Xcalar Installation Guide

Publication date: 2018-01-18

www.xcalar.com

Table of Contents

Xcalar installation overview

This section provides an overview of the Xcalar installation tasks.

Audience

This guide is intended for system administrators who install and configure analytics software and are familiar with Linux operating systems, networking, and computer cluster concepts.

Overview of the Xcalar installation tasks

The following is an overview of the installation procedure for Xcalar:

1. Fill out the Questionnaire on the Xcalar customer portal at:

   http://myxcalar.zendesk.com/

2. Review system requirements. For more information, see Xcalar system requirements.
3. Perform the pre-installation tasks. For more information, see Planning your Xcalar installation and Xcalar pre-installation tasks.
4. Install and deploy Xcalar. For more information, see Installing Xcalar.

Ensuring a successful Xcalar installation

Follow these guidelines for a successful Xcalar installation:

- Read the Xcalar system requirements. This ensures that your system has the required base hardware and software.
- Record all the required configuration values, such as host names, port numbers, user names, and passwords.

  During the pre-installation tasks, record any new configuration values as you create them. You will be required to enter these configuration values later when you install Xcalar. For more information, see Information requirements.

- After installing Xcalar, verify that the Xcalar software stack installed successfully.

If you have any issues during the installation and deployment of Xcalar, see Troubleshooting.

Terms used in this guide

Term	Description
Xcalar cluster	A group of two or more bare metal computers or Cloud virtual machines (called nodes) that run Xcalar Design and Xcalar Compute Engine on each node.
Xcalar Admin	The operating system username that is used on all the nodes of the Xcalar cluster, which owns the Xcalar software and runs the Xcalar Design and Xcalar Compute Engine processes.
Xcalar Root Directory	The network file system mount (NFS) that is shared between all nodes of the Xcalar cluster. Xcalar Design and Xcalar Compute Engine write configuration information and session data into this filesystem.
Xcalar Install Directory	The directory on each node in which the Xcalar software is installed.
LDAP Authentication server	Xcalar uses an LDAP server for authentication, such as Microsoft Active Directory. The Xcalar GUI Installer requires the following server information: • LDAP URI: the server's name or IP address and the server's port number. For example, `ldap://xcalarad.int.xcalar.com:389`. • USER DN: the location in the LDAP server in which to search for user entries. For example, dc=int,dc=xcalar,dc=net. • SEARCH FILTER: an LDAP filter that limits the returned number of user entries to one. For example, `(&(objectclass=user)(userPrincipalName=%username%))` • SERVER KEY FILE: The path to the LDAP security certificates that identify the server. • TLS usage: A true or false value that lets Xcalar know if the server accepts TLS requests. For example, `true`. • ActiveDirectory identity: A true or false value that lets Xcalar know if the server is an Active Directory server. For example, `true`.

Term	Description
Configuration Tarball	A tar archive containing software and script packages, which must be run with superuser privileges (run as root) prior to running the Xcalar Installer. The Configuration Tarball with the Xcalar GUI Installer are downloaded from the Xcalar customer portal at: https://myxcalar.zendesk.com/
Pre-Config script	A configuration script in the Configuration Tarball named **pre-config.sh**, which performs necessary operating system level configuration for each Xcalar cluster node. This script must be run by a superuser or with a **su** or **sudo** program.
Verification script	A script in the Configuration Tarball named **verify.sh**, which tests the Pre-Config Script's configuration steps. This script can be run by any user on the node.
Xcalar GUI Installer	A self-extracting shell archive file that contains a web server, a small web site, and software for installing Xcalar on all the Xcalar cluster nodes in parallel. The Xcalar GUI Installer can be run by any user on any host that has a Xcalar supported Linux operating system and that can connect to all the Xcalar cluster nodes with a secure network. The Xcalar GUI Installer and the Configuration Tarball are downloaded from the Xcalar customer portal at: https://myxcalar.zendesk.com/.
Installation host	The computer on which you run the Xcalar GUI Installer. This can be one of the nodes within the Xcalar cluster, or a host running the same version of the Xcalar supported Linux operating system that was installed on all the nodes within the Xcalar cluster.

Xcalar system requirements

This section describes the software, hardware, and information requirements for installing Xcalar.

Xcalar Compute Engine system requirements

The optimal configuration for running Xcalar Compute Engine depends on your deployment plan and the amount of data you plan to process. The factors to be considered are:

- The size of the datasets being processed.
- The number of concurrent users.
- The dataflow complexity.
- Expected processing times.

Supported Linux operating systems for the Xcalar cluster

The following table lists the supported Linux operating systems for running Xcalar Compute Engine.

Product	Linux Version
CentOS Enterprise Linux	6 or 7
Oracle Linux Enterprise Linux	6 or 7
Red Hat Enterprise Linux	6 or 7

> **Important:** All the nodes within the Xcalar cluster must run the same version of the Xcalar supported Linux operating system.

Supported Xcalar cluster environments

Xcalar can run in the following computer cluster environments:

- Microsoft Azure
- Amazon Web Services (AWS)
- Bare Metal Environment
- Google Cloud Platform
- Virtualized Environments

Supported Xcalar cluster hardware

Your environment must consist of multiple computer nodes within the computer cluster. A computer cluster of four computer nodes that hosts Xcalar is the minimum guaranteed environment.

The following list describes the minimum hardware requirements for your Xcalar cluster:

- Four computer nodes.
- Each computer node contains 16 CPU cores.
- Each computer node contains 128 GB of DRAM and a swap space of 1 to 2 times the amount of DRAM.
- The Xcalar cluster contains a minimum of 1 TB of shared storage.
- The Xcalar cluster network must use the Internet Protocol version 4 (IPv4) and contain a minimum transmission speed of 1 GbE. 10 GbE or faster is strongly recommended.

Data source environments

Xcalar Compute Engine can access data sources on a variety of data storage configurations and across various storage protocols.

Common data source environments include:

- HDFS (Hadoop 2.2.0 or higher, Cloudera Distribution for Hadoop (CDH) 5.0.0 or higher, Hortonworks Data Platform (HDP) 2.2.0 or higher, or MapR 5.0.0 or higher).
- Network file system (NFS).
- Local disk storage.
- Amazon Web Service (ASW) S3

Xcalar GUI installer requirements

The Xcalar GUI Installer must be run on a host running a version of the Linux Operating System that is supported for the Xcalar cluster. For more information, see Supported Linux operating systems for the Xcalar cluster.

Xcalar Design requirements

Xcalar Design is supported on computers with the following Web browser and screen resolution:

Web Browser	Screen Resolution
Google Chrome	Minimum: 1024 x 768 Recommended: 1600 x 900 or greater

Xcalar Design is not supported on mobile devices, such as cell phones or tablets.

Xcalar security

Xcalar recommends that you deploy Xcalar behind a firewall.

> **NOTE:** At this time only self-signed certificates are available.

Information requirements

The following table is provided for recording values that you will be required to provide during the Xcalar cluster node configuration and Xcalar installation and deployment tasks.

> **TIP:** Xcalar recommends that you print the table and record the values for future reference. This table is also available as a form on: Xcalar.com

Field	Value
Which pre-installation tasks were completed - A or B?	
Was a shared storage area created and mounted?	
Was a shared storage area created but not mounted?	
The shared storage path and directory name.	
The NFS file server server name.	
The NFS file server export path.	
The Xcalar Admin’s user name (XCE_USER).	
The Xcalar Admin's password.	
The Xcalar Admin's default group name (XCE_GROUP).	
The Xcalar Root Directory mount point path and directory name (XCE_ROOTDIR).	
The Xcalar Install Directory path and directory name (XCE_INSTALLDIR).	
The Xcalar Demand Paging path and directory name.	
The Installation host’s hostname or IP address.	

Field	Value
The Xcalar License Key.	
The number of nodes in your Xcalar cluster.	
The Private IP address or FQDN of each node.	
The Public IP address or FQDN of each node.	
The SSH port number.	
The SSL private key certificate.	
The LDAP URI.	
The USER DN.	
The SEARCH FILTER.	
The SERVER KEY FILE.	
The TLS usage.	

Planning your Xcalar installation

This section discusses the installation options available and their pre-installation tasks.

About the Xcalar installation options

Xcalar understands that you may not always want to install a full production environment. You may want to start with a small sandbox testing cluster. Therefore, Xcalar provides several installation options that allow you to create your Xcalar configuration based on your needs.

About the cluster node configuration tasks

Xcalar lets you choose whether to configure and set up your Xcalar cluster nodes yourself or let the Xcalar GUI installer do this for you.

