DELPHIX

Delphix Engine Quick Start Guide for Oracle on Solaris SPARC

December, 2017

DELPHIX

Delphix Engine Quick Start Guide for Oracle on Solaris SPARC

You can find the most up-to-date technical documentation at:

docs.delphix.com The Delphix Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to: infodev@delphix.com

Delphix Corp.
1400 Seaport Blvd, Suite 200
Redwood City, CA 94063

Quick Start Guide for Oracle on Solaris SPARC

This quick start guide, which is excerpted from the larger User Guide, is intended to provide you with a quick overview of working with Oracle database objects in the Delphix Engine. It does not cover advanced configuration options including Oracle RAC, Linking to Standby, or Best Practices for Performance. It assumes that you are working in a Lab/Dev setting, and attempting to quickly test Delphix functionality. It assumes you will use the VMware Hypervisor.

Overview

In this guide, we will walk through deploying a Delphix Engine, configuring Oracle Source and Target environments on Solaris SPARC servers, creating a dSource, and provisioning a VDB.

The following diagram describes the Delphix topology for Oracle environments. It illustrates the recommended ports to be open from Delphix to remote services, to the Delphix Engine, and to the Source and Target Environments.

For this Quick Start Guide, you can ignore the following components: XPP/Validated Sync Host, Replicated Engine, and Delphix Masking Engine.
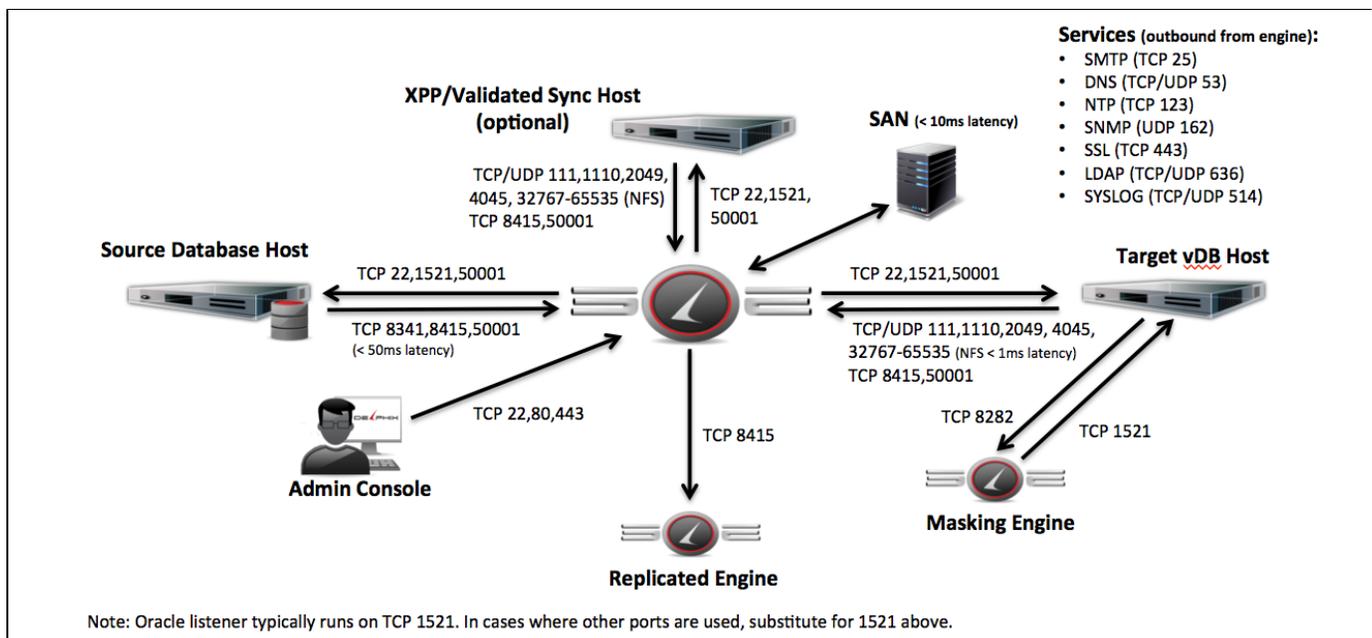
Deploy OVA on VMWare

Use the Delphix-supplied OVA file to install the Delphix Engine. The OVA file is configured with many of the minimum system requirements and deploys to one 300GB hard disk with 8 vCPUs and 64GB RAM. The underlying storage for the install is assumed to be redundant SAN storage.

1. Download the OVA file from **https://download.delphix.com**. You will need a support login from your sales team or a welcome letter.
    a. Navigate to "Virtual Appliance" and download the appropriate OVA. If you unsure, use the **HWv8_**

Standard type.

2. Login using the vSphere client to the vSphere server (or vCenter Server) where you want to install the Delphix Engine.

3. In the vSphere Client, click **File**.

4. Select **Deploy OVA Template**.

5. Browse to the OVA file.

6. Click **Next**.

7. Select a **hostname** for the Delphix Engine.
   This hostname will also be used in configuring the Delphix Engine network.

8. Select the **data center** where the Delphix Engine will be located.

9. Select the **cluster** and the **ESX host**.

10. Select one (1) **data store** for the **Delphix OS**. This datastore can be **thin-provisioned** and must have enough free space to accommodate the 300GB comprising the Delphix operating system.

