

High Availability

Oracle Database HA Features-L200

Bal Sharma
Oracle Cloud Infrastructure
October 2019





Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Database High Availability - Objectives

After completing this lesson, you should be able to:

- Describe the options of database high availability available with Oracle Cloud Infrastructure
- Features of Active Data Guard
- Network Preparation for DataGuard Setup
- Launch a Data Guard for Database Cloud Service Virtual Machines
- Launch a Data Guard for Database Cloud Service Bare Metal
- Switch Over/Failover/Reinstate in Data Guard setup
- Delete Standby Database
- Autonomous Database(ATP/ADW) Cloning
- Demo



Part 1. High Availability- Using A/DataGuard

Data Guard & Active DataGuard on VMDB, BMDB





DataGuard on Database Cloud Service- VM/BM

- Data Guard and Active Data Guard provide disaster recovery (DR) for databases with recovery time objectives (RTO) that cannot be met by restoring from backup.
- Active Data Guard extends Data Guard capabilities by providing advanced features for data protection and availability as well as offloading read-only workload and fast incremental backups from a production database.
 Active Data Guard is included in the Extreme Performance Edition and Exadata Service.
- Once Data Guard is instantiated, it maintains synchronization between the primary database and the standby database.
- To configure a Data Guard system across regions or between on-premises and Oracle Cloud Infrastructure DB systems, you must access the database host directly and use the DGMGRL utility.
- Oracle recommends that the DB system of the standby database be in a different availability domain.
- The standby databases in Oracle Cloud Infrastructure Database are physical standbys.

Currently 3 major operations are supported on OCI DbaaS VM.

- SetupDataguard
- SwitchOvar/Failover/Reinstate
- DeleteStandbyDatabase

Note: You can't terminate a primary database that has a Data Guard association with a peer (standby) database. Delete the standby database first. Alternatively, you can perform a switchover to the standby database, and then terminate the primary database. You can't terminate a DB system that includes Data Guard enabled databases. To remove the Data Guard association: For a bare metal DB system database - terminate the standby database. For a virtual machine DB system database - terminate the standby DB system.

DataGuard on Database Cloud Service-Prerequisites

A Data Guard implementation requires two DB systems, one containing the primary database and one containing the standby database. When you enable Data Guard for a virtual machine DB system database, a new DB system with the standby database is created and associated with the primary database. For a bare metal DB system, the DB system with the database to be used as the standby must already exist before you enable Data Guard(Create a database in the required AD and subnet before you attempt DG association).

Note: A Data Guard configuration on the Oracle Cloud Infrastructure is limited to one standby database per primary database.

- •Both DB systems must be in the same compartment, and they must be the same shape.
- •The database versions and editions must be identical. Data Guard does not support Standard Edition. (Active Data Guard requires Enterprise Edition Extreme Performance.)
- •The database version determines whether Active Data Guard is enabled. If you are using the BYOL licensing model and if your license does not include Active Data Guard, you must either use Enterprise Edition High Performance or set up Data Guard manually. See <u>Using Oracle Data Guard with the Database CLI</u>.
- •Both DB systems must use the same VCN, and port 1521 must be open.



Data Guard Networking Requirement

• Properly configure the security list ingress and egress rules for the subnets of both DB systems in the Data Guard association to allow TCP traffic to flow between the applicable ports. Ensure that the rules you create are stateful (the default). For example, if the subnet of the primary DB System uses the source CIDR 10.0.0.0/24 and the subnet of the standby DB system uses the source CIDR 10.0.1.0/24, create rules as shown in the following example.

The egress rules in the example show how to enable TCP traffic only for port 1521, which is a minimum requirement for Data Guard to work. If TCP traffic is already enabled on all of your outgoing ports (0.0.0.0/0), then you need not explicitly add these specific egress rules. Service Gateway can provide NW connectivity.

Security List for Primary DB System's Subnet

Rules(Prod)	Stateless	Source	IP Protocol	Source Port	Dest Port
Ingress	No	10.0.01.0/24	TCP	All	1521
Egress	No	10.0.1.0/24	TCP	All	1521
Rules(Sby)	Stateless	Source	IP Protocol	Source Port	Dest Port
Ingress	No	10.0.0.0/24	TCP	All	1521
Egress	No	10.0.0.0/24	TCP	All	1521

Data Guard Configuration supported from Console

The Console allows you to enable a Data Guard association between databases, change the role of a database in a Data Guard association using either a *switchover* or a *failover* operation, and *reinstate* a failed database.

When you enable Data Guard, a separate Data Guard association is created for the primary and the standby database.

You can use console to perform following operations

- To enable Data Guard on a bare metal DB system
- To enable Data Guard on a virtual machine DB system
- To perform a database switchover
- To perform a database failover
- To reinstate a database
- To terminate a Data Guard association on a bare metal DB system
- To terminate a Data Guard association on a virtual machine DB system

Note: Data Guard Fast Start Failover as well across region DR is manual as of today-No cloud tooling.



Enabling Data Guard on a bare metal DB system

- Open the navigation menu. Under **Database**, click **Bare Metal, VM, and Exadata**.
- Choose the **Compartment** that contains the DB system with the database for which you want to enable Data Guard.
- Click the name of the DB system that contains the database you want to assume the primary role, and then
 click the name of that database.
- Under Resources, click Data Guard Associations.
- Click Enable Data Guard.
- In the **Enable Data Guard** dialog box, configure your Data Guard association.
 - **Peer Database Availability Domain:** Shows the availability domain of the selected peer DB system. Select the Availability Domain and Fault Domains based on requirement.
 - Peer DB System: Select the DB system that will contain the peer (standby) database.
 - Protection Mode: Console Supports Max Performance Mode at the moment.
 - **Transport Type:** The redo transport type used. The Console supports only **Async**.
 - **Database Admin Password:** Enter the primary database admin password.
 - The same password is used for the standby database.
- Confirm Database Admin Password: Re-enter the Database Admin Password you specified.
- Click Enable.

When the association is created, a shield icon appears next to the name of this database and its peer, and their respective roles (primary or standby) are displayed.

Note: Peer database should exist before you try creating DG association.

Enabling Data Guard on a VM DB system

- Open the navigation menu. Under **Database**, click **Bare Metal, VM, and Exadata**.
- Choose the **Compartment** that contains the DB system with the database for which you want to enable Data Guard.
- Click the name of the DB system that contains the database you want to assume the primary role, and select database.
- Under Resources, click Data Guard Associations.
- Click Enable Data Guard.
- In the **Enable Data Guard** dialog box, configure your Data Guard association.
- **Display Name:** A friendly, display name for the DB system. The name doesn't need to be unique.
- **Availability Domain:** The availability domain in which the DB system resides.
 - Virtual Cloud Network: Shows the VCN. The VCN of the standby database must be the same.
 - **Client Subnet:** The subnet to which the DB system should attach. Do not use a subnet that overlaps with 192.168.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance.
 - **Hostname Prefix:** Your choice of host name for the DB system. Must begin with an alphabetic character, and can contain only alphanumeric characters and hyphens (-). The maximum length should not exceed 16.

Note: The host name must be unique within the subnet.

- Host Domain Name: The domain name for the DB system.
- Host and Domain URL: FQDN of Host
- Protection Mode: The protection mode used. The Console supports only Maximum Performance.
- **Transport Type:** The redo transport type used for this Data Guard association. The Console supports only **Async**.
- Database Admin Password: Enter the primary database admin password, same will be used for standby database.
- **Confirm Database Admin Password:** Re-enter the Database Admin Password you specified.
- Click Enable.

Upon completion a shield icon appears next to the name of this database and its peer, and their respective roles are display

Switch Over Operation in Data Guard Configuration

You initiate a switchover operation by using the Data Guard association of the primary database.

- Open the navigation menu. Under Database, click Bare Metal, VM, and Exadata.
- Choose the Compartment that contains the DB system with the primary database you want to switch over.
- Click the DB system name, and then click the name of the primary database.
- Under Resources, click Data Guard Associations.
- For the Data Guard association on which you want to perform a switchover, click the Actions icon (three dots), and then click **Switchover**.
- In the **Switchover Database** dialog box, enter the database admin password, and then click **OK**.
- This database should now assume the role of the standby, and the standby should assume the role of the primary in the Data Guard association.

Failover of Database in Data Guard Configuration

You initiate a failover operation by using the Data Guard association of the standby database.

