

Using IBM Database Encryption Expert to protect your sensitive data

Guard against security breaches for DB2 and Informix Dynamic Server

Skill Level: Introductory

[Masahiro Ohkawa \(mohkawa@jp.ibm.com\)](mailto:mohkawa@jp.ibm.com)

Yamato Software Development Laboratory (YSL)
IBM Japan

[Soh Kaijima \(kaijima@jp.ibm.com\)](mailto:kaijima@jp.ibm.com)

Yamato Software Development Laboratory (YSL)
IBM Japan

[Gou Nakashima \(gnaka@jp.ibm.com\)](mailto:gnaka@jp.ibm.com)

Yamato Software Development Laboratory (YSL)
IBM Japan

[Asuka Tokunaga \(asukat@jp.ibm.com\)](mailto:asukat@jp.ibm.com)

Yamato Software Development Laboratory (YSL)
IBM Japan

02 Jul 2009

IBM® Database Encryption Expert provides features to encrypt and control access to data written to file systems and database backup images. Beginning with Version 1.1 Fix Pack 3, the product supports both DB2® and Informix® Dynamic Server (IDS). This article describes some of the key features and mechanisms of Encryption Expert and shows you how to use them.

Introduction

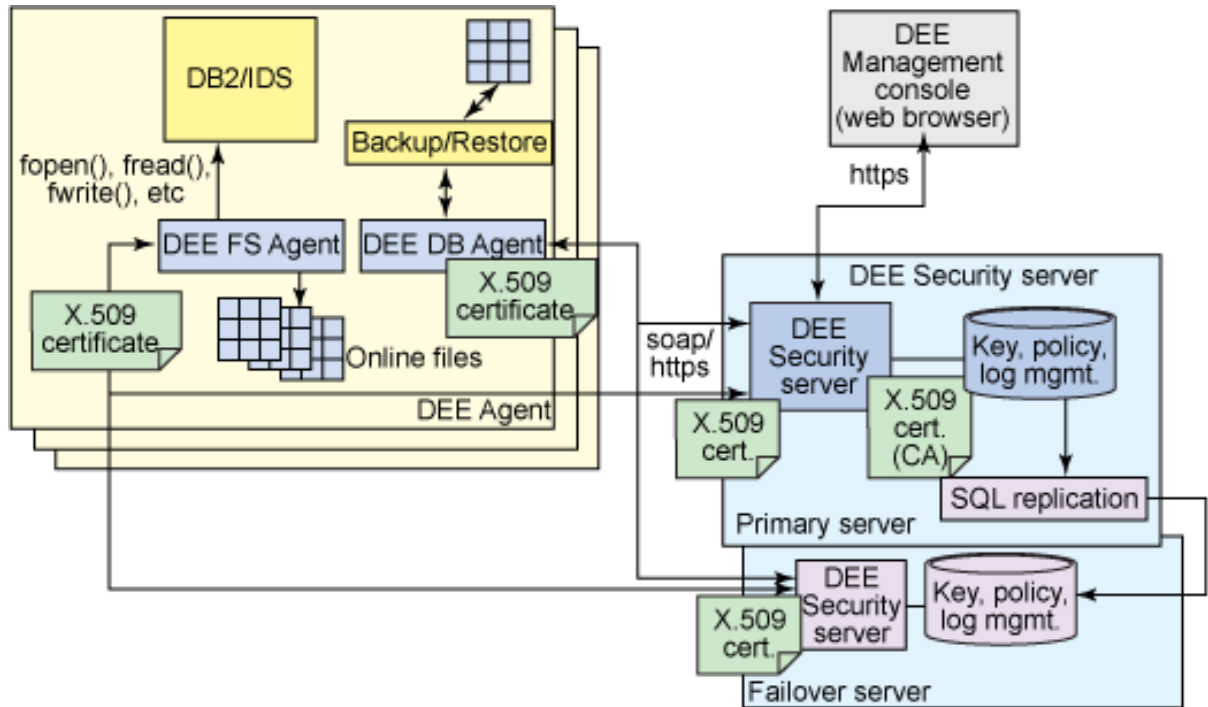
IBM Database Encryption Expert (also referred to as Encryption Expert or DEE)

protects data by using a policy-based system. The policies that Encryption Expert uses contain one or more encryption keys and one or more rules for access control. There are two types of policies:

- An *online policy* is used for encrypting data written to a file system and protecting data with access control. When an online policy is applied to a directory, the policy controls access to files and directories under the directory. The action of applying an online policy to a directory is called *Guard FS (File System)*, the directory is called the *Guard Point*, and the data read from or written to the file system is called *Online Data*. Any application that is allowed access by the policy can access the files that are under guard points as long as the application uses system libraries to access the files. Data is automatically encrypted when writing, and decrypted when reading, based on the policy. The encryption is transparent to the application, and you do not need to make any changes to the application itself.
- An *offline policy* is used for protecting database backup images. An offline policy is applied to a machine that is used for backing up and restoring database images. The offline policy controls backup and restore commands, and the encryption and decryption of database backup images. The action of applying an offline policy to a machine is called *Guard DB (Database Backup)*.