11. Select four (4) or more **data stores** for Database Storage for the Delphix Engine. The Delphix Engine will stripe all of the Database Storage across these VMDKs, so for optimal I/O performance each VMDK must be equal in size and be configured **Thick Provisioned - Eager Zeroed**. Additionally, these VMDKs should be distributed as evenly as possible across all four SCSI I/O controllers, as described in **KB045 Reconfiguring Controllers**.

12. Select the **virtual network** you want to use.
    If using multiple physical NICs for link aggregation, you must use vSphere NIC teaming. Do not add multiple virtual NICs to the Delphix Engine itself. The Delphix Engine should use a single virtual network. For more information, see **Optimal Network Architecture for the Delphix Engine**.

13. Click **Finish**.
    The installation will begin and the Delphix Engine will be created in the location you specified

> If your source database is 4 TB, you probably need 4 TB of storage for the Delphix Engine. Add at least 4 similarly sized data disks for Delphix VM e.g. for 4 TB create 4 VMDKs of 1 TB each.

> For a full list of requirements and best practice recommendations, see **Virtual Machine Requirements for VMware Platform**.

Setup Network Access to Delphix Engine

1. Power on the Delphix Engine and open the Console.

2. Wait for the Delphix Management Service and Delphix Boot Service to come online.
   This might take up to 10 minutes during the first boot. Wait for the large orange box to turn green.

3. Press any key to access the sysadmin console.

4. Enter `sysadmin@SYSTEM` for the username and `sysadmin` for the password.

5. You will be presented with a description of available network settings and instructions for editing.

```
Delphix Engine Network Setup

To access the system setup through the browser, the system must first be
configured for networking in your
environment. From here, you can configure the primary interface, DNS,
hostname, and default route. When DHCP is
configured, all other properties are derived from DHCP settings.

To see the current settings, run "get." To change a property, run "set
<property>=<value>." To commit your changes,
run "commit." To exit this setup and return to the standard CLI, run
"discard."

    defaultRoute    IP address of the gateway for the default route --
for example, "1.2.3.4."

    dhcp            Boolean value indicating whether DHCP should be used
for the primary interface. Setting this value
                    to "true" will cause all other properties (address,
hostname, and DNS) to be derived from the DHCP
                    response

    dnsDomain       DNS Domain -- for example, "delphix.com"

    dnsServers      DNS server(s) as a list of IP addresses -- for
example, "1.2.3.4,5.6.7.8."

    hostname        Canonical system hostname, used in alert and other
logs -- for example, "myserver"

    primaryAddress  Static address for the primary interface in CIDR
notation -- for example, "1.2.3.4/22"

Current settings:

    defaultRoute: 192.168.1.1
    dhcp: false
    dnsDomain: example.com
    dnsServers: 192.168.1.1
    hostname: Delphix
    primaryAddress: 192.168.1.100/24
```

6. Configure the `hostname`. If you are using DHCP, you can skip this step.

```
delphix network setup update *> set hostname=<hostname>
```

Use the same `hostname` you entered during the server installation.

7. Configure DNS. If you are using DHCP, you can skip this step.

```
delphix network setup update *> set dnsDomain=<domain>
delphix network setup update *> set
dnsServers=<server1-ip>[,<server2-ip>,...]
```

8. Configure either a static or DHCP address.

<table>
<tr><td>DHCP Configuration</td></tr>
<tr><td><code>delphix network setup update *> set dhcp=true</code></td></tr>
</table>

<table>
<tr><td>Static Configuration</td></tr>
<tr><td><code>delphix network setup update *> set dhcp=false</code>
<code>delphix network setup update *> set</code>
<code>primaryAddress=<address>/<prefix-len></code></td></tr>
</table>

> The static IP address must be specified in CIDR notation (for example, `192.168.1.2/24`)

9. Configure a default gateway. If you are using DHCP, you can skip this step.

```
delphix network setup update *> set defaultRoute=<gateway-ip>
```

10. Commit your changes. Note that you can use the `get` command prior to committing to verify your desired configuration.

```
delphix network setup update *> commit
Successfully committed network settings. Further setup can be done
through the browser at:

        http://<address>

Type "exit" to disconnect, or any other commands to continue using the
CLI.
```

11. Check that you can now access the Delphix Engine through a Web browser by navigating to the displayed IP address, or hostname if using DNS.

12. Exit setup.

```
delphix> exit
```

Setting Up the Delphix Engine

Once you setup the network access for Delphix Engine, enter Delphix Engine URL in your browser for server setup.

