Security Commander SQL Server Mirroring Guide

Content

Contact information

For contact information, see www.interlogix.com.au.

Description

Database mirroring is a software solution for increasing database reliability. In this configuration two copies of a single database exist on different servers. The principal server instance provides the database to clients. The mirror server is a standby server that becomes a source for the principal server recovery in case of possible data loss.

Preconditions

Security Commander supports SQL Server 2008 R2 mirroring in high-safety mode with automatic failover.

Three SQL Server 2008 R2 instances are required for using this configuration. Two of them (the principal server and the mirror server) should be set up using Microsoft SQL Server 2008 R2 Standard or Enterprise Edition. The third one, the witness server, can be set up using the free SQL Server Express Edition.

Provided Security Commander feature requires professional Microsoft SQL Server 2008 R2 administration skills. Security Commander supports Microsoft solution if conditions given in "Mirroring diagnostics" on page 13 are met, but mirroring configuration and maintenance remains in user's responsibility.

Installing SQL Server 2008 R2 for mirroring

During the setup procedure for SQL Server 2008 R2, set the options and values described below.

To install SQL Server 2008 R2 for mirroring:

1. In Features Selection, select at least Database Engine Services, Management Tools-Basic, and Management Tools - Complete.
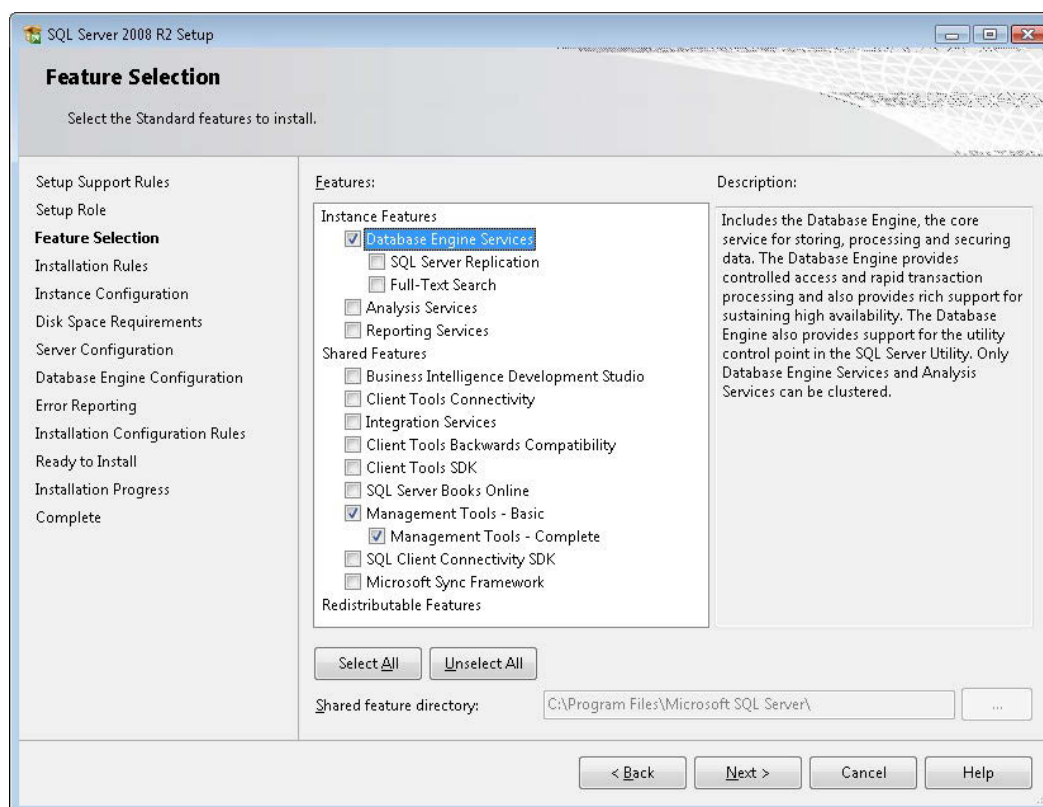
2. In Instance Configuration, click Named Instance and enter the instance name: SPSQL.
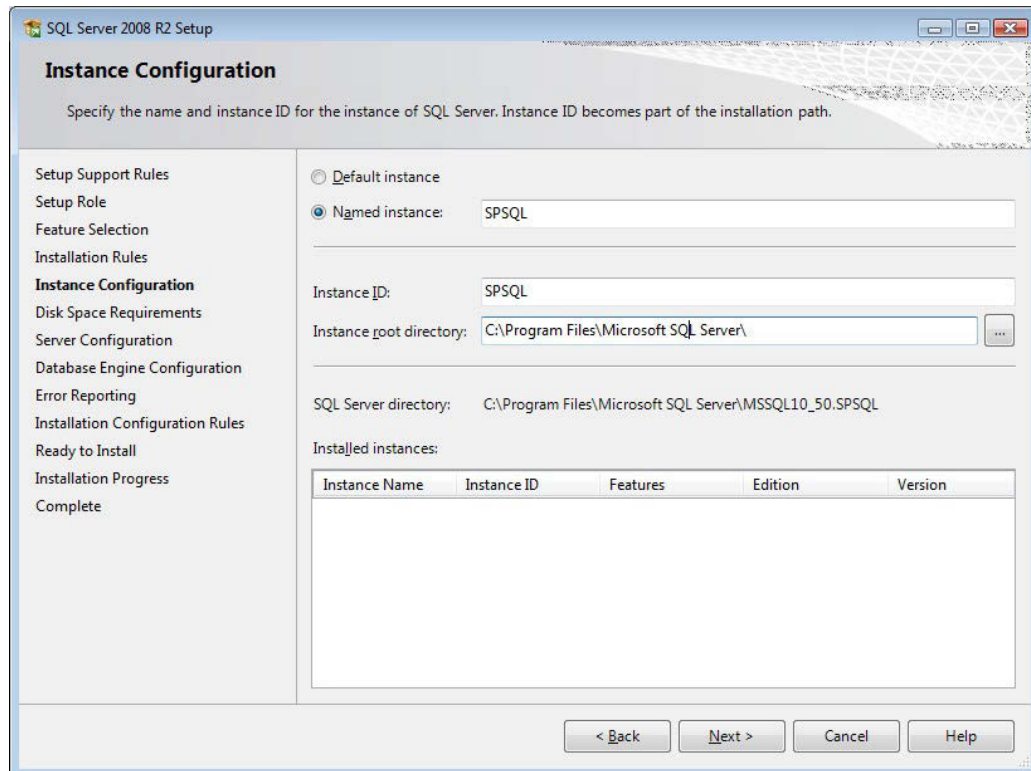
3. In Server Configuration > Service Account, Server Database Engine Account Name should be set to "NT AUTHORITY\SYSTEM"

