Informix User Management Guide

1. Introduction

Informix is a powerful database management system that allows organizations to efficiently store and manage their data. Proper user management is crucial for maintaining the security and integrity of your Informix database. This guide provides detailed information on how to manage users effectively in an Informix environment.

2. User Types

Informix supports various user types, including:

- **Regular Users:** These users can connect to the database and perform authorized operations.
- **DBA (Database Administrator):** DBAs have administrative privileges, allowing them to manage users, databases, and server settings.
- **Application Users:** These users are created for specific applications and often have limited access to only the necessary resources.
- **Anonymous Users:** These users don't require authentication and are typically used for public access.

3. User Creation

3.1. Creating a New User

To create a new user in Informix, follow these steps:

1. **Connect to the Database:** Log in as a DBA or a user with sufficient privileges.
2. **Create the User:** Use the `CREATE USER` SQL statement, specifying the username and password.
3. **Assign Privileges:** Grant the appropriate privileges to the user using `GRANT` statements.

Syntax:

```
dbaccess your_database
CREATE USER new_user WITH PASSWORD 'password';
GRANT CONNECT TO new_user;
```

(or)

```
CREATE USER username
   PASSWORD 'password'
   ATTRIBUTE 'profile=profile_name,REMOTE_PASSWORD=client_password'
   DEFAULT DATABASE dbname;
```

-> `**username**`: The name of the user.

->`**password**`: The user's password.

-> `**profile_name**`: The name of the user profile.

-> `**client_password**`: The client password for remote authentication.

-> `**dbname**`: The default database for the user.

Example:

dbaccess subvent

CREATE USER c1opera WITH PASSWORD '**********';
GRANT CONNECT TO c1opera;

3.2. Modifying User Properties

To modify user properties, use the `ALTER USER` statement:

ALTER USER username SET ATTRIBUTE attribute_name TO new_value;

ALTER USER username [WITH PASSWORD 'new_password'] [WITH USER GROUP new_groupname];

Deleting a User

To delete a user, you can use the `DROP USER` statement:

DROP USER username;

4. User Authentication

- **Password Authentication:** Users provide a username and password for authentication.
- **PAM (Pluggable Authentication Module):** Integrates with the system's PAM framework.
- **LDAP (Lightweight Directory Access Protocol):** Utilizes LDAP for authentication.
- **Kerberos:** Provides secure authentication through Kerberos tickets.

Choose the authentication method that best suits your security requirements.

5. Password Management

It's essential to implement robust password policies for user security. Informix supports password policies like:

- Password expiration.

- Password history.

- Password complexity rules.

- Account lockout on multiple failed login attempts.

Regularly remind users to update their passwords and enforce password policies.

6. Privilege Management

Informix uses role-based access control. You can grant and revoke privileges to users using SQL statements like `GRANT` and `REVOKE`. Common privileges include:

- `SELECT`: Allows users to retrieve data from tables.

- `INSERT`, `UPDATE`, `DELETE`: Permissions for data modification.

- `CREATE`, `ALTER`, `DROP`: Permissions for database schema management.

Always follow the principle of least privilege to ensure that users have only the permissions they need.

6.1. Granting Privileges

Grant privileges to users using the `GRANT` statement. Common privileges include `SELECT`, `INSERT`, `UPDATE`, `DELETE`, and more.

GRANT SELECT ON table_name TO user_name;

6.2. Revoking Privileges

To revoke privileges, use the `REVOKE` statement:

REVOKE SELECT ON table_name FROM user_name;

7. User Auditing

Enable auditing to monitor user activities and detect security breaches. Use the `AUDIT` statement to configure audit policies and the `dbaccess` utility to review audit logs.

8. User Deactivation and Removal

Deactivate or remove users who no longer require access to the database. Use the `ALTER USER` statement to disable an account temporarily and `DROP USER` to remove it permanently.

9. Best Practices

- Follow the principle of least privilege: Only grant necessary permissions to users.
- Regularly review user access and privileges.
- Implement proper backup and recovery procedures.
- Keep your Informix server and software up to date.

- Disable or delete inactive accounts.
- Update passwords periodically.
- Monitor user activity for security breaches.

- Regularly patch and update Informix to fix security vulnerabilities.
- Use encryption for data in transit and at rest.
- Limit network access to your Informix server.
- Conduct security audits and penetration testing.

10. Troubleshooting

Common user management issues may include forgotten passwords, locked accounts, or privilege-related errors. Refer to Informix documentation or contact support for assistance.

If you encounter issues with user management, consult the Informix documentation or seek support from the Informix community.

11. Conclusion

Effective user management is essential for maintaining the security and performance of your Informix database. By following the guidelines outlined in this guide, you can ensure that user accounts are properly created, managed, and secured in your Informix environment.