SAP NetWeaver '04

Security Guide

Database Access Protection: MySQL MaxDB

Document Version 1.00 – April 29, 2004

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

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
	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

SAP Security Guide: MySQL MaxDB

The following sections describe the security measures that you should observe for the MySQL MaxDB [SAP Library] database system.

For information about the MaxDB database system, see Database Administration [SAP Library].
Other documentation: Documentation Overview [SAP Library]

1 Security Measures for Database Standard Users

To protect the database standard users, you should:

- Changing the Passwords of the Standard Users
- Changing Server Authorizations for Users

Changing the Passwords of the Standard Users

To protect the standard database system users, change their passwords.

You may also want to assign the property [SAP Library] `SECONDPASSWORD`, to define a second password for a user. In this way, you can allow other people temporary access to work with a user account without needing to reveal or change the original password.

Prerequisites

The database instance is in an operational state [SAP Library] in which it is possible to change the password of the relevant user.

User	Name	Required Operational State
`<DBM_user>`	First Database Manager Operator (DBM Operator) [SAP Library]	OFFLINE
`<SYSDBA_user>`	Database system administrator (SYSDBA user) [SAP Library]	ONLINE
`DOMAIN`	DOMAIN User [SAP Library]	ONLINE

Procedure

See:

Database Manager GUI: Changing a User Password [SAP Library]

Database Manager CLI: Changing the DBM User Data

Changing Server Authorizations for Users

We recommend that zou assign the server authorizations [SAP Library] individually to the users. In this way, you distribute the various administration tasks between several users and administrators.

Procedure

Database Manager GUI: Changing the Server Authorizations [SAP Library]

Database Manager CLI: Changing the DBM User Data [SAP Library]

Changing the Database Manager Operator (DBM Operator) [SAP Library] with the Database Manager CLI
Add the following server authorization for the DBM operator DBM: Starting the database instance
Delete the following server authorization for the DBM operator DBM: Stopping the database instance

```
user_put DBM SERVERRIGHTS=+StartDB, -StopDB
```

2 Measures Under UNIX

The following sections describe the measures that you need to take for the database system under UNIX:

2.1 Security Measures for Operating System Users

To protect the operating system users, change their passwords.

User	Type	Change the Password Using
`<sid>adm`	UNIX user	UNIX command **passwd**
`sqd<sid>`	UNIX user	UNIX command **passwd**

Changing the Passwords for <sid>adm and sqd<sid>

1. Log on using the user `<sid>adm`.
2. Enter the **passwd** command at the UNIX prompt.
3. Enter the old and new passwords.

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

If you use Network Information Service (NIS), you should also refer to the NIS guide and the operating system documentation, since changing the password with an activated NIS may be different from changing it with `passwd`.

2.2 Authorization Concept for Database-Related Resources

The access rights are automatically set during installation. The authorization concept for the files and directories up to **database version 7.4.03** (inclusive) is shown in the table below:

Authorization Concept for SAP System Directories and Files (up to Database Version 7.4.03)

Directories	Privilege	Owner	Group	Comment
`/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`	
Files				
`/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
Raw devices for the database system	660	`sqd<sid>`		Link to the raw devices used as data volumes or log volumes.

You can change the access privileges. For information about how to do this, see Assigning Access Privileges for Files and Directories [Page 9] beschrieben.

New Developments with Database Version 7.5

As of the **database version 7.5**, the access privileges for the directories and files are only set during installation and, if required, by the database tools. The owner **sdb** and the group **sdba** are assigned. For more information, see the *Installation Manual*: Authorization Concept for UNIX Operating Systems [SAP Library].

In particular, all volumes also receive these access privileges. This means that all members of the **sdba** group have access to the volumes. If the security of your system requires it, the administrator can restrict these access privileges by assigning the volumes to instance-specific groups with a DBM command. To provide the highest level of security, the administrator can assign an empty group to a volume, so that only the database instance itself had access to the volumes.

Version 7.5 and an Older Version Are Installed Together on One Server

You may have to change the access privileges for the directory `/sapdb/<SID>DB` of the database version below 7.5 to 755, so that the database processes of version 7.5 have unrestricted access to all directories.

2.2.1 Assigning Access Privileges for Directories and Files

Before changing the access privileges, save your current settings. This procedure is only relevant for database instances up to **version 7.4** (inclusive).

Saving Current Settings

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` (as of **database version 7.5**, only the root user can access these directories, with either read or write accesses)

Setting Access Privileges

To change the access privileges for a file or a directory, use the `chmod` command as shown below:

```
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.

3 Measures Under Microsoft Windows

The following sections describe the measures that you need to take for the database system under Microsoft Windows operating systems:

- Security Measures for the Operating System User <SID>ADM
- Access Privileges for Database-Related Resources

Security Measures for the Operating System User <SID>ADM

To protect the operating system user <SID>ADM, change his/her password.

Access Privileges for Database-Related Resources

If you are using a Microsoft Windows operating system, the volumes of the database instance are automatically protected. Only the administrator group has full access privileges for the volumes, and all other users have no access.

However, you must protect the database directory [SAP Library] `<independent_data_path>\config`, which contains the configuration files for the database instance. Set the following access privileges for the directory `<independent_data_path>\config` and all the files it contains:

- *Full Control* access privileges for the local group `Administrators`
- No access privileges for other groups or users

If you want to exclude all other users from access to the database instance using database tools, set the following privileges for the directory `<independent_data_path>` and all its subdirectories.

- *Full Control* access privileges for the local group `Administrators`
- No access privileges for other groups or users