8002 ~ 8001 + node number has a higher priority than the **Ports and port ranges to expose (N or N-N, comma separated)** field in the **Basics** blade.

First, you must decide whether or not to have the offer create a virtual network, or use an existing virtual network and subnet. There are two experiences for having the offer create a virtual network.

- Create a new virtual network with optional DNS configuration
- Select an existing virtual network

Create a new virtual network with optional DNS configuration

To have the offer create a virtual network with default settings for **Virtual network**, **Subnet for WebLogic**, select **(new) wls-vnet** from the **Virtual network** drop-down list, then select **(new) wls-subnet** from the **Subnet for WebLogic** drop-down list.

> **Note**
>
> If you select **Yes** against **Connect to Oracle HTTP Server** in the **Oracle HTTP Server Load Balancer** blade, OHS is also created in the same subnet.

To customize the address space and subnet for the new virtual network, select the **Create new** link next to **Virtual network**. A sub-menu opens for further customization. For more details about what you can do with this sub-menu, see What is Azure Virtual Network?. You can specify the CIDR for the virtual network here.

Select an existing virtual network

To select an existing virtual network, select one of the virtual networks from the **Virtual network** drop-down list. The **Subnet for WebLogic** drop-down list allows you to select a subnet within the existing virtual network. WLS will be deployed within the selected subnet.

> **Note**
>
> When you select an existing virtual network, no public IP address will be created by the offer.

If you want to make the admin GUI accessible from the public internet, use the following steps:

1. You must associate a public IP with the admin VM, as described in Associate a public IP address to a virtual machine.
2. Create a Network Security Group whose inbound roles allows traffic from the expected source hosts to the admin VM on ports `7001` and `7002`. For complete guidance on Network Security Groups, see Network security groups.
3. Use the following steps to configure the Admin Server so that its **FrontendHost** is set to the public IP address:
   a. Connect to the admin VM using SSH. You may need to modify the Network Security Group inbound rules to allow this connection.
   b. Enter the `sudo su -` command and login as `root` user.
   c. Enter the `su oracle` command and switch to `Oracle` user.
   d. Execute the following command:

      ```
      /u01/app/wls/install/oracle/middleware/oracle_home/oracle_common/
      common/bin/wlst.sh
      ```

   e. Enter the following WLST commands to configure **FrontendHost**:

      ```
      connect('<weblogic username>','<weblogic password>','t3://adminVM:7001')
      edit()
      startEdit()
      cd('/Servers/admin/WebServer/admin')
      cmo.setFrontendHost('<your public ip hostname>')
      save()
      activate()
      ```

   f. To restart the Admin Server, run the command `systemctl restart wls_admin` as a `root` user.

Configure Custom DNS Alias? : Select **Yes** or **No** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Database >**. If you select **Yes**, you must choose either to configure a custom DNS alias based on an existing Azure DNS zone, or create an Azure DNS zone and a custom DNS alias. This can be done by selecting **Yes** or **No** for the option **Use an existing Azure DNS Zone**.

> **Note**
>
> For more information about the DNS zones, see Overview of DNS zones and records.

DNS Label Prefix: Enter a value that must be added as a prefix to the Azure generated DNS name for the provisioned virtual machine. This value is combined with the **Resource group** name, the region of the resource group, and an Azure specific value. For example, if you specify `wlsmycompany` as the DNS Label Prefix, the DNS hostname will be `wlsmycompany-myrg.eastus.cloudapp.azure.com`. The DNS Label Prefix must always start with a lowercase alphabet.

Ports and port ranges to expose (N or N-N, comma separated): Specify the ports that you want to allow in the Azure network group protocols. Ports entered here are exposed to the outside network.

You can either specify port numbers, port ranges, or a combination of both port numbers and ranges separated by comma. For example: `80,443,7001-9000`.

If you choose to configure a custom DNS alias based on an existing Azure DNS zone, by selecting **yes** for the option **Use an existing Azure DNS Zone**, you must specify the DNS configuration details by entering the values for the fields listed in Table 3-14.