Figure 1 shows an overview of the Encryption Expert architecture. It consists of one or more security servers and one or more agents. The security server has configuration information, such as online and offline policies, and audit logs from the agents. The data for the configuration information and audit logs is stored in the DB2 that is bundled with Encryption Expert.

Figure 1. IBM Database Encryption Expert architecture overview



An Encryption Expert agent is installed on a machine where data is protected (the *host* machine). Policies that are kept in the security server are sent to the agent (pushed), or retrieved by the agent (pulled) as necessary. The agent consists of a FS (File System) agent, which guards FS, and a DB (Database Backup) agent, which guards DB. Audit logs, for things such as access violations, are sent to the security server by default.

The security server provides a Web-based interface called the Management Console, which you can use for tasks such as configuring policies and browsing audit logs. To use the Management Console, open a Web browser and go to the following URL:

`https://hostname:8445`

Figure 2 is a screen shot of the Encryption Expert Management Console dashboard as displayed in a Japanese-language browser.

Figure 2. Encryption Expert Management Console

Welcome to the Encryption Expert Management Console – Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

アドレス(D) https://srv1.yamato.ibm.com:8445/app/console 移動 リンク

IBM Log Out
Logged in as: mohkawa

Dashboard Administrators Hosts Keys Policies High Availability Log Configuration

Encryption Expert Management Console

Version: 1.1.3.0, Build: uni_78i

Server Name: cube.yamato.ibm.com, Server time: 2009-04-15 09:53:42.204

Your last login was at 12:23 AM on 04/02/2009

Password is going to expire in 4 days. [Change Password](#)

There are currently 0 other administrators logged in to the security server.

HA Info: srv1.yamato.ibm.com (Primary Server)

The fingerprint for the CAs is 74:18:DF:01:98:06:E6:34:8F:EB:1B:39:BE:9F:F4:8C:D3:98:CE:DF

File System: /dev/sda1 Total Space:49213MB Free Space:29191MB Use:38% Mounted On: /

Configuration Summary	Security Summary
5 Administrator(s)	0 Access Deny events in previous hour
5 Hosts, 0 Host Groups	0 Access Deny events in previous 24 hours
31 Asymmetric Keys, 57 Symmetric Keys, 36 Key Groups	0 Access Deny events in previous week

ページが表示されました Internet

You can configure the security server over multiple machines to allow for both primary and failover servers. The failover servers are read-only and are populated by replicating with the primary server.

The primary server acts as the Certificate Authority (CA) and publishes X.509 certificates to the security servers and the agents. The X.509 certificates are used for authentication. Secure Socket Layer (SSL) protocol is used for communicating

between the security server and each agent, and between the primary server and each failover server.

Configuring for high availability

Two features of Encryption Expert that help you to ensure high availability are the use of failover servers and encryption key caching.