4. In Database Engine Configuration, click Mixed Mode.

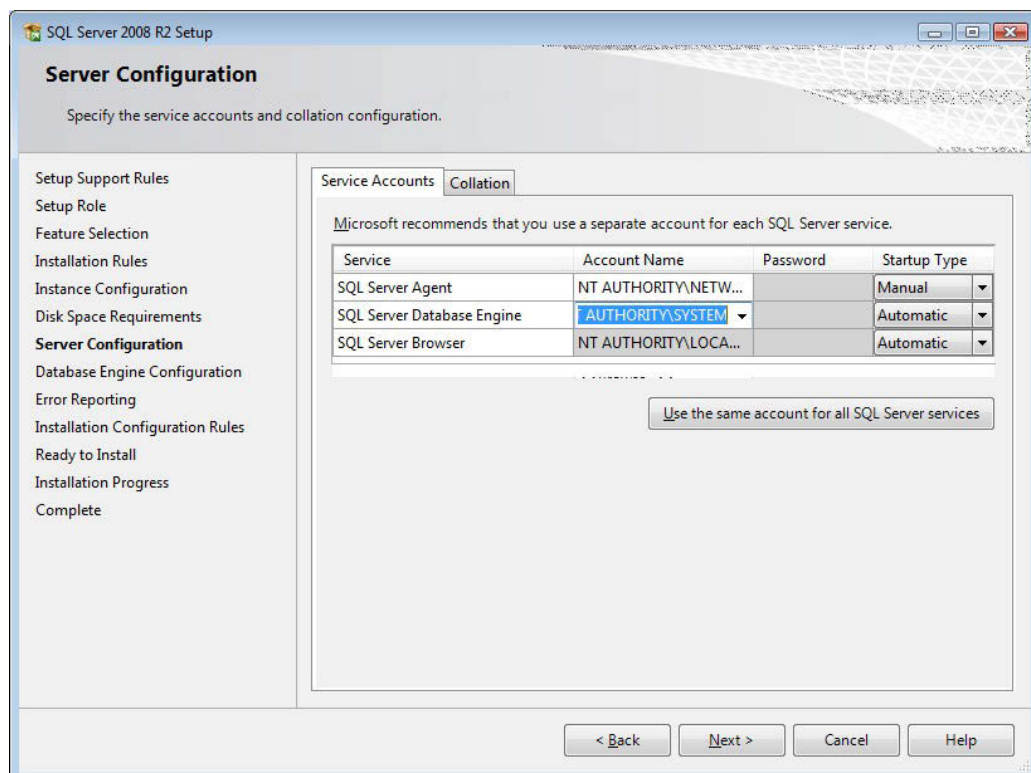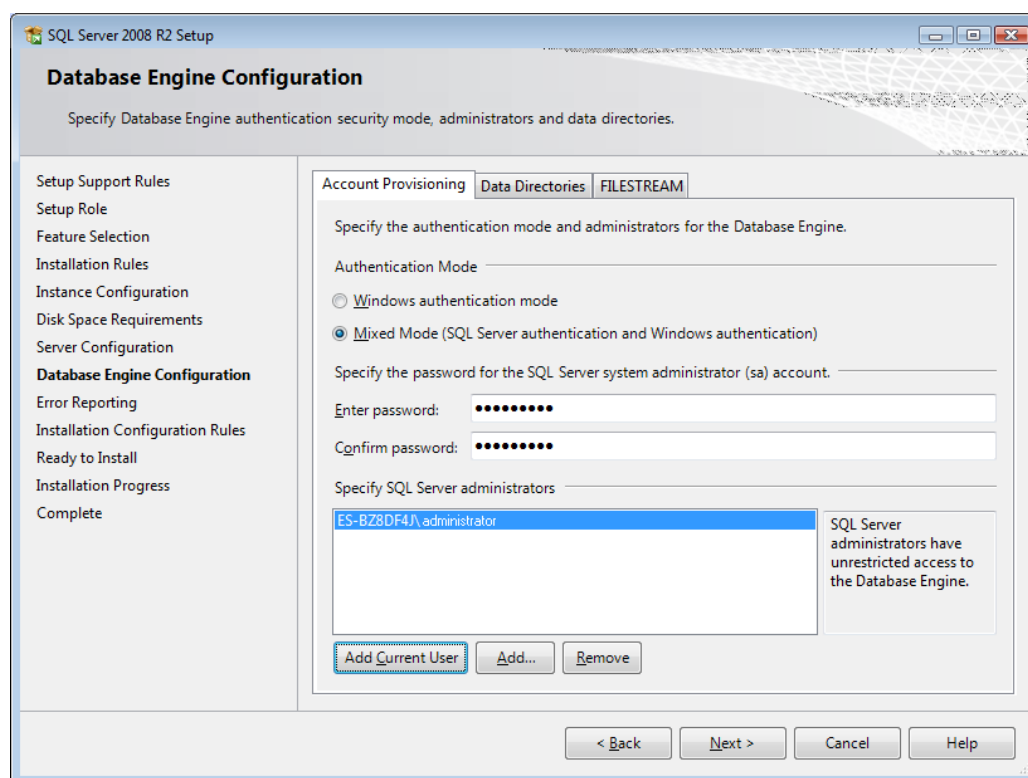Click Add Current User to add currently logged Windows user as an SQL server administrator.

