DELPHIX

Delphix Engine Pre-install Guide

January 2019

Delphix Engine Pre-install Guide
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

Installation and Initial System Configuration

These topics describe the initial installation and configuration of the Delphix Engine, the delphix_admin and sysadmin roles, and using the system console.

The admin and sysadmin User Roles

This topic describes the function of the delphix_admin and sysadmin roles.

After installation, the Delphix Engine creates a **sysadmin** user with the initial password `sysadmin` The sysadmin launches the initial **Delphix Setup** configuration application and has access to a command-line system administration console. Through the command line console or the ServerSetup application, the sysadmin can also undertake typical system administration duties such as managing memory, storage, and support logs for the Delphix Engine and performing upgrades and patches.

When the Delphix Management application launches, the Engine admin can log in using the username admin and password delphix.

After initial configuration, the **admin** user manages the Delphix Engine's user data objects: dSources, virtual databases (VDBs), users, groups, and related policies and resources, all collectively referred to as the Delphix Engine **Domain**. The admin user manages the Delphix Engine domain using either the Command Line Interface (CLI) or the browser-based **Delphix Management** application.

Email addresses are required inputs for both the sysadmin and delphix_admin accounts, and you can create additional sysadmin and delphix_admin users as described in the topics under Managing System Administrators.

> The default domain user created on Delphix Engines is now **admin** instead of delphix_admin. When engines created before 5.3.1 are upgraded to 5.3.1 or later they will retain their old username 'delphix_admin'. To avoid complications Delphix recommends creating users with an admin role and then Disabling delphix_admin.

Related Links

- Managing System Administrators

Creating a New admin User

To create a new admin user:

1. Login to the **Delphix Management** application as the default admin user.
2. Select **Manage** > **Users**.
3. Select the **Add user** plus sign located on the top-right corner.
4. In the Add User wizard create a new user with User Type **Engine Administrator**.
5. Click Next.
6. Review your user details and select **Submit**.

Related Links

- Disabling the Default admin User
- CLI Cookbook: Changing the Default admin username
- CLI Cookbook: Disabling an admin User

Disabling the Default admin User

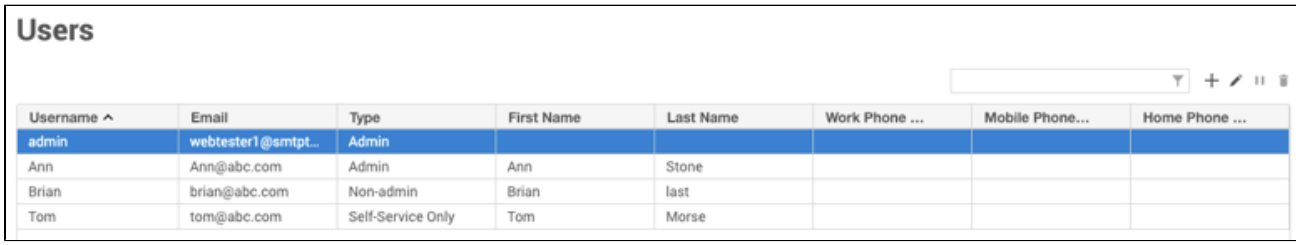
Prerequisites:

- Create a new Delphix admin user
- Login into Your Delphix Engine as the new admin user

Procedure to disable a user

To disable your default admin user (delphix_admin/admin):

1. Login to the **Delphix Management** application as the new admin user.
2. Select **Manage** > **Users**.
3. Select the default **admin** user.
4. Click the **pause** button on located on the top-right corner.



Related Links

- Creating a New admin User
- CLI Cookbook: Changing the Default admin username
- CLI Cookbook: Disabling an admin User

Using HostChecker to Confirm Source and Target Environment Configuration

This topic describes the HostChecker script that is used to check the configuration of source and target environments.

The HostChecker is a standalone program which validates that host machines are configured correctly before the Delphix Engine uses them as data sources and provision targets.

Please note that HostChecker does not communicate changes made to hosts back to the Delphix Engine. If you reconfigure a host, you must refresh the host in the Delphix Engine in order for it to detect your changes.

You can run the tests contained in the HostChecker individually, or all at once. You must run these tests on both the source and target hosts to verify their configurations. As the tests run, you will either see validation messages that the test has completed successfully, or error messages directing you to make changes to the host configuration.

The procedure Delphix administrators need to perform to validate target database servers using Hostchecker can be found at Using HostChecker to Validate Target Database Servers.

Installing the Delphix Engine

This topic describes how to install the Delphix Engine from the OVA file.

Prerequisites

Read the requirement and support information in the Installation and Initial Configuration Requirements topics.

Procedure to Install an OVA

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 are unsure, use the **HWv10 OVA** 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.
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

Procedure to Install an AMI

Use the Delphix-supplied AMI file to install the Delphix Engine.

1. On the Delphix download site, click the AMI you would like to share and accept the Delphix License agreement. Alternatively, follow a link given by your Delphix solutions architect.
2. On the **Amazon Web Services Account Details** form presented:
    a. Enter your **AWS Account Identifier**, which can be found here: https://console.aws.amazon.com/billing/home?#/account. If you want to use the **GovCloud AWS Region**, be sure to enter the ID for the AWS Account which has GovCloud enabled.
    b. Select which **AWS Region** you would like the AMI to be shared in. If you would like the AMI shared in a different region, contact your Delphix account representative to make the proper arrangements.
3. Click **Share.**
   The Delphix Engine will appear in your list of AMIs in AWS momentarily.
4. Reference the Installation and Configuration Requirements for AWS/EC2 when deploying the AMI.

Post-Requisites

After installing the server, follow the procedures in these topics to specify and customize the Delphix Engine network and to make modifications to the memory size, number of CPUs, and the number of disks used for storage.

- Setting Up Network Access to the Delphix Engine
- Customizing the Delphix Engine System Settings

Setting Up Network Access to the Delphix Engine

This topic describes how to configure the Delphix Engine network during initial installation.

Prerequisites

Follow the initial installation instructions in Installing the Delphix Engine.

> **NAT Configuration**
> Delphix communicates it's IP address in application layer data and this cannot be translated by NAT

You can configure a Delphix Engine to use either a dynamic (DHCP) IP address or a static IP address.

Procedure

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.

DHCP Configuration

```
delphix network setup update *> set dhcp=true
```

Static Configuration

```
delphix network setup update *> set dhcp=false
delphix network setup update *> set
primaryAddress=<address>/<prefix-len>
```

