opentext™

OpenText™ eDirectory CE 24.4 (v9.3)

Security Guide

January 2025

Legal Notice

Copyright 2009 - 2024 Open Text All rights reserved.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About this Book and the Library 5

1 Deployment Considerations 7

Protecting OpenText eDirectory Through Firewall . . . 7
Protecting OpenText eDirectory Data and Storage . . . 7
Protecting OpenText eDirectory DIB . . . 7
Protecting Data in Transit . . . 8

2 Restricting Access to OpenText eDirectory Server 9

Security Considerations for OpenText eDirectory Server Hosting Machine . . . 9
Security Considerations for Operating Systems . . . 9
Restricting Access to OpenText eDirectory Server . . . 10
Security Considerations for OpenText eDirectory . . . 10
Considerations for Access to Resources . . . 11
Considerations for OpenText eDirectory Rights to ACLs . . . 11
Considerations for Public Key Infrastructure (PKI) Services . . . 12
Considerations for Novell International Cryptographic Infrastructure (NICI) . . . 12
Considerations for Auditing OpenText eDirectory Events . . . 12
Password Security Recommendations . . . 13

3 Security Considerations for Implementing Authentication 15

Server Authentication . . . 15
Securing Administrator Accounts . . . 15

4 Secure Communication and Authorization 19

5 Security Considerations For OpenText eDirectory Privileges 21

6 Securing OpenText eDirectory on Cloud 25

About this Book and the Library

The *Security Guide* provides configuration guidelines to network administrators. These guidelines can help to enhance the security of an OpenText™ eDirectory CE 24.4 (v9.3) environment. The first half of the guide focuses on tasks for configuring the OpenText eDirectory components, along with examples and references. The remaining part of the guide provides additional information about the concepts described in prior sections.

Administrators should consult the product documentation (listed in "Other Information in the Library"), OpenText eDirectory TIDS, Cool Solutions, Knowledge Base articles, and stay up to date on patches and versions of both OpenText eDirectory and the host operating system on regular basis.

Intended Audience

This book is intended for network administrators who are familiar with installing, managing, and configuring the OpenText eDirectory product.

Other Information in the Library

The library provides the following information resources:

- OpenText eDirectory Product Documentation (https://www.netiq.com/documentation/edirectory-93/)
- REST API Documentation: Resource Server Mode (https://www.netiq.com/documentation/edirectory-93/resources/REST_ResourceServerMode/) and Simple Login Mode (https://www.netiq.com/documentation/edirectory-93/resources/REST_SimpleLoginMode/).

For information about the OpenText eDirectory management utility, see the *OpenText Identity Console Administration Guide (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/bookinfo.html)*

1 Deployment Considerations

This section explains basic considerations to make the OpenText eDirectory deployment more secure.

- "Protecting OpenText eDirectory Through Firewall" on page 7
- "Protecting OpenText eDirectory Data and Storage" on page 7

Protecting OpenText eDirectory Through Firewall

OpenText eDirectory should be used along with firewalls. A firewall is essential for ensuring the effective protection of network-based services. This can be built into the host operating system or obtained through third-party software. It is highly recommended to use a firewall on the host operating system to restrict network resource access available from the host system. Without it, operating systems may not be able to effectively limit access to network services.

The OpenText eDirectory tree Certificate Authority (CA) hosting system should have firewall rules assigned to it, and the following ports should be enabled on the platform supported by OpenText eDirectory:

Name	Port Range	Action	Description
SSH	TCP 22	ALLOW	Allows SSH traffic from SSH Proxy.
NCP	TCP 524	ALLOW	Allows NCP traffic for OpenText eDirectory in backend subnet.
LDAPS	TCP 636	ALLOW	Allows secured LDAP traffic in backend subnet.
SLP	Any 427	ALLOW	Allows SLP traffic in the backend subnet.
All Traffic	All	DENY	Denies all inbound traffic.

Protecting OpenText eDirectory Data and Storage

- "Protecting OpenText eDirectory DIB" on page 7
- "Protecting Data in Transit" on page 8

Protecting OpenText eDirectory DIB

Read through the following recommendations to protect your OpenText eDirectory database or Directory Information Base (DIB):

- Always create an encrypted attribute policy to secure sensitive data. For more information, see Encrypting Data in OpenText eDirectory.

