IBM Spectrum Protect

IBM Spectrum Protect Security Enhancements

Best Practice / Troubleshooting
V7.1.8, V8.1.2, V8.1.3 and V8.1.4, 8.1.5, 8.1.6

- Originator: Andre Gaschler (gaschler@de.ibm.com), ESCC Data Protection & Retention Solutions, IBM Consulting IT Specialist
- Modified by: Monika Wolf (monika.wolf@de.ibm.com) IBM Technical L2 Support

Last update 17.10.2018

Agenda

Security Enhancements

IBM Spectrum Protect Security Enhancements

Security Enhancements starting with Version 8.1.2 / 7.1.8

Starting with 8.1.2+/7.1.8+ servers are configured for SSL and TLS 1.2, by default

- Servers are configured for SSL and TLS 1.2 by default
  - At session start, server checks for copy of certificate in server's data base
  - Certificates are communicated via server-server SSL and protected via password
  - Certificates are placed into the key database automatically with an identifiable label.
  - Certificate Exchange is available only for session between 7.1.8+ and 8.1.2+ servers using V2 Authentication
  - DEFINE SERVER xxx CROSSDEFINE=YES SSL=YES allows for bi-directional exchange

Security Enhancements starting with Version 8.1.3 / 7.1.8

- **Starting with Spectrum Protect 8.1.3**
  - Server-Server sessions can dynamically acquire certificates
  - Support for additional types of sessions
  - Certificates are obtained if not already possessed
  - Storage Agent-Server **Trust-On-First-Use** acquisition is available
  - Works for most server-server sessions **and** storage agent-server sessions
  - Server to Server sessions that use administrator or node credentials to authenticate
    - Virtual Volume sessions acquire certificate of target server (but not vice versa)
    - Command routing sessions which do not initiate a server-server session (including `'PING SERVER'` command) acquire certificate of target server (but not vice versa)
    - Export Server to Server acquires certificate of target server (but not vice versa)

- **Starting with Spectrum Protect 7.1.8**
  - 7.1.8 is functionally equivalent to 8.1.3 concerning certificate exchange and security fixes
  - 7.1.8 will be able to automatically exchange certificates with 8.1.2 and 8.1.3+ servers

Security Enhancements by Version 8.1.4

- **Default** minimum password length has been changed from zero to **eight**
  - Only the default setting is changing
  - Any explicitly set MINPWLEN value will not be changed
  - During upgrade to 8.1.4+ server, server will replace old default setting with new default
    - A current setting of 0 is considered to be the old default and will be changed even if explicitly set to 0 prior to upgrade
- Affects the following kinds of server instances
  - New server instances
  - Existing server instances that have never specified a non-default value
- Administrators can still override the default and specify any value they wish (up to 64)
  - Exception: **Zero is no longer a valid value**
- Does **NOT** affect existing passwords
  - Short passwords will remain valid until they expire or are changed by a user
  - New passwords must meet or exceed the new minimum length

Security Enhancements by Version 8.1.4

- Most passwords stored on server are affected
  - e.g., Node, Admin, Server, & DB Backup passwords must all conform to minimum length rule
  - Exception: Nodes and Admins defined with AUTH=LDAP are not affected
    - (these passwords are not stored on the server)

    LDAPPASSWORD is not affected
- Informational message ANR2138I will be issued to let administrator know of change
  - `ANR2138I Minimum password length set to 8.`
- **Node Replication** Target server **must meet** the source server's minimum length

Master Encryption Key

IBM Spectrum Protect Security Enhancements

Master Encryption Key

Beginning with 8.1.2 a master encryption key is automatically generated at server start

- The key **database's password** is stored in a password stash file called **dsmkeydb.sth**
  - If the master encryption key did not previously exist
    - **Master encryption** key is stored in a new key database: **dsmkeydb.kdb**
  - If an existing master encryption key exists
    - The key is migrated from the **dsmserv.pwd** file to **dsmkeydb.kdb**
  - **Ownership / permissions** of both key db's & stash file are set to give **only** the instance user access

```
$ ls -l dsmkeydb.*
-rw-------. 1 tsminst1 tsmsrvrs 3350 Jun 26 18:13 dsmkeydb.kdb
-rw-------. 1 tsminst1 tsmsrvrs  193 Jun 26 18:13 dsmkeydb.sth
```

- **dsmserv.pwd** file, used to store the master encryption key in previous releases**, is no longer used**

UNIX location of cert.* and dsmkeydb.* files

- **SERVER:**

UNIX Standard Installation:

/home/tsminst1/tsminst1

cert* files

```
-rw-------    1 tsminst1 tsmsrvrs         80 Oct 13 2017  cert.crl
-rw-------    1 tsminst1 tsmsrvrs        129 Oct 13 2017  cert.sth
-rw-------    1 tsminst1 tsmsrvrs       5080 Oct 01 14:10 cert.rdb
-rw-r--r--    1 tsminst1 tsmsrvrs       1257 Oct 13 2017  cert256.arm
```

dsmkeydb.* files

```
-rw-------    1 tsminst1 tsmsrvrs        193 Aug 13 2017  dsmkeydb.sth
-rw-------    1 tsminst1 tsmsrvrs       3358 Sep 24 14:28 dsmkeydb.kdb
```

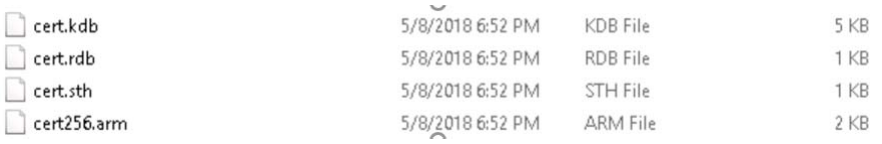
Windows location of cert.* and dsmkeydb.* files

- **SERVER:**

Windows Standard installation:

`C:\Program Files\Tivoli\TSM\server1`

cert.* files



cert.kdb	5/8/2018 6:52 PM	KDB File	5 KB
cert.rdb	5/8/2018 6:52 PM	RDB File	1 KB
cert.sth	5/8/2018 6:52 PM	STH File	1 KB
cert256.arm	5/8/2018 6:52 PM	ARM File	2 KB

dsmkeydb.* files

dsmkeydb.kdb	5/8/2018 6:56 PM	KDB File	4 KB
dsmkeydb.sth	5/8/2018 6:56 PM	STH File	1 KB

Protect Encryption Key DB's and Stash Files

- By default (since 8.1.2),
  BACKUP DB protects the master encryption key (**PROTECTKEYS=YES**)
  - Warning message displayed if not:
    ```
    ANR2784W Specifying PROTECTKEYS=NO requires the server's encryption keys
    to be backed up manually.
    ```
- Key Protection requires DB Password to be set
  ```
  SET DBRECOVERY DEVICECLASS PROTECTKEYS=YES PASSWORD=********
  BACKUP DB DEVC=DEVICECLASS TYPE=FULL PROTECTKEYS=YES PASSWORD=********
  ```
  - **Do not forget** the password – the master encryption key and/or the database cannot be restored without it!
- After PROTECTKEYS=YES is set with SET DBRECOVERY the database can be backed up without specifying a password
  ```
  BACKUP DB DEVC=DEVICECLASS TYPE=FULL
  ```
- Changing the Device Class with SET DBRECOVERY requires password
  ```
  SET DBRECOVERY DEVICECLASSNEW (will fail)
  ANR1748E The PASSWORD parameter is required when PROTECTKEYS is enabled.
  ```

➢**Recommendation**: Enable PROTECTKEYS=YES

If you lose the master key, you lose **all** of the data stored in encrypted container storage pools!
If you lose the master key, you lose **everybody's** password!

Manually back up dsmkeydb.* and cert.* files

- **Best practice** when transporting encrypted data is to transport encryption key via a separate channel
- The key database files typically do not change, so likely a one time operation
- Ideally, transport .kdb file separately from .sth file

What NOT to do

- **Do NOT delete** the cert.kdb/cert.sth files!
- The cert.* files in the server's instance directory contain the server's private key and certificate
- New server certificate will need to be distributed if deleted

Spectrum Protect Secure Passwords

IBM Spectrum Protect Security Enhancements

Spectrum Protect Server Password Encryption

Management of SSL certificates and key databases

- uses password stash file, cert.sth, for access
  - Password is stored in stash file
  - Stash file format maintained by GSKIT for best security
  - Ownership / permissions are set to only allow access by instance user
- Server commands for managing key database password have been **removed**
  - QUERY SSLKEYRINGPW
  - SET SSLKEYRINGPW
  - DELETE KEYRING
  - (undocumented) DEFINE KEYRING
  - STAKEYDBPW keyword parameter on DSMSTA SETSTORAGESERVER utility is no longer required, and will be ignored if specified

Spectrum Protect Client Secure Passwords

- Clients' passwords are now stored in keystores created using **GSKit**
  - **TSM.KDB** (holds the encrypted passwords)
  - **TSM.IDX** (index file into TSM.KDB)
  - **TSM.STH** (holds random, obfuscated encryption key used in TSM.KDB)

Regardless of where it is stored, the password file that is created by the client is always named **TSM.STH**

The password files (TSM.IDX, TSM.KDB, TSM.sth) and spclicert files (spclicert.crt, spclicert.kdb, spclicert.rdb, spclicert.sth) should be created in the location specified by the PASSWORDDIR.