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
```

Customizing the Delphix Engine System Settings

This topic describes how to customize the initial system set up requirements for memory, number of CPUs, storage disks, and network configuration.

The OVA file that you use to install the Delphix Engine is configured for the minimum system requirements. You can customize these to match the capabilities of your specific system.

Prerequisites

- Follow the initial installation instructions in Installing the Delphix Engine.

Procedure

1. Shut down the guest operating system and power off the Delphix Engine.
2. Under **Getting Started**, select **Edit Virtual Machine Settings**.
3. You can now customize the system settings.

Setting	Options
Memory Size	Set to 64GB or larger based on sizing analysis. In the **Resource Allocation** panel, ensure that **Reserve all guest memory** is checked.
Number of CPUs	Allocate 8 vCPUs or more based on your Delphix licensing. vCPUs should be fully reserved to ensure that the Delphix Engine d oes not compete for CPU cycles on an overcommitted host.
Supported Controllers	Delphix only supports LSI Parallel controllers.
Disks for Data Storage	Add virtual disks to provide storage for user data such as dSources and VDBs. The underlying storage must be redundant. Add a minimum of 150GB per storage disk. All virtual disks should be the same size and have the same performance characteristics. If using VMFS, use **thick provisioned, lazy zeroed** disks. To alleviate IO bottlenecks at the virtual controller layer, spread the virtual disks across all 4 virtual SCSI controllers.
Data Storage Multipathing Policy	For EMC storage, the multipathing policy should always be set to **round-robin** (default for 5.X). Additionally, change the **IO Operation Limit** from the default of **1000** to **1**. This should be strongly considered for other storage platforms as well. See VMware KB article EMC VMAX and DMX Symmetrix Storage Array Recommendations for Optimal Performance on VMware ESXi/ESX
Network	The network configuration is set to have a VMXNET3 network adapter. VMXNET3 is a tuned network interface that is included with the VMtools provided in the OVA file. It will be assigned to **VM Network** **JUMBO Frames** VMXNET3 supports Ethernet jumbo frames, and you can use this to maximize throughput and minimize CPU utilization. **Adding Link Aggregation via VMware NIC Teaming** To increase throughput or for failover, add multiple physical NICs to the vSwitch that is connected to the Delphix Engine. To increase throughput, NIC Teaming must use the **Route Based on IP Hash** protocol for load balancing. See VMware KB article Troubleshooting IP-Hash outbound NIC selection. **Dedicate Physical NICs to the Delphix Engine** For best performance, assign the Delphix Engine to network adapters that are used exclusively by Delphix.

Post-Requisites

- After making any changes to the system settings, power on the Delphix Engine again and proceed with the initial system configuration as described in Setting Up the Delphix Engine.

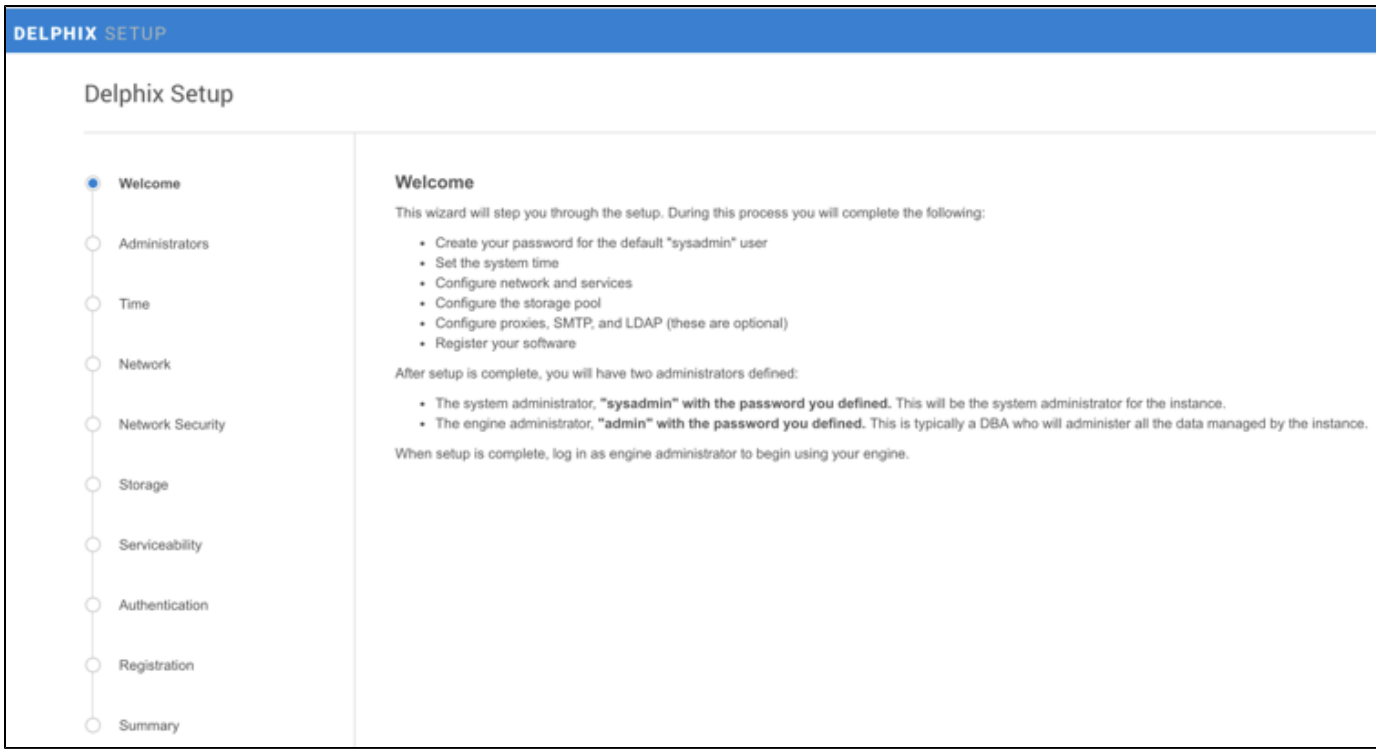
Setting Up the Delphix Engine

This topic describes how to set up the initial system configuration for the Delphix Engine, including system time, storage, web proxy, SMTP server, email to Delphix Support, and LDAP authentication.

Prerequisites

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

Procedure

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

Delphix is installed with two administrator accounts:

- System Administrator - "sysadmin" with a password that users can define (default is sysadmin). This will be the system administrator for the instance.
- Engine Administrator - "admin" with a password that users can define (default is delphix). This is typically a DBA who will administer all the data managed by the instance.

System Time

1. Select an option for maintaining the system time.

Option	Notes
Set NTP Server	After selecting this option, select an NTP server from the list, or click **Add NTP Server** to manually enter a server. Be aware that you can highlight more than one NTP Server entry in order to select more than one. When configuring a Delphix Engine on VMware, be sure to configure the NTP client on the host to use the same servers that you enter here. On a vSphere client, the NTP client is set in the **Security Profile** section of the configuration process.
Manually Select Time and Date	Click **Use Browser Time and Date** to set the system time, or select the date and time by using the calendar and clock displays. Then select the **Time Zone**. If you select **Use Browser Time and Date**, the date and time will persist as your local time, even if you change the time zone. Snapshots from dSources and VDBs reflect the time zone of the source or target environment, not that of the Delphix Engine.

2. Be sure to choose the appropriate **time zone** for the Delphix Server, using the drop-down list in the lower left-hand corner of this page.
3. Click **Next**.

Network Configuration

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

1. Under **Network Interfaces**, click **Settings**.
2. The first Network Interface is **Enabled** by default.
3. Select **DHCP** or **Static** network addressing.
   For **Static** addressing, enter an **IP Address** and **Subnet Mask**.

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

4. Select whether to use **Jumbo Frames**.
   VMXNET3 supports Ethernet jumbo frames, which can be used to maximize throughput and minimize CPU utilization.
5. Click **Save**.
6. Repeat for any other interfaces you have added to the virtual machine (VM) that you wish to configure. They will not be enabled by default.
7. Under **Routing**, enter a **Default Gateway**.
8. Under **DNS Services**, enter a **DNS Domain Name** and **DNS Server**.
9. Click **Next**.

Storage

The Delphix Engine automatically discovers and displays storage devices. For each device, set the **Usage Assignment** to **Data** and set the **Storage Profile** to **Striped**.

You can associate additional storage devices with the Delphix Engine after initial configuration, as described in Adding and Expanding Storage Devices.

> **Storage Disk Usage Assignment Options**
> There are three options for storage disk usage assignment:
>
> **Data**
> Once you set the storage unit assignment for a disk to Data and save the configuration, you cannot change it again.
>
> **Unassigned**
>
> These are disks being held for later use.
>
> **Unused**

These disks can be configured later to add capacity for existing data disks.

The Minimum Number of Storage Disks
Configure at least 4 disks for storage of user data. This makes the Delphix Engine storage manager function more efficiently, since duplicated metadata can be distributed across multiple disks.

Serviceability

1. If a Web Proxy Server is necessary for your environment, select **Use a Web Proxy** and enter the required information.
2. If you want the Delphix Engine to send information to the Delphix Support site periodically over https (SSL), select **Phone Home Service enabled**. This feature requires a connection to the internet and will use the **Web Proxy Server** configuration.

   With the release of the User-click Analytics feature (a lightweight method to capture how users interact with Delphix product user interfaces), Delphix will collect browser-based, user-click analytics data. Essentially, Delphix selectively tracks actions that a user takes in the product UI. Delphix does not collect, transmit or store any personally identifiable information (PII) which for Enterprise customers includes information such as email address, IP address, username, etc. This feature setting matches an Engine's Phone Home Service setting:

   If the Phone Home Service is enabled on an Engine, then this feature will be enabled by default.

   If the Phone Home Service is disabled on an Engine, then this feature will be disabled by default.

   If you want to opt-out please see these CLI instructions - Disabling User-click Analytics. The opt-out is not currently available in the GUI. Please note that we would like to encourage our customers to share this non-PII data with us. Please be aware that the Phone Home Service only sends occasional **support log bundles** *outbound* from the Delphix Engine to Delphix Support website. There is no way to enable *inbound* access to the Delphix Engine.
3. Select **Use an SMTP Server** and enter the required information to enable email notifications for events and alerts.

When a critical fault occurs with the Delphix Engine, it will automatically send an email alert to the **admin** user. Make sure that you configure the SMTP server so that alert emails can be sent to this user. See System Faults for more information.

Authentication Service

To avoid configuration issues, consult with your lightweight directory access protocol (LDAP) administrator before attempting to set up LDAP authentication of users for the Delphix Engine.

1. Select **Use LDAP** to enable LDAP authentication of users.
2. Enter the **LDAP Server** IP address or hostname, and **Port** number.
3. Select the **Authentication** method.
4. Select whether you want to **Protect LDAP traffic with SSL/TLS**.
   If you select this option, you must import the server certificate.
5. When you are done with the LDAP configuration, click **Test Connection**.
6. Click **Next**.

LDAP Authentication When Adding Users
If LDAP has been set up as the authentication service for the Delphix Engine, you must add new users with LDAP as their authentication mechanism. For more information, see Adding Delphix Users and Privileges. Note that you can only add individual LDAP users, not groups.

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.

To regenerate the registration code for a Delphix Engine please refer to, Regenerating the Delphix Engine Registration Code. Delphix strongly recommend that you regenerate this code and re-register the engine regularly to maximize the Support Security of the Delphix Engine. Delphix recommends doing this every six months.

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.

Post-Requisites

- After configuration is complete, the Delphix Engine will restart and launch the browser-based Delphix Management application. The URL for this will be `http://<Delphix Engine>/login/index.html#delphixAdmin`.
- After the Delphix Management application launches, the **delphix_admin** can login using the initial default username **delphix_admin** and the initial default password **delphix**. On first login, you will be prompted to change the initial password.
- You can access the DelphixSetup interface at any time by navigating to `http://<Delphix Engine>/login/index.html#serverSetup` and entering the **sysadmin** credentials.

Related Links

- The admin and sysadmin User Roles
- System Faults
- Adding Delphix Users and Privileges
- Adding and Expanding Storage Devices

Retrieving the Delphix Engine Registration Code

This topic describes how to retrieve the registration code for a Delphix Engine. We strongly recommend that you perform registration as a part of Delphix Engine setup. However, you can also retrieve the registration code for a Delphix Engine after setup.

Procedure

1. You can retrieve the Delphix Engine Registration Code through the **Delphix Setup** application after logging in with the **sysadmin** credentials.
2. In the **Registration** panel, click **View**.
3. The **Registration Code** is displayed in the bottom half of the **Registration** window.
4. If your local machine is connected to the external Internet, you can auto-register the Delphix Engine:
    a. Enter your **Support Username** and **Support Password**.
    b. Click **Register**.
5. If external connectivity is not immediately available, you must register manually.
    a. Copy the Delphix Engine registration code by either manually highlighting and copying to clipboard or clicking **Copy Registration Code to Clipboard**.
    b. Transfer the Delphix Engine's registration code to a location with an external network connection. For example, you could e-mail

the registration code to an externally accessible e-mail account.
c. On a machine with external network access, use your browser to navigate to the Delphix Registration Portal at https://register.delphix.com.
d. Login with your support credentials.
e. Paste the **Registration Code**.
f. 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.

Post-Requisites

- Following registration, you will receive an e-mail confirming the registration of your Delphix Engine.

Regenerating the Delphix Engine Registration Code

This topic describes how to regenerate the registration code for a Delphix Engine. Delphix strongly recommends that you regenerate this code and re-register the engine regularly to maximize the Support Security of the Delphix Engine. Delphix recommends doing this every six months.

Motivation

Why does regenerating registration codes increase security? The registration code contains an encrypted key that only Delphix can decrypt. This key is unique for each engine. Delphix uses this key to generate one-time authentication codes that authorized Support personnel can use to log into the engine during support sessions. Like any other keys in cryptographic security, the best practice is to rotate this key regularly.

Procedure

1. Log into the CLI (command-line interface) of the Delphix Engine with the **sysadmin** credentials.
2. Type `/registration/regenerate` and hit **enter**.
3. Type `commit` and hit **enter**. After a few seconds, the new code will be displayed.
4. Re-register the engine with this new code.

> Failing to re-register the Delphix Engine after regenerating the registration code may prevent Support personnel from accessing the engine. In such a case, a support session cannot begin until the engine has been re-registered with the new registration code.

How To Reboot The Delphix Engine

Occasionally, the management stack will hang on the GUI, or routine maintenance will require a reboot of the Delphix Engine. You can do this safely through either the Delphix Setup or CLI. Before performing a reboot, it is important that all your VDBs are shut down and dSources disabled in order to maintain data integrity.

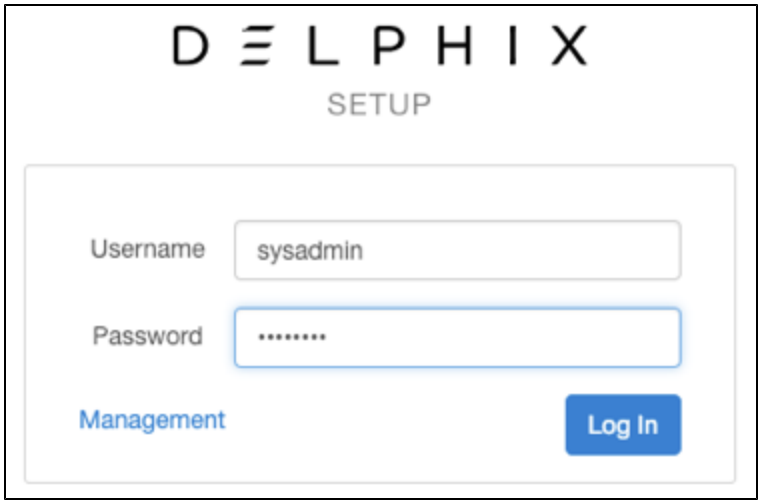
Prerequisites

- Shut down VDBS
- Shut down dSources

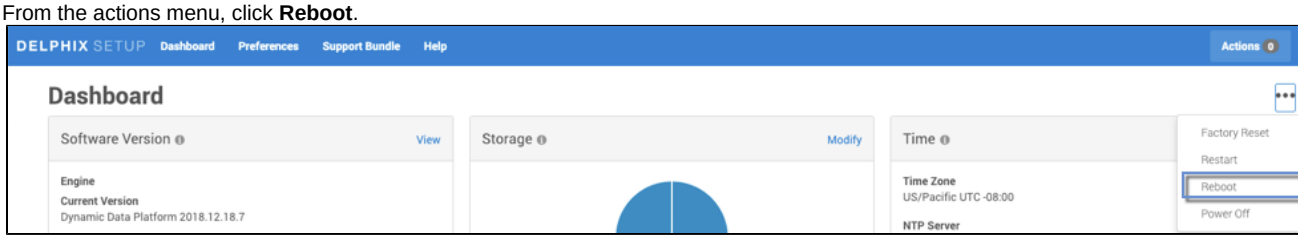
Rebooting the Delphix Engine from the GUI

Complete the following steps to reboot the Delphix Engine via the GUI.

1. Login to the Delphix Setup application using the sysadmin **username** and **password**.



2. From the actions menu, click **Reboot**.



3. Select **OK**.

If you shut down the Delphix Engine, you will have to use your hypervisor console to bring it back up.

Related Links

- CLI Cookbook: Rebooting the Delphix Engine via CLI
- How To Shut Down The Delphix Engine

How To Restart The Delphix Engine Management Process

Occasionally, jobs will hang on the GUI or the Delphix Java management process will be in a bad state. You can restart the management process safely without shutting down VDBs or disabling dSources. Restarting the process has no impact on running VDBs or dSources.

Restarting the Delphix Management Process via CLI

Complete the following steps to restart the Delphix Management Process via the CLI:

1. Login to the CLI using the sysadmin **username** and **password**.