- Open the navigation menu. Under Database, click Bare Metal, VM, and Exadata.
- Choose the Compartment that contains the DB system with the primary database's peer standby you want to fail over to.
- Click the DB system name, and then click the name of the standby database.
- Under Resources, click Data Guard Associations.
- For the Data Guard association on which you want to perform a failover, click **Failover**.
- In the Failover Database dialog box, enter the database admin password, and then click OK.
- This database should now assume the role of the primary, and the old primary's role should display as Disabled Standby.

Reinstate of database in Data Guard Configuration

- After you fail over a primary database to its standby, the standby assumes the primary role and the old
 primary is identified as a disabled standby. After you correct the cause of failure, you can reinstate the failed
 database as a functioning standby for the current primary by using its Data Guard association.
- Before you can reinstate a version 12.2 database, you must perform some steps on the database host to stop
 the database or start it in MOUNT mode.
- Set your ORACLE_UNQNAME environment variable to the value of the Database Unique Name (as seen in the Console), and then run these commands:

```
srvctl stop database -d db-unique-name -o abort srvctl start database -d db-unique-name -o mount
```

- Open the navigation menu. Under Database, click Bare Metal, VM, and Exadata.
- Choose the **Compartment** that contains the DB system with the failed database you want to reinstate.
- Click the DB system name, and then click the database name.
- Under Resources, click Data Guard Associations.
- For the Data Guard association on which you want to reinstate this database, click the Actions icon (three dots), and then click **Reinstate**.
- In the **Reinstate Database** dialog box, enter the database admin password, and then click **OK**.
- This database should now be reinstated as the standby in the Data Guard association.



Terminate Data Guard Association in VMDB/BM DB

On a Bare metal DB system, you remove a Data Guard association by terminating the standby database.

- Open the navigation menu. Under **Database**, click **Bare Metal, VM, and Exadata**.
- Choose the Compartment that contains the DB system that includes the standby database you want to terminate.
- Click the DB system name.
- For the standby database you want to terminate, click the Actions icon (three dots), and then click **Terminate**.
- In the **Terminate Database** dialog box, enter the name of the database, and then click **OK**.

On a **virtual machine DB system**, you remove a Data Guard association by terminating the standby DB system.

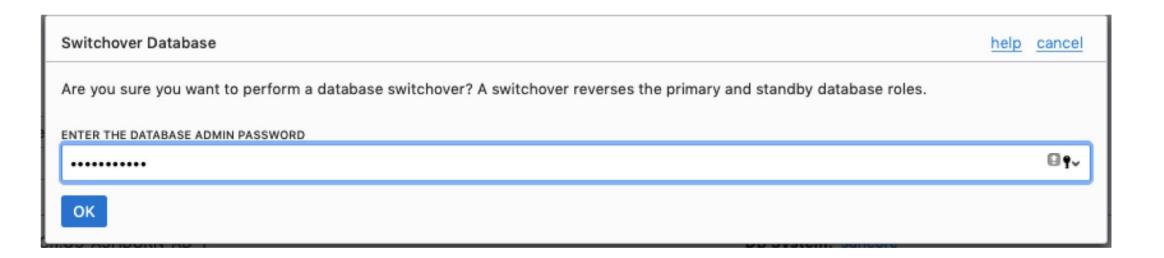
- Open the navigation menu. Under **Database**, click **Bare Metal, VM, and Exadata**.
- Choose the Compartment that contains the standby DB system that you want to terminate.
- Click the DB system name, click the Actions icon (three dots), and then click Terminate.
- Confirm when prompted.
- The DB system's icon indicates Terminating.



Supported Operation for Data Guard-"SwitchOver"

The following actions are supported for Data Guard configurations to support easier planned maintenance and also to recover from any type of failures or DR scenario.

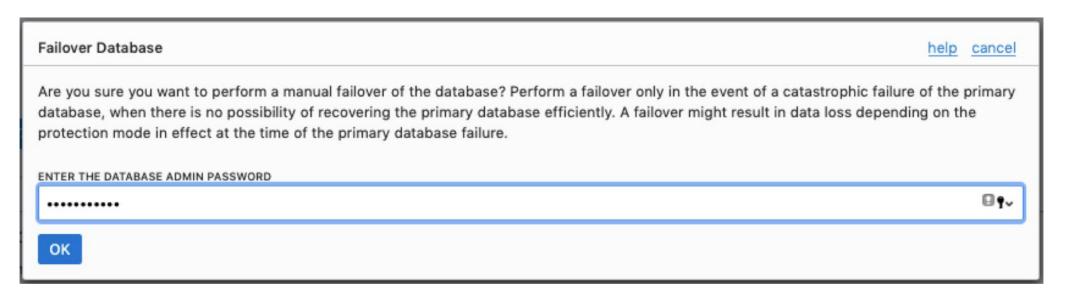
Switchover - A switchover is a role reversal between the primary database and one of its standby databases. A switchover guarantees no data loss. This is typically done for planned maintenance of the primary system. During a switchover, the primary database transitions to a standby role, and the standby database transitions to the primary role. The transition occurs without having to reenable either database.





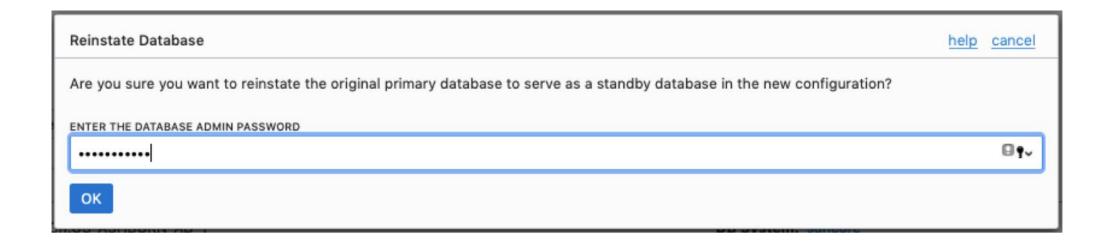
Data Guard-FailOver

Failover - A **failover** is when the primary database (all instances of a RAC primary database) fails and one of the standby databases is transitioned to take over the primary role. Failover is performed only in the event of a catastrophic failure of the primary database, and there is no possibility of recovering the primary database in a timely manner. Failover may or may not result in data loss depending on the protection mode in effect at the time of the failover. This operation is supported from the Standby database.



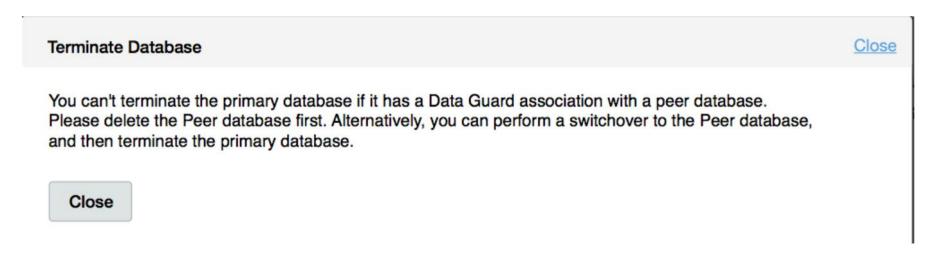
Data Guard- Reinstate

Reinstate – In some situations, the primary database can go into a failed state, which becomes irrecoverable. The reinstate allows customers to reinstate a failed primary database as a standby database after repair.



Terminating Databases/Db System in Data Guard Configuration

You need to to explicitly remove Data Guard associations by deleting the Standby Database before the Primary Database or the DB System can be terminated.



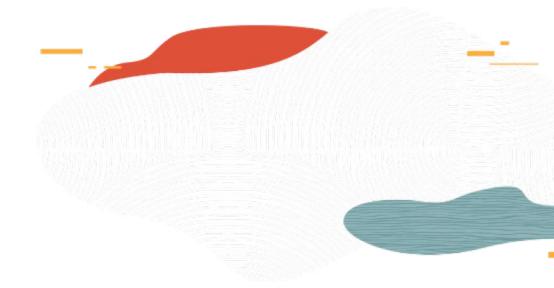
Terminate DB System

Close

You can't terminate the DB System because it includes Data Guard enabled databases. To remove the Data Guard associations, terminate the standby databases.