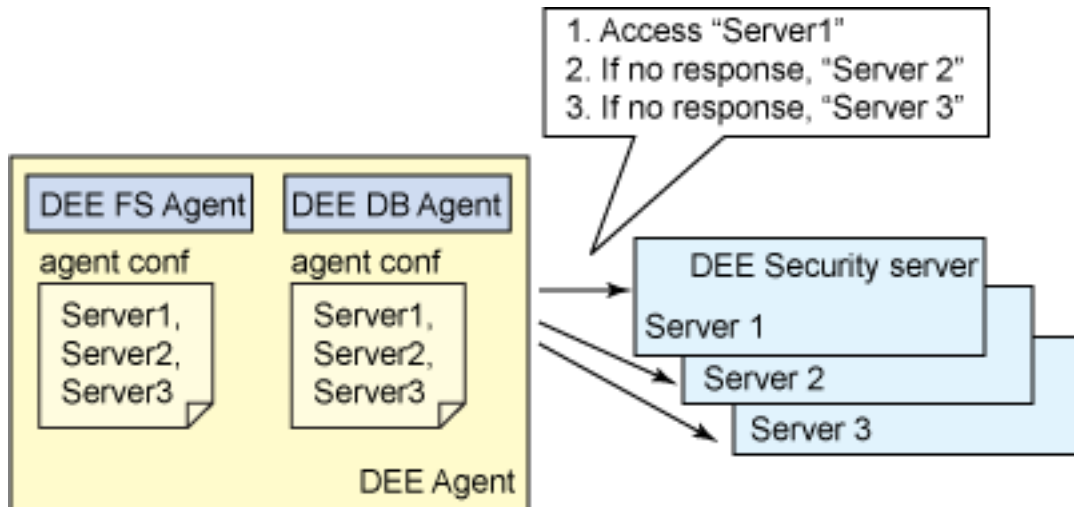
Failover servers

As mentioned in the introduction, you can configure failover servers that can take over in the event of a failure of the primary security server. Using SQL replication technology provided by Encryption Expert, you can synchronize the configuration of failover servers with the configuration of the primary server. With SQL replication, the capture program (asncap) retrieves change records from the database log and stores them to staging tables. The apply program (asnapply) retrieves data from the staging tables every minute and applies the changes to the failover servers. Both programs run on the primary server. Audit logs are not replicated. Each failover server can receive an audit log from the agents and store it independently of other security servers.

Once the failover server is set up, the agent can access it (read-only). Figure 3 shows how the agent chooses a security server to communicate with. Each FS and DB agent has its own configuration file named `agent.conf`. You can edit the `agent.conf` files to configure the order in which the security server is chosen. If the agent cannot communicate with the first server, it moves to the next, and so on.

For more information, refer to the "Installing and configuring the Encryption Expert Failover Server" section in "Chapter 3: Installing, removing, and upgrading Encryption Expert" of the *IBM Database Encryption Expert User's Guide*, which is linked to from the [Resources](#) section.

Figure 3. Failover server mechanism



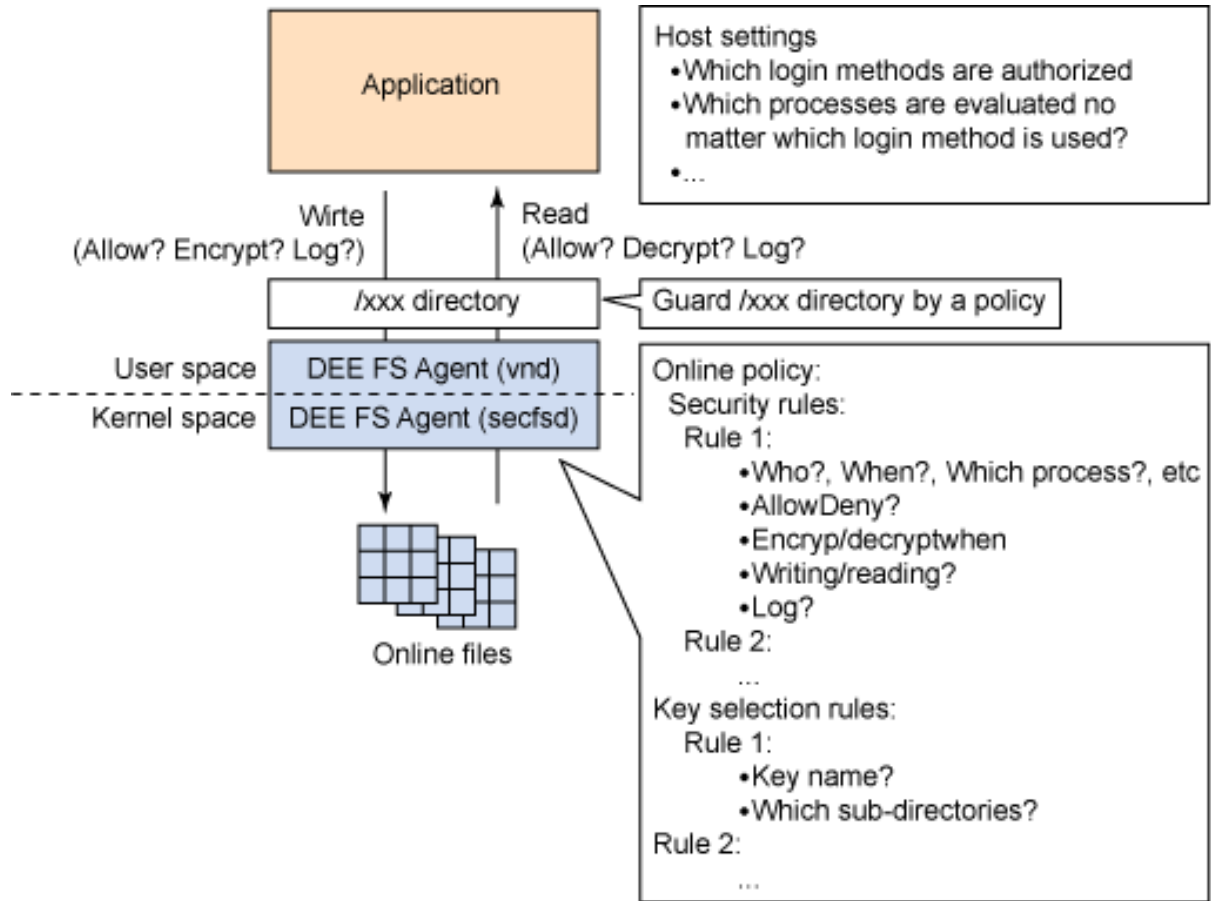
Cache the encryption key on the host

Each encryption key for online data has an option called *Cached on Host*. If an encryption key is created with this option, the encryption key is stored on the agent disk with password protection. As a result, the agent can work correctly even if the security server has not been running correctly since the agent start-up time. This is described in more detail in the following section.