Note:
Ensure these TSM* and spclicert.* files have write permissions for the user.

New Structure for Security TLS 1.2 on Client/Admin

- **UNIX:**
  - In 8.1.0, the passwords were stored in TSM.PWD in the default folder or the PASSWORDDIR folder
  - 8.1.2+, the passwords are stored in the same location as the old TSM.PWD files were stored
- **ROOT User:**
  - **Base Directory is /etc/security/adsm/**
    - Password file is /etc/security/adsm/TSM.KDB
    - Stash file is /etc/security/adsm/TSM.STH
    - IDX file is /etc/security/adsm/TSM.IDX
    - pswdFileName /etc/security/adsm/spclicert.kdb
    - idxFileName /etc/security/adsm/spclicert.idx
    - stashFileName /etc/security/adsm/spclicert.sth

New Structure for Security TLS 1.2 on Client/Admin

- **default directory for AIX - /etc/security/adsm**

```
/etc/security/adsm - root@igstsm11 # ls -ltr
total 192
-rw-------    1 root     system          193 Aug 13 2017  spclicert.sth
-rw-rw-rw-    1 root     system           80 Aug 13 2017  spclicert.rdb
-rw-rw-rw-    1 root     system           80 Aug 13 2017  spclicert.crl
-rw-------    1 root     system          193 Nov 06 2017  TSM.sth
-rw-rw-rw-    1 root     system        55080 Mar 26 2018  spclicert.kdb
-rw-rw-rw-    1 root     system         2580 Aug 15 18:57 TSM.IDX
-rw-rw-rw-    1 root     system        12445 Aug 15 18:57 TSM.KDB
```

- **other UNIX and Linux platforms - /etc/adsm**
- **NON ROOT User:**
  By default these get generated under
  <**user's home dir**>/IBM/SpectrumProtect/certs

New Structure for Security TLS 1.2 on Client/Admin

- **Password Stores on Windows:**

Password storage move from the registry into the file system using GSKit

`C:\programdata\tivoli\tsm\baclient\nodes\<nodename>`

Default Access (permissions)
- Administrators
- Systems

- **Special Password cases:**
  - Password location for VE GUI's Spectrum Protect Server Administrator Password
    - `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\tsmVmGUI`
  - Password locations for clients in cluster environments (**CLUSTERNODE YES** in the client options file)
    - Password files are stored in a subdirectory of the client options file location: `NODES\NodeName\ServerName`

dsmcert files

- Files created:
  - **dsmcert.kdb** – Keystore containing the server's public certificate
  - **dsmcert.sth** – Stash file that contains the dsmcert.kdb file's password
  - **dsmcert.idx** – Index file - maps the server's ip to the certificate label in the .kdb
- Files stored in the bin directory of the client installation (varies by platform/component)
- **API**
  - Windows `C:\Program Files\Common Files\Tivoli\TSM\api64`
  - Linux `/opt/tivoli/tsm/client/api/bin64`
  - AIX `/usr/tivoli/tsm/client/api/bin64`
- **B/A client**
  - Windows `C:\Program Files\Tivoli\TSM\baclient`
  - Linux `/opt/tivoli/tsm/client/ba/bin`
  - AIX `/usr/tivoli/tsm/client/ba/bin64`
- If the user **doesn't have write authority** to client install directory…
- **Files are stored** in the **user's home directory**
  - Windows `C:\users\<username>\IBM\SpectrumProtect\certs`
  - Linux/Unix `/home/<username>/IBM/SpectrumProtect/certs`

Spectrum Protect Secure Communication

Spectrum Protect Secure Communication - Overview

- Certificates are **automatically exchanged**
  - Certificate Exchange is available only for session between 7.1.8+ and 8.1.2+ servers using V2 Authentication

Certificates can be manually exchanged
  - gsk8capicmd_64 or ikeycmd

- New **SESSIONSECURITY** parameter for NODE, ADMIN, SERVER definitions
  - **STRICT**: Enforces all session security features the server is capable of enforcing at the given level (currently TLS 1.2)
  - **TRANSITIONAL**: TLS 1.2 is not enforced. Intended to be used temporarily while updating clients, servers, OC, admins … for strict compliance

Commands using SESSIONSECURITY

REGISTER NODE, REGISTER ADMIN, DEFINE SERVER, UPDATE NODE, UPDATE ADMIN, and UPDATE SERVER

New Server Session Security Enforcement Concept

- **NOTE:**
  - After **successful certificate acquisition**, the requesting server marks its partner as **STRICT**
  - After an administrator authenticates to a V8.1.2 or later server by using a V8.1.2 or later client, the administrator can authenticate **only** on clients or servers that are using **V8.1.2+**
  - If necessary, **create a separate administrator** account to use only with clients and servers that are using V8.1.1 or earlier software.