Close





Part2. High Availability-Demo

Creation of Standby & Data Guard operation

Bal Sharma

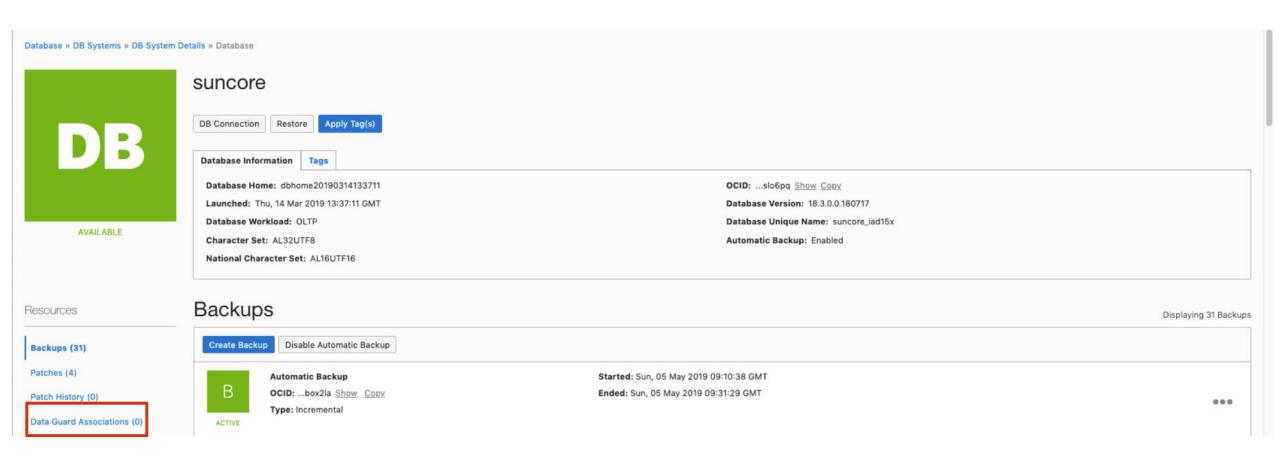
Oracle Cloud Infrastructure

October 2019



Demo: Creating Data Guard for VM DB

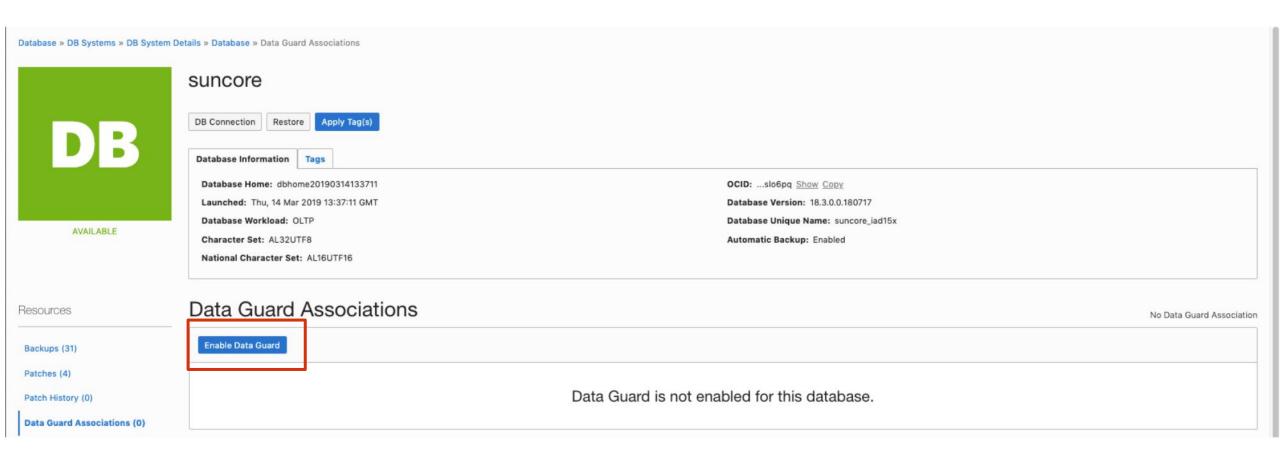
Step1: Login to Console and locate the database for which you want to enable Data Guard





Creating Data Guard for VM DB continued

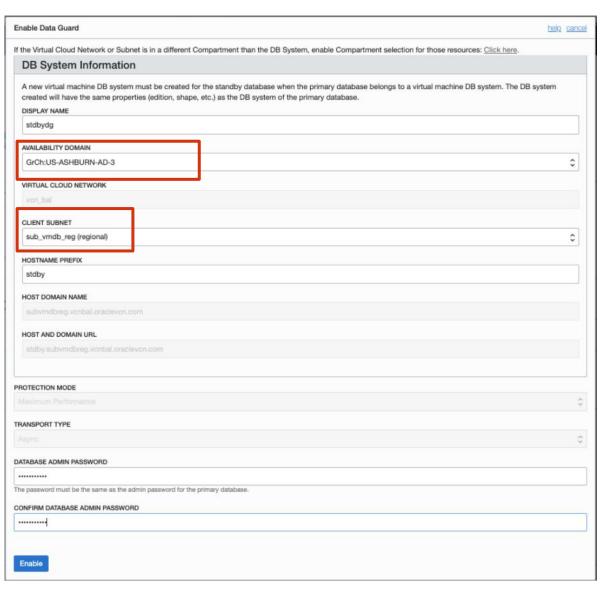
Step2. Go to Data Guard Association Page-Click on Enable Data Guard





Creating Data Guard for VM DB continued

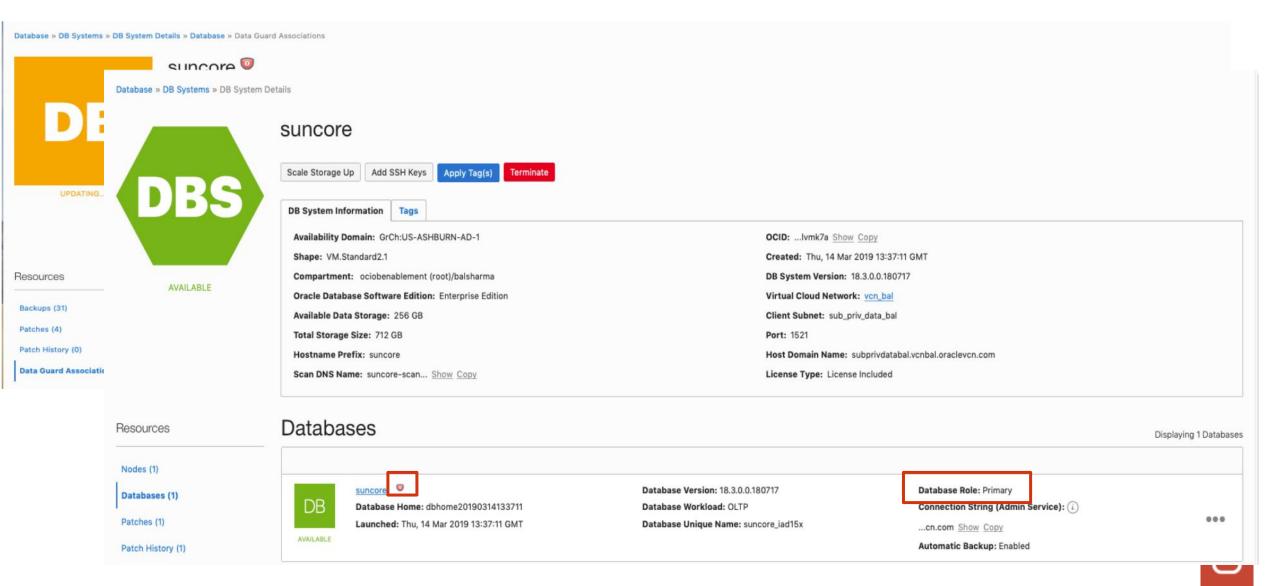
Step3. Input Enable Data Guard Association page