From the options below, decide which option best represents the Xcalar work environment you require and complete the pre-installation and storage area tasks for that option:

- **Option A**. For large production environments that require maximum security, Xcalar recommends that the configuration and setup of your Xcalar cluster environment is completed by a combination of scripts run by your IT staff and the Xcalar GUI installer.

  This Xcalar installation option is more secure because it isolates system configuration and administration tasks to a small set of steps that are run by ROOT, or a user who can run SUDO commands.

  This option gives you more control over your environment settings and allows you to debug and verify your Xcalar cluster before installation. Because you set up and configured your environment prior to running the Xcalar GUI installer, errors encountered during an installation or an upgrade are less likely. If issues do occur, you are more likely to resolve them quickly because you understand your environment.

  For more information on **option A** pre-installation tasks, see Pre-installation tasks for option A.

- **Option B**. For small testing, development, or demonstration environments that require minimal security, Xcalar recommends that the configuration and setup of your Xcalar cluster environment be completed by the Xcalar GUI installer only.

> **NOTE:** Some pre-installation tasks are required.

This Xcalar installation option is less secure because all tasks are performed by a user who can run SUDO commands as directed by the Xcalar GUI installer. This user is assigned the role of Xcalar Admin during the installation or upgrade. This option also gives you less explicit control over your environment settings, as the installation is more automated and defaults are used.

With fewer pre-installation tasks to complete and with the Xcalar GUI installer creating your NFS and your LDAP environments this option is ideally suited for test, development, and demonstration environments.

For **option B** pre-installation tasks, see Pre-installation tasks for option B.

Pre-installation tasks for option A

The following pre-installation tasks must be completed for **option A**:

1. Installing and configuring a Linux operating system on the installation host and all nodes within the Xcalar cluster. For more information, see Installing and configuring the Linux operating system.
2. Creating and mounting a shared storage area, such as NFS, on all nodes within the Xcalar cluster. For more information, see Planning your storage solution.
3. Creating and mounting a Demand Paging area on all nodes within the Xcalar cluster. For more information, see Planning your storage solution.
4. Configuring and verifying your Xcalar cluster nodes. For more information, see Configuring the cluster nodes for Xcalar.
5. Preparing the Xcalar installation host. For more information, see Preparing the Xcalar installation host.
6. Collecting and recording your LDAP environment information. For more information, see Enabling Directory Services authentication.

If you have completed the **option A** pre-installation tasks, on the PRE-CONFIG STATUS page of the Xcalar installation Wizard, select **Yes**.

Pre-installation tasks for option B

The following pre-installation tasks must be completed for **option B**.

1. Installing and configuring a Linux operating system on the installation host and all nodes within the Xcalar cluster. For more information, see Installing and configuring the Linux operating system.
2. Creating a Xcalar Admin user on each cluster node who has SUDO access to all the nodes within the cluster and who can run commands as SUDO. For more information, see Creating a Xcalar Administrator user.
3. Preparing the Xcalar installation host. For more information, see Preparing the Xcalar installation host.

The following pre-installation tasks are optional for **option B**.

1. (Optional) Storage pre-installation tasks:
    a. Creating a shared storage area, such as NFS, on all nodes within the Xcalar cluster. During installation, this area is mounted on all the nodes within the Xcalar cluster.
    b. Creating a Demand Paging area on all nodes within the Xcalar cluster. Where the local directory is on a SSD or NVMe drive.

    For more information, see Planning your storage solution.
2. (Optional) Collecting and recording your LDAP environment information. For more information, see Enabling Directory Services authentication.

If you have completed the **option B** pre-installation steps, during installing or upgrading Xcalar, on the PRE-CONFIG STATUS page of the Xcalar Wizard, select **No**.

Answering the PRE-CONFIG STATUS page questions during installing or upgrading

During a Xcalar install or upgrade you are asked whether the **pre-config.sh** and **verify.sh** scripts were run on all the cluster nodes. Running these scripts is a required pre-installation task for **option A** but not for **option B**.

Therefore, in the PRE-CONFIG STATUS page of the Xcalar installation Wizard:

- If you have completed the pre-installation tasks for **option A**, select **Yes**.
- If you have completed the pre-installation tasks for **option B**, select **No**.

Xcalar pre-installation tasks

This section describes the tasks that you perform before installing Xcalar.

About the Xcalar pre-installation tasks

The pre-installation tasks that you must complete before installing Xcalar are dependent on the installation option that you chose in Planning your Xcalar installation. Where:

- **Option A** pre-installation tasks, assume that you require an environment with maximum security. The pre-installation tasks are completed before installation by a user with superuser privileges, such as ROOT, or who can run SUDO commands.
- **Option B** pre-installation tasks, assume that you require a small testing, development, or demonstration environment with less security. The majority of the pre-installation tasks are completed during a Xcalar installation or a Xcalar upgrade.

Pre-installation tasks for option A

1. Installing and configuring a Linux operating system on the installation host and all nodes within the Xcalar cluster. For more information, see Installing and configuring the Linux operating system.
2. Creating and mounting a shared storage area, such as NFS, on all nodes within the Xcalar cluster. For more information, see Planning your storage solution.
3. Creating and mounting a Demand Paging area on all nodes within the Xcalar cluster. Where the local directory is on a SSD or NVMe drive. For more information, see Planning your storage solution.
4. Creating a setup file and configuring and verifying your Xcalar cluster nodes. For more information, see Configuring the cluster nodes for Xcalar.
5. Preparing the Xcalar installation host. For more information, see Preparing the Xcalar installation host.
6. Collecting and recording your LDAP environment information. For more information, see Enabling Directory Services authentication.

Pre-installation tasks for option B

1. Installing and configuring a Linux operating system on the installation host and all nodes within the Xcalar cluster. For more information, see Installing and configuring the Linux operating system.
2. (Optional) Storage pre-installation tasks:
   a. Creating a shared storage area, such as NFS, on all nodes within the Xcalar cluster. During installation, this area is mounted on all the nodes within the Xcalar cluster.
   b. Creating a Demand Paging area on all nodes within the Xcalar cluster. Where the local directory is on a SSD or NVMe drive.

   For more information, see Planning your storage solution.
3. Creating a Xcalar Admin user on each cluster node who has SUDO access to all the nodes within the cluster and who can run commands as SUDO. For more information, see Creating a Xcalar Administrator user.
4. Preparing the Xcalar installation host. For more information, see Preparing the Xcalar installation host.
5. (Optional) Collecting and recording your LDAP environment information. For more information, see Enabling Directory Services authentication.

Installing and configuring the Linux operating system

Must be completed for **option A** and **option B**.

Install one of the Xcalar supported Linux operating systems on the installation host and each of the Xcalar cluster nodes. For more information, see Supported Linux operating systems for the Xcalar cluster.

During the installation of the Linux operating system, do the following for the installation host and each of the Xcalar cluster nodes:

- Configure the host name.

  Record the host name in the Information requirements table.
- Configure the IP address, the Network gateway address, and the netmask.

  Record the IP address in the Information requirements table.

- Enable the Network Time Protocol (NTP) time source IP address.
- Set the time zone.

After completing the above tasks, do the following:

1. Verify that the **openssh-clients** package is installed on each node of the Xcalar cluster.

   The Xcalar Install Wizard uses the secure shell (SSH) and the secure copy protocol (SCP) for securely copying files from the installation host to the nodes within the Xcalar cluster.
2. Verify that all the nodes within the Xcalar cluster are running the same version of the Xcalar supported Linux operating system.
3. Verify that the SUDO program is installed on the installation host and each of Xcalar cluster nodes.

For complete installation instructions and general information about installing and configuring the Linux operating system, see your Linux software documentation.

Planning your storage solution

Xcalar Compute Engine and Xcalar Design creates data, such as configuration information, log files, and session data. This data must reside in a shared storage location that has read, write, and execute permissions by all the nodes within the Xcalar Cluster. It must also contain a POSIX file system interface, such as NFS. By default, this shared directory, known as the Xcalar Root Directory, is located at **/mnt/xcalar**. If required, you can mount the shared directory elsewhere.

> **IMPORTANT:** Xcalar recommends that the minimum size for the Xcalar shared storage is 1 TB.

Before installing Xcalar you must decide your shared storage area's location and who is going to create and mount your shared storage area on all the cluster nodes. You can choose who creates and performs these tasks from the following:

- You create and mount a shared storage area on all nodes within the Xcalar cluster.
  - For information on how to configure your cluster nodes for shared storage, see Configuring the cluster nodes for Xcalar.