Table 3-14 Fields in the DNS Configuration Blade

Field	Description
DNS Zone Name	Enter the DNS zone name.
Name of the resource group contains the DNS Zone in current subscription	Enter the name of the resource group that contains the DNS zone in the current subscription.
Label for Oracle WebLogic Administration Console	Enter a label to generate a sub-domain of the Oracle WebLogic Server Administration Console. For example, if the domain is `mycompany.com` and the sub-domain is `admin`, then the WebLogic Administration Console URL will be `admin.mycompany.com`.
Label for Load Balancer	This field appears if you chose to connect to the Oracle HTTP Server in the **Oracle HTTP Server Load Balancer** blade. Enter a label to generate a sub-domain of the Oracle HTTP Server load balancer.
User assigned managed identity (A section; not a field.)	Click **Add** to add user assigned identities to grant resource access to the Azure resources. In the **Add user assigned managed identities** window, select the **Subscription** and the **User assigned managed identities** from the list, and click **Add**. You must add at least one user assigned identity to access Azure resources.

If you choose to create an Azure DNS zone and a custom DNS alias, by selecting **No** for the option **Use an existing Azure DNS Zone**, you must specify the values for the following fields:

- **DNS Zone Name**
- **Label for Oracle WebLogic Administration Console**
- **Label for Load Balancer**

See Table 3-14 for the description of these fields.

> **Note**
>
> In case of creating an Azure DNS zone and a custom DNS alias, you must perform the DNS domain delegation at your DNS registry post deployment. See Delegation of DNS zones with Azure DNS.

After you specify the required details, click **Next : Database >**.

Database

The **Database** blade enables you to configure Oracle WebLogic Server to connect to an existing database. Select **Yes** or **No** for the option **Connect to Database?** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Coherence >**. If you select **Yes**, you must provide the details of your database by entering the values for the fields listed in Table 3-15.

> **Note**
>
> If you want to connect Oracle WebLogic Server to a database, ensure that all necessary network access have been granted.

Table 3-15 Fields in the Database Blade

Field	Description
Choose database type	Select an existing database that you want Oracle WebLogic Server to connect to from the drop-down list. The available options are: • Azure Database for PostgreSQL • Oracle Database • Azure SQL
JNDI Name	Enter the JNDI name for your database JDBC connection.
DataSource Connection String	Enter the JDBC connection string for your database. For information about obtaining the JDBC connection string, see Obtain the JDBC Connection String for Your Database.
Global transactions protocol	Select an existing global transactions protocol from the drop-down list. The available options are: • TwoPhaseCommit • LoggingLastResource • EmulateTwoPhaseCommit • OnePhaseCommit • None
Database Username	Enter the username of your database.
Database Password	Enter the password for the database user.
Confirm password	Re-enter the password for the database user..

After you provide the details, click **Next : Coherence >**.

Coherence

The **Coherence** blade enables you to deploy additional virtual machines (VMs) with Oracle Coherence*Web pre-installed and configured, for use as the HTTP session storage for web applications deployed in Oracle WebLogic Server. The Coherence cluster is configured as

described in Setting Up a Coherence Cluster in *Administering Clusters for Oracle WebLogic Server*. For information about using Coherence with Oracle WebLogic Server, see Using Coherence*Web with WebLogic Server in *Administering HTTP Session Management with Oracle Coherence*Web*.

Select **Yes** or **No** for the option **Use Coherence cache?** based on your preference. If you select **No**, you don't have to provide any details, and can proceed by clicking **Next : Review + create >**. If you select **Yes**, you must specify the required details for Coherence integration by entering the values for the fields listed in Table 3-16.