Note: Specify the same "sa" passwords for both the principal and mirror instances. (Security Commander License and DB Maintenance applications assume that the same "sa" passwords are set). Make sure that the selected password is in line with the password policies on the principal and mirror instances (when applicable).

Preconditions checklist

For each instance (principal, mirror, and witness), check that the TCP/IP properties are set as shown below (click Start > Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > SQL Server Configuration Manager).

Figure 1: TCP/IP properties
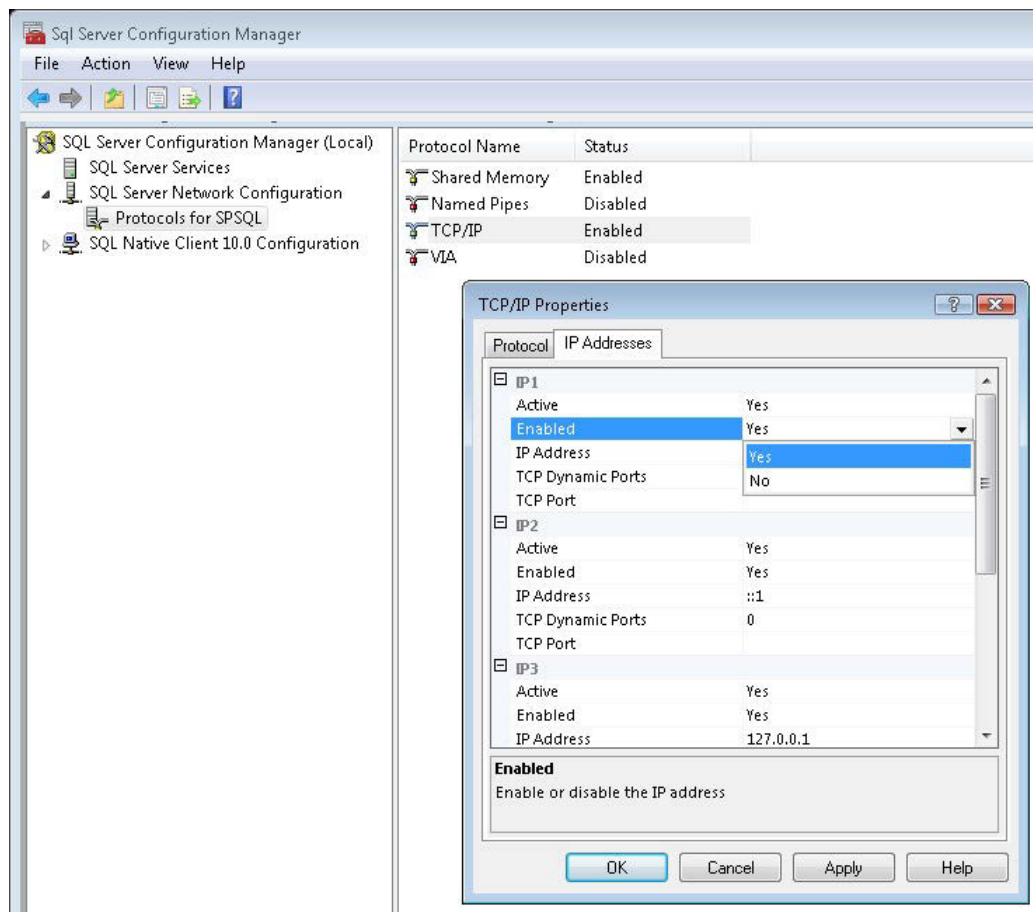
Executing scripts