  - During the installation or upgrade, you will be required to enter the path and directory name of the shared storage area. Record the path and directory name of the shared storage area in the Information requirements table.
  - During the installation or the upgrade, on the SET UP XCALAR ROOT DIRECTORY page of the Xcalar Wizard, select **Existing Shared Storage Already Mounted**.

  Must be completed for **option A**, optional for **option B**.

- You create a shared NFS file system export (or if upgrading, have an existing NFS file system export) on a NFS server that the rest of the cluster nodes can access.
  - During the installation or upgrade, you will be required to enter the server name and path of the NFS file system export. Record the server name and path of the NFS file system export in the Information requirements table.
  - During the installation or the upgrade, on the SET UP XCALAR ROOT DIRECTORY page of the Xcalar Wizard, select **Existing Shared Storage to be Mounted**. The Xcalar GUI mounts this storage area on all the nodes within the Xcalar cluster during installation.

  Optional for **option B**.

- Xcalar creates and mounts a NFS shared storage area on all the nodes within the Xcalar cluster during installation.
  - Before installation verify that the **node0** node of your cluster contains enough storage space for an NFS export and is at least 1 terabyte in size.
  - During the installation or the upgrade, on the SET UP XCALAR ROOT DIRECTORY page of the Xcalar Wizard, select **Xcalar Deployed Shared Storage**. The Xcalar GUI creates and mounts a shared storage area on all the nodes within the Xcalar cluster.

  Default for **option B**.

> **IMPORTANT:** Xcalar recommends that you create and mount your shared storage area.

About the demand paging area

The Xcalar cluster also requires a demand paging area for each cluster node. This area frees up memory for Xcalar Compute Engine and Xcalar Design operations. Once you have created the

demand paging area, record the path and directory name in the Information requirements table.

> **NOTE:** Xcalar recommends that each cluster node contains a solid-state drive (SSD) or Non- Volatile Memory Express (NVMe) drive for the demand paging area.

Creating a Xcalar Administrator user

Must be completed for **option B**.

The Xcalar GUI installer requires SUDO access on all the nodes within the Xcalar cluster when installing Xcalar for **option B**.

The installer uses a **Xcalar Admin** user to perform configuration tasks on each cluster node. This Xcalar Admin user must be able to run commands as root using SUDO. This allows the Xcalar GUI installer to access your cluster nodes, create, configure, and mount shared storage (as needed), create an LDAP environment, and install Xcalar.

To create a Xcalar administrator user:

1. On each node within the Xcalar cluster, create a Xcalar Admin user with the following attributes:
    - The user is not required to be **root**, but can run commands as root with SUDO.
    - The user name and default group name are not shared with other applications and services, unless it is required by other software. For example, Active Directory.
    - The user name and default group name, along with their associated numeric UID and GID, is identical across the Xcalar cluster.
    - Has read, write, and execute privileges (octal number 700, 750, or 755) of the Xcalar Root Directory and Xcalar Installation Directory for installing and configuring Xcalar.
    - Can log in to the nodes within the Xcalar cluster with SSH that is authenticated with either a password, a passwordless SSL private key, or another type of passwordless authentication.

> **NOTE:** Setting up a public and private key pair is beyond the scope of these instructions. For more information, see https://help.ubuntu.com/community/SSH/OpenSSH/Keys.

2. Record the Xcalar Admin's user name and default group name (by name, not ID number) in the Information requirements table.

Configuring the cluster nodes for Xcalar

Must be completed for **option A**.

This section describes how to configure your cluster nodes to work with Xcalar. If you have chosen **option A** as your installation option, the following tasks must be completed before installing Xcalar.

These tasks must be completed by a system administrator with superuser privileges, either as the **root** user or with a program that allows a user to run programs with SUDO privileges.

Configuring your Xcalar cluster nodes includes completing the following tasks:

- Creating a setup file that holds the Xcalar cluster environment and user credentials. For more information, see Creating a setup file.
- Configuring the Xcalar cluster nodes and verifying the configuration. For more information, see Configuring the Xcalar cluster nodes.

Creating a setup file

The **Pre-Config** script uses the environment and user credentials from the setup file to configure the nodes within the Xcalar cluster:

The setup file stores the following values:

- The system administrator's (Xcalar Admin) user name, password, and group name.
- The directory on each node in which Xcalar is installed (Xcalar Install Directory).
- The network file system (NFS) mount directory name and path (Xcalar Root Directory).

To create a setup file:

1. Create a Xcalar Admin user on each node within the Xcalar cluster, by doing the following:

   a. Create a Xcalar Admin user with the following attributes:

      - Does not require superuser privileges.
      - The user name and default group name are not shared with other applications and services, unless it is required by other software. For example, Active Directory.
      - The user name and default group name, along with their associated numeric UID and GID, is identical across the Xcalar cluster.
      - Has read, write, and execute privileges (octal number 700, 750, or 755) of the Xcalar Root Directory and Xcalar Installation Directory for installing and configuring Xcalar. See steps 2 and 3.
      - Can log in to the nodes within the Xcalar cluster with SSH that is authenticated with either a password, a passwordless SSL private key, or another type of passwordless authentication.

      > **NOTE:** Setting up a public and private key pair is beyond the scope of these instructions. For more information, see https://help.ubuntu.com/community/SSH/OpenSSH/Keys.

   b. Record the Xcalar Admin's user name and default group name (by name, not ID number) in the Information requirements table.

      Where, the Xcalar Admin's user name and default group name are the **Pre-Config** setup file values for XCE_USER and XCE_GROUP.

      > **NOTE:** If the Xcalar Admin has a home directory that does not follow the operating system standard, enter the Xcalar Admin's directory name and path value in the XCE_HOMEDIR parameter.

2. Create a Xcalar Root Directory at a location of your choosing and mount it on each node within the Xcalar cluster, by doing the following:

a. Create the Xcalar Root Directory and mount the shared storage.
b. Verify that the Xcalar Root Directory mount point user has read, write, and execute permissions.
c. Set the owner and group of the mount point to XCE_USER and XCE_GROUP.
d. Record the Xcalar Root Directory in the Information requirements table.

   Where, the Xcalar Root Directory mount point value is the **Pre-Config** setup file value for XCE_ROOTDIR.

> **NOTE:** For some network file systems (such as NFS), set the owner and group of the mount point to XCE_USER and XCE_GROUP on the server before the server's filesystem is mounted on the Xcalar cluster. The filesystem client then assigns the XCE_USER and XCE_GROUP values to the local filesystem's mount point.

3. Create a Xcalar Install Directory on each node within the Xcalar cluster, as follows:

> **NOTE:** This can be a local filesystem directory with an identical path on each node.

a. Create the Xcalar Install Directory.
b. Verify that the Xcalar Install Directory user has read, write, and execute permissions.
c. Set the owner and group of the Xcalar Install Directory to XCE_USER and XCE_GROUP.
d. Record the Xcalar Install Directory in the Information requirements table.

   Where, the Xcalar Install Directory value is the **Pre-Config** setup file value for XCE_INSTALLDIR.

4. On one of the nodes in the Xcalar cluster, create a **setup.txt** file for the **Pre-Config** script and enter the values you created from steps 1, 2, and 3. The file syntax is a series of bash shell variables. For example:

```
XCE_USER=xcalar_user
```

```
XCE_GROUP=xcalar_group
#XCE_HOME (uses operating system standard)
XCE_ROOTDIR=xcalar_root
XCE_INSTALLDIR=xcalar_install
XCE_FIREWALL_CONFIG=firewall_install
XCE_KERBEROS_ENABLE=kerberos_install
```

Where:

- *xcalar_user* is the Xcalar Admin user name that was created in step 1.
- *xcalar_group* is the Xcalar Admin's group name that was created in step 1.
- *xcalar_root* is the path and directory name of the Xcalar Root Directory that was created in step 2.
- *xcalar_install* is the path and directory name of the Xcalar Install Directory that was created in step 3.
- *firewall_install* determines whether or not to configure the Linux software firewall. Where, a value of **1**, modifies the *iptables* or *firewalld* firewall settings to open the network ports used by Xcalar and a value of **0** or the line is not present, does not change any firewall settings.
- *kerberos_install* determines whether or not to install Kerberos software packages on the cluster. Where, a value of **0** does not install the Kerberos packages and a value of **1** or the line is not present, installs the Kerberos packages.

> **IMPORTANT:** The Kerberos software packages are required for accessing HDFS securely. If you already have Kerberos configured on the cluster or do not wish to install Kerberos dependencies, set `XCE_KERBEROS_ENABLE` to **0**.

