SAP NetWeaver 2004s SPS 4

Security Guide

MaxDB Security Guide

Document Version 1.00 – October 24, 2005

SAP AG
Neurottstraße 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Disclaimer
Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Documentation in the SAP Service Marketplace
You can find this documentation at the following Internet address:
`service.sap.com/securityguide`

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, *F2* or *ENTER*.

Icons

Icon	Meaning
⚠	Caution
🗨	Example
💡	Note
🧭	Recommendation
syn	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* → *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Contents

MaxDB Security Guide

Purpose

The purpose of this security guide is to assist you in making your MaxDB database system secure.

Features

1 Introduction

> This guide does not replace the daily operations manual that we recommend customers create for their specific production operations.

This guide represents the latest state of development. The contents may be changed without prior notice and are not binding for SAP.

Target Audience

- Technology consultants
- System administrators

This document is part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereby the Security Guides provide information that is relevant for all life cycle phases.

Why Is Security Necessary?

With the increasing use of distributed systems and the internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation on your system should not result in loss of information or processing time. These security requirements naturally also apply to MaxDB. We offer this Security Guide to assist you in securing MaxDB.

About This Document

The Security Guide provides an overview of security-relevant information that applies to MaxDB.

Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Before You Start**

  This section contains information about why security is necessary, how to use this document, and references to other Security Guides that build the foundation for this Security Guide.

- **Technical System Landscape**

  This section provides an overview of the technical components and communication paths used by MaxDB.

- **User Administration and Authentication**

  This section provides an overview of the following user administration and authentication aspects:

  - Recommended tools for user management
  - The user types required by MaxDB
  - The standard users delivered with MaxDB

- **Authorizations**

  This section provides an overview of the MaxDB authorization concept.

- **Network and Communication Security**

  This section provides an overview of the communication paths used by MaxDB and the security mechanisms that apply.

- **Data Storage Security**

  This section provides an overview of the critical data used by MaxDB and the security mechanisms that apply.

- **Dispensable Functions with Impacts on Security**

  This section provides an overview of functions that have impacts on security and can be disabled or removed from the system.

- **Other Security-Relevant Information**

  This section contains information about:

  - User input in SQL statements

- **Trace and Log Files**

  This section provides an overview of the trace and log files that contain security-relevant information, for example, so you can reproduce activities if a security breach does occur.

- **Appendix**

  Overview of the variables and examples used in this guide

2 Before You Start

Fundamental Security Guides

For more information on security measures for MaxDB in SAP systems, see the *SAP NetWeaver Security Guide*.

A complete list of all available SAP Security Guides can be found in the *SAP Service Marketplace* at **`service.sap.com/securityguide`**

Important SAP Notes

Current SAP notes that contain security-relevant information for MaxDB can be found in the *SAP Service Marketplace* at **`service.sap.com/security`** → *Security* → *SAP Security Notes* for component BC-DB-SDB SAP DB.

Additional Information

For more information about specific topics, see the quick links shown in the table below.

Quick Links to Additional Information

Contents	**Quick Link to the SAP Service Marketplace**
Security	service.sap.com/security
Security Guides	service.sap.com/securityguide
Related SAP notes	service.sap.com/notes
Released platforms	service.sap.com/platforms
Network security	service.sap.com/securityguide
SAP Solution Manager	service.sap.com/solutionmanager

3 Technical System Landscape

The following graphic presents an overview of the MaxDB technical system landscape.

Schematic overview of the technical system landscape

Error! Objects cannot be created from editing field codes.

More Information About the Technical System Landscape

Topic	Document	Quick Link to the SAP Service Marketplace
MaxDB technical system landscape	*Concepts of the Database System*, Technical System Landscape [SAP Library]	
Technical description of SAP NetWeaver	Master Guide	service.sap.com/instguides
Security		service.sap.com/security

4 User Administration and Authentication

Before you can work with the database system, you must log on to the database instance with a database tool or via an interface. You log on with your user name. You enter your password and the database system authenticates your identity using this password.

Hazards

- **Unauthorized Access of the Database Instance**

  A person who is not authorized to access the database instance learns the user name and password of an authorized user. Particularly at risk are standard users with standard passwords that are commonly known.

  The person logs onto the database instance using the identity of the authorized user.