Protecting online data

Encryption Expert uses symmetric encryption algorithms (3DES, AES128, AES256) for encrypting online data. Figure 4 shows an overview of how this works. An online policy holds one or more encryption keys and rules for access control. You can use the same encryption key or different encryption keys against files and directories under the guard point. Rules for access control are configured as *Security Rules*. Encryption keys are configured as *Key Selection Rules*. When you apply an online policy to a directory on a host by using the Management Console, the policy is saved in the security server and is sent to the FS agent on the host.

Figure 4. Protect online data



The FS agent consists of *vmd* and *secfsd* processes. A *vmd* process communicates with the security server. A *secfsd* process holds online policies, and encrypts and decrypts data with access control. These processes stay on the system as daemons. When a *secfsd* process starts, all policies related to the host are retrieved from the security server via a *vmd* process, and the policies are cached in memory. If the process fails to retrieve the policies, it will continue to attempt to retrieve them every 5 seconds. When applying an online policy to a directory, the security server sends the policy to the agent, and the agent caches the policy in memory.

If an application attempts to access a guard point with an encryption key that uses the Cached on Host option, and the attempt is at a time when the agent hasn't cached the encryption key of the guard point in memory because the security server has not been running correctly since the agent start-up time, then the application freezes. In this case, use the command shown in Listing 1 (followed by the predefined password) to get the application to resume working correctly. After that, any applications that access a guard point on the host will work correctly without freezing if the encryption key of the guard point is configured with the Cached on Host option.

Listing 1. Retrieve encryption keys stored on the disk of the host

```
# vmsec passwd
Please enter password: xxxxxxxx
OK passwd
#
```

Figure 5 shows an example of Security Rules. In this example, if the db2admin user accesses the guard point, data is encrypted when writing, and data is decrypted when reading. If the root user reads data from the guard point, data is not decrypted, and the action is logged for audit. Other requests for access to the guard point are denied, and the action is logged for audit.

Figure 5. Security Rules example

No.	Resource	User	Process	Action	Effect	When	Allow Browsing
1		db2admin		all_ops	permit apply_key		on
2		root		read	permit audit		on
3				all_ops	deny audit		on

Host Settings

The User ID condition can be contained in Security Rules. Another setting related to User ID is called *Host Settings*. Use Host Settings to identify which login methods are allowed, which processes are allowed no matter which login method is used, and so on. For example, if you want to allow certain users to access guard points only if the users log in via ssh and telnet, add `|authenticator|` in front of the login processes as shown in Listing 2.

Listing 2. Example of Host Settings that allow user authentication only when logging in via ssh and telnet

```
|authenticator| /usr/bin/login
/usr/bin/su
|authenticator| /usr/sbin/sshd
/usr/sbin/ftpd
/usr/dt/bin/dtlogin
/usr/bin/sh
```

As shown above, `su` can also be controlled so that Encryption Expert will prevent even the root user from accessing guard points by pretending to be some user.

For more information, refer to the "Configuring host settings" section in "Chapter 6: Configuring hosts" of the *IBM Database Encryption Expert User's Guide*, which is linked to from the [Resources](#) section.

Listing 3 shows an example of a User Not Authenticated or FAKED USER error that occurs if you run a program to access a guard point after logging in via a non-authorized login method.

Listing 3. Example of a User Not Authenticated error

```
EET2604E: [SecFS, 0] [ALARM] Policy[db2admin_online_policy1]
User[db2admin,uid=222 (User Not Authenticated)] Process[/usr/bin/ls]
Action[read_dir_attr] Res[/home/db2admin/guard/] Effect[DENIED Code
(1U,2M)]
```

Data transformation

Encryption Expert provides a feature to transform data encrypted by one encryption key, or non-encrypted data, into data encrypted by another encryption key. This is called *dataxform*. An example of when you would use this would be a case where an unencrypted file exists on a directory that you are applying an online policy to. If the policy requires that the file be encrypted, you need to encrypt the file before applying the policy. To do so, use one of the following solutions:

- Use *dataxform* to transform the data before applying the policy to the directory.
- Move the file to a non-guarded directory before applying the policy to the directory. After applying the policy to the directory, move the file back into the directory. When you move the file back, it will automatically be encrypted based on the policy you applied.