For example:

```
XCE_USER=xcalar
XCE_GROUP=xcalar
#XCE_HOME (uses operating system standard)
XCE_ROOTDIR=/mnt/xcalar
XCE_INSTALLDIR=/opt/xcalar_install
XCE_FIREWALL_CONFIG=0
```

```
XCE_KERBEROS_ENABLE=1
```

5. Save the **setup.txt** file.

Configuring the Xcalar cluster nodes

Configuring the cluster nodes prepares the nodes for installation and sets up the shared storage area by:

- Installing the install package.
- Creating a Xcalar directory structure.
- Configuring the system and cluster nodes.
- Verifying the system and cluster nodes.

To configure the Xcalar cluster nodes:

1. As the Xcalar Admin user, download the Xcalar Configuration Tarball, by doing the following:
   a. On a computer that has browser access, go to the Xcalar customer portal:

      https://myxcalar.zendesk.com/

   b. Download the Configuration Tarball that is appropriate for the Linux operating system that was installed on all the nodes within the Xcalar cluster:

      `configuration_tarball-`*`version`*`-`*`xbuild`*`.`*`platform`*`.tar.gz`

      Where,

      - *version* is the Xcalar version number.
      - *xbuild* is the Xcalar Xcalar software build number for the Xcalar version number.
      - *platform* is the Linux operating system that is installed on your Xcalar cluster nodes.

      For example, `configuration_tarball-1.2.1-1044.tar.gz`.
2. As the Xcalar Admin user, configure the nodes within the Xcalar cluster, as follows:
   a. Copy the Configuration Tarball to the same directory on each node within the Xcalar cluster.
   b. Extract the Configuration Tarball, which creates a **config** subdirectory.

c. Copy the **setup.txt** file, which you created in step 4 of Creating a setup file, to the **config** subdirectory on each node within the Xcalar cluster.

3. As the superuser (*not* the Xcalar Admin), log in to each node within the Xcalar cluster and do the following:

   a. Go to the **config** subdirectory that was created in step 2.

   b. According to who you logged in as, configure each host by running one of the following commands:

      - `./pre-config.sh`
      - `sudo ./pre-config.sh`

      The **pre-config.sh** shell script downloads, installs, and configures the node in preparation for the Xcalar installation. For example, it sets SELinux to permissive mode.

   c. To set the **ulimits** configuration settings, log out and back into the node.

      > **IMPORTANT:** You must log out and log back in to the node after running the **pre-config.sh** configuration script. Failing to do so, will cause Xcalar installation errors.

   d. Verify the configuration by running the following command:

      `./verify.sh`

      The **verify.sh** shell script tests the node's configuration with a PASS or FAIL value. For example, "Does the Xcalar Install Directory exist?" For more information on the **verify.sh** tests, see Understanding the node configuration verification tests.

4. Log out of each node within the Xcalar cluster.

Preparing the Xcalar installation host

Must be completed for **option A** and **option B**.

You can run the Xcalar installation from any host server as long as it meets the following criteria:

- Runs using one of the Xcalar supported Linux operating systems.
- Can connect to all the nodes within the Xcalar cluster.

To prepare the Xcalar installation host:

1. Verify that you can establish a SSH connection from the installation host to all the Xcalar cluster nodes as the Xcalar Admin user.
2. Verify that the Xcalar supported web browser can access the installation host on port 8543.

Enabling Directory Services authentication

Must be completed for **option A**, optional for **option B**.

Xcalar Design uses the Lightweight Directory Access Protocol (LDAP) user authentication for verifying user access. During the Xcalar Deployment task the Install Wizard asks for information about your LDAP environment so that Xcalar Design can authenticate user access from the LDAP's user account entries.

Before installing Xcalar, collect and record the following LDAP environment values in the Information requirements table:

- LDAP URI: the server's name or IP address and the server's port number. For example, `ldap://Xcalarad.int.xcalar.com:389`.
- USER DN: the location in the LDAP server in which to search for user entries. For example, `dc=int,dc=xcalar,dc=net`.
- SEARCH FILTER: an LDAP filter that limits the returned number of user entries to one. For example, `(&(objectclass=user(userPrincipalName=%username%))`.
- SERVER KEY FILE: The path to the LDAP security certificates that identify the server.
- TLS usage: A true or false value that lets Xcalar know if the server accepts TLS requests. For example, `true`.
- Active Directory identity: A true or false value that lets Xcalar know if the server is an Active Directory server. For example, `true`.

For more information on LDAP Authentication, see Understanding the node configuration verification tests.

Installing Xcalar

This section describes how to install Xcalar.

Before installing Xcalar, read the following:

- Xcalar installation overview
- Xcalar system requirements
- Planning your Xcalar installation
- Xcalar pre-installation tasks

About installing Xcalar

A self-extracting shell archive (`xcalar-gui-tar-user-installer`) installs the Xcalar software stack.

The Xcalar installation tasks are as follows:

1. On your Installation host, download and run the Xcalar GUI Installer. For GUI installer instructions, see Running the Xcalar GUI installer on the installation host.
2. Install Xcalar Compute Engine and Xcalar Design to all the nodes within your Xcalar cluster.
    - For instructions on installing Xcalar software for the first time, see Installing Xcalar for the first time.
    - For instructions on upgrading Xcalar software, see Upgrading Xcalar.

Running the Xcalar GUI installer on the installation host

This section describes the procedures for running the Xcalar GUI installer.

The Xcalar GUI installer tar archive can be run by any user on the host server.

To run the Xcalar GUI installer on the Installation host:

1. Log in to the installation host as any user.
2. Verify that one of the recommended Linux operating systems is installed, by running one the following commands:

- **`cat /etc/os-release`**
- **`cat /etc/redhat-release`**

3. Download the Xcalar GUI Installer tar archive by doing the following:
   a. On the Installation host, open a terminal.
   b. Create a temporary directory (**temp_dir**).
   c. Go to the Xcalar customer portal, by opening a browser window from the computer on which the Xcalar supported web browser is installed and entering the following:

      https://myxcalar.zendesk.com/

   d. Download the Xcalar GUI Installer `xcalar-gui-tar-userinstaller-`*`version`*`-`*`build`*`.sh` tar archive to the **temp_dir** that was created in step b.

      Where:

      - *version* is the Xcalar version number.
      - *build* is the Xcalar software build number.
        For example, `xcalar-gui-tar-userinstaller-1.2.1-1044.sh`.

   e. Verify that the Xcalar GUI Installer has read, write, and execute permissions.
4. Run the Xcalar GUI Installer with the following command:

   `./xcalar-gui-tar-userinstaller-`*`version`*`-`*`build`*`.sh`

   If successful, the command print output displays the following message:

   ```
   Running installation shell archive, press Ctrl-C to stop
   ```

5. The following message is also displayed in the command print output:

   ```
   Please open your browser to one of:
   https://ip_address:8543
   https://FQDN_name:8543
   Or use the appropriate IP for where you ran this script from.
   Type Ctrl C to stop installer
   Linux_prodname System
   Xcalar trusted certificate not found
   All ready
   ```

   Where:

- *IP_address* is the IP address of the host on which the Xcalar GUI Installer is running.
- *FQDN_name* is the fully qualified domain name of the host on which the Xcalar GUI Installer is running.
- *Linux_prodname* is the Linux operating system that is running on the Installation host.

Installing Xcalar for the first time

This section describes the procedures for installing, deploying, and configuring Xcalar Compute Engine and Xcalar Design on a target cluster for the first time. For instructions on upgrading Xcalar, see Upgrading Xcalar.

To install Xcalar for the first time:

1. From the computer on which the Xcalar supported web browser is installed, open a browser window.
2. In the web browser URL field, enter the following URL:

   `https://ip_FQDN:8543`

   Where *ip_FQDN* is the IP address or FQDN name of the Installation host on which the Xcalar GUI Installer is running.

   > **TIP:** If the fully qualified domain name (FQDN) of the installation host is *host1.mycompany.com*, then enter **https://host1.mycompany.com:8543**.

3. Click **Enter**, which connects you to the Xcalar installer website.

   The Xcalar Wizard MAKE A SELECTION page appears.
4. From the options provided, select INSTALL WIZARD.
5. Click **NEXT**.

   The Xcalar Wizard STEP 1 ENTER LICENSE KEY page appears.
6. In the ENTER LICENSE KEY field, enter your Xcalar license key text exactly as provided and without trailing spaces.
7. Click **NEXT**.

   The Xcalar Wizard STEP 2 PRE-CONFIG STATUS page appears.

8. Choose one of the following:

> **TIP:** For information on how to answer the following, see Answering the PRE-CONFIG STATUS page questions during installing or upgrading.