Activities

- Changing the Passwords of Standard Users [SAP Library]
- Checking Log Files for Failed Logon Attempts [Page 6]

See also:

Concepts of the Database System, Users, Authentication and Authorizations [Page 6]

4.1 Changing the Passwords of Standard Users

Use

The following standard users are created during the installation of the MaxDB database system.

MaxDB Standard Users

Name (Default value)	**Password (Default value)**	**Description**
DBADMIN DBA (up to version 7.5 inclusive)	SECRET DBA (up to version 7.5 inclusive)	Database System Administrator [SAP Library] (SYSDBA user)
DBM	DBM	Database Manager Operator [SAP Library] (DBM operator) with all server authorizations
DBSERVICE	SECRET	Synchronization user for the Synchronization Manager [SAP Library] If you do not use the Synchronization Manager, you can delete this user and all the database objects assigned to it.

As a rule, the following standard users are created during installation in SAP systems.

SAP Standard Users for Databases

Name	**Password**	**Description**
SUPERDBA	ADMIN	Database system administrator (SYSDBA user)
CONTROL	CONTROL	Database Manager operator (DBM operator) with all server authorizations
SAPR3	SAP	In older SAP systems: Database administrator (database user of type DBA)
SAP<SAPSID>	SAP	In newer SAP systems, in particular in MCOD systems (Multiple Components One Database): Database administrator for the SAP system with the ID <SAPSID> (database user of the type DBA)
SAP<SAPSID>DB	SAP	In J2EE systems: Database administrator for the SAP system with the ID <SAPSID> (database user of the type DBA)

These users have comprehensive authorizations for working with the database system MaxDB.

Procedure

To keep unauthorized persons from learning the passwords of standard users, we recommend the following measures:

- Do **not** adopt the default passwords.
- Use secure passwords.
- Change the passwords regularly.
- To enable another user to work temporarily with the account of the database system administrator (SYSDBA user), you can temporarily assign a second password to the database system administrator. This way you do not have to reveal the password of the database system administrator.

Changing the Passwords for MaxDB Standard Users

Use the Database Manager database tool, or the CCMS in SAP systems. See:

- *Database Manager GUI*
  Changing the Password of the Database System Administrator [SAP Library]
  Changing the Password of a Database Manager Operator [SAP Library]
  Changing the Password of a Database User [SAP Library]
- *Database Manager CLI*
  Changing the DBM Operator Properties [SAP Library]
- *Database Administration in CCMS: MaxDB*, User Data [SAP Library]
- *Database Administration in CCMS: SAP liveCache*, User Data [SAP Library]

For security measures for standard **operating system** users, see Changing the Passwords of SAP Standard Operating System Users [Page 6].

Assigning a Temporary Second Password to MaxDB Standard Users

Use the database tool Database Manager. See:

- *Database Manager GUI*
  Changing the DMB Operator Properties of the Database System Administrator [SAP Library]
  Changing the DBM Operator Properties [SAP Library]
- *Database Manager CLI*
  Changing the DBM Operator Properties [SAP Library]

4.2 Checking Log Files for Failed Logon Attempts

Use

The database system logs errors and important messages in several log files. For information about the name, path and function of log files, see *Concepts of the Database System*, Log Files [SAP Library].

By monitoring the log files, you can identify unusual activity in a timely way.

Procedure

Regularly check the following log files for failed logon attempts:

- Log file of the Database Manager
- Log file of the Loader

Example

Messages from the Database Manager for the database instance `DEMODB` are logged in the log file `c:\Documents and Settings\All Users\Application Data\sdb\data\wrk\DEMODB\dbm.prt`. In the event of a failed logon attempt, the Database Manager writes the following message in this log file:

```
command user_logon
ERR_USRFAIL: user authorization failed
```

5 Authorizations

After the logon data has been authenticated, a user can, within the framework of his or her authorizations, access data in the database instance and use database tools.

The MaxDB database system has the following types of users:

- **Database System Administrator** (SYSDBA User)

  The database system administrator has comprehensive authorizations for access to the database instance and database tools.

- **Database User**

  Database users access the data in the database instance using SQL statements. The user class determines what authorizations a user has.

- **DBM Operator (Database Manager Operator)**

  DBM operators manage database instances with the database tool Database Manager. A DBM operator’s server authorizations determine what authorizations he or she has.

  For more information about server authorizations, see *Concepts of the Database System*, Server Authorizations for the DBM Server [SAP Library].

Hazards

- **Reading of data by an unauthorized user**

  A user reads confidential data that should only be visible for a restricted group of users.