```
ssh sysadmin@yourdelphixengine
```

2. Go to **system > restart**.

```
delphix > system
delphix system > restart
```

3. Commit the action.

```
delphix system restart *> commit
```

Related Links

- How To Shut Down The Delphix Engine

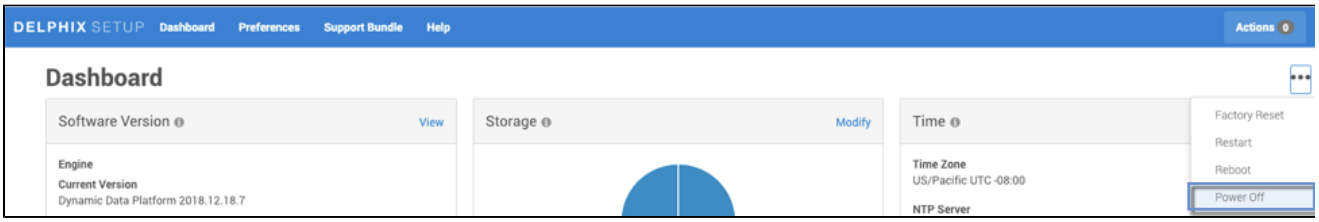
How To Shut Down The Delphix Engine

Occasionally, it is necessary to shut down the Delphix Engine for maintenance purposes. This topic outlines how to perform a safe shutdown of the Delphix Engine. Before performing a shutdown, it is important that all your VDBs are shut down and dSources disabled in order to maintain data integrity. Once the Delphix Engine is powered off, you can power it back on through the vSphere console like any other VM.

Shutting down the Delphix Engine from the GUI

Use the following steps to shut down the Delphix Engine via the GUI.

1. Login to the **Delphix Management application**.
2. Disable all dSources. Perform the following steps for each dSource:
    a. From the **Datasets panel**, select the **dSource** you want to disable.
    b. In the upper right-hand corner, from the **Actions** menu (...) select **Disable.**
    c. In the Disable dialog select **Disable**.
3. Shut down all VDBs. Perform the following for each VDB:
    a. In the **Datasets** panel, click the **VDB** to expand it.
    b. Click the red **stop** button.
3. Logout of the **Management application**.
4. Login to the **Delphix Setup application** using sysadmin credentials.
5. From the Actions menu select **Power Off**.



6. Click **OK**.

Power on the Delphix Engine through ESX Console, like any other VM.

Shutting down the Delphix Engine via CLI

Use the following steps to shutdown the Delphix Engine via CLI.

```
ssh sysadmin@yourengine
delphix > system
delphix system > shutdown
delphix system shutdown *> commit
```

Related Links

- How To Reboot The Delphix Engine

Determining the Delphix Server ID and Host Name

On occasion, it may be necessary to locate the **Delphix Server ID** and **Hostname**.

> The Delphix Engine ID and Delphix Server ID are synonymous. The GUI currently currently uses "Server," and that is the terminology that will be used in this document.

The **Delphix Server ID** uniquely identifies each Delphix Engine. It is a 36-character hexadecimal string of the form **xxxxxxxx-xxxx-xxxx-xxxxxx xxxxxx**. You can view the Delphix Server ID in the Server Setup application, the Delphix Management application, or by using the Command Line Interface (CLI) method.

The **Hostname** is a name you assign. It typically matches the IP (DNS) name assigned to the Delphix Engine. The hostname can only be viewed by using the System Setup application or the CLI method.

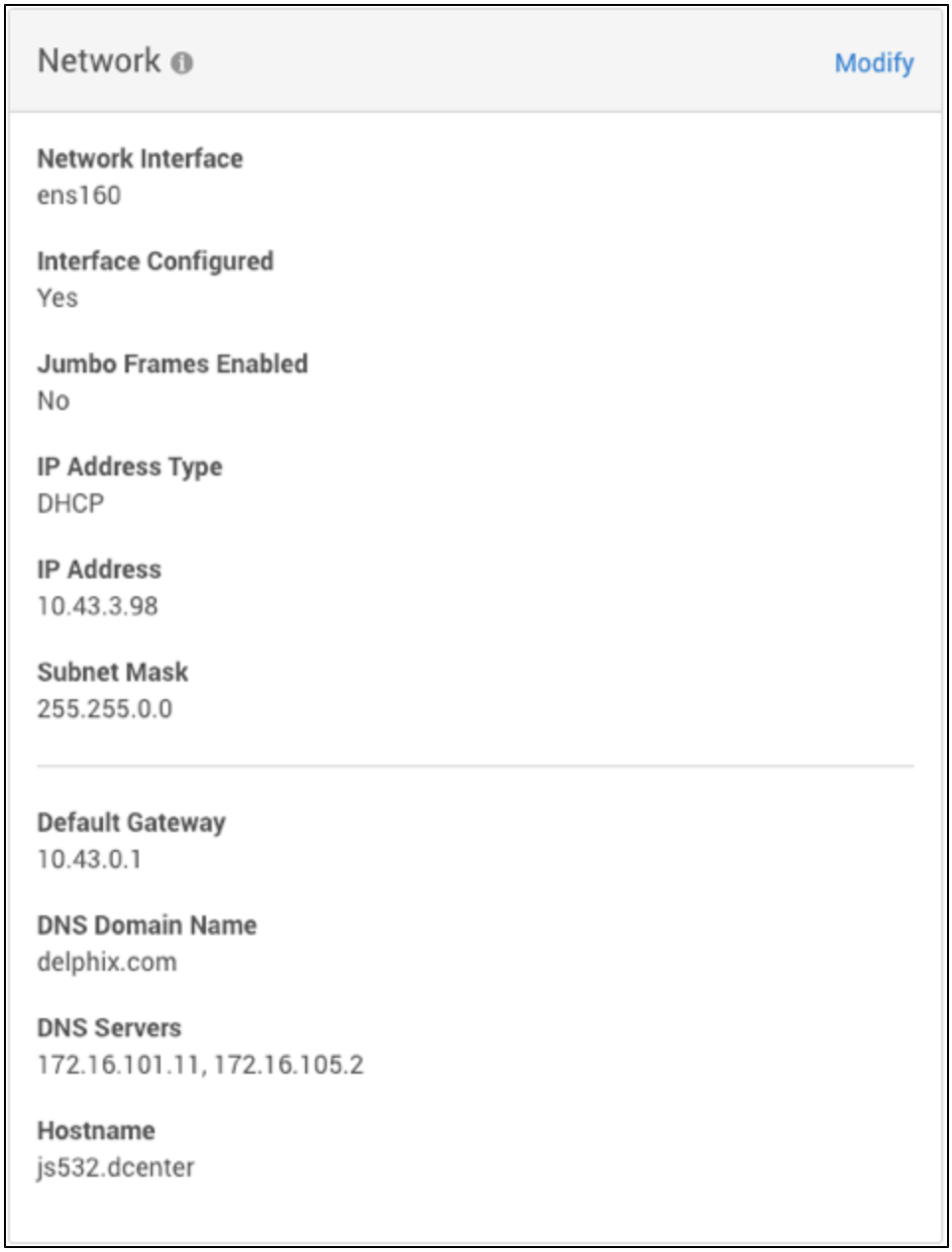
Server Setup Application Method

Login to the Delphix Setup application with sysadmin-level credentials:

1. Access the Delphix Engine through the URL: `http://<Delphix Engine>/ServerSetup.html` where `<DelphixEngine>` is the DNS name or IP address of the Delphix Engine for which you wish to find the Delphix Server ID and hostname.
2. Enter a valid **Username**.
3. Enter a valid **Password**.
4. Click **Log In**.

On the **Dashboard** screen, there is a **System Summary** panel in the lower left portion of the screen**.** The **Server ID** field displays the Delphix Server ID, in this example **564D39A8-5077-C9D0-9EFD-82E848EBDAB6.**

The Delphix Engine Hostname is located on the same screen, in the **Network** panel. The **Delphix Engine Hostname** field displays the hostname information.



Delphix Admin Application

> The Delphix Server Hostname is not available from this view but typically matches the IP (DNS) name assigned to the Delphix Engine.

Login to the Delphix Management application with delphix_admin level credentials:

1. Access the Delphix Engine through the URL: `http://<Delphix Engine>/Server.html`
   where `<DelphixEngine>` is the DNS name of the IP address of the Delphix Engine for which you wish to find the Delphix Server ID.
2. Enter a valid **Username**.
3. Enter a valid **Password**.
4. Click **Log In**.
5. Under **System Summary**, the **Server ID** field displays the Delphix Server ID.

CLI Method

1. Use SSH to access your Delphix Engine: `ssh <userid>@<delphix_engine>`

   where `<userid>` is a user ID with either delphix_admin- or sysadmin-level credentials.
2. Enter a valid password if prompted for one.
3. Enter **`system ls`**.

   You will see an output similar to this example:

```
Properties

   type: SystemInfo

   apiVersion:

   type: APIVersion

      major: 1

      micro: 0

      minor: 5

   buildTimestamp: 2015-02-24T09:24:58.000Z

   buildTitle: Delphix Engine 4.2.0.1

   buildVersion:

      type: VersionInfo

      major: 4

      micro: 0

      minor: 2

      patch: 1

   configured: true

   currentLocale: en-US

   enabledFeatures: XPP

   hostname: delphix42.dcenter

   installationTime: 2015-02-24T19:53:32.000Z

   locales: en-US

   memorySize: 3.99GB

   platform: VMware with BIOS date 04/14/2014
```

```
   processors:

      0:

          type: CPUInfo

          cores: 1

          speed: 2.40GHz

      1:

          type: CPUInfo

          cores: 1

          speed: 2.40GHz

   productName: Delphix Engine

   productType: standard

   sshPublicKey: ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAszNCFnfziuK8dBdv6DNB+LrhVP1wRWc/vXVrxrDlgYQTrq
vEx4BKgHDZ2hnbAmqq2xXHR5Ah6WDsEfo6u5B45JZc8qHpx8VZSZa053IdMK9LEgoKPepmo7JV
3kVY9oHK9PngLm9tFK+hN7AUHcGTt68IHq54GWYQNBtx0kgSR5HtkkFhVfX2amFsHIsq1K96bg
RkL0I5f3SjF4NnyElgBU9grGDajm9RXv+sz+Fn7h79AtFm0+W2Ymr5gQrdgh2vPyeFtG8G7rxn
Qx3qiRBY6lNqepBhitXnMYSduGfW+fMJpV8TOOJ9ZLCfE7rjAgH7RxPybTfb4u70sm2krS8SgQ
== root@delphix


   storageTotal: 23.07GB
```

```
    storageUsed: 2.00GB

    uuid: 564d2f7c-b84f-8bd1-6f45-2060ac9b9a65
```

The **Delphix Server ID** is shown as the `uuid` property at the bottom of the output, and the **Hostname** is displayed in the `hostname` property.

4. Enter **`exit`** to leave the command line interface.

Related Links

System Administrators and Delphix Users

How to Setup Auto-authentication

Generally, users need to enter a username and password when logging into the Delphix CLI. There are situations in which users may find entering a password cumbersome, or manual password entry may not be possible. These situations can be alleviated by setting up auto-authentication for the Delphix CLI.
There are two basic steps:

1. Generate a public and Private RSA key pair.
2. Register the public key with the specific Delphix Engine user.

There are two methods available:

- PuTTY
- OpenSSH with OpenSSL

If the examples provided do not work for you, you may need to consult your SSH documentation, we can only provide support for the Delphix Engine side of the connection. In both examples we grant password less login to the **sysadmin** user to host **Delphix5010**.

Using PuTTY

You will need both **putty.exe** and **puttygen.exe** for this.

Launch **puttygen.exe**

Set the **Type of key to generate** to *SSH-2 RSA* and the **Number of bites in generated key** to a suitable value such as *2048*. Click **Generate**

Once it has generated the key pair, leave the password fields blank and save the public and private keys to file.

Add the full contents of the public key to each Delphix Engine user you want to allow automatic login for.

```
Delphix5010> user
Delphix5010 user> select sysadmin
Delphix5010 user 'sysadmin'> update
Delphix5010 user 'sysadmin' update> set publicKey="ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAjdQYr1WU6UPr6FZqyt3eKNJEkAe8IdKQ8hcuBWa3HvRVmU
uv0Lykm5AYQlIW0B33aWusr0o+2FVTzt3/6G1lLCf7wfhCShlJsYgwgmHeEGjixK5tacFCD8r+
8dALaXlv8uOlddK0A2LPXbCCCIRL7IyVEnlSbUFY8s+E/2R3owy5XSbLJLE1el5m1lQPOyUuQd
dAh25ruWR+1HHSAWG3p+wofOh6l7czkEcq7fPjtAZvivX90e8Ggt6JQ8bv6td7aJWObU2Y9YY0
HLLHot7NQ4AT/0tXSRKAG8sIdL7tY9hbHMNHRftCLzfn7mL+Qk8TjUYni3JGB4Vyi0bmkj6nHQ
== rsa-key-20160309"
Delphix5010 user 'sysadmin' update> commit
```

1. In Putty, create a profile that uses the private key. In the PuTTY Connection settings set **SSH** > **Auth** >*Private key file for authentication* t o the private key file you just generated
2. Next, still in the PuTTY Connection settings set **Data** > *Auto-login username* to `sysadmin`@SYSTEM.

3. Test the connection by setting the connection hostname as you normally would for PuTTY and click **Open**.

```
Connection > SSH . Auth
```

Using OpenSSH with Open SSL

Generally, OpenSSH will already have default public and private keys that can be used, if not (or the default keys are password locked) you can create them this way. OpenSSL is required but OpenSSH will take care of the background OpenSSL stuff for you.

1. Create your RSA key pair to a bit length suitable for your security needs (2048 is commonly required for recent security audits)

```
$ ssh-keygen -b 2048 -t rsa -P ' ' -f /etc/ssh/ssh_host_rsa_key
```

Results in a matching public file called `/etc/ssh/ssh_host_rsa_key.pub`
If you want to create different key pairs, just specify a different file path.

2. Add the full contents of the public key (`/etc/ssh/ssh_host_rsa_key.pub` in this example) to each Delphix Engine user you want to allow automatic login for.

```
Delphix5010> user
Delphix5010 user> select sysadmin
Delphix5010 user 'sysadmin'> update
Delphix5010 user 'sysadmin' update> set publicKey="ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAjdQYr1WU6UPr6FZqyt3eKNJEkAe8IdKQ8hcuBWa3HvRVmU
uv0Lykm5AYQlIW0B33aWusr0o+2FVTzt3/6G1lLCf7wfhCShlJsYgwgmHeEGjixK5tacFCD8r+
8dALaXlv8uOlddK0A2LPXbCCCIRL7IyVEnlSbUFY8s+E/2R3owy5XSbLJLE1el5m1lQPOyUuQd
dAh25ruWR+1HHSAWG3p+wofOh6l7czkEcq7fPjtAZvivX90e8Ggt6JQ8bv6td7aJWObU2Y9YY0
HLLHot7NQ4AT/0tXSRKAG8sIdL7tY9hbHMNHRftCLzfn7mL+Qk8TjUYni3JGB4Vyi0bmkj6nHQ
== rsa-key-20160309"
Delphix5010 user 'sysadmin' update> commit
```

3. Test no password login on the command line from your client.

```
$ ssh -i /etc/ssh/ssh_host_rsa_key sysadmin@Delphix5010
```

Related Links

- Installation and Initial Configuration Requirements
- Installation and Initial System Configuration

Configuring Multiple DNS Domain Names in DNS Search List

The Delphix Engine does not support more than one DNS domain name in the DNS search list at this time.

It is possible to use the Delphix CLI if more than one DNS domain name is needed in the search list.
In order to understand if there is more than one domain name in the search list, check for "DNS Suffix Search list" from the output of `ipconfig`

`/all` in the Windows Server:

or check for "`search`" in `/etc/resolv.conf` on a Linux server:

```
[root@rhel62 ~]# cat /etc/resolv.conf
search delphix.com
nameserver 192.168.0.1
```

> Each domain name needs to be separated by a comma.

To update DNS in the CLI:

1. Log into the CLI as sysadmin and navigate to **service > dns**.

   ```
   ssh sysadmin@yourengine
   > service
   > dns
   ```

2. List the current DNS configuration and **update** to add new configurations.

   ```
   > ls
   > update
   > set domain=xxx.xxx, xxx.xxx
   ```

3. **Commit** the action and verify the new list.

   ```
   > commit
   > ls
   ```

For example:

```
delphix> /service dns
delphix service dns> ls


Properties
type: DNSConfig
domain: delphix.com
node: (unset)
servers: 192.168.0.1


Operations
update


delphix service dns> update
delphix service dns update *> set
domain=delphix.com,one.delphix.com,two.delphix.com
delphix service dns update *> commit
delphix service dns>
delphix service dns> ls


Properties
type: DNSConfig
domain: delphix.com,one.delphix.com,two.delphix.com
node: (unset)
servers: 192.168.0.1