- If the pre-configuration and validation scripts were successfully run on all the nodes within the cluster, select **Yes**.
- If the pre-configuration and validation scripts were not run on all the nodes within the cluster, select **No**.
  If you select **No**, during installation Xcalar configures your cluster nodes and validates that your cluster nodes are setup to work with Xcalar.

> **IMPORTANT:** If your cluster nodes are not configured to work with Xcalar the installation will stop. You can troubleshoot the issue from either the command output or the installer log files. For more information on the validation test, see Understanding the node configuration verification tests.

9. Click **NEXT**.
   The Xcalar Wizard STEP 3 SET UP XCALAR ROOT DIRECTORY page appears.

   Xcalar creates data, such as log files and configuration information. This data must reside in a shared storage location that has read, write, and execute permissions by all the nodes within the Xcalar cluster. By default, this shared directory, which is known as the Xcalar Root Directory, is located at **/mnt/xcalar**.

10. Choose one of the following:

> **NOTE:** Based on the option you selected in step 8, not all the following options are available.

- If you created and mounted a shared storage area, select **Existing Shared Storage Already Mounted** and in the PATH field that appears, enter the full path and directory name of the shared storage area (XCE_ROOTDIR value).

- If you created a shared storage area on an NFS server and did not mount it during pre-installation, select **Existing Shared Storage to be Mounted** and enter the following:
    a. In the PATH field, enter the full path and directory name of the shared storage area (XCE_ROOTDIR value).
    b. In the USERNAME field, enter the Xcalar Admin user name (XCE_USER value).
    c. In the GROUP field, enter the default group name (XCE_GROUP value).
- If you prefer the Xcalar GUI installer to create and mount a NFS shared storage area on all the nodes in the cluster, select **Xcalar Deployed Shared Storage**.
  A shared storage area is created and deployed during installation.

11. Click **NEXT**.
    The Xcalar Wizard STEP 4 SET UP LDAP page appears.

    Xcalar uses the Lightweight Directory Access Protocol (LDAP) for authenticating users when they log in to Xcalar.

12. Choose one of the following:

> **NOTE:** Based on the option you selected in step 8, not all the following options are available.

- If you are not currently using LDAP, select **Xcalar Deployed** and enter following:
    a. In the DOMAIN NAME field, enter your company's web address.
    b. In the NEW PASSWORD field, enter the password for the Xcalar Admin user.
    c. In the CONFIRM PASSWORD field, re-enter the password of the Xcalar Admin user.
    d. In the COMPANY NAME field, enter the full name of your company.
- If you are using LDAP, select **Existing LDAP** and do the following:
    a. From the LDAP options, select your current LDAP protocol.
    b. In the LDAP URI field, enter the LDAP URL that is used to contact the LDAP Server.

c. In the USER DN field, enter the location in the LDAP server in which to search for user entries. For example,
`cn=Users,dc=int,dc=xcalar,dc=net`.

d. In the SEARCH FILTER field, enter the LDAP filter that is used to limit the returned number of user entries to one.
For example,
`(&(objectclass=user)(userPrincipalName=%username%))`.

e. In the SERVER KEY FILE field, enter the path to the LDAP security certificates that identify the server.

f. (AD option only) In the AD USER GROUP field, enter the name of the Active Directory's user group. For example,
Xce User

g. (AD option only) In the AD ADMIN GROUP field, enter the name of the Active Directory's administrator group.

h. (Optional AD option only) In the AD DOMAIN field, enter the domain name of your Active Directory, which is used as an optional default domain name. For more information, see Optional Xcalar LDAP group parameters.

i. (Optional AD option only) If your Active Directory's top level group contains sub groups, select the **Enable Group Subtree Search** checkbox. This enables subgroup LDAP searching.

The Xcalar Admin can also enable this setting in Xcalar Design from the LOGIN CONFIGURATION page.

j. If you require secure LDAP connections, from the **Transportation Layer Security (TLS)** section, select **Enable LDAP TLS**.

> **NOTE:** If your LDAP server supports TLS, Xcalar recommends selecting the **Enable LDAP TLS** option.

For more information on how to fill out the LDAP fields, see Understanding the LDAP fields.

13. Click **NEXT**.
The Xcalar Wizard STEP 5A SET UP NODES page appears.

14. In the **Enter the number of nodes in your cluster and press Enter** field, enter the number of nodes that reside in your computer cluster.
15. Click **NEXT**.
    The Xcalar Wizard STEP 5A SET UP NODES page refreshes to display the connection requirements for each of the nodes within your Xcalar cluster.
16. In the STEP 5A **Hostnames** section, enter the following for each node:
    a. In the PUBLIC field, enter the IP address or the FQDN.
    b. (Optional) In the PRIVATE field, enter the IP address or the FQDN.
    For more information on how to fill out the Xcalar PUBLIC and PRIVATE field values, see Understanding the Xcalar Public and Private IP addresses.

> **IMPORTANT:** If you install Xcalar on a cloud platform, verify that the FQDNs can be resolved by the internal DNS resolver.

17. In the STEP 5B **Installation Directory** section, enter the Xcalar Install Directory path and directory name (XCE_INSTALLDIR value).
18. In the STEP 5C **Serialization/Deserialization Directory** section, enter the path and directory name of your Demand Paging area that will be used to store temporary Xcalar tables when the memory swapping space is low.
19. (Optional) To send daily support data to Xcalar, in the STEP 5D **Support Bundles Generation** section, select the **Enable daily support bundles** checkbox.

    You can choose to have support data from your Xcalar environment sent to Xcalar daily, which is used by the Xcalar support team to understand problems that you may be experiencing with Xcalar.

    The support bundle includes, information from recovery, UDF, sessions, and dataflow directories, log and configuration files, HTTPs server logs and system data, and CPU and memory information.

> **NOTE:** The exact information included in the support bundle may vary according to the access permissions granted to Xcalar.

The Xcalar Admin can also enable this setting in Xcalar Designfrom the **Configure Parameters** page.

20. In the STEP 5E **Credentials** section, enter the following:
    a. In the USERNAME field, enter the Xcalar Admin user name (XCE_USER value).
    b. In the SSH PORT field, enter the secure shell (SSH) port number. By default, this number is **22**.
21. In the **Password Options** section, do one of the following:
    - For authenticating access to all cluster nodes by Xcalar with a password, select **Password** and in the PASSWORD field, enter the password for the Xcalar Admin user.
    - For authenticating access to all cluster nodes by Xcalar with SSH using your SSL private key, select **SSH Key** and in the text field enter your SSL private key.
    - For authenticating access to all cluster nodes by Xcalar with SSH using an existing SSH user, select **SSH User Settings**.
22. Click **INSTALL**, which deploys Xcalar Compute Engine and Xcalar Design on all the nodes within the Xcalar cluster.
23. When the installation is completed, either click LAUNCH XD or connect to Xcalar Design on any of the Xcalar cluster nodes with the following URL:

    `https://node_name:8443`

    Where *node_name* is the IP address or FQDN of the Xcalar cluster node on which you logged in to.

Upgrading Xcalar

This section provides instructions for upgrading Xcalar.

Before upgrading Xcalar, read the following:

- Xcalar installation overview
- Xcalar system requirements
- Planning your Xcalar installation
- Xcalar pre-installation tasks

About upgrading Xcalar

This section discusses optional and mandatory tasks that are performed before upgrading Xcalar.

Optional tasks before upgrading

Before upgrading to a new Xcalar software release, you can choose to relocate your existing shared storage area (XCE_ROOTDIR) to another location.

> **NOTE:** Xcalar recommends that you relocate your existing shared storage area before upgrading.

During the upgrade the Xcalar GUI installer copies the following to the new location of your shared storage:

- Xcalar UDF and plug-in information.
- Xcalar Design configurations, which are contained in the **default.cg** configuration file.

> **IMPORTANT:** Any new configuration parameters associated with a new Xcalar release are not merged into the existing **default.cg** configuration file. You can either add them into the existing configuration file or copy your old configurations over to the new configuration file.

> A sample configuration file with the latest parameters is installed at **/install/etc/xcalar/default.cg.new**.

Mandatory tasks before upgrading

Before upgrading to a new Xcalar software release, do the following

- Upgrade to the latest LINUX patch release, which is highly recommended by Xcalar.
- Schedule the upgrade and inform your users of the Xcalar service interruption.

  > **NOTE:** During the upgrade the Xcalar GUI installer shuts down and restarts Xcalar.

- Perform a cold copy of existing files.
- Verify your cluster configuration by running the following on all nodes within your Xcalar cluster:

  ```
  ./verify.sh
  ```

  If an issue is encountered, rerun the **pre-config.sh** shell script.