To execute a script, open SQL Server Management Studio.

To access SQL Server Management Studio:

1. On the taskbar, click Start.

2. Click All Programs.

3. Click Microsoft SQL Server 2008 R2.

4. Click SQL Server Management Studio.

To execute a script in SQL Server Management Studio:

1. Connect to the database instance.

   In the example below the database instance is mirror.ace.domain\spsql.

2. Click New query.
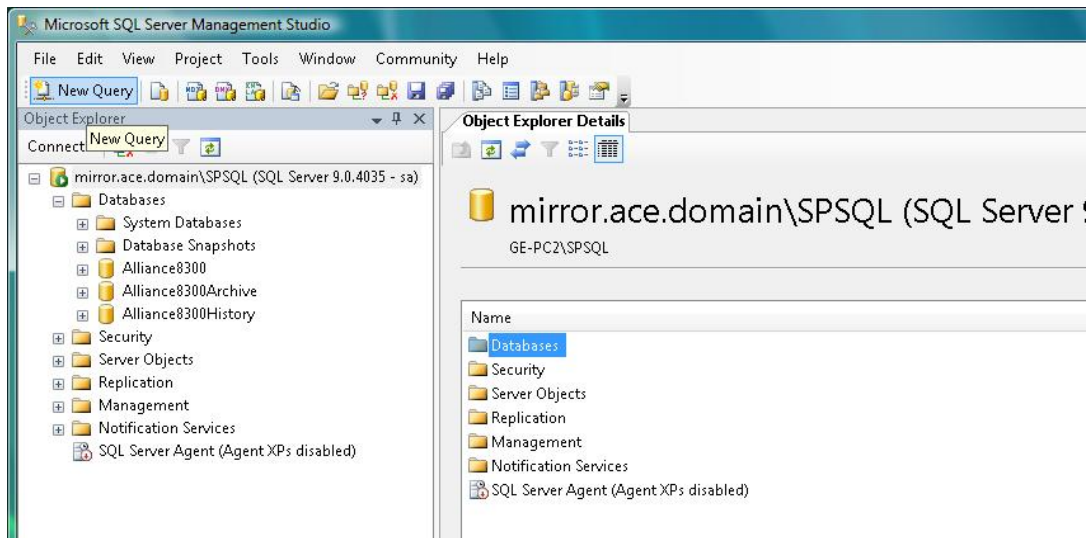
3. Enter your script to the window on the right upper and click Execute.
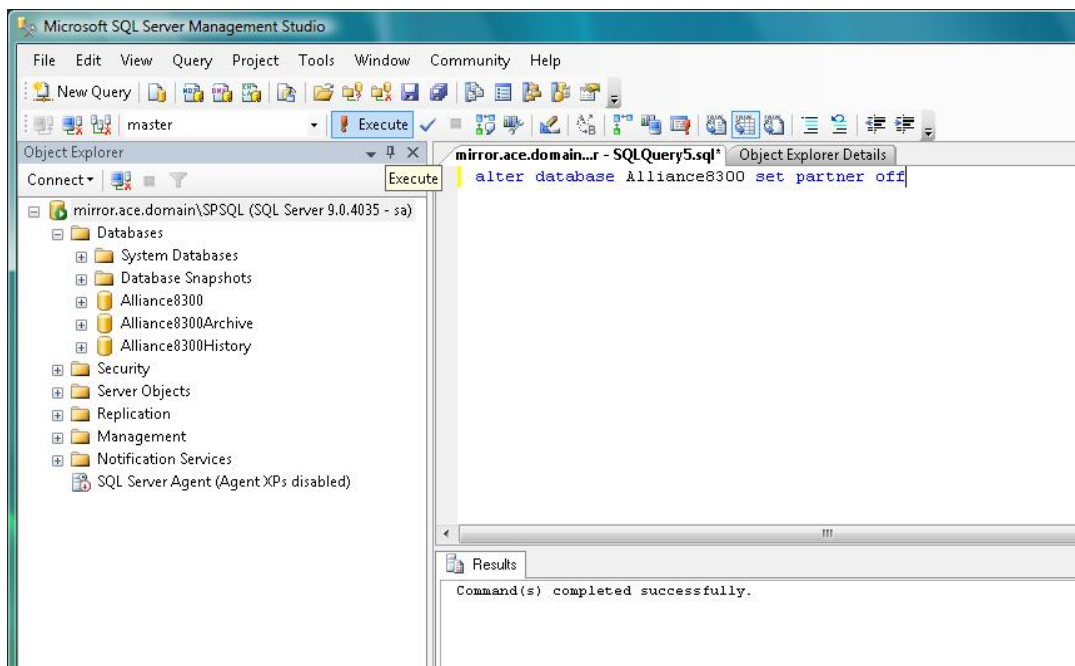
The result of the script execution is shown in the right lower window.