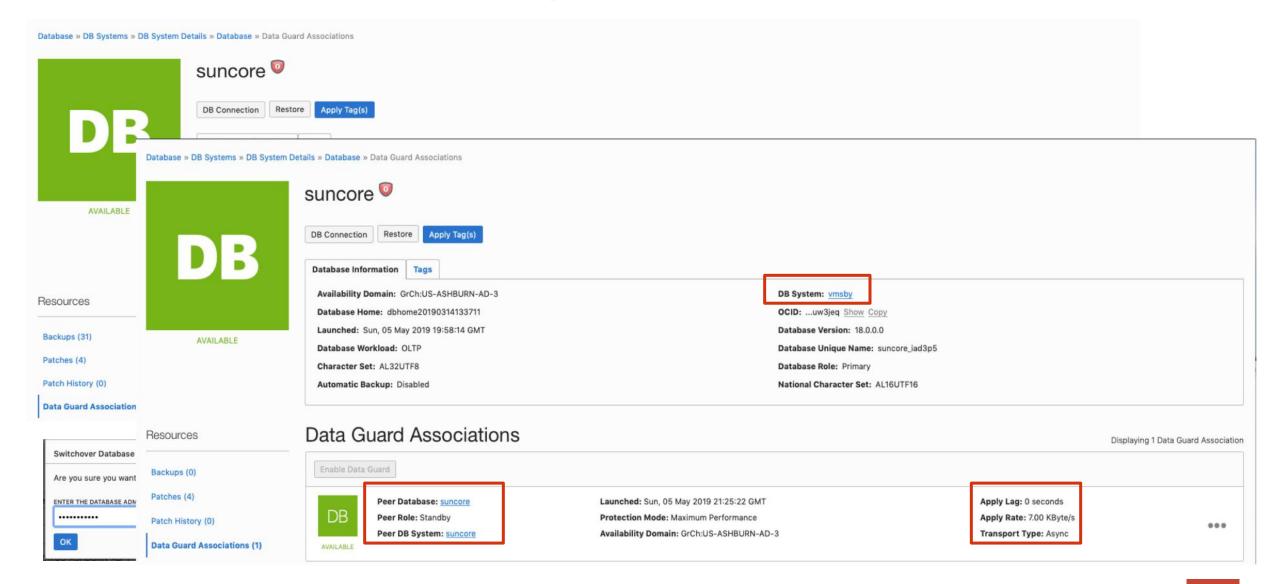
- Input Availability Domain you want DG to be created as well Subnet associated
- Provide password for Admin user same as that of Actual Production database
- Make sure port 1521 port is enabled between subnets and security list is modified as per steps before.
- Make sure Security List having security rules are associated to subnet containing prod and Standby(DG) databases you are creating.

Creating Data Guard for VM DB continued

Step4: Data Guard Association VM DB-Status

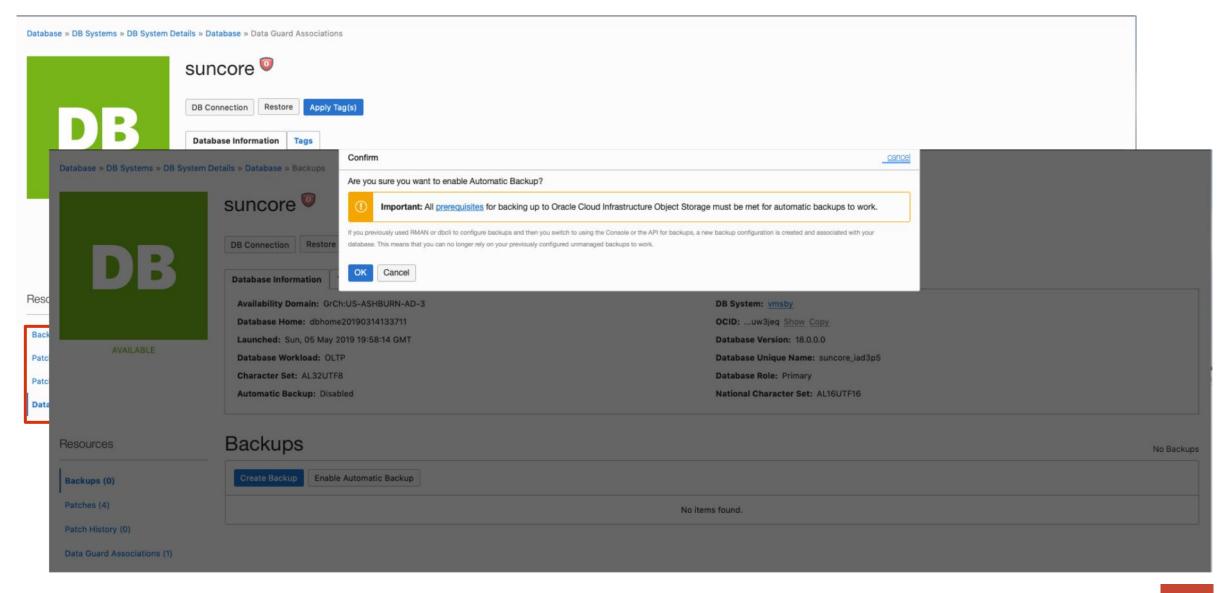


Data Guard Switch Over operation VM DB

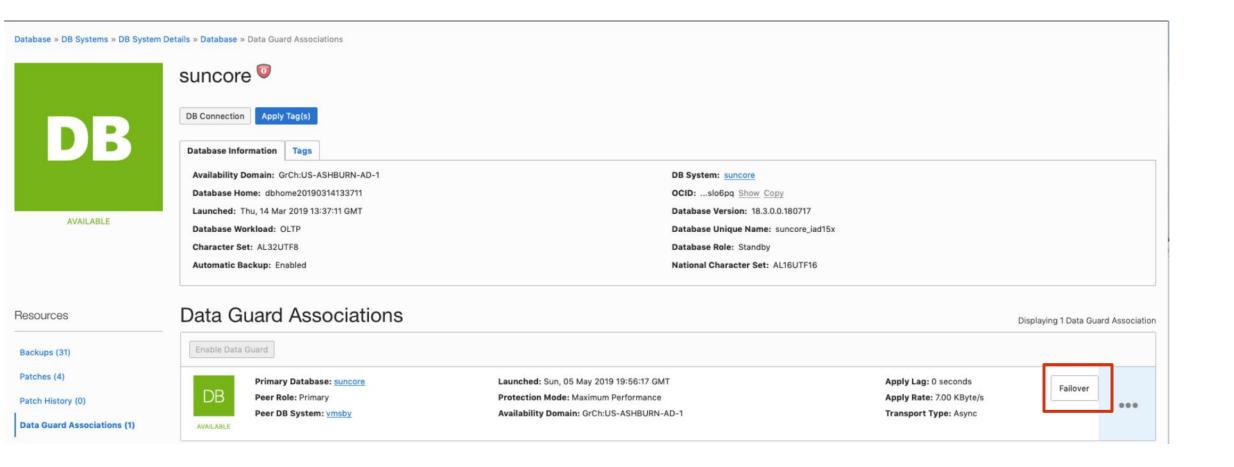




Data Guard Backup Configuration on VM DB



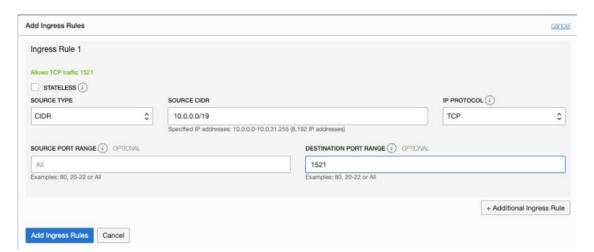
Data Guard Failover operation VM DB

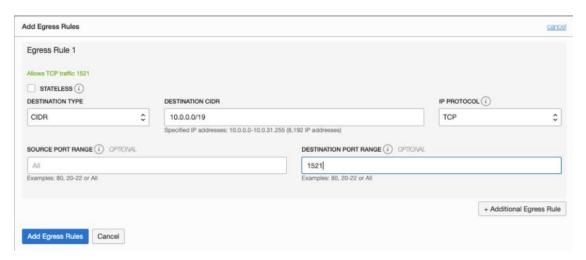




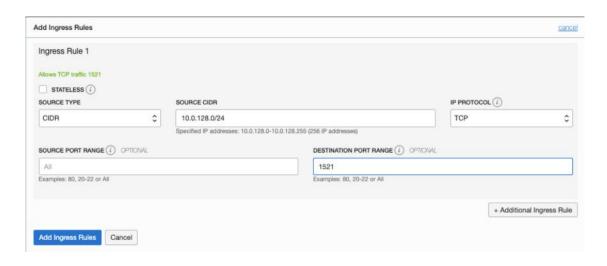
Appendix: Data Guard Association- Ingress and egress rules-VM DB