  For more information, see Configuring the Xcalar cluster nodes.

  > **NOTE:** If you choose **No** in step 10 of Upgrading Xcalar steps, the Xcalar GUI installer will run the **pre-config.sh** and the **verify.sh** scripts for you.

About automatic rollback

During the Xcalar upgrade, if there is any failure prior to the Xcalar GUI installer restarting Xcalar, your software will rollback to the previous version.

Upgrading Xcalar steps

This section describes the procedures for upgrading and configuring the Xcalar Compute Engine and Xcalar Design. For instructions on installing Xcalar on a target cluster for the first time, see Installing Xcalar for the first time.

To upgrade Xcalar:

1. Verify that an existing version of the Xcalar software exists and that the Xcalar cluster is shut down.
2. Verify that the pre-installation and mandatory upgrade tasks are completed.
3. Run the Xcalar GUI installer. For more information, see Running the Xcalar GUI installer on the installation host.
4. From the computer on which the Xcalar supported browser is installed, open a browser window.
5. In the web browser URL field, enter the following URL:

   `https://`*`ip_FQDN`*`:8543`

   Where *ip_FQDN* is the IP address or FQDN name of the Installation host on which the Xcalar GUI Installer is running.

   > **TIP:** If the fully qualified domain name (FQDN) of the installation host is *host1.mycompany.com*, then enter **https://host1.mycompany.com:8543**.

6. Click **Enter**, which connects you to the Xcalar installer website.

   The Xcalar Wizard MAKE A SELECTION page appears.
7. From the options provided, select UPGRADE WIZARD.
8. Click **NEXT**.

   The Xcalar Wizard STEP 1 UPDATE LICENSE KEY page appears.
9. Do one of the following:
   - If your license key is current, uncheck the **Upgrade License Key** check box and click **NEXT**.
   - If your license key has expired, do the following:
     a. Verify that you have a new Xcalar license key from: https://myxcalar.zendesk.com/.
     b. Verify that the **Upgrade License Key** checkbox is checked.

c. In the UPGRADE LICENSE KEY field, enter your Xcalar license key text exactly as provided and without trailing spaces.

d. Click **NEXT**.

The Xcalar Wizard STEP 2 PRE-CONFIG STATUS page appears.

10. Choose one of the following:

> **TIP:** For information on how to answer the following, see Answering the PRE-CONFIG STATUS page questions during installing or upgrading.

- If the pre-configuration and validation scripts were successfully run on all the nodes within the cluster, select **Yes**.
- If the pre-configuration and validation scripts were not run on all the nodes within the cluster, select **No**.
  If you select **No**, during installation Xcalar configures your cluster nodes and validates that your cluster nodes are setup to work with Xcalar.

> **IMPORTANT:** If your cluster nodes are not configured to work with Xcalar the installation will stop. You can troubleshoot the issue from either the command output or the installer log files. For more information on the validation test, see Understanding the node configuration verification tests.

11. Click **NEXT**.
    The Xcalar Wizard upgrading node credential page appears, which displays connection requirements for the nodes within your Xcalar cluster.
12. In the STEP 3A **Enter Node IP** section, enter the IP address or the FQDN for one of the nodes within your Xcalar cluster.
    For more information on how to fill out the Xcalar PUBLIC and PRIVATE field values, see Understanding the Xcalar Public and Private IP addresses.
13. In the STEP 3B **Installation Directory** section, enter the current Xcalar Install Directory path and directory name (XCE_INSTALLDIR value).

14. In the STEP 3C **Credentials** section, enter the following:
    a. In the USERNAME field, enter the Xcalar Admin user name (XCE_USER value).
    b. In the SSH PORT field, enter the secure shell (SSH) port number. By default, this number is **22**.
15. In the **Password Options** section, do one of the following:
    - For authenticating access to all cluster nodes by Xcalar with a password, select **Password** and in the PASSWORD field, enter the password for the Xcalar Admin user.
    - For authenticating access to all cluster nodes by Xcalar with SSH using your SSL private key, select **SSH Key** and in the text field enter your SSL private key.
    - For authenticating access to all cluster nodes by Xcalar with SSH using an existing SSH user, select **SSH User Settings**.
16. Click **DISCOVER**, which verifies the existence of a previous Xcalar installation from the node information you provided.

    The Xcalar Wizard set up Xcalar root directory page appears and lists the current Xcalar Root directory's mount path and server IP address.
17. Do one of the following:
    - If you decided not to change the location of your shared storage area (XCE_ROOTDIR), verify the list, click **NEXT**, and go to step 19.
    - If you changed the location of your shared storage area (XCE_ROOTDIR), go to step 18.
18. (Optional) If you changed the location of your shared storage area (XCE_ROOTDIR), select the **Change Xcalar Root** check box.
    a. In STEP 4A , do one of the following:

> **NOTE:** Based on the option you selected in step 10, not all the following options are available.

    - If you created and mounted a shared storage area, select **Existing Shared Storage Already Mounted** and in the PATH field that appears, enter the full path and directory name of the shared storage area (XCE_ROOTDIR value)

- If you created a shared storage area on an NFS server and did not mount it during installation, select **Existing Shared Storage to be Mounted** and enter the following:
    a. In the PATH field, enter the full path and directory name of the shared storage area (XCE_ROOTDIR value).
    b. In the USERNAME field, enter the Xcalar Admin user name (XCE_USER value).
    c. In the GROUP field, enter the default group name (XCE_GROUP value).
- If you prefer the Xcalar GUI installer to create and mount a NFS shared storage area on all the nodes in the cluster, select **Xcalar Deployed Shared Storage**. A shared storage area is created and deployed during the upgrade.

b. In STEP 4B, do one of the following:

- If you require the Xcalar GUI installer to copy your existing data over to the shared storage area, select **Yes, I want Xcalar to copy the data for me**.
- If you do not require the Xcalar GUI installer to copy your existing data over to the shared storage area, select **No, I want to copy the data myself**.

> **IMPORTANT:** If you are copying your existing data over to the shared storage area, it must be completed before upgrading.

19. Click **NEXT**.
    The Xcalar Wizard STEP 5 upgrade page appears.
20. Verify the hostnames of your cluster nodes.
21. Click **UPGRADE**, which upgrades Xcalar Compute Engine and Xcalar Design on all the nodes within the Xcalar cluster.

> **TIP:** You can check the status of the upgrade from the **Status** section next to each node's hostname.

22. When the installation is completed, either click LAUNCH XD or connect to Xcalar Design on any of the Xcalar cluster nodes with the following URL:

`https://`*`node_name`*`:8443`

Where *node_name* is the IP address or FQDN of the Xcalar cluster node on which you logged in to.

Uninstalling Xcalar

This section provides instructions for uninstalling Xcalar.

About uninstalling Xcalar

Xcalar removes all the Xcalar software on all your cluster nodes. The shared storage area, LDAP, and user data are not removed.

Before uninstalling Xcalar, you must shut down your system.

Uninstalling Xcalar steps

To uninstall Xcalar:

1. Verify that the Xcalar cluster is shut down.
2. Run the Xcalar GUI installer. For more information, see Running the Xcalar GUI installer on the installation host.
3. From the computer on which the Xcalar supported web browser is installed, open a browser window.
4. In the web browser URL field, enter the following URL:

   `https://ip_FQDN:8543`

   Where *ip_FQDN* is the IP address or FQDN name of the Installation host on which the Xcalar GUI Installer is running.

   > **TIP:** If the fully qualified domain name (FQDN) of the installation host is *host1.mycompany.com*, then enter **https://host1.mycompany.com:8543**.

5. Click **Enter**, which connects you to the Xcalar installer website.

   The Xcalar Wizard MAKE A SELECTION page appears.

6. From the options provided, select UNINSTALL WIZARD.

7. Click **NEXT**.

   The Xcalar Wizard STEP 1 uninstalling node credential page appears, which displays connection requirements for the nodes within your Xcalar cluster.

8. In the STEP 1A **Enter Node IP** section, enter the IP address or the FQDN for one of the nodes within your Xcalar cluster.

9. In the STEP 1B **Installation Directory** section, enter the current Xcalar Install Directory path and directory name (XCE_INSTALLDIR value).

10. In the STEP 1C **Credentials** section, enter the following credentials for the node you provided in step 8:

    a. In the USERNAME field, enter the Xcalar Admin user name (XCE_USER value).

    b. In the SSH PORT field, enter the secure shell (SSH) port number. By default, this number is **22**.