- When using tools like `ndscheck` and `nmasinst`, avoid entering passwords in the command line. Instead, wait for the password prompt or use `ndspassstore` utility to provide password to the tools. For more information, see Setting the sadmin Password.
- It is important to safeguard NMAS data, which includes password, secret store, configuration store, and more. To ensure maximum protection, it is recommended to use AES 256-bit key.
- All Tree partitions should be replicated across multiple servers.

  With only one server storing and serving an OpenText eDirectory replica, a server failure would result in the loss of the partition and possibly serious consequences for the rest of the OpenText eDirectory tree. To avoid this, it is recommended that every OpenText eDirectory partition is replicated on at least three servers.
- Take a backup of your OpenText eDirectory files.

  Managing OpenText eDirectory can be complex task, which makes it even more important to ensure that it is fully archived. To achieve this, it is recommended to use the OpenText eDirectory backup and restore utility. It is important to note that the built-in OpenText eDirectory backup requires a file-based backup to be performed as well. During the backup process, OpenText eDirectory data is saved to the server's file system. For more information on the processes required to take a full backup, see Backing Up and Restoring OpenText eDirectory.

Protecting Data in Transit

Read through the following recommendations to protect the data transmitted between two or more OpenText eDirectory servers:

- Make sure to have strong ciphers for SSL communication. For more information, see Configuring Protocols and Ciphers Using ldapSSLConfig Attribute.
- Strengthen TLS/SSL settings. For more information, see Chapter 4, “Secure Communication and Authorization,” on page 19.
- Install OpenText eDirectory in Suite-B mode.

  Suite B is a set of cryptographic algorithms standardized by the National Security Agency (NSA) to allow commercial products to protect traffic that is classified at secret or top secret levels. The Suite B algorithms serve as a method to ensure the security of classified and unclassified information passed through public networks. For more information, see Configuring OpenText eDirectory in Suite B Mode.
- Configure OpenText eDirectory in FIPS mode. Before enabling FIPS, it is recommended to migrate users with NDS password to use PBKDF2 (Password-Based Key Derivation Function 2). For more information, see Operating OpenText eDirectory in FIPS Mode in the *OpenText™ eDirectory CE 24.4 (v9.3) Installation Guide* and Understanding Non-Reversible Password Storage in the *OpenText™ eDirectory CE 24.4 (v9.3) eDirectory Administration Guide*.

2 Restricting Access to OpenText eDirectory Server

This section includes recommendations that can help enhance the security of an OpenText eDirectory environment.

- "Security Considerations for OpenText eDirectory Server Hosting Machine" on page 9
- "Security Considerations for Operating Systems" on page 9
- "Restricting Access to OpenText eDirectory Server" on page 10
- "Security Considerations for OpenText eDirectory" on page 10
- "Password Security Recommendations" on page 13

Security Considerations for OpenText eDirectory Server Hosting Machine

- Always ensure that the OpenText eDirectory servers are protected by a firewall. The NetWare Core Protocol (NCP) port, which is usually 524 by default, should be opened in the firewall to allow communication with other OpenText eDirectory servers in the tree. If required, you can also open the LDAPS port 636. Anonymous access and clear text LDAP port 389 should be disabled to prevent unauthorized access.
- To ensure maximum security, it is recommended to keep the servers in a physically secure location and restrict access to only authorized personnel.

Security Considerations for Operating Systems

- The operating system of the system hosting the OpenText eDirectory server should always be up-to-date with the latest updates and security patches.
- No other services should run on the hosting system except for SSH. Additionally, the SSH server must be configured with strong ciphers to ensure secure communication.
- If SSH is enabled, it is recommended to regularly audit the SSH server logs to detect any suspicious activity.
- A non-administrative account should be used for configuring and running OpenText eDirectory. There should be no other user accounts besides the non-administrative account and the root user with shell access to the system.
- An intrusion detection system should be utilized to alert the administrator of any unexpected behavior.
- It is recommended to set SELinux to Permissive mode on all RHEL machines.