Operations
update


delphix service dns>
```

Related Links

- Installation and Initial Configuration Requirements
- Installation and Initial System Configuration

Introduction to Privilege Elevation Profiles

This topic introduces the concept of Privilege Elevation Profiles, how they are managed, and how they are supported. Privilege Elevation Profiles exist to provide the Delphix Engine with a mechanism for running privileged commands in a secure way to achieve the following:

- Mount and Unmount NFS filesystems
- Create and Remove directories in paths not owned by the Delphix OS user
- Examine the running process list
- Run commands as root

Privilege Elevation Profiles is an advanced CLI topic and are not documented as part of the general Delphix Engine User Guide. Changes to the default sudo-based profile scripts, or the creation of new profiles that do not work as expected, can cause serious problems and render the Delphix Engine unusable. This article is aimed at advanced end users and Delphix Professional Services consultants.

Support for Privilege Elevation Profiles

> Writing and troubleshooting scripts, such as those required for Privilege Elevation Profiles, is out of scope and not covered by Delphix Support.

Privilege Elevation Profiles need to be tailor-made to work with non-standard environments that may use third party or proprietary a privilege elevation mechanism other than sudo. Customer are strongly encouraged to work with Delphix Professional Services to formulate reliable profile scripts. There is nothing which prevents customers from creating their own profile scripts. However, customers bear full responsibility for supporting and troubleshooting their own profile scripts. Support for profile scripts created by our Professional Services consultants are still supported by Professional Services.

How do Privilege Elevation Profiles Work?

Privilege Elevation Profiles exist within a two-tier cascading hierarchy. This means there is one default profile for the entire Delphix Engine that should contain scripts for all the operations that require privilege elevation. Additional profiles may contain a subset of the scripts. When a non default profile is used, the Delphix Engine uses that profile's scripts where they exist and reverts to the scripts in the default profile if no script for the operation exists. By default, the Delphix Engine ships with simple scripts that pass commands to the standard UNIX **sudo** command.

All Environments added to the Delphix Engine get added with the default Privilege Elevation Profile. The profile can be assigned on a per host basis. Below shows how a host using a non standard profile will use scripts in the cascading model.

default profile (sudo)	custom profile (myProfile)	host profile	script used
dlpx_mount	my_mount	myProfile	my_mount
dlpx_umount	my_umount		my_umount
dlpx_rmdir			dlpx_rmdir
dlpx_mkdir			dlpx_mkdir
dlpx_ps			dlpx_ps
dlpx_pfexec			dlpx_pfexec

Related Links

- Privilege Elevation Profiles and Delphix Replication
- Installation and Initial Configuration Requirements
- Installation and Initial System Configuration

How Much Space does ToolKit Occupy

Toolkit Size and Predicted Growth:

Each of the clients that run from the client side toolkit generates their own logs. Each client generates 4 different log files, one for each level of logging - info, trace, debug, error. Each level of logging is restricted to a maximum of 10 logfiles and these logfiles are capped at 10MB each. Therefore, Delphix will consume a maximum of 400MB per client side application. On Source server, there are currently two commonly run client side applications, SnapSyncClient and the Delphix Connector (V2P also generates its own logs so if the customer intends to V2P to the source they should account for an additional 400MB in their upper bound).

Thus, the max amount of growth for the toolkit from logging is 800MB without V2P (or 1.2GB with V2P).

Linking additional dSources does not impact the size of the toolkit on production (aside from the log messages generated during linking which is accounted for the in calculation above).

On the target server, unlike Source server, there would be only one client – Delphix Connector, which would occupy around 400 MB maximum storage space. In addition, Delphix pushes new scripts each time a VDB is provisioned which requires < 1MB space.

Therefore the maximum space occupied by the toolkit directory on Source server is its initial size (~ 400MB) + 800MB = 1.2 GB. While on target server, the maximum toolkit size is initial size (~ 400MB) + 400 MB + Number of VDBs * 1MB.

Cleaning Up

For each app, such as Snapsync, Delphix does not trim logs that are simply old as long as Delphix has not reached the end of the circular log

buffers.

Related Links

- Installation and Initial Configuration Requirements
- Installation and Initial System Configuration

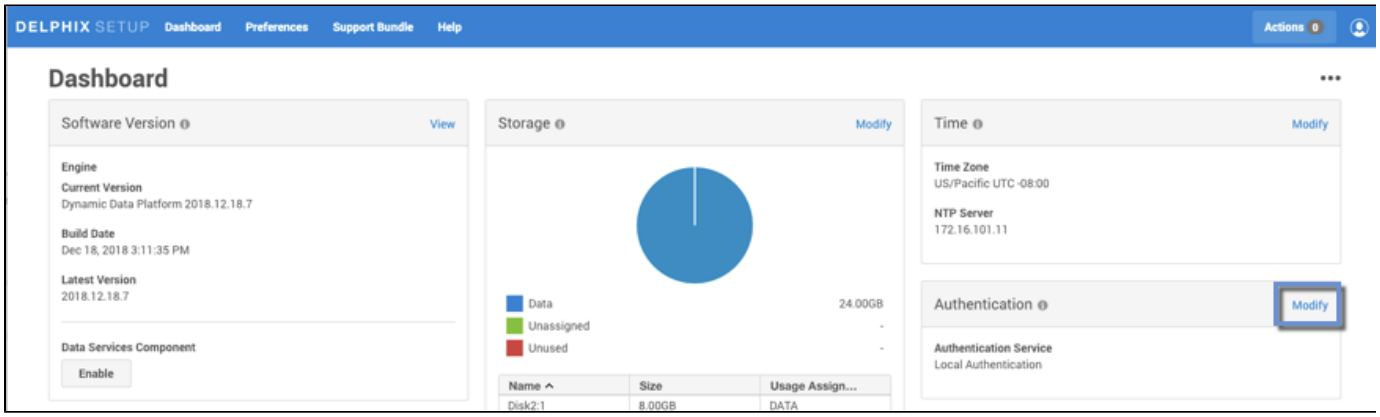
Configuring and using LDAP with the Delphix Engine

Using LDAP with the Delphix Engine requires the following:

- configure the Delphix Engine to use LDAP
- add LDAP users in the Delphix Management application

Configuring LDAP on the Delphix Engine

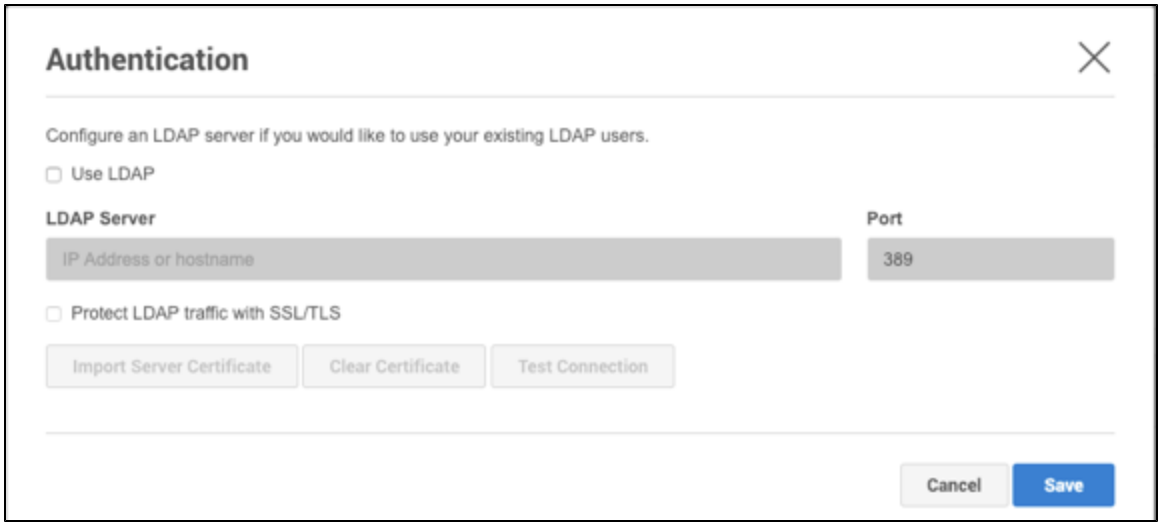
1. From the Delphix Setup application configure LDAP server with the Delphix Engine by selecting Modify in the Authentication section.



2. Enter the information about the LDAP Authentication Server.

> This must be an LDAP server that is configured for authentication. This information should come from the LDAP admin who runs the server. As a general rule only use simple auth. If using SSL/TLS typically use port 636 and import a certificate. If not using SSL/TLS, use port 389 and you will not need a certificate. If the remote LDAP server has disabled anonymous access and the user is trying to use SSL/TLS, the user will be unable to import the certificate. If this occurs file a support case so that Delphix Support can help manually upload the certificate.

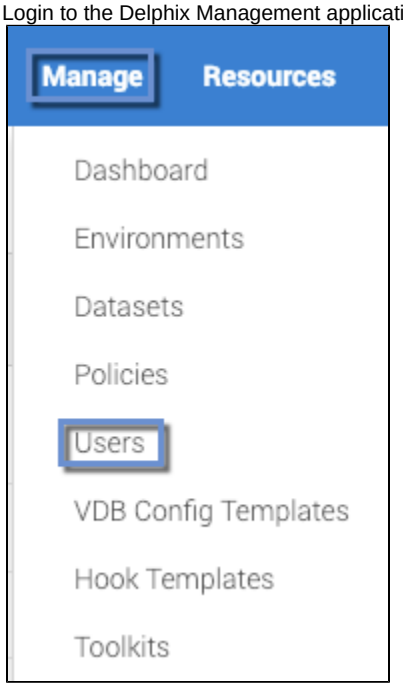
> Test Connect will issue an anonymous login request to the LDAP server. If the LDAP server has disabled anonymous access the test will fail. Test the server by adding a valid LDAP user and try logging in.



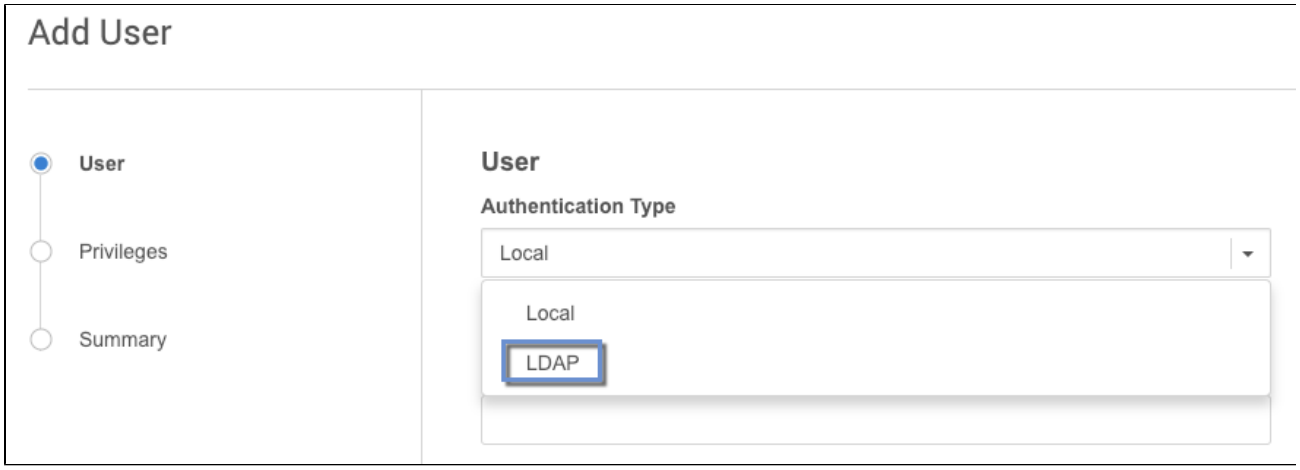
3. After updating the information and clicking the **Save** button, the *Authentication Service* section should reflect the proper information.

Create a new LDAP User account

1. Login to the Delphix Management application and go to **Manage > Users** to add a new user.



2. In the **Users** screen, click the **Add User** icon (+) and choose **LDAP** as the *Authentication Type*.



3. Fill out the data fields and decide if the user will be a *Delphix Admin*. For more info on the *Delphix Admin* setting please see this link. When adding the principal, it is mandatory to specify the entire DN of the user to be added.

> Each entry in an LDAP tree has a unique identifier; its Distinguished Name (DN). This consists of its Relative Distinguished Name (RDN), constructed from some attribute(s) in the entry, follow the parent entry's DN. Think of the DN as the full file path and the RDN as its relative filename in its parent folder (e.g. if /foo/bar/myfile.txt is the DN then myfile.txt would be the RDN). Some users prefer to use the term fully qualified DN to emphasize that a proper DN should include all of the components.

Example of LDAP Tree in which the base is:

dc=example,dc=com

and people are stored in a People subtree with RDN:

ou=people

and each individual is keyed by the cn (common name) attribute.

An example DN in this case would be: cn=Tony,ou=people,dc=example,dc=com

> When adding an LDAP user you will be asked for the following information:
>
> - Principal - which is the DN from above
> - email address
> - username - used to login into Delphix

A password is no longer required because it will authenticate against the password already stored in the LDAP entry, which is presumably known to the individual already. It is probably best if someone familiar with the LDAP tree and using it for authentication were involved at least initially to help understand how to describe the fully qualified DN for users.

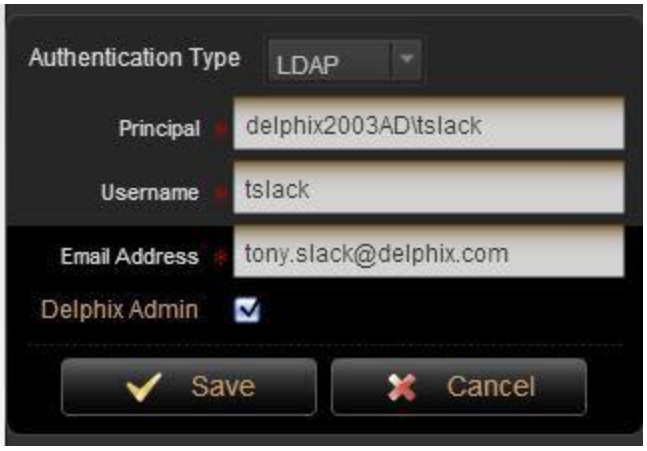
Using Microsoft AD as an LDAP server

Using Microsoft AD as a modified LDAP server is also possible. Microsoft AD allows some shortcuts in the specification of the DN when binding.