11. In the **Password Option** section, do one of the following:

    - For access to all cluster nodes by Xcalar with a password, select **Password** and in the PASSWORD field, enter the password for the Xcalar Admin user.
    - For access to all cluster nodes by Xcalar with SSH using your SSL private key, select **SSH Key** and in the text field enter your SSL private key.
    - For access to all cluster nodes by Xcalar with SSH using an existing SSH installation, select **SSH User Settings**.

12. Click **DISCOVER**, which verifies a Xcalar installation from the node information.

    The Xcalar Wizard STEP 2 uninstall page appears.

13. Verify the hostnames of your cluster nodes.

14. Click **UNINSTALL**, which uninstalls Xcalar Compute Engine and Xcalar Design on all the nodes within the Xcalar cluster.

Xcalar installation reference

This section provides installation reference content.

Understanding the node configuration verification tests

The following table describes the node configuration verification shell script (**verify.sh**) tests:

Test	Description
`Platform Support Test:`	Tests that the Xcalar cluster node runs the Xcalar supported Linux operating system.
`User xcalard exists:`	Tests that the Xcalar Admin user name exists.
`Group xcalard exists:`	Tests that the Xcalar Admin group exists and that the Xcalar Admin user name is a member of the Xcalar Admin group.

`* Install directory tests`
`* Xcalar install directory exists:`
`* Install directory owner is xcalard:`
`* Install directory group is xcalard:`
	Tests that all nodes within the Xcalar cluster contain the Xcalar Install Directory, that the Xcalar Admin owns the Xcalar Install Directory, and that the Xcalar Install Directory has Xcalar Admin group access.

`Xcalar install directory test results:`	The results of all the Install directory tests.

Test	Description

`Shared data directory tests`
`* Xcalar shared data directory exists:`
`* Data directory owner is xcalard:`
`* Data directory group is xcalard:`
`* Data directory size ( >= 1TB ):`
	Tests that the Xcalar Root Directory exists, that the Xcalar Admin owns the Xcalar Root Directory, that the Xcalar Root Directory has Xcalar Admin group access, and that the Xcalar Root Directory's disk space size is greater than or equal to 1 TB.

`Xcalar install directory test results:`	The results of all the root directory tests.
`System RPM dependencies:`	Tests that all system repository dependencies are installed. Missing dependencies are listed.
`Xcalar RPM dependencies:`	Tests that all Xcalar generated dependencies are installed. Missing dependencies are listed.

Test	Description

`Xcalar limits tests:`
`* Test of -c:`
`* Test of -u:`
`* Test of -n:`
`* Test of -l:`
	Tests the limits that are applied to the node's processing resources.
	
	Where,
	
	-c, is the maximum file size that you can have open.
	
	-u, is the maximum number of processes that can be run by an individual user.
	
	-n, is the maximum number of files that can be open during a session.
	
	-l, is the maximum number of bytes of memory that is locked in RAM and that cannot be paged out.
	
	> **NOTE:** this number can reduce the amount of memory that is available for other processes.
	
	The values are set in the **/etc/security/limits.conf** configuration file.
	
	> **IMPORTANT:** After making changes to the **limits.conf** configuration file, you must close all active session windows, log out of the node, and log back in to the node.

`Xcalar limit test results:`	The results of all the limit tests.

`Xcalar sysctl tests:`
`* Test of kernel.core_pattern:`
`* Test of fs.suid_dumpable:`
`* Test of vm.swappiness:`
	Sets where the core dump file is generated, tests if the node can create core dumps from the file system, and tests how much and how often your Linux kernel copies RAM content to the swap space.

Test	Description
`Xcalar sysctl test results`	The results of all the sysclt tests.
`SELinux mode is PERMISSIVE:`	Tests that SELinux is set to Permissive mode.
`Testing transparent hugepage defrag:`	Tests that hugepage defragmentation is disabled.
`Testing transparent hugepage khugepaged defrag:`	Tests that hugepage khugepaged defragmentation is disabled.
`Testing total amount of free RAM:`	Tests that the node has the Xcalar supported RAM size.

`* Testing space on /dev/shm:`
`* Total amount of /dev/shm space:`
`* Amount of free /dev/shm space:`
	Tests the amount of shared memory space.
	Tests the node's shared memory size.
	Tests the node's available shared memory space.

`Xce /dev/shm test results:`	The results of all the shared memory tests.
`Testing swap size (>= 2x amount of RAM:`	Tests that the swap size is less than or equal to two times the amount of RAM.

Understanding the Xcalar Public and Private IP addresses

Xcalar uses both Public and Private IP addresses or the fully qualified domain names (FQDNs) for deploying Xcalar Compute Engine and Xcalar Design on the nodes within the Xcalar cluster.

Where:

- PUBLIC, is the IP address or FQDN used by the Xcalar GUI Installer to install software on the cluster.
- PRIVATE, is the IP address or FQDN used by the Xcalar cluster nodes to communicate with each other if they are different from the PUBLIC IP addresses or FQDNs.

For example, **A** and **B** contain the IP addresses that are used by a set of nodes within a Xcalar cluster to communicate with other devices and between the nodes in the Xcalar cluster.

A	192.168.1.2 192.168.1.3
B	10.0.1.34 10.0.1.35

- **Case 1**: If the Xcalar GUI Installer is installing software on node hosts on another network that uses **A**'s IP addresses and where each node communicates with each other with **B**'s IP addresses, then both Public and Private IP addresses are used. In this case, you would enter **A**'s IP addresses in the PUBLIC field and **B**'s IP addresses in the PRIVATE field.
- **Case 2**: If the Xcalar GUI Installer is run on a host that has an IP address of 10.0.1.36 and where each node communicates with each other with **B**'s IP addresses, then only **B**'s IP addresses are used. In this case, you would enter **B**'s IP addresses in the PUBLIC field.

Understanding the LDAP fields

The following table describes the fields in the SET UP LDAP page.

Field	Description
LDAP URI	Specifies the protocol, host name (or IP address), and port where the LDAP server (Active Directory or OpenLDAP) is located. The protocol can be either ldap (for unencrypted LDAP) or ldaps (for encrypted, secure LDAP). The standard network port for the LDAP protocol is 389. The following is an example of the input for this field: `ldap://xcalarad.int.xcalar.com:389`

Field	Description

USER DN	The value depends on how the LDAP server authenticates:
	• For servers, such as OpenLDAP, this field presents the complete Distinguished Name (DN) of the LDAP entry, where user information, including the user password, can be found and used for LDAP server authentication. Xcalar supplies the **%username%** macro that is replaced with the user name that the user enters during the Xcalar Design login.
	For example, if you enter the **%username%** macro in the USER DN, such as:
	`mail=%username%,ou=People,dc=xcalar,dc=com`
	When the user enters jsmith@xcalar.com to log in to Xcalar Design, it resolves to the following DN:
	`mail=jsmith@xcalar.com,ou=People,dc=xcalar,dc=com`
	• For servers, such as an Active Directory, authentication is completed outside the LDAP directory. This DN indicates the LDAP location where LDAP entries for all users can be found and is generally of this format:
	`dc=int,dc=xcalar,dc=>net`

Field	Description

SEARCH FILTER	Specifies an authentication filter that is used to reduce the search space to find user information or limit Xcalar access to selected groups of users. The **%username%** macro can also be used in the SEARCH FILTER. How you specify the filter depends on your server:
	• On an Active Directory server, you can use the following filter:
	`(&(objectclass=user)(userPrincipalName=%username%))`
	This filter limits the search for user information to user objects, where the **userPrincipalName** name matches the Xcalar Design **login** name.
	Authentication fails if at least one user object is not found.
	You can specify additional filters to limit Xcalar access to users whose entries have other attributes.
	• On other LDAP servers, such as OpenLDAP, you can limit Xcalar access to members of a group. Create a **groupOfUniqueNames** object with a **uniqueMember** value for every Xcalar user specified by the USER DN.
	For example, to specify a group and its membership:
	a. **groupOfUniqueNames** object, which contains the appropriate **uniqueMember** values:
	`cn=xceUsers,ou=Groups,dc=xcalar,dc=com`
	b. Then specify the following filter to limit Xcalar access:
	`(memberof=cn=xceUsers,ou=Groups,dc=xcalar,dc=com)`

SERVER KEY FILE	Specifies the path to your LDAP security certificate.