For more information, refer to the "Using *dataxform*" section in "Chapter 10: Changing encryption keys" of the *IBM Database Encryption Expert User's Guide*, which is linked to from the [Resources](#) section.

Commands

Encryption Expert provides commands you can use to obtain agent information. For example, to get guard point information, you could enter the command shown in Listing 4.

Listing 4. Example of command to obtain guard point information

```
# secfsd -status guard
GuardPoint          Policy          Type   ConfigState   Status   Reason
-----
/home/db2admin/guard1  db2admin_policy1  local  guarded      guarded  N/A
/home/db2admin/guard2  db2admin_policy2  local  guarded      guarded  N/A
```

You can use the *secfsd* and *vmd* processes as commands by specifying options.

For more information on these and other Encryption Expert commands, refer to "Chapter 16: Maintaining Encryption Expert" of the *IBM Database Encryption Expert*

User's Guide, which is linked to from the [Resources](#) section.

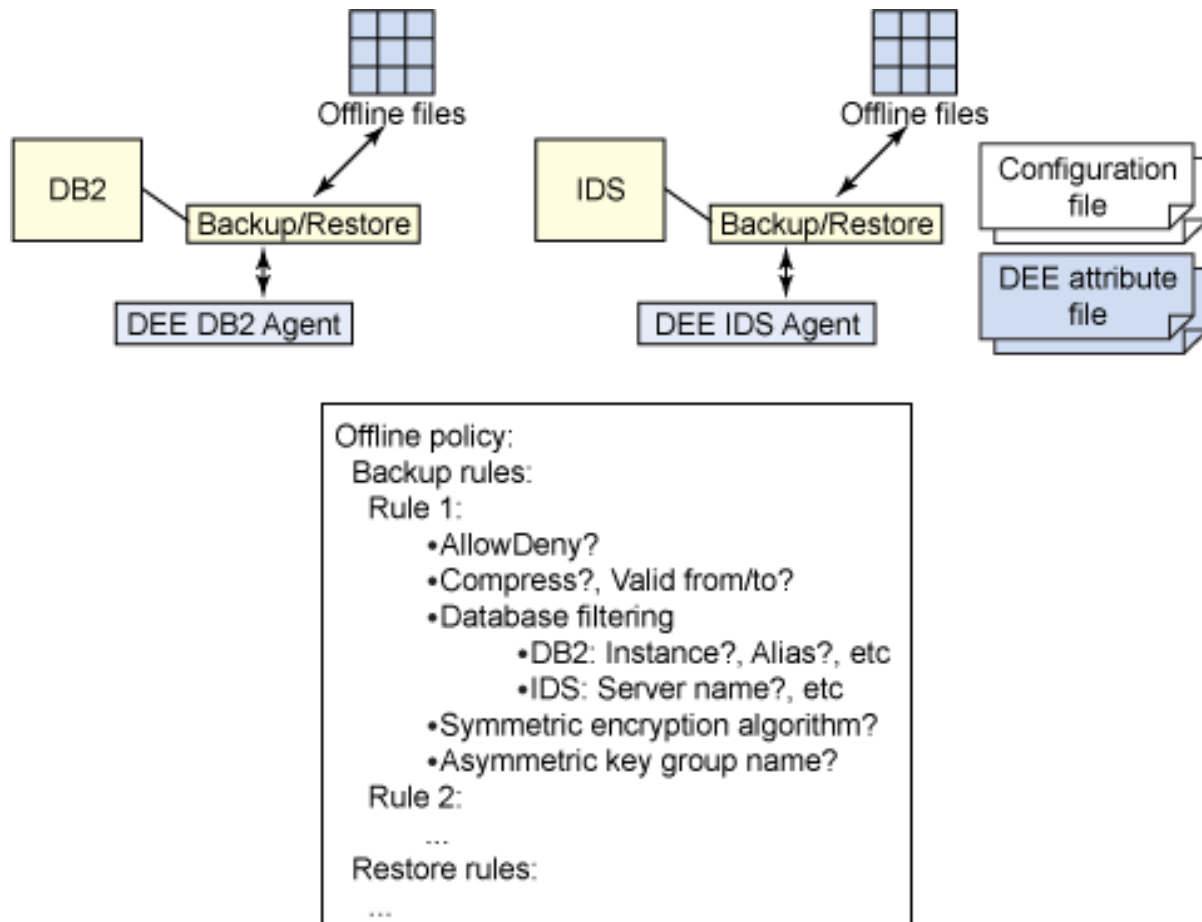
Protecting database backup images

Encryption Expert uses a hybrid encryption algorithm for encrypting database backup images. A symmetric key is dynamically created and used for encrypting a database backup image. The symmetric key itself is encrypted by one or more asymmetric keys (public keys). For symmetric encryption algorithms, you can use either AES128 or AES256. For asymmetric encryption algorithms, you can use RSA1024, RSA2048, or RSA4096.