Secure Communication: Spectrum Protect Server

- TCPPORT and TCPADMINPORT now accept TCP and SSL enabled connections
  - SSLTCPPORT and SSLTCPADMINPORT remain as optional SSL only ports – **no need** to be configured for SSL communication with 8.1.2+
- Certificates are automatically exchanged
  - Requires the default certificate "**TSM Server SelfSigned SHA Key**" with a SHA signature (**cert256.arm**)
  - Certificates are placed into the truststore automatically with an identifiable label
    - Server: **cert.kdb**
    - Admin/client: **dsmcert.kdb**
    - OC: **gui-truststore.jkm**
  - Requires Server Options to be configured:
    - `SET SERVERHLA`
    - `SET SERVERLLA`
    - `SET SERVERPASSWORD`
    - `SET CROSSDEFINE ON`
  - DEFINE SERVER xxx CROSSDEFINE=YES SSL=YES allows for bi-directional exchange

NOTE: Do not use the SSL or TLS protocols for communications with a DB2® database instance that is used by any IBM Spectrum Protect servers.

Secure Communication: Spectrum Protect Server Certificate

- The **server default certificate is automatically updated** to use a certificate with a SHA signature

  Beginning in V8.1.2 the default certificate is labeled "**TSM Server SelfSigned SHA Key**" with a SHA signature (**cert256.arm**)

- More Information:
  Technote 22004844: IBM Spectrum Protect security updates in V7.1.8, V8.1.2, V8.1.3 and V8.1.4

Trust on first use (TOFU) – Automatic Certification Exchange

- Trust on first use (TOFU) is available for **admin**, **server** and **client** sessions
  – Allows certificates to be exchanged automatically
- Requires SESSIONSECURITY=TRANSITIONAL to be set (default after update to 8.1.2+)
- Once an admin-ID, server-ID or client-node connects to a 8.1.2+ Spectrum Protect server, SESSIONSECURITY for this entity (admin, server, client) is set to STRICT
  – Applies to: **Operations Center**, **dsmadmc**, **VE client**
- Reset SESSIONSECURITY to TRANSITIONAL to re-enable TOFU
  – For example to allow automatic certification exchange for multiple dsmadmc clients
- **Recommendation:**
  Update all clients to 7.1.8 / 8.1.2+ where administrative CLI is used (dsmadmc)
- **If TOFU fails: Certificates need to exchanged manually**

Migration

IBM Spectrum Protect Security Enhancements

Install / Configuration / Migration

- After install, all newly defined servers are in transitional state by default.
  - As servers connect, exchanging certificates and meeting the criteria for strict mode, they will be marked as strict.
- Servers at levels below 8.1.2/7.1.8 remain in transitional state.
- SSL configuration for Servers below 8.1.2/7.1.8 has not changed; Servers which are migrated to 8.1.2+/7.1.8 and which exchange certificates will succeed in doing so.

What happens at migration

- The first time a server starts following an upgrade to 8.1.2+
  - If the server had a master encryption key, it will move the key from dsmserv.pwd to dsmkeydb.kdb
    - Existing dsmserv.pwd will be renamed to dsmserv.pwd.YYYYMMDDHHMMSS.deletionsave
    - Renamed dsmserv.pwd can be deleted once you're satisfied that upgrade succeeded

```
ANR2278I The server master encryption key was moved from the server password file,
dsmserv.pwd, to the server key database.

ANR2279W An existing server password file, dsmserv.pwd, was found during an upgrade
operation.  It was renamed to dsmserv.pwd.20170316085320.deletionsave.
```

  - If the server did not have a master encryption key, one will be generated and stored in dsmkeydb.kdb
    - Key generation will occur even if server password has not been set
  - Existing passwords for all nodes and administrators defined with AUTH=LOCAL will be re-encrypted using AES256

UPGRADE Scenario:

➔ Some homework is required before upgrading !!!!!!!!!!