Examples:

- <domain>\<user logon name>
- <user logon name>@<domain>.com

As with generic LDAP, it is probably best if someone familiar with using the AD LDAP instance for authentication was involved.



When users log in, they will enter the username as chosen above, and the password that matches the principal entered above.

Related Links

- The delphix_admin and sysadmin User Roles
- Customizing the Delphix Engine System Settings

How to Change the Host Name or IP Address of the Delphix Engine

1. Stop all running VDBs by clicking the red **Stop** button on the VDB card.
2. Disable all dSources as described in Enabling and Disabling dSources.
3. You can use either the command line interface or the Delphix Setup application to change the IP address of the Delphix Engine.
    a. To use the command line interface, press **F2** and follow the instructions described in Setting Up Network Access to the Delphix Engine.
    b. To use the Delphix Setup application, go to to **System > Server Setup** in the Delphix Management interface, or click **Server Setup** in the Delphix Engine login screen.
        i. In the **Network** panel, click **Modify**.
        ii. Under **DNS Services**, enter the new IP address.
        iii. Click **OK**.
4. Refresh all Environments by clicking the Blue/Green Refresh Symbol on the Environments screen.
5. Enable all dSources as described in Enabling and Disabling dSources.
6. Start all VDBs by clicking the **Start** button on the VDB card.

Upgrading the Delphix Engine

These topics describe processes for upgrading the Delphix Engine.

If you are using version 5.2 or above of the Delphix Engine, you may be able to upgrade to later versions with less direct involvement from Delphix Support than was previously required.

- Upgrading the Delphix Engine: an Overview
    - Types of Upgrade
- Upgrade Prerequisites
    - Verifying the Integrity of the Downloaded Upgrade Image
    - Verifying Connectivity to Datasets and Environments
- Uploading the Upgrade Image
    - Upgrade Verification
    - Resolving Upgrade Checks
- Applying the Upgrade
    - Failure to Quiesce a Dataset
- Post Upgrade

Upgrading the Delphix Engine: an Overview

- Types of Upgrade
- Outline of the Upgrade Process
- Related Links

> If you are using version 5.2 or above of the Delphix Engine, you may be able to upgrade to later versions with less direct involvement from Delphix Support than was previously required.

Upgrading the Delphix Engine is a multi-step process which requires some preparation. Before you begin, contact Delphix Support to perform some pre-checks. The engine upgrade process may affect the availability of the Delphix Engine administrative interface and virtual datasets during the operation. Upgrades typically take 1-2 hours.

The following sections explain the steps involved in the upgrade process with links to detailed instructions for proceeding through each of them.

Types of Upgrade

There are three types of upgrades, which are characterized by the impact they have on VDBs during the operation:

Upgrade Type	Description
Application-only Upgrade	The user interface, API and CLI (Command Line Interface) will only be available to the user performing the upgrade. dSources will stop refreshing from production. Policies execution will be delayed until after the upgrade has completed. Jobs will be cancelled (and resumed after upgrade if supported). Access to VDB data will not be affected by this upgrade and can be used normally.
Full Upgrade (Delphix Application + DelphixOS)	In addition to performing an application upgrade, DelphixOS, the operating system that runs Delphix, will be upgraded and the machine will reboot to the new OS as part of the upgrade process. The Delphix Engine will automatically disable all VDBs and dSources during the upgrade process in order to safely reboot to the new version, and thus you should schedule downtime for your VDB applications.
Deferred DelphixOS Upgrade	When upgrading between minor versions of the Delphix Engine – for example, when the first two digits in the version number does not change – you sometimes have the option of deferring the DelphixOS upgrade portion. This allows for application-level bug fixes and new features to be available without having to schedule VDB downtime.

For more details, see Types of Upgrade.

Outline of the Upgrade Process

The following is an outline of the steps for upgrading the Delphix Engine:

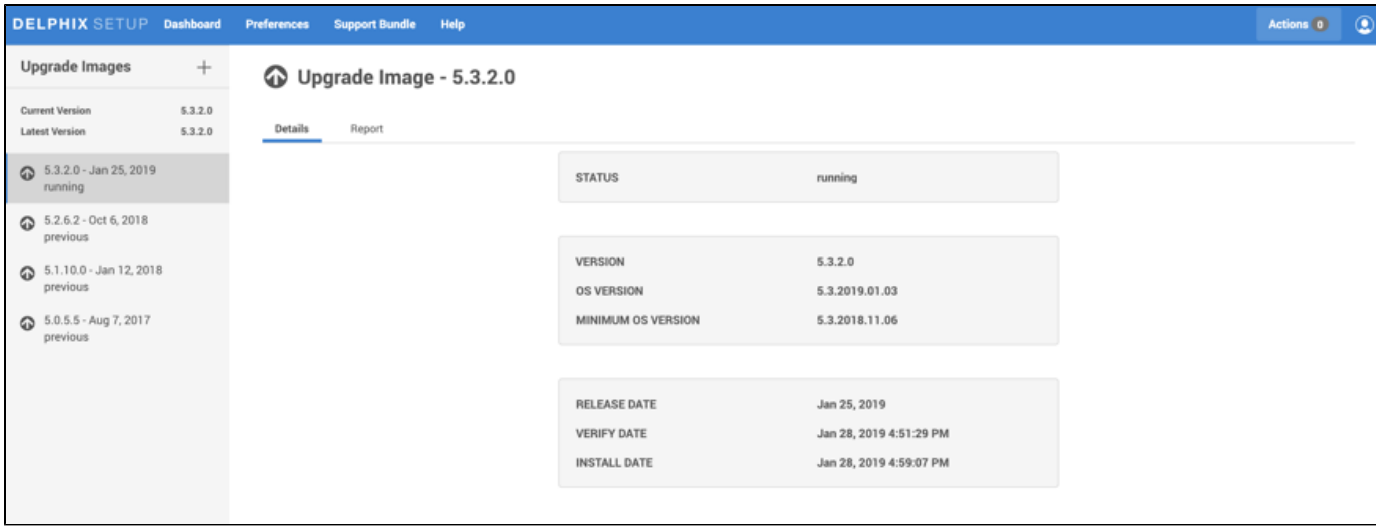
1. Before you begin the upgrade process, contact Delphix Support to perform some pre-checks. If you are using version 5.2 or above of the Delphix Engine, you may be able to upgrade to later versions with less direct involvement from Delphix Support than was previously required.
2. Download the upgrade image to your computer from the Delphix download site (and optionally verify the integrity of the image).
3. Upload the upgrade image to the Delphix Engine.
4. Verify and resolve the system requirements and known defects before starting the upgrade.
5. Decide on the type of upgrade to perform and schedule the appropriate downtime.
6. Verify dataset and environment connectivity.
7. Start the upgrade.
8. Address any runtime failures that happen as part of the upgrade.
9. Verify that upgrade completed successfully.

Related Links

- Types of Upgrade

Types of Upgrade

Each Delphix Engine upgrade image contains both Delphix Management software and software for DelphixOS, the operating system that runs Delphix. Once you have uploaded an image, you can see this information in the **Server Setup**, **Upgrade Images** view, on the **Details** tab of the image, as described in Uploading the Upgrade Image.



You can determine which type of upgrades are applicable by looking up your current version of the Delphix Engine (visible in **Server Setup** > **System Upgrade Management**) and the version to which you are upgrading in the Upgrade Matrix.

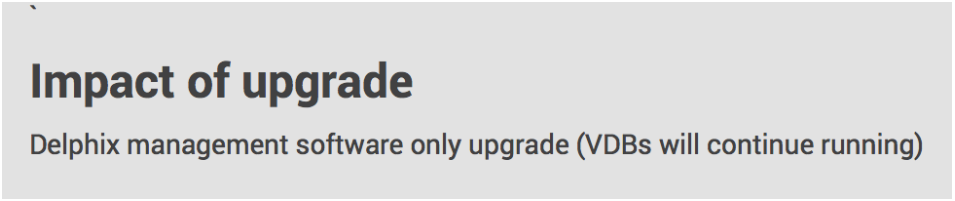
Application-only Upgrade

If the current version, and the uploaded version being upgraded to, have the same OS version, then an upgrade of the OS is not necessary. As a result, when upgrading to this target version, the appliance automatically detects that this upgrade does not require a system reboot, so VDBs will not be affected during the upgrade window and can be used normally.

However, the following downtime will still be observed:

- The user interface, API and CLI (Command Line Interface) will only be available to the user performing the upgrade (only with basic functionality related to the upgrade).
- Policies execution will be delayed until after the upgrade has completed.
- dSources will stop refreshing from production.
- Replication will be suspended.
- Any jobs not pertaining to the upgrade will be cancelled (and resumed after upgrade if supported).

As shown below, an application-only upgrade will show an **Impact of upgrade** message in the UI.



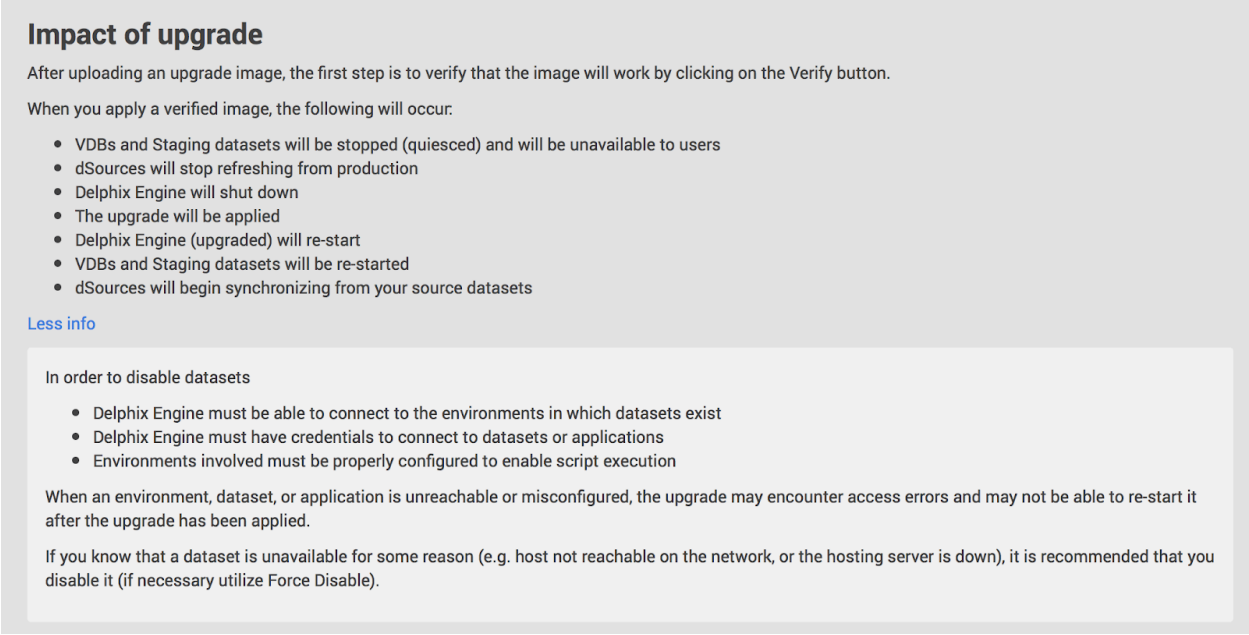
Full Upgrade

If the current version, and the uploaded version being upgraded to, do not have the same OS version, then a DelphixOS upgrade will also be performed at the same time as the application upgrade by default. As a result, on top of the downtime observed from an application-only upgrade described above, you will also observe that:

- VDBs will not be available during the upgrade window

The length of downtime varies based on a number of factors, including: the number of VDBs on the engine, the historical usage of the engine, and the performance of target hosts.

As shown below, a full upgrade will show an **Impact of upgrade** message in the UI.



Deferred DelpixOS Upgrade

If the current version, and the uploaded version being upgraded to, do not have the same OS version, you may still have the option to defer upgrading the DelphixOS, and perform just the application upgrade. You will still face the same downtime as an application-only upgrade described above, but a deferred DelphixOS upgrade may be advantageous when it is hard to schedule for VDB downtime.

To check to see if a deferred DelphixOS upgrade is supported, the current OS version must meet the “Minimum OS Version” requirement of your uploaded version. This check can be done in the Upgrade Images view, or in the Command Line Interface (CLI). For example:

```
delphix system version> list
NAME     STATUS             OSRUNNING  BUILDDATE
4.0.6.0  UPLOADED           false      2014-06-17T03:12:48.000Z
4.0.5.0  CURRENTLY_RUNNING  true       2014-06-10T14:41:28.000Z
```

Here, the running OS comes from version 4.0.5.0. You want to see if the OS version in 4.0.5.0 meets the minimum requirements for version 4.0.6.0, to which you are upgrading:

```
delphix system version> select 4.0.5.0 get osVersion
   4.0.2014.06.07
delphix system version> select 4.0.6.0 get osVersion
   4.0.2014.07.01
delphix system version> select 4.0.6.0 get minOsVersion
   4.0.2014.04.24
```

In this example, although 4.0.6.0 includes a newer version of DelphixOS than what is currently running, the currently running OS meets its minimum OS version requirement.

Once you have verified a deferred upgrade is possible to your uploaded image, you can choose to do a deferred upgrade, which is only supported in the CLI currently. To do this, set the defer property to true in the apply context.

```
delphix system version> select 4.0.6.0
delphix system version ‘4.0.6.0’> apply
delphix system version ‘4.0.6.0’ apply *> set defer=true
delphix system version ‘4.0.6.0’ apply *> ls
Properties
   type: ApplyVersionParameters
   defer: true
   enableSourcesOnFailure: true
   ignoreQuiesceSourcesFailures: false
   quiesceSources: true
   reboot: true
   verify: true
delphix system version ‘4.0.6.0’ apply *>
```

Once in this state, run commit to start the deferred upgrade.

After performing a deferred DelphixOS upgrade, the OS version will still be installed, but the system OS will not reboot to that new version. Only the Delphix management software will restart to the new version, but this restart will not result in downtime for VDBs. After that point, the STATUS column of the running version will show DEFERRED instead of CURRENTLY_RUNNING. This indicates that although this version is running, the OS upgrade was deferred.

Later, you can update the OS to the current version by applying the running version again and not setting the defer property. When you do this, the system will reboot to the current version of DelphixOS. This will result in downtime for your VDBs. Note that a system reboot without applying the running version again will not result in an OS update.

Contact Delphix support to determine whether a deferred OS upgrade is appropriate for your Delphix Engine. You should be aware of what changes are included in the new OS version before making this determination.

Related Links

- Uploading the Upgrade Image

Upgrade Prerequisites

> Before you begin the upgrade process, contact Delphix Support to perform some pre-checks.

Scheduling Downtime

If a new version of the operating system is included in the new Delphix version, then your Delphix Engine will automatically disable all VDBs and dSources during the upgrade process in order to safely reboot to the new version. This will only happen if a new version of the OS is being installed. To determine if an upgrade will result in a reboot and VDB downtime, compare the OS version in the currently-running Delphix version with the OS version in the newly-uploaded Delphix version to which you will be upgrading. The OS version is included in the version details displayed in the **System Setup** application's **System Upgrade Management** screen.

If the OS will not be updated as part of the upgrade, then the upgrade process will have no impact on the availability of VDBs, and you do not need to schedule any downtime for your VDB applications.

If the OS will be updated as part of the upgrade, then you should schedule appropriate downtime for your VDB applications. The Delphix Engine will automatically disable VDBs and dSources during upgrade. The length of downtime will be proportional to the number of VDBs.

> Longrunning jobs including replication and SnapSync will fail during any upgrade.

The upgrade file for the version to which you want to upgrade should be downloaded from the Delphix download site.

Delphix Upgrade images are approximately 3GB in size; it is recommended to have both a fast internet connection to the Delphix download site as well as to the Delphix Engine.

The upgrade image should be downloaded or moved to a location accessible to the computer used for navigating the Delphix Management application.

For example, if we want to upgrade to 5.1.8.0, you would need to download the following files:

1. “5.1.8.0/media/delphix_5.1.8.0_2017-08-09-16-07.upgrade.tar.gz”
2. “5.1.8.0/media/delphix_5.1.8.0_2017-08-09-16-07.upgrade.tar.gz.md5sum”

The first file is the actual upgrade file. The contents of the second text file is used to verify the MD5 hash value of the actual upgrade file. For instructions on using the md5sum file, see Verifying the Downloaded Upgrade Image.

> Delphix Engines can only perform replication to engines on the same version; it is recommended to upgrade all engines in a replication group at the same time. Upgrading a replication source or target without upgrading its replication peers will cause replication between those peers to fail.

Related Links

- Verifying the Integrity of the Downloaded Upgrade Image

Verifying the Integrity of the Downloaded Upgrade Image

Md5 checksum is used to verify the integrity of files, as virtually any change to a file will cause its MD5 hash to change. Most commonly, md5 checksum is used to verify that a file has not changed as a result of a faulty file transfer, a disk error or non-malicious meddling.

The “md5sum” program is included in most Unix-like operating systems, or compatibility layers such as Cygwin.

Please note that the following step is optional.

On linux based systems, the command is md5sum <upgrade.tar.gz>, on mac, the command is md5 <upgrade.tar.gz> and on windows, the command is “CertUtil -hashfile <upgrade.tar.gz> MD5>. Verify that the output of the command’s md5 checksum is the same as the one in the md5sum file.

Related Links

- Uploading the Upgrade Image

Verifying Connectivity to Datasets and Environments

If a new version of the operating system is included in the new Delphix version, then your Delphix Engine will automatically quiesce all VDBs and dSources during the upgrade process in order to safely reboot to the new version.

At the end of the upgrade process, the Delphix Engine will also update the Delphix platform toolkit on each connected environment.

To perform these tasks, the Delphix Engine must be able to connect to the environments in which datasets exist and must have credentials to connect to datasets or applications. Environments involved must be properly configured to enable script execution.

When an environment, dataset, or application is unreachable or misconfigured, the upgrade may encounter access errors, and may not be able to re-start it after the upgrade has been applied.

If you know that a dataset is unavailable for some reason (e.g. host not reachable on the network, or the hosting server is down), it is recommended that you **disable** it (if necessary utilize **Force Disable**).

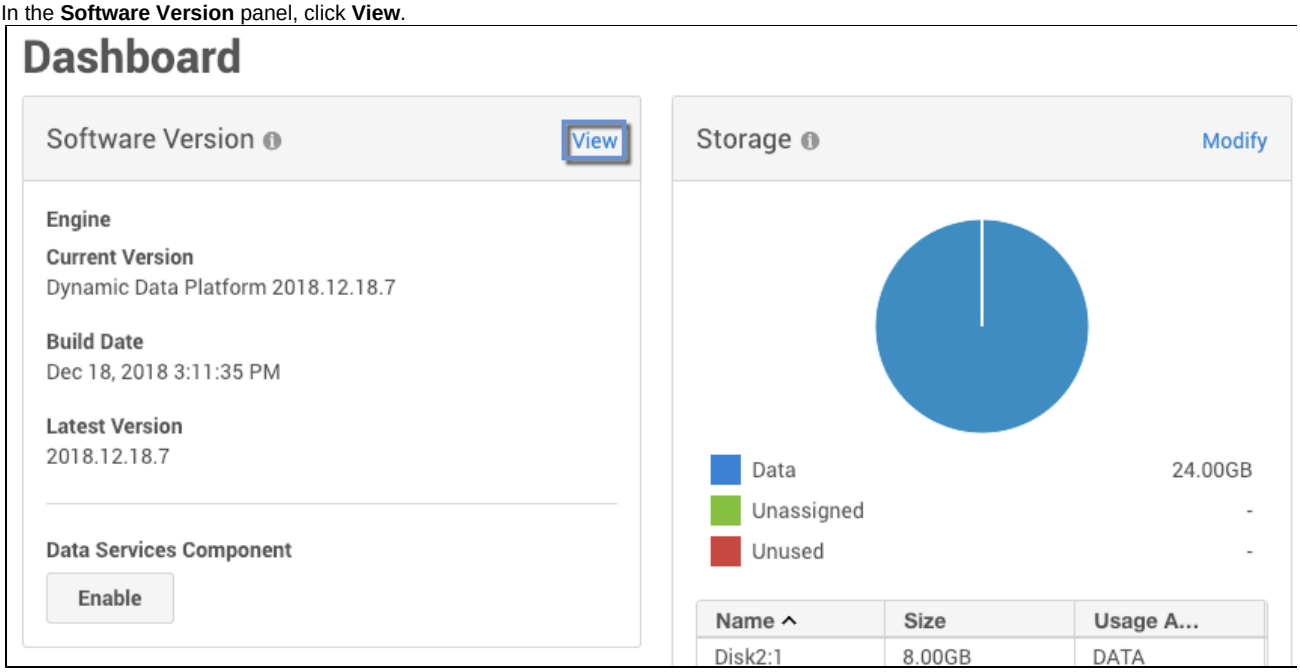
The **Impact** of **Upgrade** section in the **Details** tab contains the list of datasets which have been identified as unreachable, misconfigured or not behaving correctly and are at risk of not functioning after the upgrade.

Review the warnings in this section (if any) and take appropriate actions before applying the upgrade.

Uploading the Upgrade Image

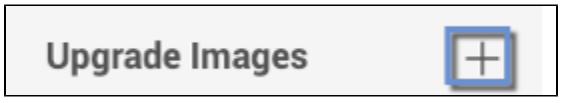
The procedure for uploading an upgrade version to the Delphix Engine is:

1. Login to the **Delphix Setup** application.
2. In the **Software Version** panel, click **View**.



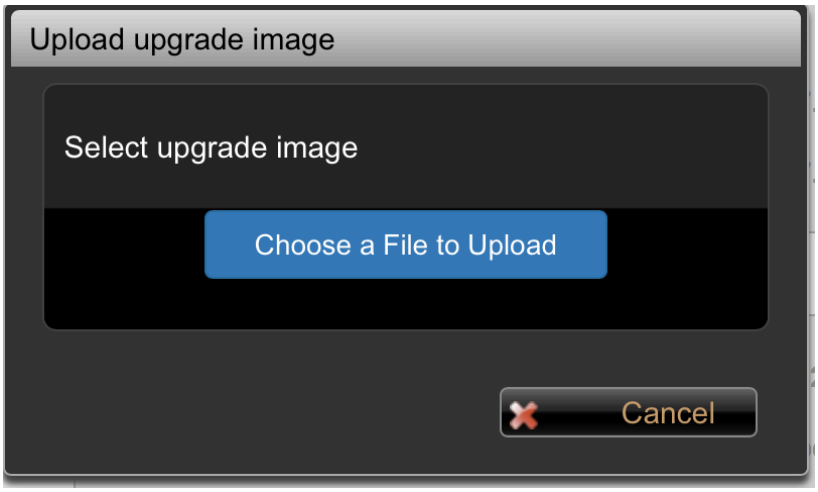
The Delphix Setup Dashboard

3. Click the **plus** icon to upload a new version.



Uploading an upgrade image

4. Select the upgrade version you downloaded from the download site.



Once the file has been uploaded to the Delphix Engine, it will be unpacked in the background and ultimately displayed in the list of versions on the left-hand side of the **System Upgrade Management** screen.

The Delphix Engine starts the upgrade verification automatically after an upgrade image is uploaded. This verification job will use information stored within the uploaded upgrade image to examine the state of the Delphix Engine and make a best effort to validate that applying the upgrade image will succeed. It also will notify you of any potential problems that require intervention from either you or Delphix support. The new version of the Delphix Engine cannot be installed before the verification has completed. You can track the progress of the verification from the **Actions** side bar. If issues are found during the verification process, they will be listed on the version page. An upgrade will not be possible until the issues are resolved.

For more details, see Resolving Upgrade Checks.

Related Links

- Resolving Upgrade Checks
- Upgrading the Delphix Engine

Upgrade Verification

The Delphix Engine provides a feature that allows you to verify an upgrade before applying it. Each new version of the Delphix Engine can introduce new requirements for networking, hypervisor usage, configuration of Delphix Engine objects and more. Verification can determine if the current Delphix Engine does not meet these requirements. It can also detect if the Delphix Engine is in an unexpected state before an upgrade, in which case the best solution might be to contact support. It is recommended that customers read the release notes for any version they are upgrading to and look for new Delphix Engine requirements.

As soon as the upgrade image is uploaded, a verification job is started. This verification job will use information stored within the uploaded upgrade image to examine the state of the Delphix Engine and make a best effort to validate that applying the upgrade image will succeed. It also will notify the user of any potential problems that require either customer or support intervention.

After resolving problems noted by the verification process, verification can be run again. It is expected that customers will continue to fix problems and re-verify until no more problems remain, or until none of the remaining problems are critical.