Setting up mirroring

Create the alliance database on the principal SQL server instance. Use Security Commander > Create Security Commander Database.

Create master key encryption to generate certificates on each instance.

Principal: On the principal SQL server execute the following script (change the italic text to fit your requirements). See "Executing scripts" on page 5 for more details.

```
create master key encryption by password = 'enter your
password';

create certificate HOST_Principal_cert with subject =
'HOST_Principal certificate', start_date = '2008/11/01',
expiry_date = '2020/11/01';

GO

create endpoint endpoint_mirroring state = started as
tcp(listener_port = 5022, listener_ip = all) for
database_mirroring (authentication = certificate
HOST_Principal_cert, encryption = required algorithm RC4,
role = ALL);

backup certificate HOST_Principal_cert to file =
'C:\HOST_Principal_cert.cer'
```

Note: The password, start and expiry dates, and port number that you provide in the script above must be the same for all following scripts for other instances.

Mirror: On the mirror SQL server execute this script (change the italic text to fit your requirements).

```
create master key encryption by password = 'enter your
password';

create certificate HOST_Mirror_cert with subject =
'HOST_Mirror certificate', start_date = '2008/11/01',
expiry_date = '2020/11/01';

GO

create endpoint endpoint_mirroring state = started as
tcp(listener_port = 5022, listener_ip = all) for
database_mirroring (authentication = certificate
HOST_Mirror_cert, encryption = required algorithm RC4, role
= ALL);

backup certificate HOST_Mirror_cert to file =
'C:\HOST_Mirror_cert.cer'
```

Witness: On the witness SQL server execute this script (change the italic text to fit your requirements).

```
create master key encryption by password = 'enter your
password';

create certificate HOST_Witness_cert with subject =
'HOST_Witness certificate', start_date = '2008/11/01',
expiry_date = '2020/11/01';

GO
```

```
create endpoint endpoint_mirroring state = started as
tcp(listener_port = 5022, listener_ip = all) for
database_mirroring (authentication = certificate
HOST_Witness_cert, encryption = required algorithm RC4,
role = Witness);

backup certificate HOST_Witness_cert to file =
'C:\HOST_Witness_cert.cer'
```

For the operations above, we recommend using Microsoft SQL Server Management Studio.

Granting connection rights between each instance

Before executing the following scripts, you need to copy all certificate files created and saved in the previous step to all machines taking part in the mirroring process (the principal, mirror, and witness servers).

Principal: On the principal SQL server it is necessary to grant connection rights for the mirror and witness servers. Execute these scripts. Change the italic text to fit your requirements.

To grant mirror connection rights on the principal instance, run the following script.

```
create login HOST_Mirror_login with PASSWORD = 'enter your
password';

create user HOST_Mirror_user from login HOST_Mirror_login;

create certificate HOST_Mirror_cert Authorization
HOST_Mirror_user From file = 'C:\HOST_Mirror_cert.cer'
ACTIVE FOR BEGIN_DIALOG = ON;

grant CONNECT ON Endpoint::endpoint_mirroring to
[HOST_Mirror_login]
```

Note: The password that you provide in the script above must be the same for all following scripts for other instances.

To grant witness connection rights on the principal instance, run the following script.

```
create login HOST_Witness_login with PASSWORD = 'enter your
password';

create user HOST_Witness_user from login
HOST_Witness_login;

create certificate HOST_Witness_cert Authorization
HOST_Witness_user From file = 'C:\HOST_Witness_cert.cer'
ACTIVE FOR BEGIN_DIALOG = ON;
```

```
grant CONNECT ON Endpoint::endpoint_mirroring to
[HOST_Witness_login]
```

Mirror: On the mirror SQL server it is necessary to grant connection rights for Principal and Witness hosts. Execute these scripts. Change the italic text to fit your requirements.