The welcome screen below will appear for you to begin your Delphix Engine setup.
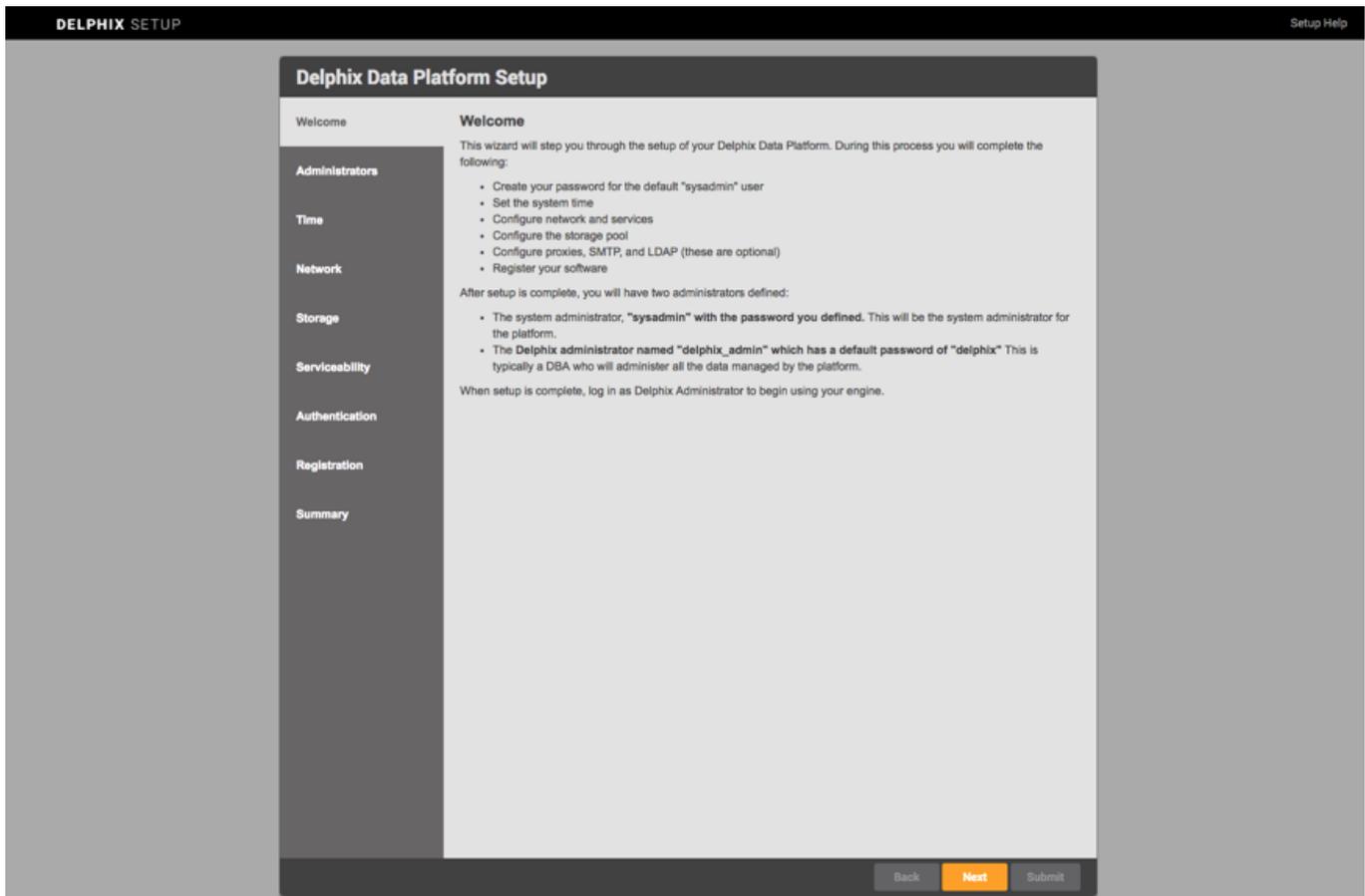
Delphix Engine Setup Screen

The setup procedure uses a wizard process to take you through eight configuration screens:

- Administrators
- System Time
- Network
- Storage
- Serviceability
- Authentication
- Registration
- Summary

1. Connect to the Delphix Engine at `http://`**`<Delphix Engine>`**`/login/index.html#serverSetup`
.
The **Delphix Setup** application will launch when you connect to the server.
Enter your **sysadmin** login credentials, which initially defaults to the username **sysadmin**, with the initial default password of **sysadmin**. On first login, you will be prompted to change the initial default password.
2. Click **Next**.

Administrators

The Delphix Engine supports two types of administrators:

- System administrator (**sysadmin**) - this is the engine system administrator. The sysadmin password is defined here**.**
- Delphix Administrator (**delphix_admin)** - this is typically a DBA who will administer all the data managed by the engine.

On the Administrators tab you set up the sysadmin password by entering an email address and password. The details for the delphix_admin are displayed for reference.

System Time

Choose your option to setup system time in this section.

For a Quick Start, simply set the time and your timezone. You can change this later.

Network

The initial out-of-the-box network configuration in the OVA file is set to use a single VMXNET3 network adapter.

You've already configured this in the initial configuration. Delphix supports more advanced configurations, but you can enable those later.

Storage

You should see the data storage VMDKs or RDMs you created during the OVA installation. Click Next to configure these for data storage.

Serviceability

Choose your options to configure serviceability settings.

For a Quick Start, take the defaults. You can change this later.

Authentication

Choose your options to configure authentication services.

For a Quick Start, take the defaults.You can change this later.

Registration

If the Delphix Engine has access to the external Internet (either directly or through a web proxy), then you can auto-register the Delphix Engine:

1. Enter your **Support Username** and **Support Password**.
2. Click **Register**.

If external connectivity is not immediately available, you must perform manual registration.