The verification does a “dry run” of some of the upgrade procedures in order to alert the administrator of potential problems before continuing with the upgrade. It is strongly recommended that you perform this verification a day or two in advance, before your upgrade downtime begins, in order to give yourself time to address any problems flagged by the verification. Perform a re-verify closer to the upgrade, when issues have been resolved.

The procedure for verifying an upgrade is:

1. Login to the **Delphix Setup** application.
2. In the **System Upgrade Management** panel, click **View**.
3. On the left-hand side, select the version to which you will be upgrading. Details on the version will be displayed on the right.
4. In the upper right-hand section of the Details tab, click **Verify Upgrade**.

Verification will be run in the background. You can view the progress of the verification in the Action sidebar.

Related Links

- Release Notes

Resolving Upgrade Checks

When verifying an upgrade, the verification job can sometimes detect particular action items called "upgrade checks". These checks are items that the Delphix Engine is not capable of fixing on its own, and require customer and/or Delphix support action. Every upgrade check that appears must be resolved, ignored, or acknowledged before upgrade can proceed.

Upgrade Severities Checks

Severity	Description
CRITICAL	These checks indicate a potential problem post-upgrade with the Delphix Engine. The Delphix Engine cannot be upgraded while CRITICAL checks are present; it is likely that the engine will fail to upgrade or break catastrophically post-upgrade.
WARNING	These checks indicate problems that are local to some objects on the Delphix Engine, but the overall engine can continue running. For example, WARNING checks may indicate a problem with the configuration of a particular Windows environment and indicate that if an upgrade occurs, that environment will not function properly.

The following is a list of checks that have been added to the Delphix Engine:

1. **OS tunable settings** (CRITICAL) - Upgrade verification checks that only a certain set of operating system tunables have been adjusted. If tunable settings not on this acceptable list have been changed, please contact Delphix support.
2. **Hotfix** (CRITICAL) - Upgrade verification checks if any hotfixes have been applied to this Delphix Engine. If so, upgrade is definitely possible, but we ask that you contact Delphix support to assist with the upgrade.
3. **Snapshot directory visible** (CRITICAL) - This is an internal Delphix Engine problem that Delphix support can resolve for our customers.
4. **Replication** (WARNING) - It indicates that your Delphix Engine has replication set up as either a target or source. Delphix Engines can only perform replication to engines on the same version, so it is recommended to upgrade all engines in a replication group at the same time.

An Upgrade check can result in multiple check results. Check results are essentially a to-do list of action items required before performing an upgrade. For example, the OS Tunables will create one line item in the UI for each present tunable that is not on our acceptable list. There are three actions that can be performed on each check result.

Upgrade Check Actions

Action	Description
resolve	You have taken the action necessary to solve the problem and complete the action item. Marking a result as resolved means that the customer believes the check result indicated will no longer be a problem. The next verification run will check the result again, but if it is fixed will not create any new check results.
ignore	You have no intention of fixing the problem indicated by the check result. Future verification runs will not generate that check result again if it is present. CRITICAL severity checks cannot be ignored.
reset	Checks that have been ignored, resolved, or acknowledged can be reset back to the unresolved state. This might be used if you desire to fix a check that was previously ignored and add it back to the list of action items.

Related Links

- Verifying the Integrity of the Downloaded Upgrade Image
- Upgrade Verification

Applying the Upgrade

Once you have uploaded an upgrade version, verified the upgrade, optionally reviewed the warnings in the Impact of Upgrade section, scheduled downtime pertaining to the type of upgrade you are performing, you can apply the upgrade.

1. Login to the **Delphix Setup** application.
2. In the **Upgrade Images** panel, click **View**.
3. On the left-hand side, select the version to which you will be upgrading.
4. Click **Apply Upgrade** to initiate the upgrade process.

The upgrade will run in the background. You can view the progress of the upgrade in the Action sidebar . Only the current system admin user can view the progress.

The status of the upgrade will be visible on the screen - if the upgrade is successful, the page will be redirected to the login view.

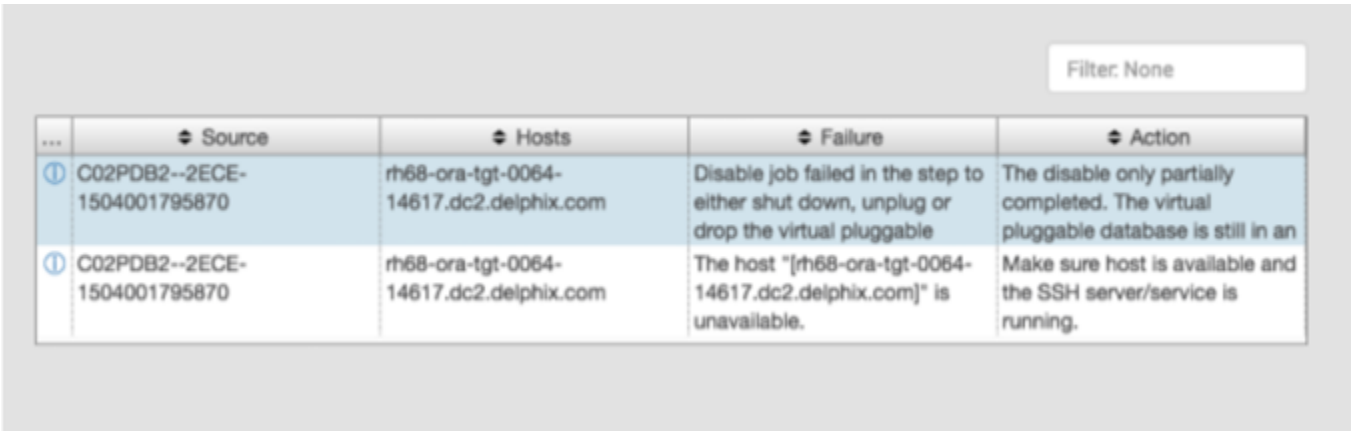
If the upgrade fails, the appliance will rollback to the version running prior to the upgrade. The version page will show the new version in an UPLOADED state and the Action sidebar will show that a rollback was performed. If automatic rollback was disabled through the CLI (not advised), you will have to contact support to proceed further, since you may not even be able to log in to the Delphix Engine.

Failure to Quiesce a Dataset

If Upgrade has failed to quiesce a dataset, it will pause and you will see the following banner at the top of the **Upgrade** page:

While the upgrade is paused, datasets which have been quiesced are unavailable until you either roll back or continue the upgrade.

To review the list of failures, open the **Report** tab:



The datasets listed in the report were identified as having issues which prevented them from being quiesced, and may not be available after the upgrade is complete. Review the messages in the report and take the suggested corrective actions.

If you think that the errors may be the result of transient failures, you can click **Retry** to try again. Otherwise, it is recommended that you manually quiesce datasets that are still running. To do so:

1. Use a different browser or use an incognito window to go to the **Delphix Management** application.
2. Either resolve issues such as a wrong password, or stop the dataset using **Force Disable**.
3. In the original browser or window, click **Retry** to try applying the upgrade again.

If you want to ignore the failures to quiesce datasets and proceed with the upgrade:

1. Click **Continue Upgrade**. This will attempt to quiesce all datasets which have not yet been quiesced, but will not pause on failures.

   > This may result in datasets remaining unavailable after the upgrade is complete and the Delphix Engine restarts, since the underlying storage that backs the datasets will be unreachable during the upgrade. This may cause the databases or applications to fail over or transition to a failure state, thus requiring administrator intervention to recover.

2. Review the messages in the report and take the suggested corrective actions.
3. If any of the listed datasets are critical, and you are unable to resolve the configuration errors in the report, you can **Rollback** the upgrade. If you choose **Rollback**, all changes will be reversed, upgrade will end, and the Delphix Engine will be in the state it was in before you started the upgrade.

Related Links

- Applying the Upgrade
- Upgrading the Delphix Engine

Post Upgrade

After the upgrade is done, you will be redirected back to the login page.

Login to **Delphix Setup** to make sure that upgrade succeeded and that the new version is running. If upgrade failed, the appliance will have automatically rolled back and the APPLY job will be marked as failed.

A **post upgrade cleanup** job is run automatically after upgrade (or rollback) is done. This job refreshes environments and re-enables sources to bring objects back into a working state.

VDB Access

For a full upgrade, VDB access will not be available at all until the environments have been refreshed and the objects are re-enabled by the job **P erform cleanup tasks following a Delphix Engine upgrade**.

For an application-only or deferred upgrade, access to VDB data will not be interrupted during the upgrade window, but VDB operations through the Delphix Management application will still not be available until this job has refreshed all environments. This may take a while. You can monitor progress in the **Jobs** view or **Action** sidebar.

Failures

If you used **Continue Upgrade** to force the upgrade as is described in Failure to Quiesce a Dataset, the **Report** tab will contain the list of pre-upgrade quiesce failures. Upgrade will make a best effort to restore functionality to these datasets, but it may still hit the same errors that prevented the datasets from being quiesced successfully before upgrade. You may need to manually bring up these datasets on the target hosts.

Related Links

- Upgrading the Delphix Engine

Factory Reset

This topic describes the process for returning the Delphix Engine to "factory default" settings. This completely removes all DATA and CONFIGURATION.

Prerequisites

It is recommend to shut down and remove all VDBs before resetting the Delphix Engine. Failure to do so could possibly lead to stale data mounts in target environments. (NFS, for *nix environments, or iSCSI I/O errors in Windows environments) For the same reason, disable all dSources that use pre-provisioning (all SQL Server dSources, and any Oracle dSources with validated sync enabled).

> Use **Factory Reset** only when a complete reset and reconfiguration of the Delphix Engine is necessary, as all Delphix Engine objects will be de-allocated

Procedure

1. Connect to the Delphix **Setup** application (e.g. http://DelphixEngine/login/index.html#serverSetup, or http://DelphixEngine/ and select "Server Setup")
2. Login as **sysadmin** or with other system administrator credentials.
3. Select **Factory Reset** from the menu

Alternative procedure via Command Line Interface (CLI)

1. Connect to the CLI via SSH
2. Login as **sysadmin** or with other system administrator credentials.
3. "system ; factoryReset ; commit ; exit"