Read through the comprehensive technote covering the security updates

Security updates beginning in IBM Spectrum Protect V8.1.2 and Tivoli Storage Manager V7.1.8

http://www.ibm.com/support/docview.wss?uid=swg22004844

What you should know about security before you install or upgrade the server

https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.6/srv.install/r_srv_knowsec_c.html

IBM Spectrum Protect Version 8.1.6.000 fix pack readme files

https://www-01.ibm.com/support/docview.wss?uid=swg27051133

Upgrade to 8.1.6, 7.1.9, or newer levels

TIP:

If your system environment includes a storage agent, you **must** upgrade the **storage agent** to **V8.1.6** when you upgrade the server to V8.1.6. If you do not upgrade the storage agent, you will experience issues when you attempt to restore or retrieve client data by using LAN-free data movement.

2. Secure administrator connections

- Upgrade systems where dsmadmc is run to 8.1.6+, 7.1.8+, or newer client levels.
- Consider eliminating administrator ID's with the same name as nodes that were automatically created.

3. Upgrade client systems to 8.1.6, 7.1.8, or newer levels.

Tips for certificate distribution

The automatic transfer of a server's public certificate is only performed on **the first** connection to a server with enhanced security

– After this first connection the **sessionsecurity** attribute of a node changes from transitional to strict

– A node, administrator, or server can be temporarily placed back in a **transitional** state to allow for another automatic transfer of the certificate

- `update admin <name> sessionsecurity=transitional`
- `update node <name> sessionsecurity=transitional`
- `update server <name> sessionsecurity=transitional`

- Alternatively, the public certificate can be manually transferred and imported using the dsmcert utility

- `dsmcert -add -server servername -file cert.arm`

Multiple applications which use GSKit on the same system

Multiple applications may be installed on the same system which all depend on GSKit – Global installation versus local installation
– All applications sharing a global install is usually not a problem
– There are some combinations where incompatible GSKit levels are picked up.

There are a number of **solutions to these problems**:

- IBM Spectrum Protect backup-archive client, Space Management or API processes can fail when used in combination with other products like IBM Spectrum Scale or IBM Db2 and using SSL/TLS communication with the IBM Spectrum Protect Server
  http://www.ibm.com/support/docview.wss?uid=swg22011742
- IBM Spectrum Protect Version 8.1.5.000 fix pack readme files
  http://www-01.ibm.com/support/docview.wss?uid=swg27050721
- After upgrading to a later version of IBM Global Security Kit (GSKit), an IBM Tivoli Storage Manager or IBM Spectrum Protect server might fail to start.
  https://www-01.ibm.com/support/docview.wss?uid=swg22007298

Clients with a DB2 database

If a DB2 is configured on the Client which is upgraded to 7.1.8+ / 8.1.2+ **you need** to follow these instructions.

- **DB2 API backup fail with RC 927 after Client upgrade to 7.1.8 or 8.1.2 and higher**
  https://www-01.ibm.com/support/docview.wss?uid=swg22010129
- **GSKit Versions Shipped with DB2**
  https://www-01.ibm.com/support/docview.wss?uid=swg21617892
- **Configuring DB2 and IBM Spectrum Protect in Unix / Linux**
  http://www-01.ibm.com/support/docview.wss?uid=swg22004184
- **Creating a symbolic link to access the latest GSKit library**
  https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.4/client/t_cfg_ssl_symb_lnk_gskit.html

Configuring a storage agent to use SSL

You must have the **server's certificate and the port** number that the server is using.

1. **Initialize the storage agent and add communication information to the device configuration file** and the storage agent options file **dsmsta.opt** by issuing the **DSMSTA SETSTORAGESERVER** command. You must specify the **SSL=YES** parameter to create the key database file in dsmsta.opt. All passwords are encrypted in dsmsta.opt.

e.g.

```
dsmsta setstorageserver myname=storage_agent_name mypa=sta_password
myhla=ip_address servername=server_name serverpa=server_password hla=ip_address
lla=ssl_port ssl=yes
```

2. **Create the key database certificate and default certificates by starting the storage agent.**

Configuring a storage agent to use SSL

3. For the storage agent and the server, import the other's cert256.arm or CA-certificate files:

```
gsk8capicmd_64 -cert -add -label ip_address -db cert.kdb -stashed   -
file cert256.arm
```

Tip: Use the IP address as the label name.