1. Copy the **Delphix Engine registration code** in one of two ways:
    a. Manually highlight the registration code and copy it to clipboard. Or,
    b. Click **Copy Registration Code to Clipboard**.
2. Transfer the Delphix Engine's registration code to a workstation with access to the external network Internet. For example, you could e-mail the registration code to an externally accessible e-mail account.
3. On a machine with access to the external Internet, please use your browser to navigate to the Delphix Registration Portal at **http://register.delphix.com**.
4. Login with your Delphix support credentials (username and password).
5. Paste the **Registration Code**.
6. Click **Register**.

> While your Delphix Engine will work without registration, we strongly recommend that you register each Delphix Engine as part of setup. Failing to register the Delphix Engine will impact its supportability and security in future versions.

Summary

The final summary tab will enable you to review your configurations for System Time, Network, Storage, Serviceability, and Authentication.

1. Click the **Back** button to go back and to change the configuration for any of these server settings.
2. If you are ready to proceed, then click **Submit**.
3. Click **Yes** to confirm that you want to save the configuration.
4. Click **Setup** to acknowledge the successful configuration.
5. There will be a wait of several minutes as the Delphix Engine completes configuration.

Source Host Requirements

1. Create an operating system user (**delphix_os**). This user is easily created by the **createDelphixOSUser.sh** script.

    a. Profile and privileges should be the same as the Oracle user (i.e. **oracle**) on the host. For example, **delphix_os** should have the same environment variable settings ($PATH, $ORACLE_HOME, etc.), umask, and ulimit settings, as **oracle**.

    > Shortcut: Source the **oracle** login script from the **delphix_os** login script.

b. Group memberships:

    i. The primary OS group of the Delphix Engine software owner account's (i.e. **delphix_os**) should be the same as the Oracle software owner account (i.e. **oracle**). In most cases, this is an OS group named **oinstall**. There are lots of cases where the OS group named **dba** fils ls this role, so be sure to check the group membership of the Oracle software owner account.

> **Oracle Inventory OS group**
> The explanation of which OS group is primary on all Oracle software owner accounts is documented in the "Oracle12c Database Installation Guide" in the chapter on "**Configuring Users, Groups, and Environments for Oracle Database**", which states explicitly that the OS group for the Oracle Inventory **oinsta ll** should be primary. However, please be aware that not all Oracle installations necessarily follow these guidelines.

The reason Delphix Engine software owner account (i.e. **delphix_os**) must have membership in the same OS groups as the Oracle software owner (i.e. **oracle**), specifically in the OSDBA group, is so that the engine can execute the Oracle RMAN executable, which to do so requires connection to the database instance as SYSDBA.

OS accounts belonging to the OSDBA group can employ "OS authentication" when connecting to an Oracle database instance by specifying either username nor password (i.e. **rman target /**), thus eliminating the need to store or retrieve a SYSDBA password.

> **Oracle 12c**
> For Oracle 12c and later versions of Oracle databases which provide better role separation, the **delphix_os** user can also use OSBACKUPDBA as its primary group. This is typically the **backupdba** group on the host. For more information, please refer to the "Oracle12c Database Installation Guide" in the chapter sub-section on "**Extended Oracle Database Groups for Job Role Separation**".

    ii. If the Oracle OSDBA group (typically **dba**) is not already the primary OS group of the Delphix software owner account (i.e. **delphix_os**), then it must be set as a secondary group.

    iii. If the Oracle ASM ownership groups (typically **asmadmin** and **asmdba**) exist on the host, they should be assigned to the Delphix Engine software owner account (i.e. **delphix_os**) as secondary groups.

> **Summary**
> An excellent "rule of thumb" to follow is that the setup of OS groups for the Delphix Engine software owner account (i.e. **delphix_os**) should be the same as for the Oracle software owner account (i.e. **oracle**).

2. There must be a directory on the source host where the Delphix Engine Toolkit can be installed, for

example: /var/opt/delphix/Toolkit.

    a. The **delphix_os** user and primary OS group (i.e. **oinstall**) must own the directory.

    b. The directory must have permissions -rwxrwx--- (0770), but you can also use more permissive settings.

    c. The directory should have 1.5GB of available storage: 400MB for the toolkit and 400MB for the set of logs generated by each client that runs out of the toolkit.

3. The Delphix Engine must be able to make an SSH connection to the source host (typically port 22).

On a Solaris host, **gtar** must be installed. Delphix uses `gtar` to handle long file names when extracting the toolkit files into the toolkit directory on a Solaris host. The `gtar` binary should be installed in one of the following directories:

- /**bin:/usr**
- /**bin:/sbin:/usr**
- /**sbin:/usr/contrib**
- /**bin:/usr/sfw**
- /**bin:/opt/sfw**
- /**bin:/opt/csw/bin**

Sudo access to `pargs` on the Solaris operating system is required for the detection of listeners with non-standard configurations on both source and target environments. Super-user access level is needed to determine the `TNS_ADMIN` environment variable of the user running the listener (typically **oracle**, the installation owner). From `TNS_ADMIN`, the Delphix OS user **delphix_os** can derive connection parameters.

Example: Solaris /etc/sudoers entries for a Delphix Source

```
Defaults:delphix_os !requiretty
delphix_os ALL=NOPASSWD:/usr/bin/pargs
```

On a Solaris target, `sudo` access to `mount` and `umount` is also required.