  To do this, navigate to the SELinux configuration file located in `/etc.selinux/config` location and set SELinux to permissive mode as follows:

```
SELINUX=permissive
```

- For console access restrictions, it is recommended that the server be placed in secured room and accessed only by authorized users.
- Non-root users (systems non-admin users) should have non-root password policies. Users should have strong password policies.
- It is recommended to only have an administrator account on Windows, and no other user accounts.
- Lastly, Linux operating system can be installed in FIPS mode for added security.

Restricting Access to OpenText eDirectory Server

- It is recommended to use high-strength ciphers for SSH keys. For more information, see Configuring Protocols and Ciphers Using ldapSSLConfig Attribute.
- It is also important to audit logins and access to the system to keep a report of all activities performed by any user at the console. This can be achieved by using third-party tools such as Check Pass Act to monitor user activities.
- It is essential to set filesystem permissions correctly, particularly for DIB and config files, to ensure that only the user hosting the service has all the necessary permissions. Other users should not have read permission.
- To prevent data modification, it is recommended to create RO replicas and partitions.
- Recommended to use LDAP proxy.
- It is important for Network Administrators to take necessary measures to prevent DOS attacks.

Security Considerations for OpenText eDirectory

To install and configure eDirectory, make sure to follow the installation instructions. For more information, see *OpenText™ eDirectory CE 24.4 (v9.3) Installation Guide*. After installation, check that the following conditions are met:

- The Enhanced Background Authentication (EBA) protocol is enabled so that traffic between servers is encrypted.
- SNMP is disabled.
- OpenText eDirectory is not listening on port 389.
- LDAP and HTTP services are configured to use ECDSA certificates only.
- Access to the SSH should be secure.
- No other services should be configured in the system.

Additionally, make sure that the following security measures in place for secure OpenText eDirectory operations:

- “Considerations for Access to Resources” on page 11
- “Considerations for OpenText eDirectory Rights to ACLs” on page 11
- “Considerations for Public Key Infrastructure (PKI) Services” on page 12

- "Considerations for Novell International Cryptographic Infrastructure (NICI)" on page 12
- "Considerations for Auditing OpenText eDirectory Events" on page 12

Considerations for Access to Resources

- It is recommended removing the Browse right from the [Public] trustee at the top of the tree.
- Recommend giving all users basic rights and privileges, such as compare and browse rights, but no read/write or supervisory rights.
- For NMAS access control, provide strong passwords using password management utility in OpenText Identity Console. For more information, see Managing Login and Post-Login Methods and Sequences (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/t4dfij7kxycg.html)

  To provide authentication access to OpenText eDirectory using NMAS login methods, see NMAS Functionality.
- DSA access control: It is an important that only authorized users should have rights to perform certain operations, such as partitioning rights, server rights, ndscheck rights, backup/restore rights, NICI backup, and rights to perform certain operations in imonitor, as well as schema extension.
- Proxied Authorization Control- Allows clients to specify an authorization identity for each operation. This feature is particularly helpful for clients who need to perform multiple operations on behalf of different users.
- In PKI server, the administrator or authorized user should be provided specific entry rights to manage OpenText Certificate Server. Recommended to provide rights over CA, issue certificates, CRL, revoking server certificate, and more. For more information, see Entry Rights Needed to Perform Tasks.
- In the LDAP server attributes, check the rights of the "Anonymous user". Recommendations to set the bind restrictions as per the requirements. For more information, see the `ldapBindRestrictions` attribute description in Configuring LDAP Objects.

Considerations for OpenText eDirectory Rights to ACLs

The Access Control List (ACL) is also called the Object Trustees property in OpenText eDirectory. Whenever you make a trustee assignment, the trustee is added as a value to the Object Trustees (ACL) property of the target. This property has strong implications for network security, so you must be careful giving Add Self rights to all properties of a container object. That assignment makes it possible for the trustee to become Supervisor of that container, all objects in it, and all objects in containers beneath it.

Take note of the following recommendations:

- List attributes which contain sensitive information and add rights to the Object Trustees (ACL) property to specific users or supervisors only.

- Encrypt the attributes which contain sensitive information.
- Assign the rights within OpenText eDirectory to perform tasks using Roles and Access Control (RAC) in OpenText Identity Console. When you assign a role to a user, RAC assigns the necessary rights to perform the tasks of that role. For more information on setting up RAC using OpenText Identity Console, see (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/alw1iwfbb112.html).