Field	Description
AD USER GROUP	Specifies the group name of the Active Directory's Xcalar users for authenticating user access by Xcalar: • If you select the **Enable Group Subtree Search** check box, enter the full LDAP Distinguished Name for the top level user group. For example, `cn=GlobalXcalarUsers,dc=int,dc=somecompany,dc=com` **IMPORTANT**: You must enter a valid value. • If you do not select the **Enable Group Subtree Search** check box, you do not have to enter a value. The default User group name (Xce User) is used. Create the group Xce User on your Active Directory server and add at least one user. • If you do not want to use the default User group name (Xce User), enter a valid Active Directory user group name.
AD ADMIN GROUP	Specifies the group name of the Active Directory's Xcalar administrators for authenticating administrator access by Xcalar: • If you select the **Enable Group Subtree Search** check box, enter the full LDAP Distinguished Name for the top level administrator group. For example, `cn=GlobalXcalarAdmins,dc=int,dc=somecompany,dc=com` **IMPORTANT**: You must enter a valid value. • If you do not select the **Enable Group Subtree Search** check box, you do not have to enter a value. The default Admin group name (Xce Admin) is used. Create the group Xce Admin on your Active Directory server and add at least one user. • If you do not want to use the default Admin group name (Xce Admin), enter a valid Active Directory administrator group name.

Field	Description
AD DOMAIN	Specifies the domain name of the Active Directory. For more information, see Optional Xcalar LDAP group parameters.

Optional Xcalar LDAP group parameters

This section discusses the Xcalar LDAP optional parameters.

1. Xcalar classifies users as one of the following:

   - An authentic Xcalar user who is entitled to access Xcalar.
   - An authentic Xcalar user who is entitled to access Xcalar and has system administrative privileges.

   By default, Xcalar authenticates user access by checking that the user is a member of one of the following Active Directory Xcalar groups:

   - **Xce User**, for regular Xcalar users.
   - **Xce Admin**, for Xcalar admin users.

   The Active Directory LDAP connector allows you to assign the same user and administrator roles to existing or new Active Directory server groups, by using the following LDAP parameters:

   - **AD USER GROUP**, which changes the Xce User group name to an existing or new Active Directory group.
   - **AD ADMIN GROUP**, which changes the Xce Admin group name to an existing or new Active Directory group.

   > **NOTE:**If you require all users to be admins, the same group name can be entered in both fields.

2. Larger enterprise customers may prefer to divide the responsibilities for Xcalar access and administrator privilege across multple organizations, rather than administer Xcalar users and admins as single groups. Active Directory allows groups to be members of other groups. Xcalar can detect User and Admin access levels in as many groups as your

Active Directory supports, providing that the Xcalar Active Directory connector points to the top level user and admin group that are at the root of a membership tree containing all the other users and groups.

3. By default, the Active Directory LDAP connector requires that when a user logs in to Xcalar Design they enter their user name followed by their Windows domain name. For example, `username@some.msn.domain.com`.

   However, you can configure a default domain, with the **Set-AdDomain** setting, where the user is not required to enter a domain name during log in.

Understanding the Xcalar Active Directory LDAP authentication

The Lightweight Directory Access Protocol (LDAP) is a protocol used by Microsoft Active Directory server, which adds user access security authentication for the Xcalar Design Web user interface.

Active Directory authentication

The Microsoft Active Directory service manages user authentication, shared storage, printing, and other services. Active Directory manages authentication with the Kerberos and the LDAP protocols.

The authentication process for the Xcalar Active Directory LDAP connector consists of four steps:

1. When an LDAP client provides a user name and a password, the Active Directory service verifies that the user name and password are valid. The LDAP connection from the connector is bound, allowing the connector to access the contents of the Active Directory LDAP schema.
2. User information like **first name**, **last name**, and **e-mail address**, which is displayed on the Xcalar Design user interface, is located by the connector from Active Directory. To do this, the connector performs an LDAP search using the user distinguishing name (USERDN). The choice of USERDN depends on how Active Directory is configured. A common starting point for user information is the LDAP version of the Windows Domain. For example, the USERDN for the **int.xcalar.net** domain is:
   `dc=int,dc=xcalar,dc=net`
3. The LDAP schema contains records for multiple users, as well as groups, printers, and

other administrative information. As Xcalar Design displays information for a single LDAP record, the LDAP search request is filtered to return only those results that match the conditions set by the filter for a single record from the LDAP server. A common filtering strategy for Active Directory is to filter by user name and the type of the LDAP record. These are represented in the LDAP schema as the **userPrincipalName** and **objectClass** fields. For example, a common Active Directory filter looks like this:

```
(&(objectClass=user)(userPrincipalName=%username%)
```

The **%username** is a macro in the Xcalar LDAP connector that is replaced by whatever the user enters in the **Username** field of the Xcalar Design log in screen.

Depending on how Active Directory is configured, other filters can be used. For more information to determine what will work best for you, see the Active Directory documentation, as well as, inspect your LDAP schema on your server(s) for the Windows Domain.

4. After a single record is returned by the filtered LDAP search, the connector determines the user Xcalar privileges by checking if the user belongs to (at most) two Active Directory groups:
    - Membership in a group specified by the connector parameter adUserGroup (default: **Xce User**)
    - Membership in a group specified by the connector parameter adAdminGroup (default: **Xce Admin**)

Troubleshooting

This section provides guidelines when encountering issues with the Xcalar installation. If after reading this section problems still exist, contact Xcalar technical support.

Licensing issues

The following table describes the Xcalar license key error messages:

Error Message	Solution
Invalid license key. The license key that you have entered is not valid. Please check the key and try again	The license key is not in the correct format. You might have inadvertently included illegal characters or spaces. Copy and paste the license key again, taking care to copy the entire string.
Invalid server license key. The license key that you have entered is not valid. Please check the key and try again.	The license key is in the correct format but is invalid. Copy and paste the license key again, taking care to copy the entire string. Verify that there are no trailing spaces at the end. Also, verify that the license key is the one issued for this cluster.

Cluster issues

The following table describes the Xcalar cluster settings error messages:

Error Message	Solution
NFS Server Invalid. You must provide a valid NFS Server IP or FQDN	The Install Wizard cannot locate the server for the file system on which you want to mount the Xcalar Root Directory. Make sure that you entered the correct IP address or the FQDN name. Also, make sure that there are no connectivity problems between the installation host and the NFS server.

Error Message	Solution
No hosts. You must install on at least 1 host	You have not entered any information about the nodes. You must provide an IP address or FQDN name for at least 1 node.
Empty Username / Port. Your SSH user name / port cannot be empty	You must fill out both the USERNAME and SSH PORT fields. Otherwise, the Install Wizard cannot copy files to the specified nodes.
Empty Password. For passwordless SSH, upload your SSH key	You must provide a password used for SSH connections to the nodes. If no SSH password is provided, enter the SSH key.
Empty SSH Key. Your SSH key is generally located at **~/.ssh/id_rsa**	You have not provided the SSH key, which is necessary for SSH connections that do not use a password. Copy and paste the key from the file where the key is stored.
No public name. You must provide a public name for all private names	You have not provided the public address for the node. Even though the nodes use private IP addresses for internal communication, you must enter the public IP addresses.
Private / Public Hostname Error. Either provide private hostnames / IPs for all or none of the hosts	You have provided one or more private addresses, but have not provided public hostnames for all of the nodes. Public names for all nodes are mandatory.
Duplicate Hosts. Public Hostname is a duplicate	You have entered a duplicate public hostname for a node. Public hostnames must be unique.
Duplicate Hosts. Private Hostname is a duplicate	You have entered a duplicate private hostname for a node. Private hostnames must be unique.

Error Message	Solution
mount.nfs: requested NFS version or transport protocol is not supported	An NFS server firewall issue exists. The port for rpc.mountd, RPC portmap, or a related service that needs to be opened in the firewall is currently blocked. Make sure that the firewall service on the first node is correctly configured.

LDAP issues

The following table describes the Xcalar LDAP configuration error messages:

Error Message	Solution
Blank arguments. Please populate all fields	You chose an existing LDAP server but did not provide the configuration information about LDAP. Fill out the required information so that Xcalar can use the LDAP server for user authentication.
Passwords different, Passwords must be the same	The password entered for confirmation is different from the password entered the first time. Re-enter the password correctly.
AD or OpenLDAP. Please select AD or OpenLDAP	You chose an existing LDAP server but did not specify your directory service (Active Directory or OpenLDAP). You must specify your directory service.
TLS. Please select whether to use TLS	You chose an existing LDAP server but did not specify if Xcalar can use TLS. You must specify if your LDAP server uses TLS.

Xcalar application initial log in

The Xcalar Design web user interface is accessed through an encrypted (secure) HTTPS connection. At the initial login, your web browser may not recognize the server and displays the **This Connection is Untrusted** warning message. Click **Confirm Security Exception** to proceed.

> **Note:** This message appears when using a self-signed certificate.

Copyright and trademark information