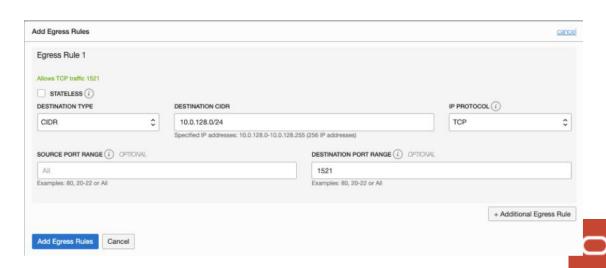
Source Database Ingress and egress rules in Security List





Target(Stdby) Database Ingress and egress rules in security List

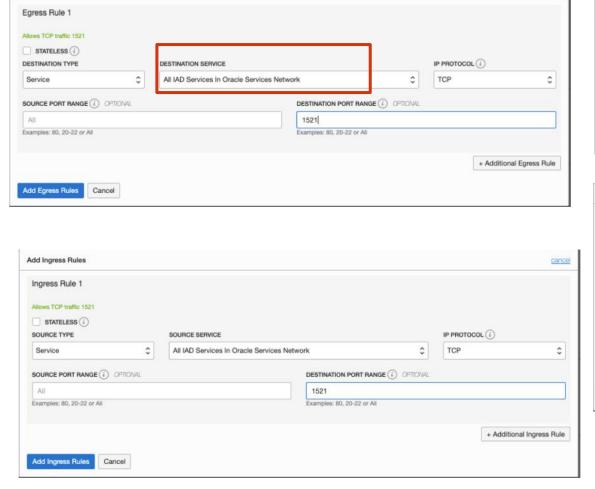




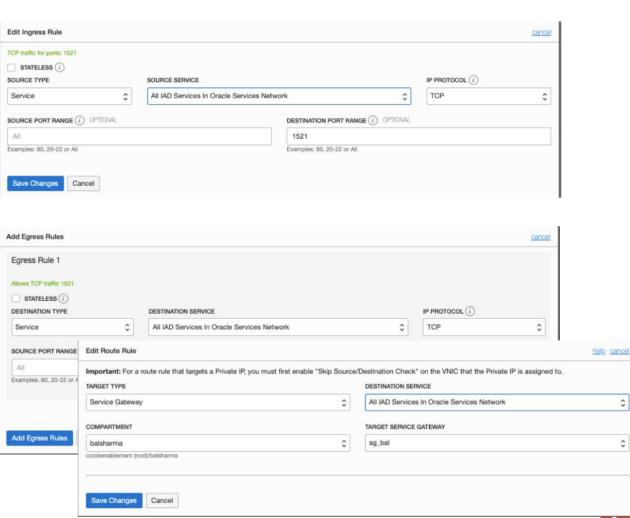
Appendix: Modifying egress ingress rules for Service Gateway.

cancel

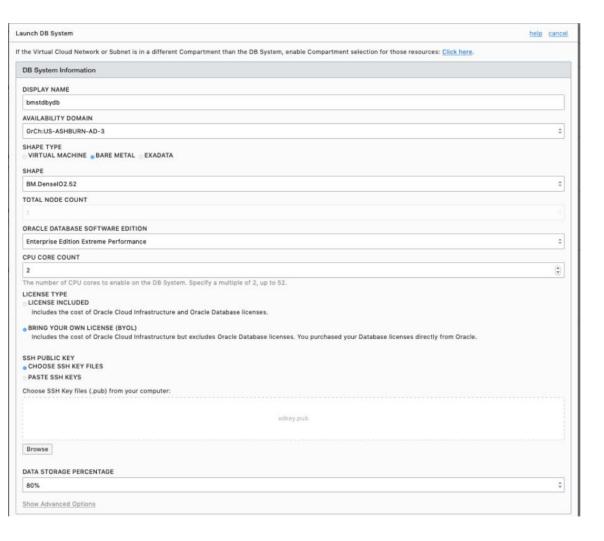
Incase you use Service Gateway and no NAT/IGW, configure rules for Service GW- Make sure your SGW is created using "All IAD Services in Oracle Service Network"

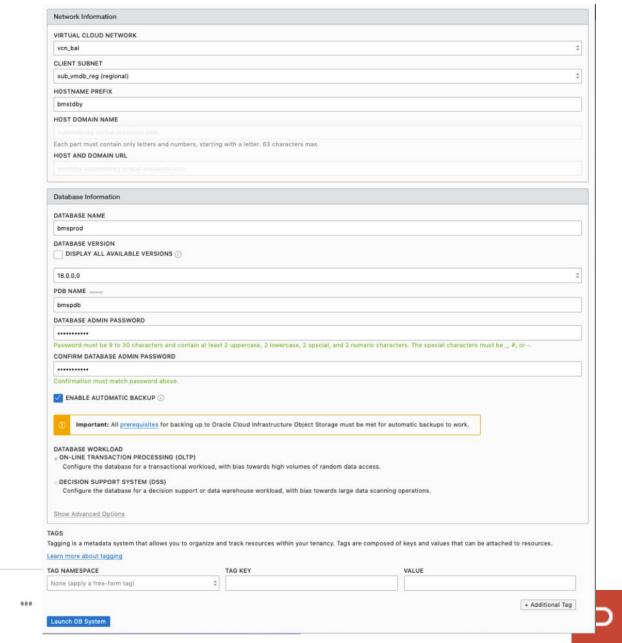


Add Egress Rules



Demo: Data Guard BM-Prepare Peer Database





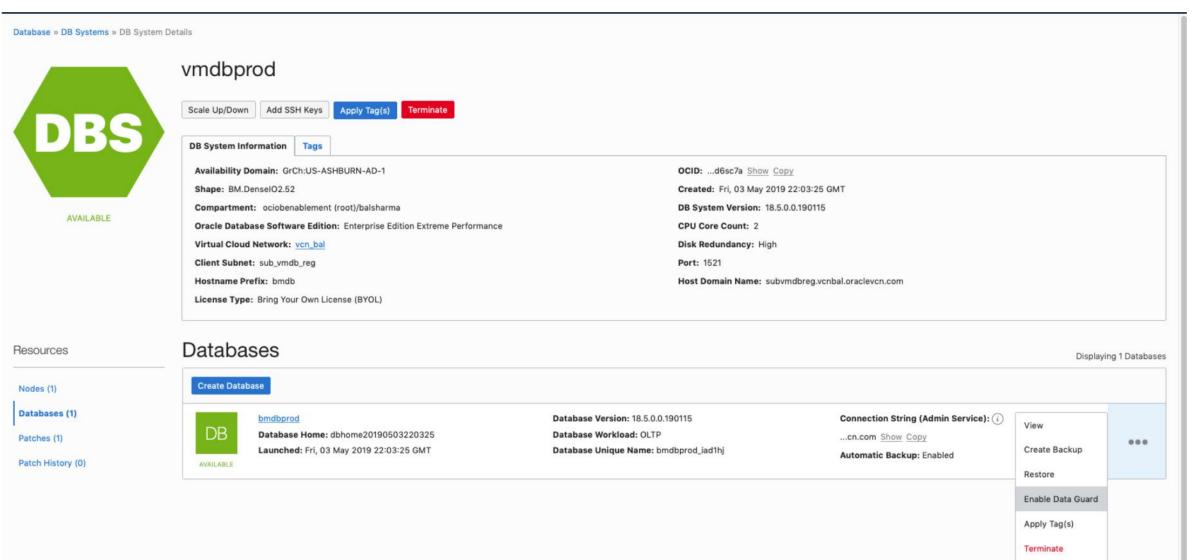
Availability Domain: GrCh:US-ASHBURN-AD-3

OCID: ...lį65ma Show Copy

Oracle Database Software Edition: Enterprise Edition Extreme Performance CPU Core Count: 2 Shape: BM.Densei02.52 Virtual Cloud Network: ycn_bal Launched: Sun, 05 May 2019 20:07:48 GMT Client Subnet: sub_ymdb_reg
Private IP: Loading...

Public IP: Loading...