Considerations for Public Key Infrastructure (PKI) Services

- All operations related to certificates should be performed by the Admin user only. It is highly advised not to delegate this responsibility to any other user. In the event that it is delegated, the user should not have any other permissions in the tree.
- The PKI has its own DIB and is secured using the Novell International Cryptographic Infrastructure (NICI).
- Certificate Authority (CA) should be secured and only accessed by authorized users.
- Take regular backups of the CA certificates.
- Use Elliptic Curve (EC) certificates and the Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) certificate. The use of RSA certificates, however, may not be recommended.

Considerations for Novell International Cryptographic Infrastructure (NICI)

NICI is the cryptography module that provides keys, algorithms, various key storage and usage mechanisms, and a large-scale key management system. NICI controls the introduction of algorithms and the generation and use of keys. NICI allows a single commodity version of security products to be produced for worldwide consumption that supports strong cryptography and multiple cryptographic technologies. OpenText eDirectory is one of the service that is built on NICI infrastructure.

Take note of the following recommendations:

- Secure all the file systems and ensure that non-admin users do not have permissions to access them.
- Avoid having multiple trees on the same server.
- Take regular backups of the NICI using the DSBK backup utility provided by OpenText eDirectory.
- Upgrade the tree key to either 3DES or AES256.

Considerations for Auditing OpenText eDirectory Events

- Audit events related to logins, as well as operations such as add/modify/delete.
- Use secure TLS for communication between OpenText eDirectory and the Auditing servers (such as Sentinel and ArcSight).
- Enable Security Events to detect intruders and monitor logins.

Password Security Recommendations

Read through the following recommendations:

- Generate an AES 256-bit tree key and re-encrypt passwords with it.
- Disable Universal Password and enable Password Based Key Derivation Function 2 (PBKDF2) hashes of passwords in the following conditions:
  - If you are using OpenText eDirectory without OpenText Identity Manager.
  - If you do not require user password retrieval.
- If Universal Password is required, it should be enabled only for the users who need it, not for the whole tree.
- Configure password policies to enforce:
  - Strong passwords
  - Changing passwords periodically and frequently
  - Password history

3 Security Considerations for Implementing Authentication

User authentication is a security feature of the directory. Before a user logs in, a User object must be created in the directory. The User object has certain properties, such as name and password. When the user logs in, OpenText eDirectory checks the password against the one stored in the directory for that user and grants access if they match.

Review the following security guidelines related to user authentication:

- "Server Authentication" on page 15
- "Securing Administrator Accounts" on page 15

Server Authentication

Take note of the following recommendations for server authentication:

- All non-root users must follow a non-root password policy, particularly for systems where the user is not an administrator.
- All users must follow a strong password policy.
- When installing OpenText eDirectory on a Windows operating system, only the Administrator account should be used as the user account.
- Audit logins and system access to effectively monitor user activities on the console. You can use a third-party tool to generate reports and track these activities efficiently.
- Grant the user hosting the service full file system rights, including access to DIB and config files. Read access should not be granted to any other user.

Securing Administrator Accounts

This applies to both OpenText eDirectory Admin and server administrator.

The Administrator account created during OpenText eDirectory installation have full rights to the OpenText eDirectory components. This account must be secured. To secure this account, read the following recommendations:

- Do not place Administrator account in a container where there are other users.

  It is recommended to store the OpenText eDirectory Administrator accounts in a separate directory context or container than regular user accounts. This reduces the possibility of unauthorized access attempts, which may compromise the password or temporarily disable the administrator account.
- Do not use common names for Administrator account.

It becomes harder to discover the account, which reduces attempts at brute-force attack on the password or unauthorized access to temporarily disable the administrator account.

- Set password restrictions for Administrator account.

  When creating the Admin user, there are no password constraints in place. It is recommended to configure the standard OpenText eDirectory password restrictions for this account to satisfy the minimum security criteria for passwords. In OpenText Identity Console, select the **User Management** option, type the name and context of the object or use the search feature to find it, then click the **Search** button. Select the user object from the users list and click the **Modify** icon. Go to **Restrictions** and set the password restrictions for the account.