4. You can view the certificates in the key database by issuing the following command:

```
gsk8capicmd_64 -cert -list -db cert.kdb –stashed
```

5. Restart the storage agent and the server.

6. Establish communication between the server and the storage agent

```
define server sta hla=ip_address lla=port serverpa=password ssl=yes
```

Spectrum Protect Client Secure Passwords
*TCA (non root user) Trusted Communications Agent **removed** in 8.1.2*

- PREVIOUSLY: TCA allowed non root users to perform operations that required access to the passwords stored in the root only TSM.PWD
- 8.1.2+: Root users can use the following methods to allow non-root users to manage their files:
  - **Help desk method:**
    - Root user runs all backup and restore operations
    - The non-root user must contact the root user to request certain files to be backed up or restored
  - **Authorized user method:**
    - Non-root user is given read/write access to the password store by using the PASSWORDDIR option
    - Point to a password location that is readable and writable by the non-root user
    - Allows non-root users to back up and restore their own files, use encryption, and manage their passwords with the passwordaccess generate option
- Enable non-root users to manage their own data:
  https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.4/client/c_cfg_nonadmin.html

Creating a Certificate Authority (CA)

IBM Spectrum Protect Security Enhancements

Creating a CA using GSKit

1.) Initialize the CA key database and create the CA certificate

For example:

```
gsk8capicmd_64 -keydb -create -db ca.kdb -pw mypass -
stashgsk8capicmd_64 -cert -create -db ca.kdb -stashed -dn
CN=CA,O=CA,C=US -expire 7300 -label "CA cert" -default_cert yes -ca
true
```

2.) Extract the CA's root certificate

This certificate must be installed at **both** the clients and servers:

```
gsk8capicmd_64 -cert -extract -db ca.kdb -stashed -label "CA cert" -
format ascii -target ca.arm
```

For clients to verify a server's identity, the CA must issue a signed server certificate to the server.

Issuing a server certificate with a CA

1.) The CA's root certificate must be added to the server's key database and marked as trusted

```
gsk8capicmd_64 -cert -add -db server.kdb -stashed -label "My CA root"
-file ca.arm -format ascii -trust enable
```

2.) At the server, create a server certificate request

```
gsk8capicmd_64 -certreq -create -db server.kdb -stashed -label "My CA
signed certificate" -dn "CN=host.mycompany.com,OU=unit,O=company" -
file cert_request.arm
```

You can also request a subject alternative name (SAN) extension by using -san_dnsname or -san_ipaddr options.

For example:

```
gsk8capicmd_64 -certreq -create -db server.kdb -stashed -label "My CA
signedcertificate" -dn "CN=host.mycompany.com,OU=unit,O=company"
-san_dnsname"host1.mycompany.com,host2.mycompany.com" -san_ipaddr
"10.10.10.1,10.10.10.2" -filecert_request.arm
```

Issuing a server certificate with a CA

3.) The certificate request must be transported to the CA, and the CA must sign the certificate

```
gsk8capicmd_64 -cert -sign -file cert_request.arm -db ca.kdb -stashed
-label "CA cert" -target cert_signed.arm -expire 364
```

If a SAN extension was requested in the server certificate request, you can either use the -preserve option to keep the requested values or override them by specifying your own **-san_dnsname** or **-san_ipaddr** options with the **-sign** command (not supported in version

If you use both **-preserve** with **-san_dnsname or -san_ipaddr**, the values are merged with the ones requested.

For example:

```
gsk8capicmd_64 -cert -sign -file cert_request.arm -db ca.kdb -stashed
-label "CA cert" -target cert_signed.arm -expire 364 -preserve
-san_dnsname"host3.mycompany.com" -san_ipaddr "10.10.10.3"
```


Issuing a server certificate with a CA

4.) The server must receive the signed certificate from the CA and set it as the default for communicating with clients

```
gsk8capicmd_64 -cert -receive -db server.kdb -stashed -file
cert_signed.arm -default_cert yes
```

Distributing the CA root certificate to clients

For your clients to validate the signed certificate that they receive from the server during an SSL connection, they **must trust your Certificate Authority**. This is achieved by installing the **CA root certificate** on the clients.

1. **Transfer** the CA root certificate to **clients**. (See the ca.arm file created above.)

2. **Add** the CA root certificate to the client key database and **enable trust** as follows:

```
gsk8capicmd_64 -cert -add -db client.kdb -stashed -label "My CA root"
-file ca.arm -format ascii -trust enable
```

Or with dsmcert:

```
dsmcert -cert -add -db client.kdb -stashed -label "My CA root" -file
ca.arm -format ascii -trust enable
```


Troubleshooting

IBM Spectrum Protect Security Enhancements

GSKIT levels

- **7.1.8 / 8.1.2 / 8.1.4 upgrades GSKIT to level 8.0.50.78**
  - Previous level was 8.0.50.66
  - Level shipped with DB2 11.1 is 8.0.50.57
  - 8.1.2 upgrades GSKit to level 8.0.50.78
  - 8.1.5 upgrades GSKit to level 8.0.50.86
- **Changes starting with GSKit 8.0.5.78 include a couple incompatible changes**
  - An incompatible change to password stash file format to make it more secure
  - An incompatible change to the API used to manage 'secret keys' stored in key database
  - **As a result, mixing GSKIT versions can result in failures in the server!**
  - Usually a result of incorrect **LIBPATH** (AIX) **or LD_LIBRARY_PATH** (Linux) setting

LIBRARY PATH

Review the instructions in IBM Knowledge Center for creating a server instance. Verify that the library path was modified to use the version of GSKit that is installed with the server and **NOT** the version installed with DB2.