You can import public keys created by other Encryption Expert security servers. By doing so, a database backup image encrypted by one DB agent and managed by one security server, can be restored to another DB agent managed by another security server.

Figure 6 shows an overview of how Encryption Expert provides protection for a database backup image. The figure shows backup agents for both IDS and DB2, but you cannot use both agents on the same machine. An offline policy that contains multiple backup rules and restore rules can be applied to a machine. Backup and restore operations with the DB agent are logged for audit and sent to the security server by default.

Figure 6. Protect database backup image



Integrating with DB2 backup and restore

You can issue the DB2 backup command with an external module as an option. This enables you to use the DB2 agent module with a backup, which enables you to encrypt a database backup image by communicating with the security server. The database backup image contains the DB2 agent module and information required for decrypting it. The DB2 restore command invokes the DB2 agent contained in the database backup image, and the DB2 agent decrypts it by communicating with the security server.

You can also issue the DB2 restore command with an external module as an option. When an external module is specified, it is used instead of the module contained in the database backup image. If the DB2 agent is upgraded after you backup the database and you want to use the upgraded module, specify the module with the DB2 restore command.

Listing 5 contains an example of a DB2 backup command using the DB2 agent module.

Listing 5. DB2 backup command example

```
% DB2 BACKUP DB dbname compress comprlib  
/opt/IBM/DB2TOOLS/LUWEEncryptionExpert/agent/db2/lib/libeetdb2.so
```

You can use other options with the above syntax such as `USE TSM` to specify use of Tivoli Storage Manager (TSM).

Listing 6 contains an example of a DB2 restore command using the DB2 agent module.

Listing 6. DB2 restore command example

```
% DB2 RESTORE DB dbname
```

Integrating with IDS backup and restore

There are two types of backup in IDS: `ontape` and `onbar`. In both cases, you can specify the IDS agent executable module in the `$INFORMIXDIR/etc/$ONCONFIG` configuration file. The IDS agent executable module needs an attribute file that describes how to handle data. Use the `-f` option to identify the attribute file.

Listing 7 shows an example of a configuration file.

Listing 7. IDS configuration file example

```
BACKUP_FILTER '/opt/IBM/DB2TOOLS/LUWEEncryptionExpert/agent/ids/bin/eetidsagt -f /home/informix/attr.w'  
RESTORE_FILTER '/opt/IBM/DB2TOOLS/LUWEEncryptionExpert/agent/ids/bin/eetidsagt -f /home/informix/attr.r'
```

Listing 8 shows an example of a backup attribute file (`attr.w`).

Listing 8. Example of a IDS agent attribute file for backup

```
ENV=INFORMIXSERVER, SERVERNUM  
OPERATION=write
```

In the example in Listing 8, the attribute file specifies that:

- `INFORMIXSERVER` and `SERVERNUM` environment variables are used for evaluating conditions of the policy.

- This is for backup.

Listing 9 shows an example of a restore attribute file (attr.r).

Listing 9. Example of IDS agent attribute file for restore

```
ENV=INFORMIXSERVER, SERVERNUM  
OPERATION=read
```

In the example in Listing 9, the attribute file specifies that:

- INFORMIXSERVER and SERVERNUM environment variables are used for evaluating conditions of the policy.
- This is for restore.

Listings 10 show and 11 show examples of IDS backup commands.

Listing 10. Example of IDS backup command (onbar)

```
% onbar -b -w
```

Listing 11. Example of IDS backup command (ontape)

```
% ontape -v -s -L 0 -t STDIO > ../../backup.000
```

Listings 12 and 13 show examples of IDS restore commands.

Listing 12. Example of IDS restore command (onbar)

```
% onmode -ky  
% onbar -r
```

Listing 13. Example of IDS restore command (ontape)

```
% onmode -ky  
% cat ../../backup.000 | ontape -r -t STDIO -v
```

For ontape IDS backups, you also have the option of specifying the IDS agent module as a command that receives the output of the backup or restore command.

Listings 14 and 15 show examples of the commands with this option.

Listing 14. Example of IDS backup command (ontape) specifying the IDS agent module

```
% ontape -v -s -L 0 -t STUDIO |  
/opt/IBM/DB2TOOLS/LUWEncryptionExpert/agent/ids/bin/eetidsagt -f  
/home/informix/attr.w > ../../backup.000
```

Listing 15. Example of IDS restore command (ontape) specifying the IDS agent module

```
% cat ../../backup.000 |  
/opt/IBM/DB2TOOLS/LUWEncryptionExpert/agent/ids/bin/eetidsagt -f  
/home/informix/attr.r | ontape -r -t STUDIO -v
```

For more information about IDS backup and restore, refer to "Chapter 12: Backing up and restoring IDS databases" of the *IBM Database Encryption Expert User's Guide*, which is linked to from the [Resources](#) section.