  The password is not case-sensitive by default. For more information on how to make your password case-sensitive, see Managing Passwords.

- Set login restrictions for Administrator account.

  Login restrictions are limitations set on user accounts to control network access. For example, when a user violates the login restriction by entering an incorrect or an expired password and exceeds the number of login attempts, the account gets disabled and stops any other user to log in using the same username. This measure ensures unauthorized users are unable to log in.

  Note the following restrictions which are imposed in OpenText Identity Console for each user:

  - Make password mandatory. You can customize the requirements, such as set a minimum length, decide if it needs to be changed periodically and how often, make it unique, and enable the option for only strong passwords to be used. You can also restrict users from changing their passwords. For more information, see Managing Password Policies (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/t4dfte3qg6l8.html)
  - Limit the maximum number of logins with an expired password and the maximum number of incorrect login attempts that can be made.
  - Set limits on the account, such as account balance and expiration date.
  - Limit the number of simultaneous connections that a user can have.
  - Specify (by node address) which workstations users can login to.
  - Restrict the time when users can log in (you can assign all users the same hours, or you can restrict users individually).
  - Device-specific or node-specific accounts can be restricted.

    When you access services on a Novell Core Protocol (NCP) server using an OpenText eDirectory account, it is possible for OpenText eDirectory to limit access to a user account based on the requesting network address. This means that the user account can only be used by a specific device or node with a fixed TCP/IP (not a dynamic one using DHCP), such as a printer or other non-user entity. These types of account can be restricted to only allow authentication from certain network addresses.

    You can set network address restrictions for service accounts and a particular user as well.

    1. Login to OpenText Identity Console.
    2. Select any user, then click **Modify User** > **Restrictions** > **Address Restrictions** and provide the IP Address as per requirement and save.

- Configure LDAP proxy user.

LDAP, by default, uses the PUBLIC object to obtain permissions for retrieving information from OpenText eDirectory, which is insecure as it allows non-authenticated users to read that same information in OpenText eDirectory. To ensure secure LDAP connectivity, we recommend using an LDAP proxy user instead of relying on the PUBLIC object. However, it is important to ensure that this LDAP proxy user does not have access to sensitive areas of the tree, such as administrator users containers, server containers, or SLP scope containers.

- Disallow anonymous bind on LDAP.

  Allowing LDAP anonymous binds has an adverse impact on security, especially when public browse rights for the OpenText eDirectory tree have not been revoked. Therefore, it is recommended that the anonymous bind on LDAP be disallowed.

- Set intruder detection policy.

  OpenText eDirectory provides an option to disable specific accounts for a period of time if the number of invalid authentication attempts reaches a certain limit. This is critical for preventing attempts of brute-force attack from revealing accounts and passwords.

  You can set up an intruder detection policy on the `novell` container, which is the container where the Admin user is created. To set up the policy in OpenText Identity Console, see Checking and Clearing the Intruder Lockout (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/t4939mmf1wkb.html)

- Backup the Admin user.

  When you install OpenText eDirectory, just one Admin user is created. If you forget the username or password, you will not be able to access OpenText eDirectory. To avoid this, it is recommended that you create a backup user who has the required privileges of an Admin user.

- Set strong password policies for OpenText eDirectory administrator and system administrator.
- Reset the admin account if you forget account credentials.
- Disable password retrieval for OpenText eDirectory Admin account.
- Use Multi-factor Authentication for Advanced Authentication and other products.
- Disable simple passwords.

  Using simple passwords to manage multiple password hashes for different services in OpenText eDirectory is not secure. It is recommended to enable Universal Password instead. Universal Password is a modern framework that offers password policies and services for Novell OpenText eDirectory. It ensures a consistent password policy across various authentication systems, including Native File Access. With Universal Password services, you can have case-sensitive passwords, use extended characters, and enforce advanced password policies like password complexity, which enhances security.

- Enable account access time restrictions.

  To enhance security, you may limit the active hours of certain accounts that should not be authorized to log in at certain times of the day.

- Enable password policies.

  To ensure secure authentication of user accounts, it is important to enforce restrictions on passwords. This can be done in OpenText eDirectory by setting specific attributes on user objects. Enabling Universal Password offers added security advantages such as case sensitivity. Be sure to follow the rule of enabling Universal password capabilities.