Table 3-16 Fields in the Coherence Blade

Field	Description
Coherence virtual machine size	Enter the Azure VM size for each of the servers in the Coherence cluster. The recommended size is Standard_A2_v2 or higher. To change the VM size, click **Change Size**, select the preferred size from the list in the **Select a VM size** window, and then click **Select**.
Number of Coherence cache servers	Enter the number of VMs in the Coherence cluster.
Coherence Web Local Storage enabled	Use this to enable or disable the local storage for the Coherence*Web cluster tier. Select **Yes** or **No** based on your preference. For information about the Coherence cluster member storage settings, see Configure Coherence Cluster Member Storage Settings in *Administering Clusters for Oracle WebLogic Server*

Click **Next : Review + create >** to continue.

Review + create

In the **Review + create** blade, review the details you provided for deploying an Oracle WebLogic Server dynamic cluster. If you want to make changes to any of the fields, click **< previous** or click on the respective blade and update the details.

If you want to use this template to automate the deployment, download it by clicking **Download a template for automation**.

Click **Create** to create this offer. This process may take 30 to 60 minutes. For more information about the IaaS offers, see Azure documentation on IaaS.

The WebLogic Administration Server starts automatically when the virtual machine starts.

After the provisioning is complete, the Oracle WebLogic Server Administration Console will be accessible or inaccessible depending on the options you selected in the Basics blade. Table 3-17 lists the ports on which the Administration Console will be accessible for different use cases:

Table 3-17 Ports on Which the WebLogic Server Administration Console is Accessible

Value Set for "Deny public traffic for admin server?"	Value Set for "Enable HTTP Listen Port on WebLogic Administration Server?"	WebLogic Administration Console Accessible or Inaccessible on the HTTP Port and Path `:7001/console`	WebLogic Administration Console Accessible or Inaccessible on the HTTPS Port and Path `:7002/console`
No	**Yes**	Accessible	Accessible

Table 3-17 (Cont.) Ports on Which the WebLogic Server Administration Console is Accessible

Value Set for "Deny public traffic for admin server?"	Value Set for "Enable HTTP Listen Port on WebLogic Administration Server?"	WebLogic Administration Console Accessible or Inaccessible on the HTTP Port and Path `:7001/console`	WebLogic Administration Console Accessible or Inaccessible on the HTTPS Port and Path `:7002/console`
No	**No**	Inaccessible	Accessible
Yes	**Yes** or **No** The **Deny public traffic for admin server?** field takes a higher priority.	Inaccessible	Inaccessible

The HTTPS TLS/SSL certificate management is not handled by the offer and must be configured after installation. For more information about configuring certificates and keystores, see Configuring Keystores in *Administering Security for Oracle WebLogic Server*.

A
Common Administration Tasks

After an offer is provisioned, that is, after you have deployed virtual machines with Oracle WebLogic Server, you can access them via SSH. If you have configured WebLogic Administration Server, you can access the WebLogic Administration console and manage the applications.

Obtain the JDBC Connection String for Your Database

Depending on the database you are using, follow the instructions in the respective section to obtain the JDBC connection string:

- Oracle Database
- Azure Database for PostgreSQL
- Azure SQL Server

Oracle Database

The format of the JDBC connection string for Oracle Database is:

```
jdbc:oracle:thin:@HOSTNAME:1521/DATABASENAME
```

For example:

```
jdbc:oracle:thin:@benqoiz.southeastasia.cloudapp.azure.com:1521/pdb1
```

Azure Database for PostgreSQL

To obtain the JDBC connection string for Azure Database for PostgreSQL, do the following:

1. Deploy an Azure Database PostgreSQL as described in Quickstart: Create an Azure Database for PostgreSQL server in the Azure portal.
2. Access the Azure portal at https://portal.azure.com, and go to the service instance.
3. Click **Connection Strings** under **Settings**.
4. Locate the **JDBC** section and click the copy icon on the right to copy the JDBC connection string to the clipboard. The JDBC connection string will be similar to the following:

   ```
   jdbc:postgresql://20191015cbfgterfdy.postgres.database.azure.com:5432/
   {your_database}?
   user=jroybtvp@20191015cbfgterfdy&password={your_password}&sslmode=require
   ```