- **Changing of data by an unauthorized user**

  A user changes data that should only be changed only by a restricted group of users.

Activities

- Defining Clear Authorizations for Users [SAP Library]
- **See also:**
- *Concepts of the Database System*, Database Users [Page 6].

5.1 Defining Clear Authorizations for Users

To ensure that users have only the authorizations that they need for their work, we recommend the following measures:

- *Create an authorization concept that specifies clear authorizations for individual users:*
  - Define which database users are to have access to what data.
  - Define which Database Manager operators are to carry out what administration tasks.
- *Create a separate database user for each person who works with the database instance. In doing this, use the user classes STANDARD and RESOURCE where possible.*
- *Distribute the administration tasks. In addition to defining the database system administrator, define database users of the user class DBA and Database Manager operators.*
- *Assign Database Manager operators only the server authorizations that they really need.*

> In some cases it can make sense to create a Database Manager operator that can check the operational state of the database instance but cannot perform any administration tasks.

Creating Database Users and Defining User Classes

On Microsoft Windows, use the database tool Database Manager GUI:

- Database Manager GUI, Creating/Changing/Deleting a Database User [SAP Library]

In other operating systems, use the database tool SQLCLI and the corresponding SQL statements for the authorization of users:

- SQLCLI, Executing an SQL Statement [SAP Library]
- Reference Manual, Authorization [SAP Library]

Creating Database Manager Operators and Adjusting Server Authorizations

To create Database Manager operators, use the database tool Database Manager:

- Database Manager GUI, Creating/Changing/Deleting a DBM Operator [SAP Library]
- Database Manager CLI, Creating DBM Operators [SAP Library]

To adjust the server authorizations of Database Manager operators, use the database tool Database Manager:

- Database Manager GUI: Changing the Server Authorizations [SAP Library]
- Database Manager CLI: Changing the DBM Operator Data [SAP Library]

6 Network and Communication Security

The database system consists of several components that can be located on different computers and in different networks. Data is transferred between these components as well as between database system and database application (for example an SAP system).

Hazards

- **Data is intercepted**

  Unauthorized persons intercept data while this is being transferred between computers.

- **Unauthorized access to database computer via the network**

  Unauthorized persons exploit security gaps in other programs in order to gain access to the database computer via a network connection.

Activities

- Securing Communication Channels [Page 6]
- Using the MaxDB X Server Behind a Firewall [Page 6]
- Using Web Tools Behind a Firewall [Page 6]

See also:

Technical System Landscape [Page 6]

6.1 Securing Communication Channels

Use

Data is transferred via the following communication channels, among others:

Communication Channels

From	To	Protocol
MaxDB X Server	MaxDB client (database tool, interface)	TCP/IP
Optional: SSL (only in SAP systems)		
MaxDB X Server	SAProuter	NI (SAP protocol)
Optional: NISSL (only in SAP systems)		

Procedure

In SAP systems you can encrypt a data transfer to ensure that no data is intercepted during transfer between two computers.

For more information, see the *Installation Guide* for your SAP system; see SAP note 767598.

When logging onto a database instance, the user's password is encrypted rather than being transferred in plain text. See *Concepts of the Database System*, Authentication [SAP Library].

See also:

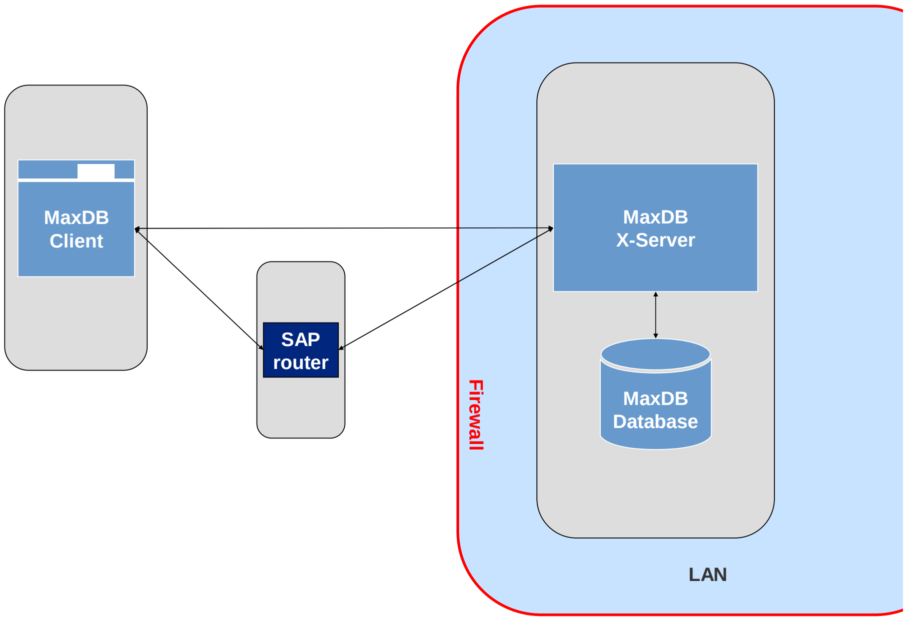
Documentation for SAProuter at *SAP NetWeaver* → *SAP NetWeaver Configuration* → *SAP Web Application Server* → *SAPRouter*