- Limit concurrent connections.

To prevent account and password sharing, or multiple workstations being authenticated to OpenText eDirectory, it is recommended to restrict the number of times user accounts can be authenticated to a tree.

- Remove or disable inactive account.

  Inactive accounts are a security risk as they can be exploited to compromise a network system. It is recommended to deactivate accounts that have been inactive for 90 days or more.

4 Secure Communication and Authorization

Review the following guidelines for secure communication and authorization in OpenText eDirectory:

- TLS 1.0 and TLS 1.1 are disabled by default in OpenText eDirectory and should not be enabled.

  By default, OpenText eDirectory operates in FIPS mode and is associated with an RSA certificate. This configuration disallows SSLv3 communication and only allows connections from TLS 1.2 clients.

- Disable unencrypted LDAP

  During a standard LDAP TLS session, a clear-text connection is established first. Then, the STARTTLS (an extended LDAP operation) is then issued to enable a secure encrypted connection. Finally, authentication takes place in a secure manner. However, a flaw can occur if the LDAP client is configured incorrectly or a client is not configured to use STARTTLS. In such cases, the user name and password are transmitted in clear text before the client software is notified through an error message that authentication requires TLS. This can lead to unauthorized access to usernames and passwords by software that monitors network traffic.

  Therefore, it is recommended to disable TLS and use SSL-tunnel encrypted LDAP on port 636, even if TLS is required for LDAP on port 389. This is because the SSL-encrypted tunnel session is established before authentication can occur, which eliminates the risk of transmitting sensitive information in clear text. SSL-tunnel encrypted LDAP is usually on port 636 and is a more secure option.

- Even if the LDAP group requires TLS binds, in an attempted unsecured bind, the information is still sent to the server before being denied, and could be captured. Therefore, it is necessary to use TLS for all LDAP server operations.
- Make sure that the LDAP proxy user requires TLS for simple binds with a password. If the standard LDAP port 389 is disabled, this requirement is not necessary.
- When using OpenText eDirectory with a load balancer, whether on cloud or on-premises, it is recommended to not access iMonitor, eMBox, and DHost Console over HTTP traffic. Instead, it is recommended that you disable these modules and perform all related operations using NDS utilities.

5 Security Considerations For OpenText eDirectory Privileges

Check your administrator users for unauthorized equivalence

Setting a user to be an administrator equivalent grants them all of the administrator user's rights. Unauthorized users who have acquired access can use this to permanently provide administrator access to their account.

To check if there are users having unauthorized equivalence, perform the following steps in OpenText Identity Console:

1. Click the **User Management** option from the OpenText Identity Console landing page.
2. Select a user.
3. Under Modify Object, go to **Security** tab.
4. In the **Security Equal to Me** option, check that no accounts have been set as equal to your administrator accounts that are not authorized to do so.

Use a User template object when creating users

Make sure you use a User template object when creating a user account. It ensures that the necessary security-related configurations have been completed. You can use custom forms for user account in OpenText Identity Console. For more information, Managing Custom Forms (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/alw1iwfbb2eer.html).

Disable Anonymous Directory Browsing

Even without authenticating to OpenText eDirectory, users can attach to the directory and browse through the contexts and users by default. Security best-practices recommend only allowing authenticated users to see only the users and objects that they need access to

Do Not Assign Privileges to All Groups

Assign privileges based on job function, like organizational role, specific groups, or container objects. It is recommended not to assign privileges to any group where all users are members.

Rights, especially Supervisor rights, should be assigned only where required

It is easy, but violates a basic security principle, to assign more rights than what are necessary for a user to perform the work they are authorized to perform. Determine what rights are needed by each person that is performing work on your system, then ensure that the minimum rights are assigned to allow the user to perform their work.

Restrict access to the tree [Root] object

The [Root] object is the top object in any OpenText eDirectory tree. Unless the rights given at the [Root] are blocked from being inherited, any rights assigned here flow down throughout all parts of the tree. Aside from the primary OpenText eDirectory administrator user object, other users, groups, organizational roles, or container objects should not have access to the [Root] object without a specific organizational need.