   When passing this value to the `datasourceConfig-postgres.sh` command, remove the database user and password values, and place them as arguments to the script (<*dsUser*>

and <*dsPassword*>. In the above JDBC connection string sample, the value for `dsConnectionURL` argument after removing the database user and password, will be:

```
jdbc:postgresql://20191015cbfgterfdy.postgres.database.azure.com:5432/
{your_database}?sslmode=require
```

Azure SQL Server

To obtain the JDBC connection string for Azure SQL Server, do the following:

1. Deploy Azure SQL Server as described in Quickstart: Create a single database in Azure SQL Database using the Azure portal, PowerShell, and Azure CLI.
2. Access the Azure portal at https://portal.azure.com, and go to the service instance.
3. Click **Connection Strings** under **Settings**.
4. Locate the **JDBC** section and click the copy icon on the right to copy the JDBC connection string to the clipboard. The JDBC connection string will be similar to the following:

   ```
   jdbc:sqlserver://
   rwo102804.database.windows.net:1433;database=rwo102804;user=jroybtvp@rwo102
   804;password={your_password_here};encrypt=true;trustServerCertificate=false
   ;hostNameInCertificate=*.database.windows.net;loginTimeout=30;
   ```

   When passing this value to the `datasourceConfig-azuresql.sh` command, remove the database user and password values, and place them as arguments to the script (<*dsUser*> and <*dsPassword*>. In the above JDBC connection string sample, the value for `dsConnectionURL` argument after removing the database user and password, will be:

   ```
   jdbc:sqlserver://
   rwo102804.database.windows.net:1433;database={your_database};encrypt=true;t
   rustServerCertificate=false;hostNameInCertificate=*.database.windows.net;lo
   ginTimeout=30;
   ```

Access a Virtual Machine via SSH

After an offer is provisioned, you can access a virtual machine via SSH using the credentials that you had defined in the **Credentials** blade during offer creation.

> **Note**
>
> Depending on the security rules in your Azure subscription, you may need to expose port 22, or whitelist the IP from which you are initiating the SSH connection. For more information, refer to the Azure documentation.

To access a virtual machine via SSH:

1. Log in to the Azure portal using the following URL:

   https://portal.azure.com/
2. Click the hamburger button at the top left corner of the portal.
3. Click **Resource groups**.

4. In the **Filter by name** field, enter the resource group name that you specified in **Basics** blade during deployment. Find and click on the desired resource group. Depending on the offer, you will see different quantities and varieties of resources in the resource group.
5. Click on the desired resource with type Virtual machine. To easily locate the resource, sort the rows by type by clicking the **Type** column header.

   When you select the resource, the details pane for that virtual machine is displayed. It contains useful metrics of the health and status of the virtual machine.
6. On the Virtual machine details pane, click on the clipboard icon next to the value of the **DNS name** field. This copies the hostname to the clipboard.
7. SSH into the virtual machine host using an SSH client of your choice and the credentials you specified for the admin account of the virtual machine. For example:

```
ssh weblogic@wls101401.eastus.cloudapp.azure.com
[weblogic@WebLogicServerVM ~]$ pwd
/home/weblogic
[weblogic@WebLogicServerVM ~]$
```

   Some of the directories are accessible only to the `root` user. To switch to the `root` user, use the `sudo` command as shown in the following example:

```
[weblogic@WebLogicServerVM wls]$ sudo su -

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for weblogic:
[root@WebLogicServerVM ~]#
```

Access the WebLogic Server Administration Console

The offers that include WebLogic Administration Server configuration, starts the server by the end of the deployment process. Once the deployment is complete, you can access the Administration console.

To access the WebLogic Server Administration console:

1. Log in to the Azure portal using the following URL:

   https://portal.azure.com/
2. Click the hamburger button at the top left corner of the portal.
3. Click **Resource groups**.
4. In the **Filter by name** field, enter the resource group name that you specified in **Basics** blade during deployment. Find and click on the desired resource group. Depending on the offer, you will see different quantities and varieties of resources in the resource group.
5. Click on the desired resource with type Virtual machine. To easily locate the resource, sort the rows by type by clicking the **Type** column header.