Example: Solaris /etc/sudoers entries for a Delphix Target

```
# Delphix issues sudo -l so we need to allow it via listpw. Never set it to
always when using public key authentication
Defaults      listpw=all

User_Alias DELPHIX_USER=delphix_os

Cmnd_Alias DELPHIX_CMDS= \
/usr/sbin/mount, \
/usr/sbin/umount, \
/usr/bin/pargs

DELPHIX_USER ALL=(ALL) NOPASSWD: DELPHIX_CMDS
```

Source Database Requirements

1. Source databases must be in **ARCHIVELOG** mode to ensure that redo logs are archived. **(Mandatory).** Archive logs are required to make SnapSyncs consistent and provisionable.

2. There must be a database user (**delphix_db**) created by the **createDelphixDBUser.sh** script. This script is part of the HostChecker bundle, and grants **SELECT** privileges on specific system tables for the user. See the topics **Using HostChecker to Validate Oracle Source and Target Environments** for more about using the HostChecker bundle.

   > **Oracle pluggable databases**
   >
   > For an Oracle pluggable database, there must be one database user (**delphix_db**) for the pluggable database and one common database user (**c##delphix_db**) for its container database. The **createDelphixDBUser.sh** script can create both users.

3. Enable **Block Change Tracking (BCT)**. **(Highly Recommended)**. Without BCT, incremental SnapSyncs must scan the entire database.

   > BCT is an Enterprise Edition feature.

   > **Patch Required**
   >
   > In order to use BCT in versions 10.2.0.5 and 11.2.0.2 (even for primary databases) Oracle installation should have patch for Oracle Bug 10170431. Without this fix BCT might use too much CPU. See MOS 10170431.8
   >
   > If an Oracle installation has already been patched or once the patch is applied, use the CLI to update the repository for this installation so that appliedPatches includes Oracle bug number 10170431, this will let SnapSync know that the bug has been fixed. If the repository does not indicate that Oracle bug 10170431 has been addressed, SnapSync will show a warning about this bug for each SnapSync.
   >
   > See **Updating repository for Oracle applied patches with the Command Line Interface**

   > See **Linking Oracle Physical Standby Databases** for restrictions on enabling BCT on Oracle Physical Standby databases.

   Enter this command to enable BCT:

   ```
   alter database enable block change tracking using file '<user specified
   file>';
   ```

   The "*USING FILE user_specified_file*" clause defines the location of the change tracking file on the OS. This can be omitted by enabling OMF (Oracle-Managed Files).

4. Enable **FORCE LOGGING**. **(Highly Recommended)**. This prevents **NOLOGGING** operations on

Source Databases. Oracle requires FORCE LOGGING for proper management of standby databases.

Enter this command to enable FORCE LOGGING:

```
SQL> ALTER DATABASE force logging;
```

> If you do not enable FORCE LOGGING and NOLOGGING operations take place, you will get a Fault from the Delphix Engine. If you must use NOLOGGING to meet specific performance criteria, take a new snapshot of the source database after doing the NOLOGGING operations to bring the dSource up-to-date before provisioning VDBs. To avoid repeated Faults, you can disable "Diagnose Nologging" on your dSource.

5. If the online redo log files are located on RAW or ASM devices, then the Delphix Engine LogSync feature can operate in **Archive Only** mode only. See the topics **Advanced Data Management Settings for Oracle dSources** and **Linking Oracle Physical Standby Databases** for more information.

Target Host Requirements

1. Create an operating system user (**delphix_os**). This user is easily created by the **createDelphixOSUser.sh** script.

    a. Profile and privileges should be the same as the Oracle user (i.e. **oracle**) on the host. For example, **delphix_os** should have the same environment variable settings ($PATH, $ORACLE_HOME, etc.), umask, and ulimit settings, as **oracle**.

    > Shortcut: Source the **oracle** login script from the **delphix_os** login script.

    b. Group memberships:
        i. The primary OS group of the Delphix Engine software owner's account (i.e. **delphix_os**) should be the same as the Oracle software owner's account (i.e. **oracle**). In most cases, this is an OS group named **oinstall**. There are lots of cases where the OS group named **dba** fills this role, so be sure to check the group membership of the Oracle software owner account.

        > **Oracle Inventory OS group**
        > The explanation of which OS group is primary on all Oracle software owner accounts is documented in the "Oracle12c Database Installation Guide" in the chapter on "**Configuring Users, Groups, and Environments for Oracle Database**", which states explicitly that the OS group for the Oracle Inventory **oinstall** should be primary. However, please be aware that not all Oracle installations necessarily follow these guidelines.

        The reason Delphix Engine software owner account (i.e. **delphix_os**) must have membership in the same OS groups as the Oracle software owner (i.e. **oracle**), specifically in the OSDBA group, is so that Delphix can execute the Oracle RMAN executable, which to

do so requires connection to the database instance as SYSDBA.

OS accounts belonging to the OSDBA group can employ "OS authentication" when connecting to an Oracle database instance by specifying either username nor password (i.e. **rman target /**), thus eliminating the need to store or retrieve a SYSDBA password.