6.2 Using the MaxDB X Server Behind a Firewall

Use

You can use the MaxDB X Server behind a firewall, for example in a company LAN (local area network).

Example of a network with a firewall



Procedure

To access a MaxDB X Server behind a firewall using a MaxDB client such as a MaxDB database tool, open the necessary ports in your firewall. See your firewall documentation for information about opening ports.

Ports and Protocols of the MaxDB X Server

Port Number	Log	Remarks
7210	TCP/IP	
7269	NI	Only in SAP systems
7270	SSL NISSL	Only in SAP systems

See also:

X Server, Ports and Protocols of the X Server [SAP Library]

Concepts of the Database System, Network Communication [SAP Library]

Documentation for SAPRouter at *SAP NetWeaver → SAP NetWeaver Configuration → SAP Web Application Server → SAPRouter*

6.3 Using Web Tools Behind a Firewall

The further development of MaxDB Web DBM, MaxDB Web Server and the MaxDB Web Server Manager has been stopped. These programs are only included in the MaxDB software package up to and including version 7.5.

The default values for the installation are based on the assumption that MaxDB Web Tools will be operated in a secure environment behind a firewall.

If you have particularly stringent requirements for the security of your systems, change the default configuration as soon as you have installed the software for the Web Server and Web Tools as part of the standard software installation.

7 Data Storage Security

The data that comprises the database instance is stored in the file system. There are several operating system users that have comprehensive authorizations for accessing database resources using the commands and functions of the operating system.

Access of Database Resources by Operating System Users

Database Resource	**Access (UNIX/Linux)**	**Access (Microsoft Windows)**
Volumes	`<sdb_user>` (owner) Members of the group `<sdba_group>`, if there is no support group Members of the support group	Members of the groups *Administrators, System, Creator/Owner*
Backups	`<sdb_user>` (owner) Members of the group `<sdba_group>`	Members of the groups *Administrators, System, Creator/Owner*
Files and directories of the database software	`<sdb_user>` (owner) Members of the group `<sdba_group>`	All
Database processes	`<sdb_user>` (owner)	*Local system account*
X Server	`<sdb_user>` (owner)	*Local system account*

In SAP systems there can be additional operating system users that have access to database resources and that can replace the `<sdb_user>` operating system user.

Access of Database Resources by SAP Standard Operating System Users

Database Resource	**Access (UNIX/Linux)**	**Access (Microsoft Windows)**
All	`<sid>adm` (SAP system administrator and database administrator in SAP systems) Member of the group `<sdba_group>` For liveCache database instances, also owner	`<SID>ADM`
All	`<sqd>sid` Obsolete, not for liveCache database instances Owner	`<SQD>SID`

`<sid>` = System ID of the SAP system

Hazards

- **Access to unprotected database resources**

  A normal operating system user uses operating system commands to access database resources that are not protected by restrictions on the operating system level.

- **Unauthorized access to protected database resources using external user data**

  A normal operating system user learns the password of a privileged operating system user and accesses protected database resources using operating system commands.

Activities

- Restricting Access to Database Resources (UNIX/Linux up to Database Version 7.4.03) [Page 6]
- Restricting Access to Database Resources (Microsoft Windows) [Page 6]
- Changing Passwords of SAP Standard Operating System Users [Page 6]

See also:

Appendix [Page 6]

See *Concepts of the Database System*, Special Operating System Users and Groups (UNIX/Linux) [SAP Library]

7.1 Restricting Access to Database Resources (UNIX/Linux up to Database Version 7.4.03)

⚠

A new authorization concept came into effect as of database version 7.5. See *Concepts of the Database System*, Special Operating System Users and Groups (UNIX/Linux) [SAP Library] The measures described in the following are relevant only for older database versions.