To grant principal connection rights on the mirror instance, run the following script.

```
create login HOST_Principal_login with PASSWORD = 'enter
your password';
create user HOST_Principal_user from login
HOST_Principal_login;
create certificate HOST_Principal_cert Authorization
HOST_Principal_user From file =
'C:\HOST_Principal_cert.cer' ACTIVE FOR BEGIN_DIALOG = ON;
grant CONNECT ON Endpoint::endpoint_mirroring to
[HOST_Principal_login]
```

To grant witness connection rights on the mirror instance, run the following script.

```
create login HOST_Witness_login with PASSWORD = 'enter your
password';
create user HOST_Witness_user from login
HOST_Witness_login;
create certificate HOST_Witness_cert Authorization
HOST_Witness_user From file = 'C:\HOST_Witness_cert.cer'
ACTIVE FOR BEGIN_DIALOG = ON;
grant CONNECT ON Endpoint::endpoint_mirroring to
[HOST_Witness_login]
```

Witness: On the witness SQL server it is necessary to grant connection rights for Principal and Mirror hosts. Execute these scripts. Change the italic text to fit your requirements:

To grant principal connection rights on the witness instance, run the following script.

```
create login HOST_Principal_login with PASSWORD = 'enter
your password';
create user HOST_Principal_user from login
HOST_Principal_login;
```

```
Create certificate HOST_Principal_cert Authorization
HOST_Principal_user From file =
'C:\HOST_Principal_cert.cer' ACTIVE FOR BEGIN_DIALOG = ON;

Grant CONNECT ON Endpoint::endpoint_mirroring to
[HOST_Principal_login]
```

To grant mirror connection rights on the witness instance, run the following script.

```
create login HOST_Mirror_login with PASSWORD = 'enter your
password';

create user HOST_Mirror_user from login HOST_Mirror_login;

Create certificate HOST_Mirror_cert Authorization
HOST_Mirror_user From file = 'C:\HOST_Mirror_cert.cer'
ACTIVE FOR BEGIN_DIALOG = ON;

Grant CONNECT ON Endpoint::endpoint_mirroring to
[HOST_Mirror_login]
```

Backing up database for mirroring on the principal server

You need to set full recovery model for your databases to enable the mirroring feature. Run the following scripts.

```
ALTER DATABASE Alliance8300 SET RECOVERY FULL

ALTER DATABASE Alliance8300Archive SET RECOVERY FULL

ALTER DATABASE Alliance8300History SET RECOVERY FULL
```

To back up the database and database logs, run the following scripts.

```
Backup Database Alliance8300 to
DISK='C:\Alliance8300_FULL.bak';

Backup Database Alliance8300Archive to
DISK='C:\Alliance8300Archive_FULL.bak';

Backup Database Alliance8300History to
DISK='C:\Alliance8300History_FULL.bak';

Backup Log Alliance8300 to
Disk='C:\Alliance8300_FULL_Log.bak';

Backup Log Alliance8300Archive to
Disk='C:\Alliance8300Archive_FULL_Log.bak';

Backup Log Alliance8300History to
Disk='C:\Alliance8300History_FULL_Log.bak';
```

Restoring database files for mirroring on the mirror server

To restore the database and database logs, copy all six backup files to the mirror server, and then run the following script.

```
Restore Database Alliance8300 from
DISK='C:\Alliance8300_FULL.bak' with replace, NORECOVERY,
MOVE 'Alliance8300DAT' TO 'C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\Data\Alliance8300.mdf', MOVE
'Alliance8300_log' TO 'C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\Data\Alliance8300.ldf';

Restore Database Alliance8300Archive from
DISK='C:\Alliance8300Archive_FULL.bak' with replace,
NORECOVERY, MOVE 'Alliance8300ArchiveDAT' TO 'C:\Program
Files\Microsoft SQL
Server\MSSQL.1\MSSQL\Data\Alliance8300Archive.mdf', MOVE
'Alliance8300Archive_log' TO 'C:\Program Files\Microsoft
SQL Server\MSSQL.1\MSSQL\Data\Alliance8300Archive.ldf';

Restore Database Alliance8300History from
DISK='C:\Alliance8300History_FULL.bak' with replace,
NORECOVERY, MOVE 'Alliance8300HistoryDAT' TO 'C:\Program
Files\Microsoft SQL
Server\MSSQL.1\MSSQL\Data\Alliance8300History.mdf', MOVE
'Alliance8300History_log' TO 'C:\Program Files\Microsoft
SQL Server\MSSQL.1\MSSQL\Data\Alliance8300History.ldf';


Restore Log Alliance8300 from
Disk='C:\Alliance8300_FULL_Log.bak' with replace,
NORECOVERY;

Restore Log Alliance8300Archive from
Disk='C:\Alliance8300Archive_FULL_Log.bak' with replace,
NORECOVERY;

Restore Log Alliance8300History from
Disk='C:\Alliance8300History_FULL_Log.bak' with replace,
NORECOVERY;
```

Starting mirroring

Mirror: On the mirror instance execute following scripts. Use full domain addresses (see the Note on page 12).

```
alter database Alliance8300 set partner =
'TCP://principal.ace.domain:5022'

alter database Alliance8300History set partner =
'TCP://principal.ace.domain:5022'
```

```
alter database Alliance8300Archive set partner =
'TCP://principal.ace.domain:5022'
```

Principal: On the principal instance execute following scripts. Use full domain addresses (see the Note below).

```
alter database Alliance8300 set partner =
'TCP://mirror.ace.domain:5022'
alter database Alliance8300History set partner =
'TCP://mirror.ace.domain:5022'
alter database Alliance8300Archive set partner =
'TCP://mirror.ace.domain:5022'
```

```
alter database Alliance8300 set witness =
'TCP://witness.ace.domain:5022'
alter database Alliance8300History set witness =
'TCP://witness.ace.domain:5022'
alter database Alliance8300Archive set witness =
'TCP://witness.ace.domain:5022'
```

Witness: On the witness machine restart SQL Server service.

