

Preparation and Prerequisites for OracleDB for Azure

This topic provides information on what you need to do to get ready for OracleDB for Azure setup.

Azure Roles

To set up and use OracleDB for Azure, you need an existing Azure account with the necessary Azure roles.

There are two sets of required roles: admin roles needed for initial OracleDB for Azure setup, and user roles needed by application and database developers. OracleDB for Azure setup is a one-time operation, and the roles required for setup are therefore needed for a limited amount of time.

OracleDB for Azure Onboarding Roles

To set up OracleDB for Azure, your Azure user must have at least one of the following roles assigned:

- Application Administrator
- Cloud Application Administrator
- Privileged Role Administrator
- Global Administrator

You can remove the role assignment from your user account for security purposes after the sign up is complete. See [Remove Azure role assignments](#) in the Azure documentation for information.

Alternately, you can create an Azure admin user specifically for OracleDB for Azure onboarding, and then delete this account once setup is complete.

Azure Subscription Linking

Whether you choose fully-automated OracleDB for Azure configuration or guided account linking, you will need to specify which Azure subscriptions you want to link to your OCI tenancy. By design, OracleDB for Azure does not link all Azure subscriptions to the OCI tenancy. This is because many Azure accounts have hundreds or thousands of subscriptions, and Azure account administrators in many cases only want to use a subset of their subscriptions with OracleDB for Azure.

To view and link an Azure subscription in the OracleDB for Azure portal, you must have Owner privileges for the subscription. OracleDB for Azure does not display subscriptions for which your Azure user is not an owner.

See [Add or change Azure subscription administrators](#) in the Azure documentation for more information.

For [Guided Onboarding](#), the OracleDB for Azure administrative user setting up the service have the "Multicloudlink Administrator" role in the Oracle Database Service (ODS) multitenant application that OracleDB for Azure deploys in the Azure tenancy.

For each subscription being linked, the onboarding user or an Azure administrator must grant the Oracle Database Service multitenant application the following roles:

- Contributor
- EventGrid Data Sender
- Monitoring Metrics Publisher
- Network Contributor

These roles allow the Oracle Database Service multitenant application to:

- Create and manage resources in the subscription (for example, the custom dashboard, Azure App Insights, and Azure Log Analytics workspaces OracleDB for Azure creates for each provisioned database).
- Stream OCI Database metrics to Azure App Insights and events to Azure Log Analytics.
- Configure network settings in Azure so Azure resources can access the database resources in OCI.
- Submit events to Azure Event Grid.

These role assignments are the minimum requirements for ODSA to operate in a customer's Azure tenant and must remain in effect as long as the subscription is used in ODSA. For instructions for assigning those roles see [To assign the Multicloud Link Administrator role to an OracleDB for Azure user](#) and [To link Azure subscriptions to OracleDB for Azure](#).

Identity Federation Options for OracleDB for Azure Onboarding

Decide in advance whether you want to enable identity federation in your environment. You should also review the documentation to determine whether you want for OracleDB for Azure to setup federation for you, or if want to do it yourself. See [Using Identity Federation in OracleDB for Azure](#) for more information. Note that the fully-automated configuration option requires that you grant more permissions to Oracle's account linking program than the guided account linking option.

Azure Virtual Networks

Some OracleDB for Azure database products require you to specify an Azure Virtual Network (VNet) in Azure during provisioning. For example, when provisioning Oracle Base Database systems or Oracle Exadata Cloud VM clusters, you must have an Azure Virtual Network available to OracleDB for Azure to complete the provisioning operation. Work with your Azure administrators or Networking team to create one or more Azure Virtual Networks for OracleDB for Azure systems.


OCI Account and Regions

Identify the primary OCI region you want to use as your default region for OracleDB for Azure resource provisioning. During OracleDB for Azure setup, this region becomes the primary OCI region associated with your OCI account. See [Oracle Database Service for Azure Regional Availability](#) for a list of locations offering OracleDB for Azure.

If you're working with Oracle Sales to acquire OracleDB for Azure, your OCI account billing and partial account setup will be already done for you. During onboarding, all you must do is provide a name for your OCI tenancy, set a password for the OCI account associated with your primary email address, and select the primary or home region for your account.

If you already have an OCI account, you can use that account to onboard with OracleDB for Azure. Be sure to perform the onboarding with an OCI user that has admin permissions if you are using an existing OCI account.

If you don't have an OCI account, the OracleDB for Azure onboarding process allows you to create a new account during OracleDB for Azure setup.

 **Note**

While OracleDB for Azure works with personal accounts backed with a credit card, to deploy dedicated Exadata infrastructure in OracleDB for Azure, you must have a direct billing relationship with Oracle. You cannot use dedicated Exadata infrastructure with a pay as you go account.

Was this article helpful?



Updated 2024-07-17