Up to and including database version 7.4.03, access rights in SAP systems on UNIX/Linux are automatically configured during installation as follows.

Access Rights in SAP Systems up to and Including Database Version 7.4.03: Directories

Directory	Privilege	Owner	Group	Notes
/sapdb/<SID>/sapdata	750	sqd<sid>	sapsys	
/sapdb/<SID>/saplog	750	sqd<sid>	sapsys	
/sapdb/<SID>/sapsys	750	sqd<sid>	sapsys	
/sapdb/<SID>/dbsys	750	sqd<sid>	sapsys	No longer applies as of 7.4
/sapdb/<SID>/db	750	sqd<sid>	sapsys	If a database version 7.5 or higher is installed on a computer together with an older version, change the access privileges for the directory `/sapdb/<SID>/db` of the older database version to 755 to ensure that the database processes of the newer versions have unrestricted access to it.

Access Rights in SAP Systems up to and Including Database Version 7.4.03: Files

File	Privilege	Owner	Group	Notes
/sapdb/<SID>/sapdata/*	660	sqd<sid>	sapsys	
/sapdb/<SID>/saplog/*	660	sqd<sid>	sapsys	
/sapdb/<SID>/sapsys/*	660	sqd<sid>	sapsys	
/sapdb/<SID>/dbsys/sys	660	sqd<sid>	sapsys	No longer applies as of 7.4

Access Rights in SAP Systems up to and Including Database Version 7.4.03: Raw Devices

Raw device	Privilege	Owner	Group	Notes
Raw devices for the database system	660	sqd<sid>		Link to the raw devices used as data volumes or log volumes

Procedure

To restrict access rights, proceed as follows:

1. Save the original settings. To do so, enter the following commands:

   ```
   cd /usr/sap
   ls -lR > sap_perm.txt

   cd /sapmnt
   ls -lR > sap_sw.txt

   cd /sapdb/<SID>
   ls -lR > sapdb_perm.txt
   ```

2. Grant the desired access privileges for files and directories with the **chmod** command:

   ```
   chmod <access_privileges_in_octal_format> <file_or_directory>
   ```

   ```
   chmod 750 /sapdb/<SID>/sap*
   chmod 750 /sapdb/<SID>/sapdata/*
   chmod 750 /sapdb/<SID>/saplog/*
   ...
   ```

   Do not use **chmod** recursively. It is very easy to make unintended changes to authorizations when doing so.

7.2 Restricting Access to Database Resources (Microsoft Windows)

On Microsoft Windows, only operating system users that belong to the groups *Administrators, System* or *Creator/Owner* are able to access the volumes and backups of the database instance using operating system commands. All other database resources are accessible to all operating system users.

Procedure

To protect other database resources, you can restrict access to the directory `<independent_data_path>\config`.

1. Log onto the operating system as an operating system user of the group *Administrators or the group Creator/Owner*.

2. Grant the following access privileges for the directory `<independent_data_path>\config` and all the files it contains:

   - Access privilege *Full Control* for the groups *Administrators, System* and *Creator/Owner*
   - No access for all other groups and users

   For information about granting access privileges, see your operating system documentation.

See also:

Appendix [Page 6]

Concepts of the Database System, Configuration Files [SAP Library]

7.3 Changing the Passwords of SAP Standard Operating System Users

Many SAP systems make use of standard operating system users that, on the operating system level, have comprehensive access rights to database resources.

Standard Operating System Users in SAP Systems

Operating system user	Use
`<sid>adm`	SAP system administrator and database administrator in SAP systems
`sqd<sid>`	Owner of the database resources

`<sid>` = system ID of SAP system

Procedure

To keep unauthorized persons from learning the passwords of standard operating system users, we recommend the following measures:

- Do **not** adopt the default passwords.
- Use secure passwords.
- Change the passwords regularly.

Changing the Password of an Operating System User (UNIX/Linux)

1. Log on to the operating system with the `<sid>adm user.`
2. Open a shell.
3. Enter the command **`passwd`**.
4. Enter the old and new passwords.

Repeat the procedure for the `sqd<sid>` user.

If you use the Network Information Service (NIS), you can read how to change the passwords of operating system users in the NIS Guide.