Typical objects seen as trustees of [Root] are objects such as [Public] with only Browse Entry Rights, [Root] with only Browse Entry Rights, one or more administrator user, group, or organizational role objects with full rights including Supervisory rights, and Role Based Services objects with Supervisor Entry Rights. Any unknown objects with Supervisory rights or with rights that exceed Browse Entry Rights, especially to the All Attributes Rights or Entry Rights are a concern and should immediately be investigated.

WARNING: Removing a rights or trustee objects from the [Root] that are required to be there by some process may cause certain processes or authentications to fail. However, failing to secure the [Root] object properly exposes your entire tree to unauthorized access and modifications.

Examine top-level container for excessive privileges

The top-level container(s) in an OpenText eDirectory tree should be examined for objects in the tree, such as users, groups, containers, organizational roles, with unauthorized access privileges.

1. Examine the trustee rights on the top-level Organization or other top-level containers, this includes all objects directly under the Root object.
2. Look for unauthorized objects, such as users, groups, containers, or organizational roles that have been given access to this container and usually all child containers and objects.

Restrict access to all NCP server objects

NCP Server objects are Linux Novell Core Protocol servers, which are typically file servers with clients running the Novell Client software. Ensure that all non-administrator users have no more than Browse, Compare, and Read rights.

Perform the following tasks:

1. Examine the trustee rights on the top-level Organization or other top-level containers, this includes all objects directly under the Root object.
2. Look for unauthorized objects, such as users, groups, containers, or organizational roles that have been given access to this container and usually all child containers and objects.

Inherited rights filters should be used sparingly

Inherited rights filters (IRF) are used to block rights inheritance in the tree. This method of limiting access should be used sparingly, because it becomes difficult to determine where rights are being inherited.

Additive rights: directly assigning rights to all objects, versus subtractive rights: assigning rights at a higher level and then removing rights from specified lower levels, are normally less complex and easier to administer. You should only use IRFs in limited-scope cases where directly assigning all of the rights is more complex than using IRFs.

Say for instance, that a parent container and all children but one should allow all users browse access, but that one child container should be hidden from all users. Assign access only to organizational roles and groups directly to the objects and folders that organizational role or group requires. Be aware that the default behavior for rights is to flow down and be inherited by all child containers and objects.

Use effective rights testing to ensure that proper rights are assigned to applicable objects.

WARNING: Be cautious when using an IRF to block supervisor rights. Normally, you are required to directly assign another supervisor-rights object to the object that you are using an IRF to block supervisor rights to.

Security Equivalence to user objects should not be used

The use of security equivalence or “security equal to me” settings on a user object is an easy, but outmoded use of security privileges. It is a better practice to and easier to audit by assigning access privileges through organizational roles or groups.

It is also easy for administrators who have set up the equivalence or other administrators unfamiliar with the user equivalence to delete the user object that the other users are equivalent to, thus wiping out the only record of all the privileges and forcing a backup restore or rebuilding all of the required privileges from scratch.

Create an organizational role or group object. Assign the rights to this object that you desire your security equivalent objects to have. Locate all objects using the security equivalence setting. Make the user object a member of the group or organizational role object. Remove the security equivalence.

To locate objects using security equivalence, perform the following steps in OpenText Identity Console:

1. Click the **Search** option from the OpenText Identity Console landing page.
2. In the Search window, select type as `user` and click on search icon next to it to open advanced search window.
3. Select attribute as `security equals` and operator as `is present`.
4. Click OK.

   The users who have used “Security equals” are listed. Similarly, one can filter by “Security equals to me” and make the necessary modifications in accordance with security requirements.

6 Securing OpenText eDirectory on Cloud

In addition to the guidelines in other sections, consider the following recommendations while deploying eDirectory on cloud platforms, such as Amazon Web Services EC2 and Microsoft Azure.

- If you use SUSE Linux Enterprise Server or RHEL service, ensure that operating system is updated with the latest patch. Operating system packages must be up to date at all times.
- Do not use keys with less than 1024 bits in size on port 22.
- Install eDirectory on a private subnet. For information about protecting the console in a cloud environment, see Deploying OpenText eDirectory on Amazon Web Services EC2 or Deploying OpenText eDirectory on Microsoft Azure based on your requirement.