When you select the resource, the details pane for that virtual machine is displayed. It contains useful metrics of the health and status of the virtual machine.

6. On the Virtual machine details pane, click on the clipboard icon next to the value of the **DNS name** field. This copies the hostname to the clipboard.
7. Access the following URL from a browser:

   `http://dnsname:7001/console`
   Log in using the WebLogic Administrator username and password that you provided in the **Credentials** blade during offer provisioning.

Use Azure Resource Manager Templates to Work With Existing Deployment

If you have an existing Oracle WebLogic Server deployment, you can use the Azure Resource Manager (ARM) templates to configure Database and Azure Application Gateway with Oracle WebLogic Server.

For the list of templates available for working with Oracle WebLogic Server with Administration Server, see Single Node Oracle WebLogic Server with Admin Server.

For the list of templates available for working with Oracle WebLogic Server configured cluster, see Oracle WebLogic Server Cluster.

For the list of templates available for working with Oracle WebLogic Server dynamic cluster, see Oracle WebLogic Server Dynamic Cluster.

Configure Keystores

TLS/SSL provides secure connections by allowing two applications connected over a network to authenticate each other's identity, and by encrypting the data exchanged between the applications.

Authentication allows a server and optionally a client to verify the identity of an application on the other end of a network connection. Encryption makes data transmitted over the network intelligible only to the intended recipient.

TLS/SSL in Oracle WebLogic Server

TLS/SSL in WebLogic Server is an implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) specifications. WebLogic Server supports TLS/SSL on a dedicated listen port which defaults to 7002. For more information about configuring SSL in an Oracle WebLogic Server environment, see Configuring SSL.

By default, WebLogic Server provides demo certificates or keystores for working in a development or a test environment. Ensure that these certificates are not used in a production environment.

Self-signed certificates are created and configured in WebLogic Server in development or test environments. For a production environment, you must procure CA-signed TLS/SSL certificate from a valid Certificate Authority (CA), such as Verisign, Let's Encrypt, GoDaddy and so on, to create keystores from it.

To configure SSL in WebLogic Server, you need the following security files:

- Trust store: This file contains the certificates from the intermediate or root CA, or from any trusted third parties that are used in the TLS/SSL communication.

- Identity store: The identity store (or keystore) file contains the private key and the server TLS/SSL certificates. This file is stored in either JKS or PKCS12 format.

Keystore Formats

Keystore is a storage facility to store cryptographic keys and certificates. The supported keystore formats are:

- JKS - Java Key Store
- PKCS12 - Public Key Cryptography Standards

Keypass and Storepass

Keypass is a password used to protect the private key of a generated key pair. Storepass is a password used to protect the integrity of a keystore. If you don't provide a keypass, then the keypass is set to the same value as the storepass.

Identity and Trust Keystores

WebLogic Server uses private keys, digital certificates, and trusted certificates issued by certification authorities to establish and verify server identity and trust. See Identity and Trust in *Understanding Security for Oracle WebLogic Server*.

To create identity and trust keystores, you must use the `keytool` utility. Keytool is a key and certificate management utility that is included in the JDK. For more information, refer to the following topics:

Create Identity and Trust Keystores for Self-Signed Certificates

Use the `keytool` utility to create identity and trust keystores for self-signed certificates.