Changing the Password of an Operating System User (Microsoft Windows)

1. Log on to the operating system as a user from the *Administrators* group.
2. Change the password of the operating system user `<SID>ADM`.

8 Dispensable Functions with Impacts on Security

You may not need all of the functions of the MaxDB database system.

Hazards

The more functions you have installed, the more potential hazards there are.

Activities

We recommend the following measures:

- Install only those software components that you really need. See *Installation Manual*, Software Components [SAP Library].
- Switching off the MaxDB X Server for Local Communication [Page 6]
- Starting the MaxDB X Server Without NI Support (Unix/Linux) [Page 6]
- Removing Demo Data [Page 6]

8.1 Switching Off the MaxDB X Server for Local Communication

Use

The MaxDB X Server is needed only for network communication. See *Concepts of the Database System*, Network Communication [SAP Library].

For local communication, that is, when the database instance and the database application (or database tool or the interface) are on the same computer, MaxDB uses shared memory. Two exceptions are the Event Dispatcher and the JDBC interface, which require the X Server even for local communication.

Prerequisites

You are using neither the Event Dispatcher nor the JDBC interface.

Procedure

Stop the X Server with the following command:

```
x_server stop
```

See also:

X Server, Stopping the X Server [SAP Library]

8.2 Starting the MaxDB X Server Without NI Support (Unix/Linux)

Use

On UNIX/Linux, when the MaxDB X Server is started, the MaxDB NI Server is automatically started as a separate process to support the SAP NI network protocol.

If you use MaxDB outside of SAP systems, NI support is not necessary.

Procedure

Use option –Y when starting the X Server:

```
x_server –Y start
```

See also:

X Server, Starting the X Server [SAP Library]

8.3 Removing Demo Data

Use

MaxDB is delivered with a demo database. This database was developed for practice and testing purposes and contains several predefined demo users and demo data.

Procedure

To prevent unauthorized users from logging on to a production system using the logon data of a demo user, we recommend the following:

- Use the demo database only for practice and testing purposes.
- If you build your database on the demo database, remove all demo users and their database objects.

See also:

Concepts of the Database System, Demo Database [SAP Library]

9 Other Security-Relevant Information

Hazards

- **SQL Injection**

  Users insert invalid values into SQL statements and thereby cause errors in the database, precipitate a system failure or attempt to gain access to other systems.

Activities

- Checking User Input in SQL Statements [Page 6]

9.1 Checking User Input in SQL Statements

To prevent users from entering invalid values in SQL statements and thereby causing unwanted changes to the data records or to the behavior of the database application (SQL injection), we recommend the use of prepared statements.

The following table shows which prepared statements can be used with which MaxDB interfaces.

MaxDB Interfaces: Prepared Statements

Interface	Prepared Statements
JDBC	Class `PreparedStatement`
ODBC	Method `SQLPrepare`
SQLDBC	Class `SQLDBC_PrepareStatement`
PHP	`maxdb_prepare`
Perl	`prepare`
Python	Method `prepare`, class `SAPDB_Prepared`

For more information on the MaxDB interfaces, see *Concepts of the Database System*, Interfaces [SAP Library].

Example

The table APPLICATION_USER contains the users and passwords for a database application that accesses the database instance DEMODB via the MaxDB JDBC interface.

Unsecure Statement

The following user logon implementation is unsecure. It could allow an unauthorized person, by entering an invalid value, to access the database instance without entering a valid password.

```
Statement s = connection.createStatement();

ResultSet rs = s.executeQuery("SELECT * FROM APPLICATION_USERS WHERE
username = '" + username + "' and password = '" + password + "'");

 if(rs.next()) {

      // ... continue with successful logon

  } else {

      // ... unsuccessful logon

  }
```

If a person knows a valid user name, he or she can log on without entering a valid password. The value **`abcdefg' or 1=1`** , for example, could be entered for `password`.

The password would then look like this:

```
password='abcdefg' or 1=1'
```

Because `1=1` is always true, the database system always evaluates the whole expression for the password as true, regardless of whether `abcdefg` is a valid password or not.

Improved Statement

The following user logon implementation makes use of prepared statements and protects against SQL injection because special characters like `'` , for example, can no longer be entered as a password.

```
PreparedStatement ps = connection.prepare("SELECT * FROM
APPLICATION_USERS WHERE username=? and password=?");

ps.setString(1, username);

ps.setString(2, password);

 ResultSet rs = ps.executeQuery();

 if(rs.next()) {

      // ... continue with successful logon

  } else {

      // ... unsuccessful logon

  }
```

10 Trace and Log Files

Whenever the database system and database tools are in operation, log files are written. To better locate errors, you can also make use of various traces, which log additional actions. Traces can contain, for example, extracts from inserted data.