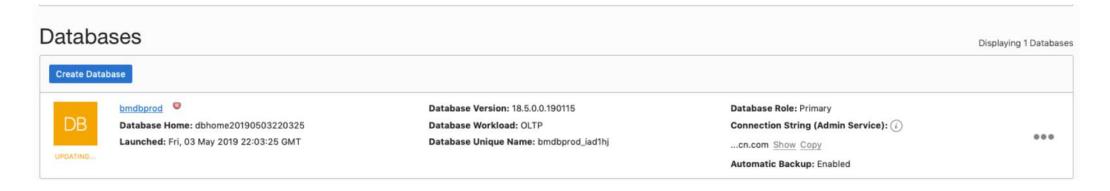
Bare Metal DB - Enabling DG after peer database created



Bare Metal DB - Enabling DG

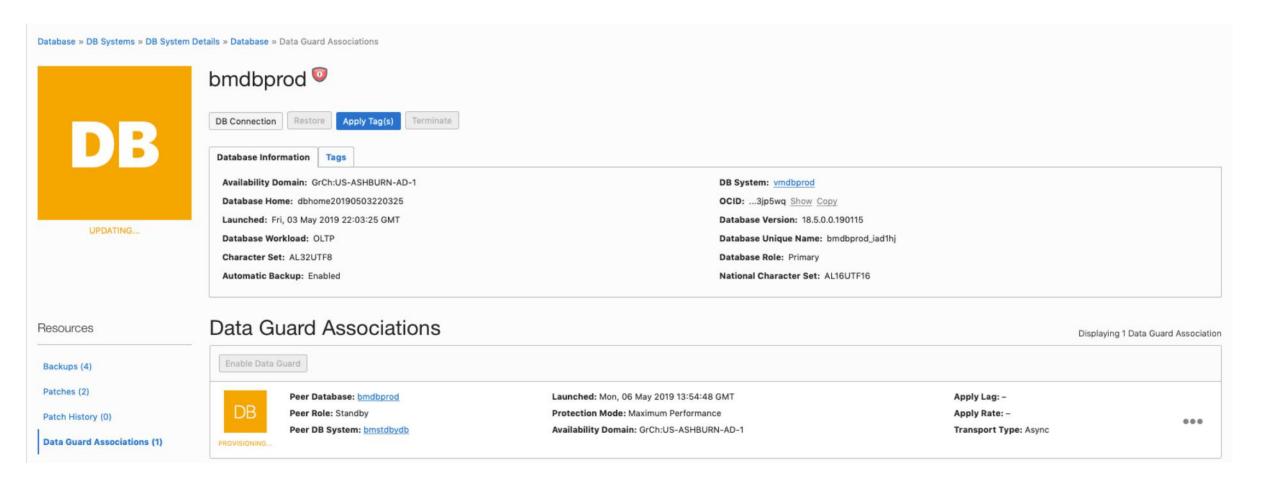


- Select Availability Domain and Peer database Created.
- Specify password for Admin(SYS)- Same as that of Production
- Click Enable-Database will show as "Updating".