To do this:

1. Create an identity keystore:

   ```
   keytool -genkey -alias <private_key_alias> -keyalg <key_algorithm> -
   keysize <key_size> -sigalg <signature_algorithm> -validity
   <validity_period_in_days> -keystore <keystore_fileName> -keypass
   <key_passphrase> -storepass <identity_keystore_passphrase>
   ```

   For example:

   ```
   keytool -genkey -alias servercert -keyalg RSA -keysize 2048 -sigalg
   SHA256withRSA -validity 365 -keystore identity.jks -keypass
   identityKeyPassword -storepass identityStorePassword
   ```

2. (Optional) To use the identity keystore in PKCS12 format, convert the keystore from JKS type to PKCS12 type:

   ```
   keytool -importkeystore -srckeystore <keystore_file_in_JKS_Format> -
   destkeystore <keystore_file_in_PKCS12_format> -deststoretype pkcs12
   ```

For example:

```
keytool -importkeystore -srckeystore identity.jks -destkeystore
identity.p12 -deststoretype pkcs12
```

3. Export the identity keystore to create a certificate:

```
keytool -export -alias <private_key_alias> -noprompt -file
<certificate_name> -keystore <identity_keystore_filename> -storepass
<identity_keystore_passphrase>
```

For example:

```
keytool -export -alias servercert -noprompt -file server.cert -keystore
identity.jks -storepass identityStorePassword
```

4. Import the certificate into the trust keystore:

```
keytool -import -alias <trust_store_alias> -noprompt -file
<certificate_name> -keystore <trust_keystore_filename> -storepass
<trust_keystore_passphrase>
```

For example:

```
keytool -import -alias trustcert -noprompt -file root.cert -keystore
trust.jks -storepass trustKeyStorePassword
```

5. (Optional) To use the trust keystore in PKCS12 format, convert the keystore from JKS type to PKCS12 type:

```
keytool -importkeystore -srckeystore <keystore_file_in_JKS_Format> -
destkeystore <keystore_file_in_PKCS12_format> -deststoretype pkcs12
```

For example:

```
keytool -importkeystore -srckeystore identity.jks -destkeystore
identity.p12 -deststoretype pkcs12
```

6. Validate the identity and trust keystores:

```
keytool  -list -v -keystore <keystore_file>
```

For example:

```
keytool -list -v -keystore identity.jks -storepass identityStorePassword
keytool -list -v -keystore trust.jks -storepass trustKeyStorePassword
```

Create Identity and Trust Keystores for CA-Signed Certificate

Use the `keytool` utility to create identity and trust keystores for self-signed certificates.

To do this:

1. Create a keystore:

```
keytool -keystore <keystore_file_in_JKS_Format> -genkey -alias
<private_key_alias>
```

For example:

```
keytool -keystore clientkeystore -genkey -alias client
```

Enter the required details when prompted. For example:

```
Enter keystore password: javacaps
What is your first and last name?
[User]:  example.org.com
What is the name of your organizational unit?
[User]:  Development
What is the name of your organization?
[User]:  example org
What is the name of your City or Locality?
[User]:  San Francisco
What is the name of your State or Province?
[User]:  California
What is the two-letter country code for this unit?
[User]:  US
Is <CN=example.org.com, OU=Development, O=example org, L=San Francisco,
ST=California,
C=US> correct?
[no]:  yes

Enter key password for <client>
(RETURN if same as keystore password):
```

2. Generate a Certificate Signing Request (CSR):

```
keytool -keystore <keystore_file> -certreq -alias <private_key_alias> -
keyalg <key_algorithm> -file
      <certificate_signing_request_file>
```

For example:

```
keytool -keystore clientkeystore -certreq -alias client -keyalg rsa -file
client.csr
```

Enter the required details when prompted. For example:

```
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [User]: example.org.com
What is the name of your organizational unit?
  [User]: Development
What is the name of your organization?
  [User]: example org
```

```
What is the name of your City or Locality?
  [User]: San Francisco
What is the name of your State or Province?
  [User]: California
What is the two-letter country code for this unit?
  [User]: US
Is CN=example.org.com, OU=Development, O=example org, L=San Francisco,
ST=California, C=US correct?
  [no]: yes

Enter key password for <client>
        (RETURN if same as keystore password):
Re-enter new password:
```

3. Submit the Certificate Signing Request to Certification Authority (CA):

   Submission of CSR to CA can be done online or through Email. After the CSR is received by the CA, the request will be verified and a TLS/SSL certificate will be issued. After the verification process is complete, the CA either sends the TLS/SSL certificate over an Email or provides access to the client to download the certificate using an online account.