You can read traces and log files using either a text editor or the database tool Database Manager.

Hazards

- **Unauthorized reading of data**

  An unprivileged operating system user reads a trace or log file and thereby gets information about the operation of the database and possibly data from the database instance.

Activities

- Use traces only to search for errors. Delete the trace files when you have finished evaluating them.
- Restricting Access to Log Files [SAP Library]

See also:

Checking Log Files for Failed Logon Attempts [SAP Library]

Concepts of the Database System, Log Files [Page 6] and Traces [Page 6]

10.1 Restricting Access to Log Files

Use

Users can access log files using operating system commands and functions as well as with the database tool Database Manager.

Procedure

Restricting Access with Operating System Commands and Functions

On UNIX/Linux, unprivileged operating system users cannot access log files; only members of the special user group <sdba_group> can do so.

On Microsoft Windows, all operating system users can access log files. To restrict access in Microsoft Windows, proceed as described in Restricting Access to Database Resources (Microsoft Windows) [Page 6].

Restricting Access with the Database Manager

Withdraw the server authorization for reading database files from all Database Manager operators that should not have access to log files.

- *Database Manager GUI*: Withdraw the server authorization *Database File Access*. Proceed as described in Changing the Server Authorizations [SAP Library].
- *Database Manager CLI*: Withdraw the server authorization *DBFileRead*. Proceed as described in Changing the DBM Operator Data [SAP Library].

See also:

- Defining Clear Authorizations for Users [Page 6]
- *Concepts of the Database System*, Server Authorizations for the DBM Server [SAP Library]

11 Appendix

In the documentation, the syntax of commands is described using variables indicated by the angle brackets around them. The following table lists the most commonly used variables and examples.

Variable	Description	Examples
<build>	Build number of the database software	
<database_computer>	Name of the computer on which the database instance is installed	GENUA PARMA
<database_instance_type>	Database instance type	OLTP LVC
<database_name>	Name of the database instance	DEMODB
<database_user>	Database users	MONA
<database_user_password>	Password of the database user	RED BLUE
<dbm_user>	Name of a Database Manager operator	DBM OLEG
<dbm_user_password>	Password of the Database Manager operator	DBM MONDAY

Variable	Description	Examples
`<dependent_path>`	Location of the server software dependent on the database version	*Software installation only:* Microsoft Windows*: `C:\Program Files\sdb\<version>` UNIX/Linux: `/opt/sdb/<version>` *Installation of software and database instance:* Microsoft Windows*: `C:\Program Files\sdb\<database_name>` UNIX/Linux: `/opt/sdb/<database_name>`
`<file_name>`	File Name	
`<independent_data_path>`	Location of the data, configuration and run directories of database instances and applications	Microsoft Windows*: `c:\Documents and Settings\All Users\Application Data\sdb\data` UNIX/Linux: `/var/opt/sdb/data`
`<independent_program_path>`	Location of the programs and libraries used jointly by database instances and applications	Microsoft Windows*: `C:\Program Files\sdb\programs` UNIX/Linux: `/opt/sdb/programs`
`<inst_path>`	Installation path	
`<inst_profile>`	Name of the installation profile	
`<os_user>`	Name of the operating system user	ANNA
`<os_user_password>`	Operating system user’s password	MAY
`<os>`	Name of the operating system	
`<password>`	Password	
`<path>`	Path	
`<sdb_user>`	UNIX/Linux: Name of the owner of the database software (special operating system user)	sdb
`<sdba_group>`	UNIX/Linux: Name of the special operating system user group	sdba

Variable	Description	Examples
<sysdba_user>	Name of the SYSDBA user (database system administrator)	DBADMIN
<sysdba_user_password>	Password of the SYSDBA user	SECRET
<user_home>	Home directory of the operating system user	Microsoft Windows: C:\Documents and Settings\anna UNIX/Linux: /home/anna
<user_key>	User key of an XUSER entry	SAMPLEKEY
<user_name>	Name of the user	
<version>	Version number according to four-digit version notation	

* System default if MaxDB software has not yet been installed. If an older version of MaxDB exists, the installation program proposes the paths belonging to this version for the new installation.