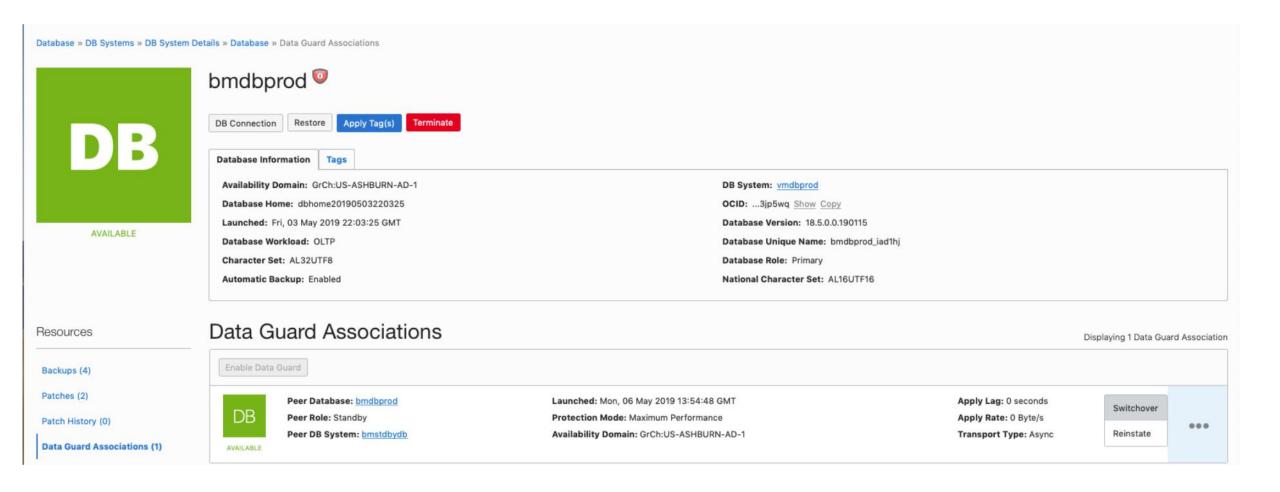


Demo: Bare Metal DB - Enabling DG tracking in console



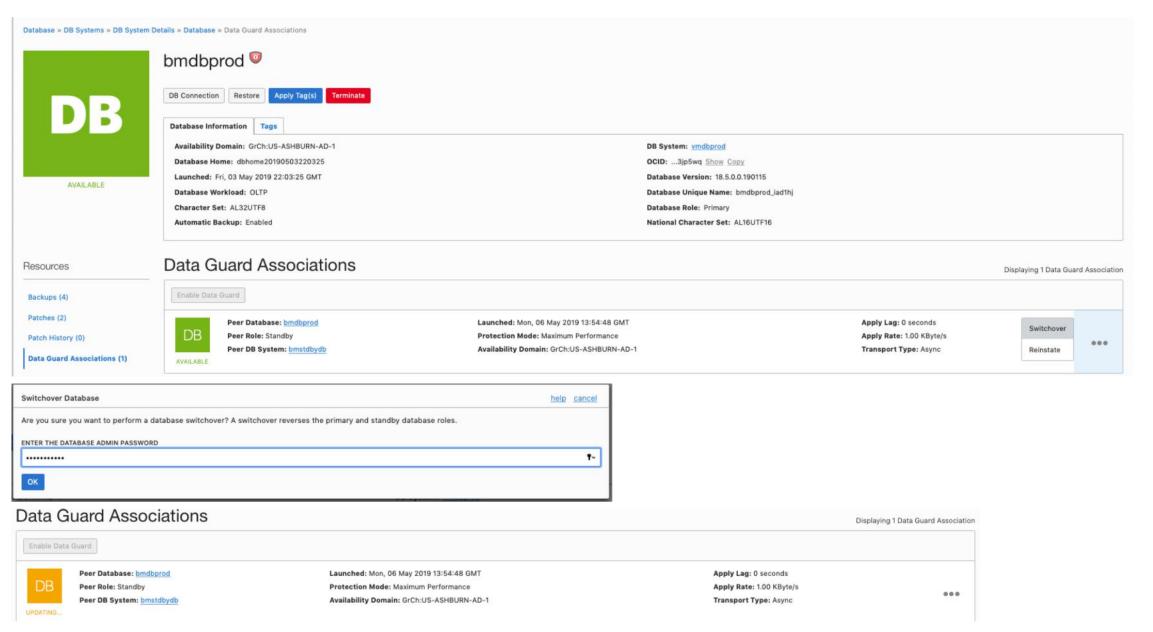


DG Association-BM DB.. Continued

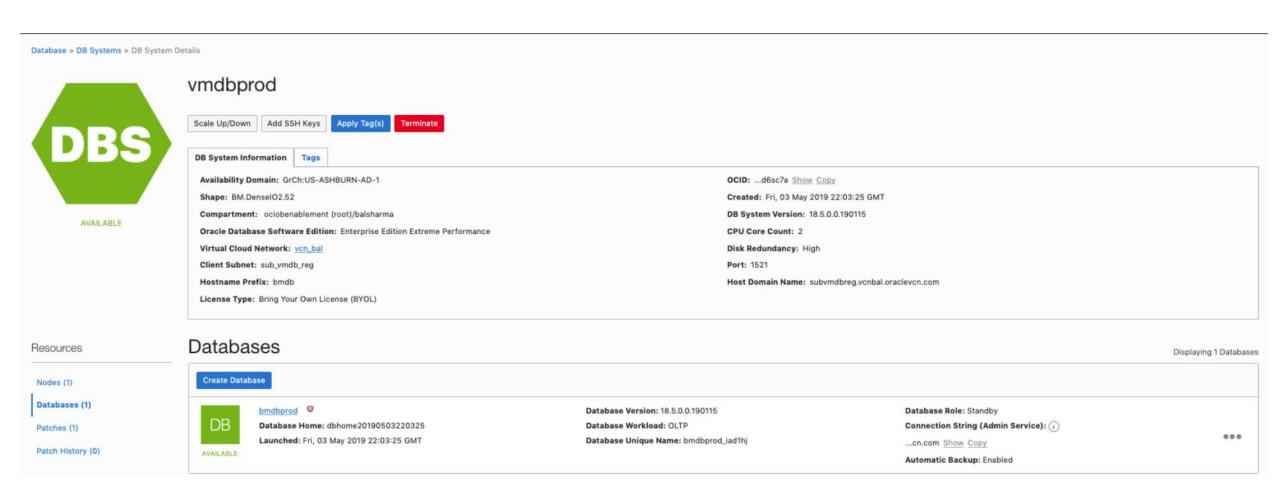




Demo: DG Switchover-BM DB

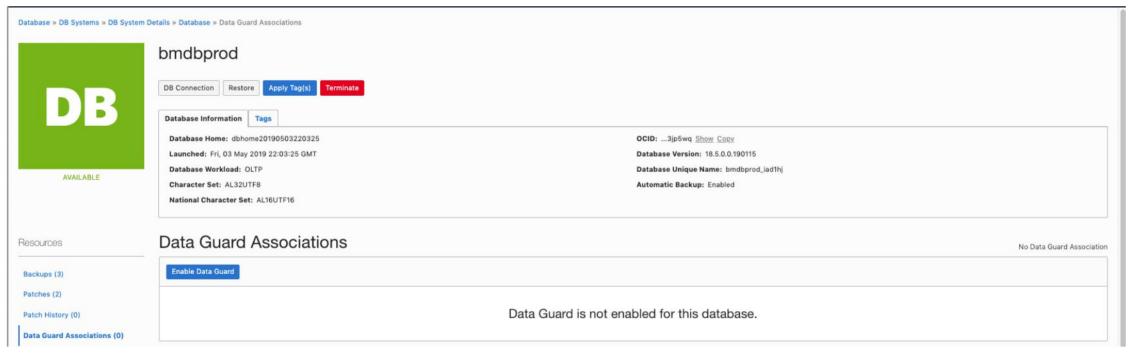


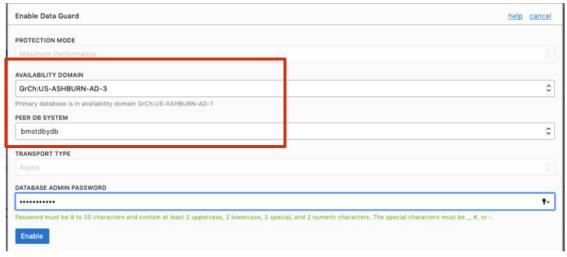
DG Switchover-BM DB Role transition





Appendix: Create Peer database for BM DB

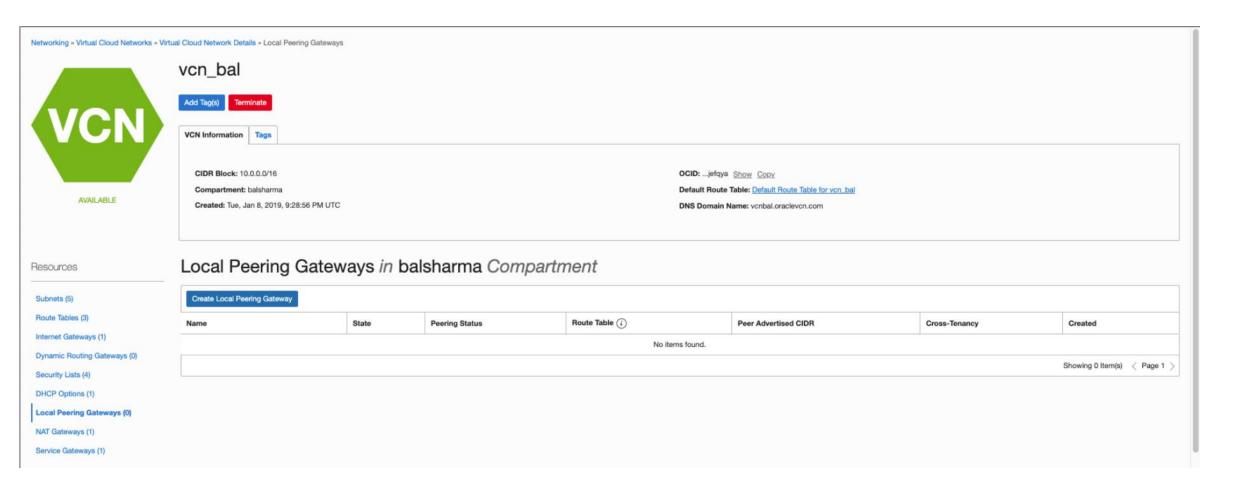




Note: Before attempting Data Guard association make sure you have created the peer Db system in advance in required AD

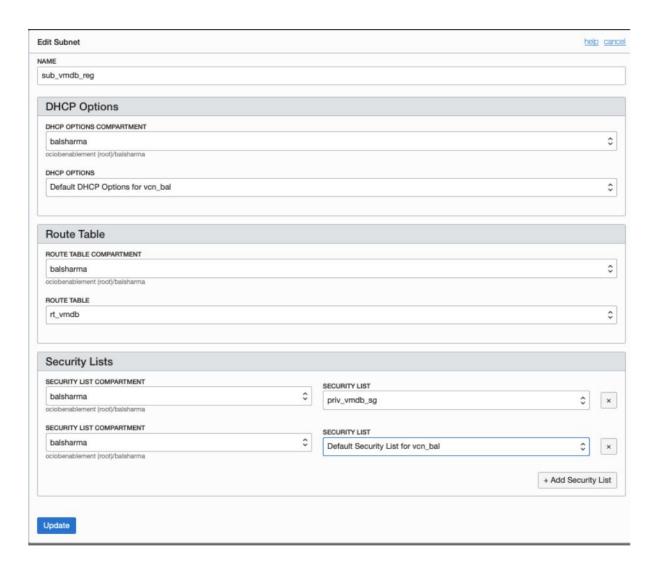


Appendix: Not supported across VCN





Appendix: Modifying Security List, Routing for BM DB DataGuard



dd Ingress Rules					can
Ingress Rule 1					
Allows TCP traffic for ports STATELESS () SOURCE TYPE	s: all	SOURCE CIDR		IP PROTOCOL (i)	
CIDR	0	0 10.0.128.0/24		TCP	٥
		Specified IP addresses: 10.0.128	.0-10.0.128.255 (256 IP addresses)		
SOURCE PORT RANGE (i) OPTIONAL		DESTINATION PORT RANGE	OPTIONAL.	
All			All		
Examples: 80, 20-22 or All			Examples: 80, 20-22 or All		
				+ Addition	al Ingress Rul
Add Ingress Rules	Cancel				
	Cancel				car
dd Ingress Rules	Cancel				car
dd Ingress Rules Ingress Rule 1 Allows TCP traffic for ports STATELESS ()		SALIBOS CIDE		IP PROTOCOL (I)	can
did Ingress Rules Ingress Rule 1 Allows TCP traffic for ports STATELESS () SOURCE TYPE	x all	SOURCE CIDR		IP PROTOCOL (1)	
dd Ingress Rules Ingress Rule 1 Allows TCP traffic for ports STATELESS ()		10.0.128.0/24	.0-10.0.128.255 (256 IP addresses)	IP PROTOCOL ① TCP	can
Add Ingress Rules dd Ingress Rules Ingress Rule 1 Allows TCP traffic for ports STATELESS () SOURCE TYPE CIDR SOURCE PORT RANGE (s: all	10.0.128.0/24	.0-10.0.128.255 (256 IP addresses) DESTINATION PORT RANGE (3)	ТСР	
dd Ingress Rules Ingress Rule 1 Allows TCP traffic for ports STATELESS () SOURCE TYPE CIDR	s: all	10.0.128.0/24		ТСР	
dd Ingress Rules Ingress Rule 1 Allows TCP traffic for ports STATELESS () SOURCE TYPE CIDR SOURCE PORT RANGE (s: all	10.0.128.0/24	DESTINATION PORT RANGE (i)	ТСР	
dd Ingress Rules Ingress Rule 1 Allows TCP traffic for ports STATELESS () SOURCE TYPE CIDR SOURCE PORT RANGE (All	s: all	10.0.128.0/24	DESTINATION PORT RANGE (i)	OPTIONAL TCP	