   The Certification Authority provides a ZIP file that contains:

   - Server SSL Certificate
   - Root and Intermediate Certificates
   - Private Key

   > **Note**
   >
   > The CA can provide a combined or a separate root and intermediate certificates. Also, there can be multiple intermediate certificates. The root and intermediate certificates need to be combined to form a single certificate, which can be used to configure TLS/SSL in WebLogic Server.

4. Create a combined certificate by doing the following:

   a. Open a text editor.

   b. Copy the contents of the root certificates including `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`, and paste them one below the other in the text editor.

   c. Save the file as `combined.crt`.

5. Validate the combined certificate:

   ```
   bash>openssl verify -CAfile combined.crt certificate.crt
   certificate.crt: OK
   ```

6. Create a trust store file:

   ```
   keytool -noprompt -import -alias <server_alias> -file <CA_certificate> -
   keystore <trust_store_file> -storepass <trust_store_password>
   ```

For example:

```
keytool -noprompt -import -alias trustcert -file ca_bundle.crt -keystore
trust.jks -storepass mypassword
```

If there are multiple root or CA certificates, import them individually into the same keystore file. For example:

```
keytool -import -file /u01/app/cascerts/rootCA.cert -alias rootCA -
keystore trust.jks
keytool -import -file /u01/app/cascerts/firstCA.cert -alias firstCA -
keystore trust.jks
keytool -import -file /u01/app/cascerts/secondCA.cert -alias secondCA -
keystore trust.jks
keytool -import -file /u01/app/cascerts/thirdCA.cert -alias thirdCA -
keystore trust.jks
```

7. Merge all intermediate certificates into one file (for example, `combined.crt`):

```
cat ca_1.crt ca_2.crt > combined.crt
```

8. Create an identity store file:

```
openssl pkcs12 -export -in <server_certificate> -inkey <private_key> -
chain -CAfile <combined_certificate_file> -name <private_key_alias> -out
<identity_keystore_in_PKCS12_format>
```

```
keytool -noprompt -importkeystore -destorepass
<destination_store_password> -destkeystore <destination_keystore_file> -
srckeystore <source_keystore_file> -srcstoretype <source_keystore_type> -
srcalias <source_alias> -destalias <destination_alias> -srckeypass
<source_key_password>
```

For example:

```
openssl pkcs12 -export -in certificate.crt -inkey private.key -chain -
CAfile combined.crt -name servercert -out mycert.p12
```

```
keytool -noprompt -importkeystore -deststorepass mypassword -destkeystore
identity.jks -srckeystore mycert.p12 -srcstoretype PKCS12 -srcalias
servercert -destalias servercert -srckeypass mypassword
```

Store Keystores and Passphrases in Azure Key Vault

Secure key management is essential to protect data in the cloud.

An Azure Key Vault lets you to store the TLS/SSL certificates, confidential keys, and other secrets, such as passwords. The following example shows how to store TLS/SSL certificates and keystores in Azure KeyVault:

```
az keyvault secret set --vault-name mySecureKeyVault  --encoding base64 --
description text/plain --name identityKeyStoreData --file identity.jks
az keyvault secret set --vault-name mySecureKeyVault  --name
```

```
"identityKeyPassPhrase" --value "identityKeyPassword"
az keyvault secret set --vault-name mySecureKeyVault  --encoding base64 --
description text/plain --name trustKeyStoreData --file trust.jks
az keyvault secret set --vault-name mySecureKeyVault  --name
"trustKeyPassPhrase" --value "trustKeyPassword"
az keyvault secret set --vault-name mySecureKeyVault  --name
"privateKeyAlias" --value "servercert"
az keyvault secret set --vault-name mySecureKeyVault  --name
"privateKeyPassPhrase" --value "myPrivateKey"
```

For more information about managing the Azure Key Vault secrets, see Microsoft documentation on Azure Key Vault Secrets.