Note: If you are using workgroups, use this file to simulate domain addresses: c:\WINDOWS\system32\drivers\etc\hosts.

Hosts file content example:

```
3.228.248.158 principal.ace.domain
3.228.95.120 mirror.ace.domain
3.228.95.121 witness.ace.domain
```

Note: If you are using a hosts file to simulate domain addresses, remember to modify it on every Security Commander machine, because Security Commander gets the mirroring information from the principal database server and uses simulated domain addresses to gain database access.

Mirroring diagnostics

Use Microsoft SQL Server Management Studio to diagnose the mirroring state. Right-click on any of Security Commander databases, and then click Launch Database Mirroring Monitor from the context menu (note that Microsoft SQL Server Management Studio Express does not include this tool). Register all three Security Commander databases and check whether the connections are established. Properly configured mirroring should look like the following example.

Figure 2: Correctly configured mirroring
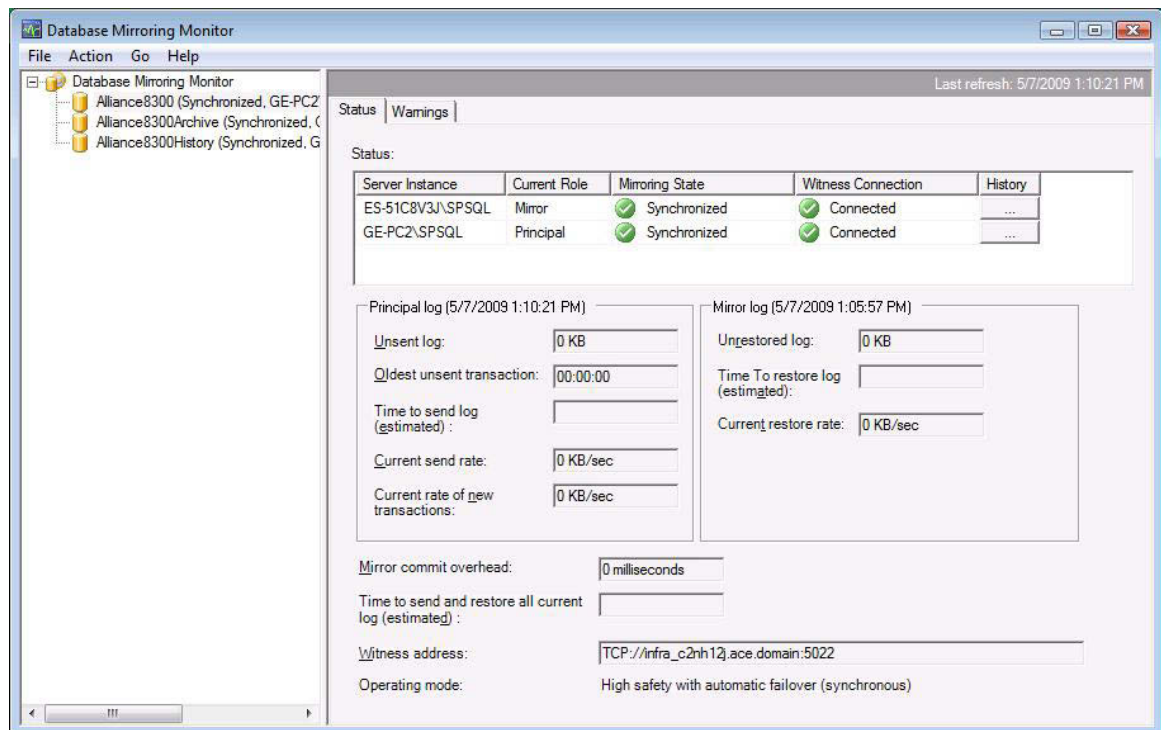
Security Commander License Setup

Security Commander License Setup checks the mirroring configuration. If the mirroring is properly configured, the databases are synchronized, and the witness instance is connected, then License Setup sets up the mirror instance for Security Commander while registering its license. Every Security Commander Client has to be registered to use the mirroring feature.

DB Maintenance

Before using the Security Commander DB Maintenance tool, please use Database Mirroring Monitor to check that all Security Commander databases are synchronized, and that the Principal role of each is set for the same machine (GE-PC2 in Figure 2 on page 13). In case if one of the Security Commander databases is currently on other machine, you must use the following script to safely failover the database. This example is for the Alliance8300History database. Execute the following script on the principal instance for the Alliance8300History database.

```
alter database Alliance8300History set partner failover
```

The backup function backs up Security Commander databases to the current principal server local file system.