> **Oracle 12c**
> For Oracle 12c and later versions of Oracle databases which provide better role separation, the **delphix_os** user can also use OSBACKUPDBA as its primary group. This is typically the **backupdba** group on the host. For more information, please refer to the "Oracle12c Database Installation Guide" in the chapter sub-section on "**Extended Oracle Database Groups for Job Role Separation**".

    ii. If the Oracle OSDBA group (typically **dba**) is not already the primary OS group of the Delphix software owner account (i.e. **delphix_os**), then it must be set as a secondary group.

    iii. If the Oracle ASM ownership groups (typically **asmadmin** and **asmdba**) exist on the host, they should be assigned to the Delphix Engine software owner account (i.e. **delphix_os**) as secondary groups.

> **Summary**
> An excellent "rule of thumb" to follow is that the setup of OS groups for the Delphix Engine software owner account (i.e. **delphix_os**) should be the same as for the Oracle software owner account (i.e. **oracle**).

2. There must be a directory on the target host where the Delphix Engine Toolkit can be installed, for example: /var/opt/delphix/Toolkit.
   a. The **delphix_os** user and primary OS group (i.e. **oinstall** or **dba**) must own the directory.
   b. The directory must have permissions -rwxrwx--- (0770), but you can also use more permissive settings.
   c. The directory should have 1.5GB of available storage: 400MB for the toolkit and 400MB for the set of logs generated by each client that runs out of the toolkit.

3. There must be a directory (e.g. "/delphix" or "/mnt/provision/") that will be used as a container for the NFS mount points that are created when provisioning a VDB to the target host.
   a. The **delphix_os** user and primary OS group (i.e. **oinstall** or **dba**) must own the directory.
   b. The directory must have permissions -rwxrwx--- (0770), but you can also use more permissive settings.
   c. There is no requirement for space in this directory, because NFS mount points take up no space
   d. There must be no symbolic links in the path of this directory, because NFS can mount into a directory with symlinks in it's path, but cannot unmount.
   e. It is permissible to use the Delphix Engine Toolkit directory (*see above*) for this purpose, as that mandatory directory already has the proper permissions and ownership.

4. The following permissions are usually granted via sudo authorization of the commands. See **Sudo Privilege Requirements for Oracle Environments** for further explanation of the commands, and **Sudo File Configuration Examples for Oracle Environments** for examples of the /etc/sudoers file on different operating systems.

    a. Permission to run `mount, umount, mkdir, rmdir` as super-user.

    b. Permission to run `pargs` on Solaris hosts and `ps` on AIX, HP-UX, Linux hosts, as super-user.

    c. If the target host is an AIX system, permission to run the `nfso` command as super-user.

5. Write permission to the `$ORACLE_HOME/dbs` directory (i.e. chmod g+w $ORACLE_HOME/dbs)

6. An Oracle listener process should be running on the target host. The listener's version should be equal to or greater than the highest Oracle version that will be used to provision a VDB.

7. As the Delphix Engine uses NFSv3 for mounting target host filesystems, the prerequisite packages to support NFSv3 client communication are required for normal operation, and the required services to support NFS client communications (including file locking) must be running. This includes

    i. portmapper / rpcbind

    ii. status daemon (rpc.statd)

    iii. NFS lock manager (rpc.lockd/lockmgr)

8. The Delphix Engine must be able to make an SSH connection to the target host (typically port 22).

On a Solaris host, **gtar** must be installed. Delphix uses `gtar` to handle long file names when extracting the toolkit files into the toolkit directory on a Solaris host. The `gtar` binary should be installed in one of the following directories:

- /**bin:/usr**
- /**bin:/sbin:/usr**
- /**sbin:/usr/contrib**
- /**bin:/usr/sfw**
- /**bin:/opt/sfw**
- /**bin:/opt/csw/bin**

Deploy Hostchecker to Validate Delphix Requirements

1. Download the appropriate **HostChecker tarball** for your engine from **https://download.delphix.com/**. T arballs follow the naming convention "hostchecker_<OS>_<processor>.tar". For example, if you are validating a linux x86 host you should download the hostchecker_linux_x86.tar tarball.

2. Create a working directory and extract the **HostChecker files** from the **HostChecker tarball**.

    ```
    mkdir dlpx-host-checker
    cd dlpx-host-checker/
    tar -xf hostchecker_linux_x86.tar
    ```

3. Run the `sh` script contained within:

```
sh hostchecker.sh
```

This will extract the JDK included in the tarball (if necessary) and invoke the HostChecker.

```
ora10205@bbdhcp:/home/ora10205/hostchecker-> sh hostchecker.sh
Extracting the JDK from the tarball jdk-6u45-linux-i586.tar.gz.
```

> **Don't Run as Root**
> Do not run the HostChecker as root; this will cause misleading or incorrect results from many of
> the checks.

4. Select which **checks** you want to run.

> **Run Tests without the Interface**
> You can also run checks without spawning the interface. Enter `--help` to get a list of arguments
> you can pass to the HostChecker.

5. As the checks are made, enter the requested **arguments**.

6. Read the output of the check.
   The general format is that severity increases as you scroll down the output. First comes informational
   output, then warnings, then errors.

> **Internal Errors**
> If you see a message that starts with `Internal Error`, forward it to Delphix Support
> immediately. This represents a potential bug in the HostChecker, and not necessarily a problem
> with your environment.

7. Error or warning messages will explain any possible problems and how to address them. Resolve the
   issues that the HostChecker describes. Do not be surprised or undo your work if more errors appear the
   next time you run HostChecker, because the error you just fixed may have been masking other
   problems.