Configuring the audit log

Use the Management Console to configure parameters for the audit log. Each host and each agent (FS agent, DB2 agent, and IDS agent) has its own configuration. For example, you can specify if the log is sent to the security server, how many logs are sent at once, and the minimum and maximum number of seconds the agent should wait before sending the logs.

If an attempt is made to send a log when all security servers are not working correctly, the log is stored in a temporary file on the agent. Retry attempts are made after the minimum time interval specified for sending logs. This does not affect the application's ability to access the guard points.

For more information about configuring the audit log, refer to "Chapter 15: Setting Preferences" of the *IBM Database Encryption Expert User's Guide*, which is linked to from the [Resources](#) section.

Maintaining X.509 certificates

Each X.509 certificate published by the primary server has an expiration date. The expiration period of X.509 certificates for the CA and the primary server is 10 years. The expiration period for other certificates is 4 years.

The following list shows the directories that X.509 certificates are in. The CA's certificates are created on the primary server. The CA's certificates are copied to the failover servers and the agents when creating and registering their certificates.

- Security server (primary and failover)
/opt/IBM/DB2TOOLS/LUWEncriptionExpert/server/pem
- FS agent
/opt/IBM/DB2TOOLS/LUWEncriptionExpert/agent/vmd/pem
- DB2 agent
/opt/IBM/DB2TOOLS/LUWEncriptionExpert/agent/db2/pem
- IDS agent
/opt/IBM/DB2TOOLS/LUWEncriptionExpert/agent/ids/pem

Listing 16 shows an example of the command you can use to view an X.509 certificate. An example of why you might want to do this would be to verify the expiration date of a certificate.

Listing 16. Command syntax for browsing X.509 certificate

```
openssl x509 -in filename -noout -text
```

In the command, *filename* is the X.509 certificate file name under the directory as shown in the list above.

Listing 17 shows an example of the information that is returned from the command for viewing an X.509 certificate.

Listing 17. X.509 certificate example

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      0c:82:d5:ad:e7:f2:b0:fd:d7:22:14:e2:9f
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: CN=EET CA (S) on srv1.yamato.ibm.com, OU=I, O=IBM, L=Yamato, ST=Kanagawa,
    C=JP // Issuer: Certificate Authority (CA)
    Validity
      Not Before: Dec 14 06:52:41 2008 GMT
      Not After : Dec 14 06:52:41 2012 GMT // Expiration date
    Subject: OU=This agent certificate was automatically generated, CN=EET FS_VMD Agent
    on host1.yamato.ibm.com // Subject: primary server, failover server, or agent
    .....
```

To verify the expiration date of each Encryption Expert component, check the X.509 certificate files shown in Table 1. The table shows the certificate file name and expiration period for each Encryption Expert component.

Table 1. X.509 certificate information

Encryption Expert component (Subject)	X.509 Certificate File (one of them)	Expiration Period
CA	donkey_signer-cert.pem	10 years
Primary server	donkey_server_hostname-cert.pem	10 years
Failover server	donkey_server_hostname-cert.pem	4 years
Agent	agent-cert.pem	4 years

Listing 18 shows the command to renew the CA's X.509 certificates. Issue the command on the primary server.

Listing 18. Command to renew the CA's X.509 certificates

```
# /opt/IBM/DB2TOOLS/LUWEncryptionExpert/server/bin/re_gen_cert_auth
```

When you renew the CA's X.509 certificates, other X.509 certificates are invalidated. Therefore you also need to renew the X.509 certificates for the primary server, the failover servers, and the agents.

Listing 19 shows the two commands you can use to renew the primary server's X.509 certificates.

Listing 19. Commands to renew the primary server's X.509 certificates (use one or the other)

```
# /opt/IBM/DB2TOOLS/LUWEncryptionExpert/server/bin/re_gen_cert
# /opt/IBM/DB2TOOLS/LUWEncryptionExpert/server/bin/re_sign_cert
```

The `re_gen_cert` command recreates the key. The `re_sign_cert` command reuses the key.

Listing 20 shows the two commands you can use to renew the failover server's X.509 certificates.

Listing 20. Commands to renew the failover server's X.509 certificates (use one or the other)

```
# /opt/IBM/DB2TOOLS/LUWEncryptionExpert/server/bin/re_gen_failover_cert  
# /opt/IBM/DB2TOOLS/LUWEncryptionExpert/server/bin/re_sign_failover_cert
```

The `re_gen_failover_cert` command recreates the key. The `re_sign_failover_cert` reuses the key.

To renew the agent's X.509 certificates, do the following:

1. From the agent machine, issue the following commands to delete the appropriate agent's X.509 certificates.
To delete the FS agent's X.509 certificate:

```
# /opt/IBM/DB2TOOLS/LUWEncryptionExpert/agent/vmd/bin/register_host clean
```

To delete a DB2 agent's certificates:

```
# /opt/IBM/DB2TOOLS/LUWEncryptionExpert/agent/db2/bin/register_host clean
```

To delete an IDS agent's certificates:

```
# /opt/IBM/DB2TOOLS/LUWEncryptionExpert/agent/ids/bin/register_host clean
```

2. Select the host in the Management Console. Clear the **Registration Allowed** check boxes, and click **Apply**. As a result, Certificate Fingerprint becomes empty.
3. From the Management Console, check the **Registration Allowed** check boxes .
4. From the agent machine, issue the following commands to register the appropriate agent's X.509 certificates.
To register the FS agent's certificates:

```
# /opt/IBM/DB2TOOLS/LUWEncryptionExpert/agent/vmd/bin/register_host
```

To register a DB2 agent's certificates:

```
# /opt/IBM/DB2TOOLS/LUWEncryptionExpert/agent/db2/bin/register_host
```

To register an IDS agent's certificates:

```
# /opt/IBM/DB2TOOLS/LUWEncryptionExpert/agent/ids/bin/register_host
```

5. Select the host again in the Management Console. Check the **Communication Enabled** check boxes, and click **Apply**.
6. If the failover servers are set up, enroll the access points again in the agent.conf files on the following directories of the host:
 - FS agent
/opt/IBM/DB2TOOLS/LUWEncryptionExpert/agent/vmd/etc
 - DB2 agent
/opt/IBM/DB2TOOLS/LUWEncryptionExpert/agent/db2/etc
 - IDS agent
/opt/IBM/DB2TOOLS/LUWEncryptionExpert/agent/ids/etc

For more information refer to the "Configuring an agent to use Security Servers" section of "Chapter 6: Configuring hosts" in the *IBM Database Encryption Expert User's Guide*, which is linked to from the [Resources](#) section.

Conclusion

IBM Database Encryption Expert protects data with a policy that contains one or more encryption keys and one or more rules for access control. The policies are centrally managed by the security server and are sent to the agents that protect data as necessary. Audit logs for events such as access violations can also be managed by the security server. To ensure high availability requirements, you can set up multiple security servers.

The FS agent provides a feature to encrypt and decrypt data written to or read from file systems. Any application that the policy allows access to can access the files that are under guard points as long as the application uses system libraries to access the files. Data is automatically encrypted when writing, and decrypted when reading, based on the policy. The encryption is transparent to the application, and

you do not need to make any changes to the application itself. If the Cached on Host option is enabled with an encryption key, the encryption key is stored on the disk of the FS agent machine with password protection. As a result, the FS agent can work correctly even if all security servers have not been running correctly since the FS agent start-up time. The FS agent process retrieves all related online policies at start-up time and caches them in memory. So after that, the FS agent works correctly even if all security servers become unavailable regardless of whether the Cached on Host option is enabled or not.

The DB agent provides a feature to encrypt and decrypt DB2 and IDS database backup images with controlling backup and restore commands. The DB agent communicates with the security server for the policy every time a backup or a restore command is issued with the DB agent.

SSL protocol is used for communicating between the security server and each agent, and between the primary server and each failover server. X.509 certificates are used for authentication. The X.509 certificates have expiration dates so you should be sure to renew them before they expire.

Resources

Learn

- Refer to the [IBM Database Encryption Expert for Linux, UNIX, and Windows User's Guide](#) for more details on using this tool.
- Refer to the [IBM Database Encryption Expert product web site](#) for system requirements such as supported platforms and supported databases.
- Use the [Information Management area on developerWorks](#) as a resource for advancing your skills on DB2, Informix, and many other products in the IBM Information Management portfolio.
- Find news and links at the [Integrated Data Management developerWorks Space](#).
- Keep up with the latest topics by following the [Integrated Data Management expert blog](#).

Discuss

- Check out [My developerWorks blogs](#) and get involved in the [My developerWorks community](#).

About the authors

Masahiro Ohkawa

Masahiro Ohkawa is a member of database tooling development team in Yamato Software Development Laboratory (YSL), IBM Japan.

Soh Kaijima

Soh Kaijima is a member of database tooling development team in Yamato Software Development Laboratory (YSL), IBM Japan.

Gou Nakashima

Gou Nakashima is a member of database tooling development team in Yamato Software Development Laboratory (YSL), IBM Japan.

Asuka Tokunaga

Asuka Tokunaga is a member of database tooling development team in Yamato Software Development Laboratory (YSL), IBM Japan.