The restore function requires mirroring to be stopped. To stop mirroring on the principal instance, execute the following scripts.

```
alter database Alliance8300 set witness off
alter database Alliance8300History set witness off
alter database Alliance8300Archive set witness off

alter database Alliance8300 set partner off
alter database Alliance8300History set partner off
alter database Alliance8300Archive set partner off
```

Restore functions can now be run.

Note: Mirroring must be stopped as well before removing Security Commander database.

The restoring process runs on the PC that was chosen as a database server during the Security Commander installation. The backup files must be accessible locally on this PC.

After the restore operation, you must go to backup for mirroring (see "Backing up database for mirroring on the principal server" on page 10) and start mirroring again.

Note: The database logs are not automatically compressed and archived when mirroring is configured and working. In this case the user is responsible for handling Security Commander database log files and assuring the necessary disk space for DB services.

Troubleshooting

Error Message 1418: The server network address cannot be reached

This SQL Server message indicates that the server network address cannot be reached or does not exist, and it suggests that you check the network address name and reissue the command.

Corrective action might be required on both partners. For example, if this message is raised when you are trying to run SET PARTNER on the principal server instance, the message might imply that you only have to take corrective action on the mirror server instance. However, corrective actions might be required on both partners.

Take the following additional corrective actions:

- Check the DNS entries.

- Make sure that the mirror database is ready for mirroring.

- Make sure that that name and the port of the mirror server instance are correct.

- Make sure that the destination mirror server instance is not behind a firewall.

- Make sure that the principal server instance is not behind a firewall.

- Verify that the endpoints are started on the partners by using the state or state_desc column the of the sys.database_mirroring_endpoints catalog view. If either endpoint is not started, execute an ALTER ENDPOINT statement to start it.

- Make sure that the principal server instance is listening on the port assigned to its database mirroring endpoint and that and the mirror server instance is listening on its port. For more information, see "Verifying Port Availability," later in this topic. If a partner is not listening on its assigned port, modify the database mirroring endpoint to listen on a different port.

Database connection is lost

When the database connection is lost, Security Commander displays the following message.

Figure 3: Restore database message

Restore the database connection by clicking Restore. After the "Connection restored" message appears, use the Database Mirroring Monitor to diagnose the mirroring configuration and check that all instances are connected (as described in "Mirroring diagnostics" on page 13).

Cannot connect to database on remote computer during Security Commander installation or during database mirroring configuration

Check the following:

• TCP is enabled in SQL Server (configuration is described in "Preconditions checklist" on page 4)

• Proper exceptions are configured in Windows Firewall (ports 5022 as given in the examples before, 1433, 1434, UPnP Framework (in Windows XP) and SQL Server Surface Area are enabled)

• SQL Server Browser is started

The remote copy of database "Alliance8300" has not been rolled forward...

MS SQL Management Studio displays the error message: "The remote copy of database 'Alliance8300' has not been rolled forward to a point in time that is encompassed in the local copy of the database log (Microsoft SQL Server, Error: 1412)" when trying to start mirroring (see "Starting mirroring" on page 11) on the principal instance.

Try to put databases on the principal instance offline after backing up the database for mirroring on the principal server (see "Backing up database for mirroring on the principal server" on page 10). Put these back online before starting mirroring on the mirror server.

Here is an example script that puts databases offline (on the principal instance):

```
ALTER DATABASE Alliance8300 SET SINGLE_USER WITH ROLLBACK
IMMEDIATE

ALTER DATABASE Alliance8300Archive SET SINGLE_USER WITH
ROLLBACK IMMEDIATE

ALTER DATABASE Alliance8300History SET SINGLE_USER WITH
ROLLBACK IMMEDIATE

EXEC sp_dboption 'Alliance8300', 'offline', 'TRUE';

EXEC sp_dboption 'Alliance8300Archive', 'offline', 'TRUE';

EXEC sp_dboption 'Alliance8300History', 'offline', 'TRUE';
```

Here is an example script that puts databases online (on the principal instance):

```
ALTER DATABASE Alliance8300 SET MULTI_USER

ALTER DATABASE Alliance8300Archive SET MULTI_USER

ALTER DATABASE Alliance8300History SET MULTI_USER

EXEC sp_dboption 'Alliance8300', 'offline', 'FALSE';

EXEC sp_dboption 'Alliance8300Archive', 'offline', 'FALSE';

EXEC sp_dboption 'Alliance8300History', 'offline', 'FALSE';
```

Glossary

Mirror role. Database server partner that acts a passive role, meaning it is not available for database client. Depending on the mirroring configuration, transaction logs are synchronously or asynchronously updated basing on Principal activity.

Principal role. Database server partner that acts an active role, meaning it is available for database client connections.

Quorum. Minimal number of participants required for a failover decision (switching principal/mirror roles).

Witness role. Database server partner, acting as a quorum member, supports switch role decision.