AIX: Creating the server instance
https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.4/srv.install/t_srv_install_createdbinst-aix.html

Windows: Creating the server instance
https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.4/srv.install/t_srv_install_createdbinst-windows.html

Linux: Creating the server instance
https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.4/srv.install/t_srv_install_createdbinst-linux.html

Creating a symbolic link to access the latest GSKit library
https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.4/client/t_cfg_ssl_symb_lnk_gskit.html

Bundled library and process rules
https://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.sec.doc/doc/r0060220.html

LIBRARY PATH

Related DB2 documents:

IBM DB2 on HP requires global GSKit to be at the same level as the GSKit embedded into the product.

http://www-01.ibm.com/support/docview.wss?uid=swg21674102

Setting system variables for IBM Global Security Kit on HP

http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.swg.tivoli.gskit.install.doc/doc/c0055537.html

GSKIT VERSION

GSKit Version can be identified

- **Windows:**

– C:\Program Files\IBM\gsk8\bin

gsk8capicmd_64 ==> properties

– regedit /e gskitinfo.txt "HKEY_LOCAL_MACHINE\software\ibm\gsk8\" notepad gskitinfo.txt

- **UNIX**

- gsk8ver_64

GSKit V8 - Instructions to find current installed version details:

http://www-01.ibm.com/support/docview.wss?uid=swg21576643

Certificate distribution failed

SYMPTOM

- Certificate distribution failed for a Client/Server/Storage Agent
- For nodes and administrators, set the **SESSIONSECURITY** parameter to **TRANSITIONAL**
- For storage agents, update the **STASESSIONSECURITY** option in the storage agent options file dsmsta.opt by changing the STRICT value to **TRANSITIONAL.**
- For servers update the server to **SESSIONSECURITY** parameter to **TRANSITIONAL**
- Restart the servers. Certificate changes do not take effect **until you restart the servers** or storage agents.
- If you are still unable to exchange certificates manually add the certificates to the servers and storage agents and restart them.
- For instructions, see

Configuring storage agents, servers, clients, and the Operations Center to connect to the server by using SSL.

Lost master encryption key

- Client attempts to log in fail with client message

```
ANS1025E Session rejected: Authentication failure
```

and server messages

```
ANR0150E Failed to open Admin ADMIN. There was an error decrypting the Admin
     password.
ANR0423W Session 1 for administrator ADMIN (xxx.xxx.xxx(44058)) refused –
      administrator name not registered.
```

Solution: Restore the master encryption key from a backup and restart the server

- Replace dsmkeydb.kdb & dsmkeydb.sth with copy from DR site, or
- Restore from recent database backup

```
dsmserv restore db restorekeys=only password=xxxxxxxx
```


Out of Sync Conditions

It is possible for one server to be out of synch with it's partner:

- Certificate is manually removed from key data base
- Data base restore which is missing newly added certificates in the security table
- Update session security

- The Primary mechanism to allow certificate exchanges to occur is to re-sync both servers is:
  Update Server partnerserver **sessionsecurity=transitional forcesync=yes**

Note that the use of forcesync=yes will cause the certificate to be deleted from the security table

Additional tools:

- There are a variety of tools available for looking at certificates and verifying certificate chains. **OpenSSL** and **GSKIT** both provide such tools.

APAR's / TECHNOTES

IT20713: AT START-UP, DSMC AND/OR DSMTCA PROCESSES TAKE A LOT OF CPU RESOURCES ON ZLINUX WHEN PASSWORDACCESS GENERATE IS USED

http://www-01.ibm.com/support/docview.wss?uid=swg1IT20713

IT23533: UNDETECTED INCOMPATIBLE LOCAL GSKIT VERSION MAY YIELD UNWANTED RESULTS WITH THE 7.1.8 AND 8.1.2 CLIENT SECURITY ENHANCEMENTS

http://www-01.ibm.com/support/docview.wss?uid=swg1IT23533

IT23560: PREVENTING INCOMPATIBILITY OF LOCAL GSKIT WITH THE SECURITY ENHANCEMENTS INTRODUCED IN CLIENT VERSIONS 7.1.8 AND 8.1.2