Data Guard- CLI Options

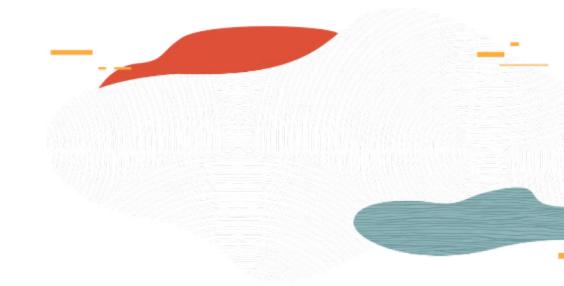
[opc@bmdb ~]\$ sudo /opt/oracle/dcs/bin/dbcli list-dgconfigs







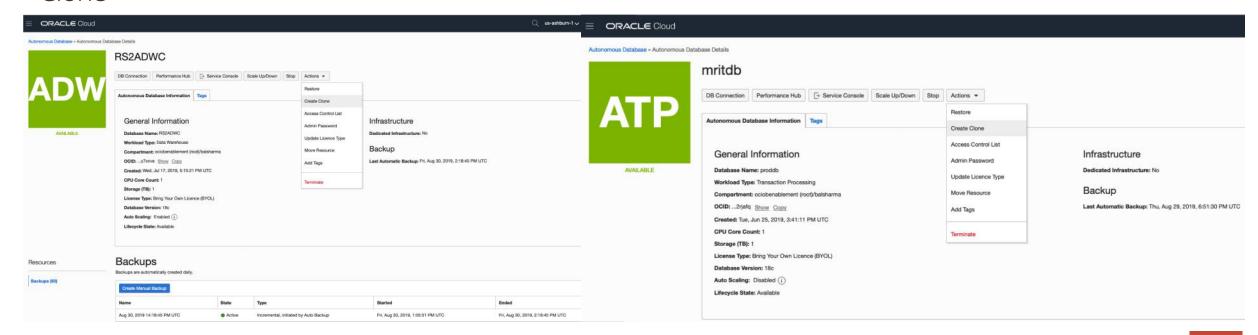
Autonomous Database Cloning





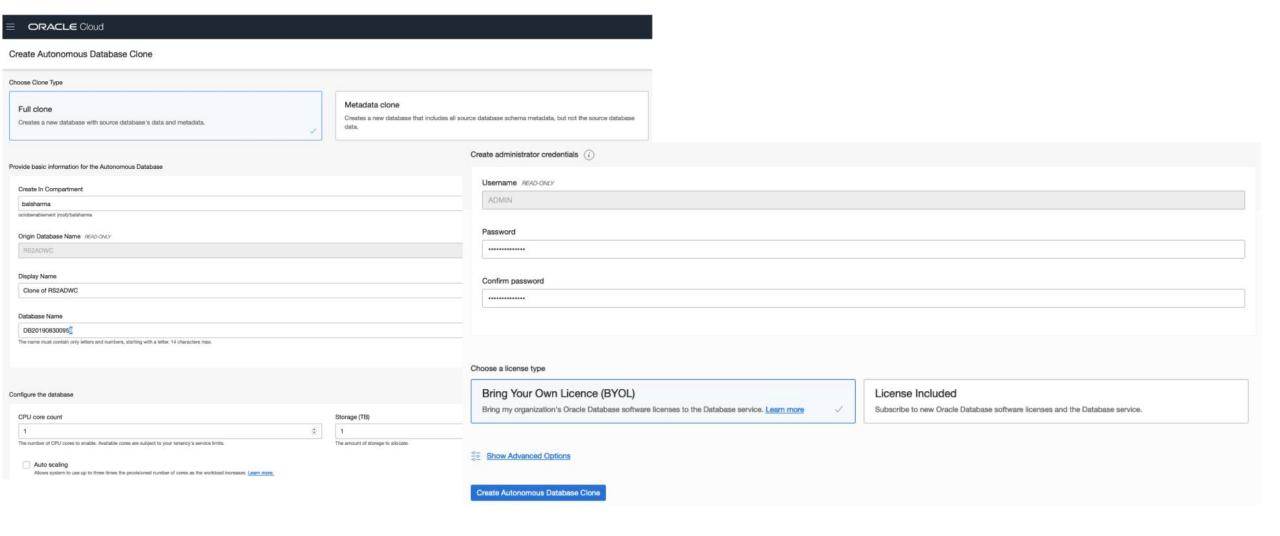
Autonomous Database(ATP/ADW) Cloning

- Cloned databases can we used for multiple purposes such as Testing/development, experimentation, analytics, and others.
- Customers have an ability to quickly create point-in-time copy of a particular autonomous database using OCI Console, API, CLI, SDK, and Terraform.
- Creating clone of an existing ATP/ADW is easy. To clone a database using OCI console, go to OCI
 Console -> Autonomous Transaction Processing OR OCI Console → Autonomous Data Warehouse →
 List of Autonomous Database -> View Details of Selected Autonomous Database -> Actions -> Create
 Clone



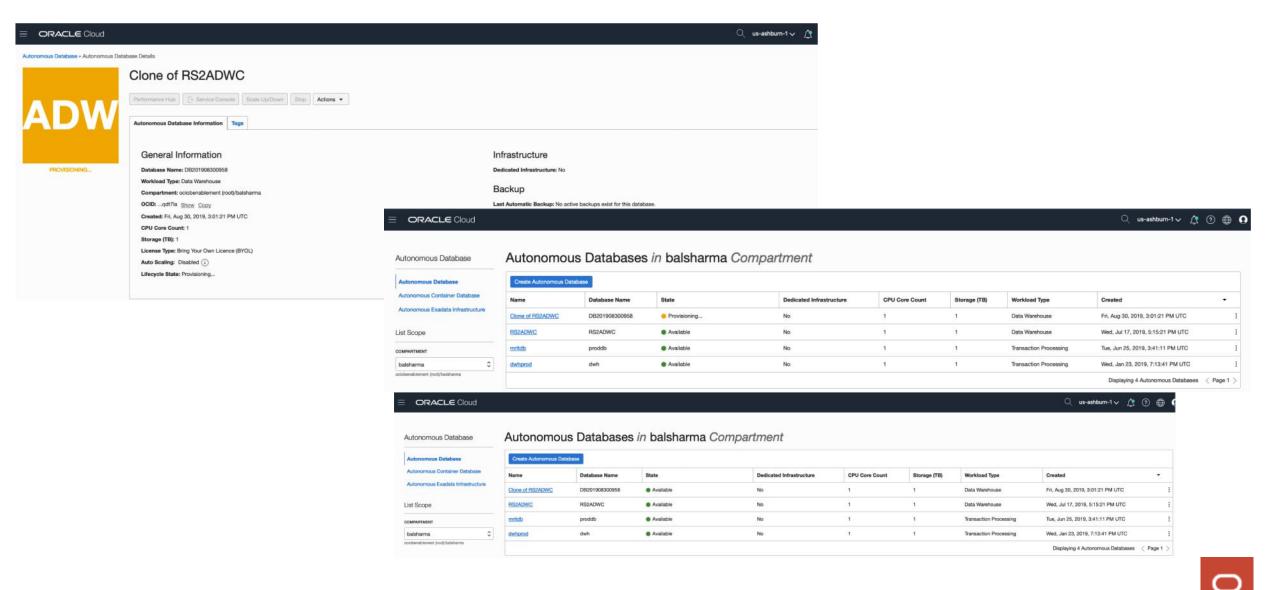


Autonomous Database(ATP/ADW) Cloning Demo





Autonomous Database(ATP/ADW) Cloning Demo Cont.



Summary

After completing this training you should have learnt:

- Database service offers High availability options such as Data Guard, Active Data Guard
- Offers complete lifecycle automation Data Guard creation, Switch Over, Failover, Reinstate
- Manual Data Guard can be created using API/CLI
- Autonomous Database Cloning.

ORACLE

Oracle Cloud always free tier:

oracle.com/cloud/free/

OCI training and certification:

oracle.com/cloud/iaas/training oracle.com/cloud/iaas/training/certification education.oracle.com/oracle-certification-path

OCI hands-on labs:

ocitraining.qloudable.com/provider/oracle

Oracle learning library videos on YouTube:

youtube.com/user/OracleLearning