8. Repeat steps 3 - 7 until all the checks return no errors or warnings.

Adding Oracle Source and Target Environments

Follow the steps below to add **both** source and target environments for oracle.

1. Login to the **Delphix Management** application using the **Delphix Admin** credentials.

2. Click **Manage**.

3. Select **Environments**.

4. Click the **Plus** icon next to **Environments**.

5. In the **Add Environment** dialog, select **Unix/Linux**.

6. Select **Standalone Host** or **Oracle Cluster**, depending on the type of environment you are adding.

7. For standalone Oracle environments enter the **Host IP** address.

8. For Oracle RAC environments, enter the **Node Address** and **Cluster Home.**

9. Enter an optional **Name** for the environment.

10. Enter the **SSH** port.
    The default value is **22**.

11. Enter a **Username** for the environment.
    See **Requirements for Oracle Target Hosts and Databases** for more information on the required privileges for the environment user.

12. Select a **Login Type**.
    For **Password**, enter the password associated with the user in Step 10.

> **Using Public Key Authentication**
> If you want to use public key encryption for logging into your Unix-based environment:
>
> a. Select **Public Key** for the **Login Type.**
>
> b. Click **View Public Key**.
>
> c. Copy the public key that is displayed, and append it to the end of your `~/.ssh/authori zed_keys` file. If this file does not exist, you will need to create it.
>   i. Run `chmod 600 authorized_keys` to enable read and write privileges for your user.
>   ii. Run `chmod 755 ~` to make your home directory writable only by your user.
>
> The public key needs to be added only once per user and per environment.
>
> You can also add public key authentication to an environment user's profile by using the command line interface, as explained in the topic **CLI Cookbook: Setting Up SSH Key Authentication for UNIX Environment Users**.

13. For **Password Login**, click **Verify Credentials** to test the username and password.

14. Enter a **Toolkit Path**.
    The toolkit directory stores scripts used for Delphix Engine operations, and should have a persistent working directory rather than a temporary one. The toolkit directory will have a separate sub-directory for each database instance. The toolkit path must have 0770 permissions and at least 345MB of free space.

15. Click **Submit**.

Linking an Oracle Data Source

1. Login to the **Delphix Management** application using the **Delphix Admin** credentials.

2. Click **Manage**.

3. Select **Datasets**.

4. Click the **plus** icon.

5. Select **Add dSource**.

6. In the **Add dSource** wizard, select the source database.

> **Changing the Environment User**
> If you need to change or add an environment user for the source database, see **Managing Oracle Environment Users**.

7. Enter your login credentials for the source database and click **Verify Credentials**.
   If you are linking a mounted standby, Click **Next**. See the topics under **Linking Oracle Physical Standby Databases** for more information about how the Delphix Engine uses non-SYS login credentials.

8. Enter an name for your dSource.

9. Select a **Database Group** for the dSource.

10. Click **Next**.
    Adding a dSource to a database group lets you set Delphix Domain user permissions for that database and its objects, such as snapshots. See the topics under **Users, Permissions, and Policies** for more information.

11. In **Add dSource/Add Environment wizard**, you can set the **Toolkit Path** to /tmp (or any unused directory).

12. Select an **Initial Load** option.
    By default, the initial load takes place upon completion of the linking process. Alternatively, you can set the initial load to take place according to the SnapSync policy, for example if you want the initial load to take place when the source database is not in use, or after a set of operations have taken place.

13. Select a **SnapSync** policy.
    For more information, see **Advanced Data Management Settings for Oracle dSources**.

14. Click **Next**.

15. Review the **dSource Configuration** and **Data Management** information, and then click **Submit**.
    The Delphix Engine will initiate two jobs, **DB_Link** and **DB_Sync,** to create the dSource. You can monitor these jobs by clicking **Active Jobs** in the top menu bar, or by selecting **System > Event Viewer**. When the jobs have successfully completed, the database icon will change to a dSource icon on the **Environments > Databases** screen, and the dSource will be added to the list of **Datasets** under its assigned group.

> After you have created a dSource, you can view information about it on the dSource's **Configuration** tab, where you can also modify its policies and permissions. The **Configuration** tab provides information such as the **Source Database** and **Data Management** configuration. For more information, see **Advanced Data Management Settings for Oracle dSources**.

Provisioning an Oracle VDB

1. Login to the **Delphix Management** application.

2. Select **Manage > Datasets**.

3. In the **Datasets** panel on the left-hand side, click the **group** containing the dSource or VDB from which you want to provision.

4. Click the **TimeFlow** tab.

5. Select a **snapshot**.
   For more information on provisioning options, see **Provisioning by Snapshot and LogSync** in this topic.

   > You can take a snapshot of the dSource from which to provision. To do so, click the **Camera** icon.