https://www-01.ibm.com/support/entdocview.wss?uid=swg1IT23560

IT23535: DOCUMENTATION TO PREVENT UNWANTED RESULTS WITH THE 7.1.8 AND 8.1.2 CLIENT ENHANCEMENTS BY INCOMPATIBLE LOCAL GSKIT VERSION

https://www-01.ibm.com/support/entdocview.wss?uid=swg1IT23535

APAR‘s / TECHNOTES

After upgrading to version 8.1.2, the Data Protection Oracle backups are failing

https://www-01.ibm.com/support/docview.wss?uid=swg22011609

Configuring Data Protection for Oracle when using IBM Spectrum Protect client V8.1.2 with new security settings

https://www-01.ibm.com/support/docview.wss?uid=swg27050606

Setting the Data Protection SAP HANA password after upgrading to 7.1.8 or 8.1.2

https://www-01.ibm.com/support/docview.wss?uid=swg22010515

ANR8586E seen during server startup and no certificate created

https://www-01.ibm.com/support/docview.wss?uid=swg21988655

Connection fails with GSK_ERROR_BAD_DATE (401)

https://www-01.ibm.com/support/docview.wss?uid=ibm10732283

IT26545: CLIENT TO CLIENT PROXY COMMUNICATION FAILING WITH ANS1579E AND GSK_ERROR_BAD_DATE

https://www-01.ibm.com/support/docview.wss?crawler=1&uid=swg1IT26545

Useful Commands and Information

IBM Spectrum Protect Security Enhancements

Server Certificate / Check Session Security

- Show the current default certificate:
  ```
  gsk8capicmd_64 -cert -getdefault -db cert.kdb -stashed
  ```
- Set the default certificate:
  ```
  gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed -label "TSM Server
  SelfSigned SHA Key"
  ```
- Add source certificate on target server
  ```
  gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii -label "TSM
  Server SelfSigned SHA Key - SRVNAME" -file cert256.SRVNAME.arm
  ```
- List certificates
  ```
  gsk8capicmd_64 -cert -list all -db cert.kdb –stashed
  ```
- Validate certificates

```
gsk8capicmd_64 -cert -validate -label "xxxx"  -db cert.kdb -stashed
```


Client Certificate

- Import the certificate into the client key database by using the following command as root:

```
dsmcert -add -server <servername> -file <path_to_cert256.arm>
```

- List client cerificates

```
gsk8capicmd_64 -cert -list all -db dsmcert.kdb -stashed
```

- Validate client certificates

```
gsk8capicmd_64 -cert -validate -label "xxx" -db dsmcert.kdb –stashed
```

Secure Sockets Layer (SSL) allows industry standard SSL-based secure communications between the IBM Spectrum Protect™ client and server.

https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.4/client/t_cfg_ssl.html

Useful links

- **SSL/GSKIT basics**

  https://www.ibm.com/developerworks/library/se-gskit/

- **IBM Global Security Kit GSKit version 8**
  https://www.ibm.com/support/knowledgecenter/SSAL2T_8.2.0/com.ibm.cics.tx.doc/pdf/GSK_CapiCmd_UserGuide.pdf

- **IBM Spectrum Protect security updates in V7.1.8, V8.1.2, V8.1.3, and V8.1.4**
  http://www-01.ibm.com/support/docview.wss?uid=swg22004844

Update Tipp's for 8.1.3 and later (beside the Enhanced Security stuff)

1. IT22897: NODES "LAST ACCESS DATE/TIME" AND " DAYS SINCE LAST ACCESS" FIELDS ARE NOT UPDATED in 7.1.8 and 8.1.3 servers
   – http://www-01.ibm.com/support/docview.wss?uid=swg1IT22897
2. Beginning with IBM Spectrum Protect Version 8.1.2, you can no longer use the web client to connect to the IBM Spectrum Protect V8.1.2 or later server.
   – https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.2/client/c_bac_webclient_deprecate.html
3. Consider using Shared Memory communication for the Spectrum Protect Database Backups (usually better performance) for Unix only
   – Set `COMMMethod SHAREdmem` and `SHMPort 1510` in dsmserv.opt and TSMDBMGR stanza in dsm.sys file
4. Remove `PASSWORDACCESS GENERATE` from TSMDBMGR stanza in dsm.sys file
5. Spectrum Protect Database Backup allows now up to 32 backup streams
   – `BACKUP DB … NUMStream=32`
6. Update to 8.1.3 start using dsm.sys file in /opt/tivoli/tsm/server/bin/dbbkapi/ for TSMDBMGR stanza
   – `dsm.sys` file is automatically created and environment variables in `<instance_dir>/sqllib/userprofile` and `<instance_dir>/sqllib/usercshrc` are updated