6. **Optional:** Select

   📄

   to open LogSync timeline.
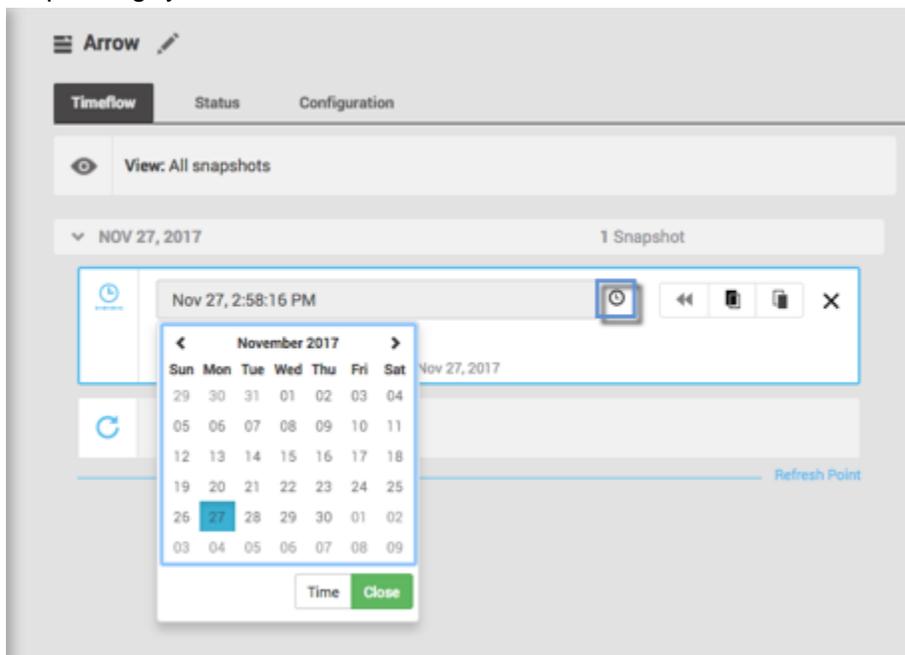
7. Select

   🕐

   to provision from a point of time within a snapshot. You can select by date or time.

8. Click

   📄

   and the **Provision VDB** wizard will open:
   a. For **Oracle Single Instance** the fields **Installation Home**, **Database Unique Name**, **SID**, **Database Name**, **Mount Base**, and **Environment User** will auto-populate with information from the parent.

   b. For **Oracle RAC** the fields **Installation Home**, **Database Unique Name**, **SID**, **Database Name**, **Mount Base**, **Instance Number, Instance Name** and **Environment User** will auto-populate with information from the parent.

> **Editable Fields in the VDB Provision Wizard**
> The following fields are editable:
>
> Installation Home (need to have an additional compatible target)
>
> Database Unique Name
>
> SID
>
> Database Name
>
> Mount Base
>
> Instance Number (RAC Only)
>
> Instance Name (RAC Only)

9. If you need to add a new target environment for the VDB, click the green **Plus** icon next to the **Filter Target** field, and follow the instructions in **Adding an Oracle Single Instance or RAC Environment**.

10. Review the information for **Installation Home**, **Database Unique Name**, **SID**, and **Database Name**. Edit as necessary.

11. Review the **Mount Base** and **Environment User**. Edit as necessary.
    The Environment User must have permissions to write to the specified Mount Base, as described in **Requirements for Oracle Target Hosts and Databases**. You may also want to create a new writeable directory in the target environment with the correct permissions and use that as the Mount Base for the VDB.

12. Select **Provide Privileged Credentials** if you want to use login credentials on the target environment that are different from those associated with the **Environment User**.

13. Click **Advanced** to customize the VDB online log size and log groups, archivelog mode, local_listener parameter (TCP/IPC protocol addresses), additional VDB configuration settings or file mappings, or custom environment variables.
    For more information, see **Customizing Oracle VDB Configuration Settings**, **Customizing VDB File Mappings**, and **Customizing Oracle VDB Environment Variables**.

> If you are provisioning to a target environment that is running a Linux OS, you will need to compare the `SGA_TARGET` configuration parameter with the shared memory size in `/dev/shm`. The shared memory configured on the target host should match the SGA memory target. You can check this by opening the **Advanced** settings, and then finding the value for `SGA_TARGET` under **VDB Configuration Templates**.

14. Click **Next**.

15. Select a **Target Group** for the VDB.

16. Enable Auto VDB Restart to allow the VDB to be automatically restarted when target host reboot is detected by Delphix.

17. Click **Next** .

18. Select a **Snapshot Policy** for the VDB.

19. Click **Next**.

20. Enter any operations that should be run at Hooks during the provisioning process.
    For more information, see **Customizing Oracle Management with Hook Operations**.

21. Click **Next**.

22. Click **Submit**.

When provisioning starts, you can review progress of the job by selecting the VDB and clicking on the **Status** t
ab, or by selecting **Manage/Dashboards** and viewing the **Job History** panel. Alternatively you could see this
in the **Actions Sidebar.** When provisioning is complete, the VDB will be included in the group you designated
and listed in the **Datasets** panel. If you select the VDB in the **Datasets** panel and click the **Configuration** tab
, you can view information about the database and its Data Management settings.

Next Steps

Congratulations! You've provisioned your first virtual database!

You should attempt some simple functional tests with your application. You can connect your app to the VDB
using standard TNS/JDBC techniques. Delphix has already registered the VDB for you on the Target listener.

We suggest the following next steps:

- dropping a table and using the VDB Rewind feature to test recovery of your VDB
- Take a snapshot of your dSource and Refresh your VDB to quickly get fresh production data
- Provision a new VDB from your VDB to test sharing data quickly with other teams
- Mask your new VDB to protect sensitive data. Provision new VDBs from that Masked VDB to quickly
  provide safe data to development and QA teams.