IBM Db2 Analytics Accelerator for z/OS 7.5.10

Encryption of Data in Motion

SH12-7100-02

Note

Before you use this information and the product it supports, read the information in “Notices” on page 29.

Third Edition, December 2022

This edition applies to version 7.5.10 of IBM® Db2® Analytics Accelerator for z/OS® (product number 5697-DA7), and to all subsequent releases and modifications until otherwise indicated in new editions. This edition replaces SH12-7100-01. Changes to this edition are marked with a vertical bar.

Contents

Figures

Chapter 1. Enabling encryption of data in motion

If the setup recommendations are followed (dedicated private network between the mainframe computer or LPAR and accelerators), IBM Db2 Analytics Accelerator for z/OS can be considered a safe product even if network traffic is not encrypted. However, this type of setup often does not align well with existing network infrastructures because some organizations want to route all network traffic, including sensitive data through their corporate intranet. Other organizations have restrictive security standards demanding that any sensitive data sent across a network must be encrypted. Hence a network encryption feature was added to the product.

Naturally, the use of encryption comes at a price, and that is a slower performance, which is due to the fact that data has to be encrypted before it enters the network and decrypted after it leaves it. Both processes require a considerable amount of time, and the data volumes that are handled by IBM Db2 Analytics Accelerator for z/OS are usually extremely high. Customers rightfully expect remarkable acceleration rates despite the use of encryption, and IBM Db2 Analytics Accelerator for z/OS satisfies this demand.

To reduce the CPU consumption on the mainframe, IBM recommends the use of z Systems® Integrated Information Processors (zIIPs) for TLS processing. However, despite faster and specialized hardware, there will be a noticeable performance impact on bulk transmissions of data, such as table load jobs or queries with huge result sets. Queries with small or moderate result sets, on the other hand, will not be impacted by the use of encryption.

Features of encryption solution

- AES-GCM symmetric encryption for the network payload
- RSA 2048 bit encryption keys

Some components must be configured for TLS network encryption with IBM Db2 Analytics Accelerator for z/OS. For an in-depth discussion, see:

- *IBM z/OS V2R1 Communications Server TCP/IP Implementation Volume 4: Security and Policy-Based Networking*, chapters 3,4, and 12.
- *IBM z/OS Communications Server: IP Configuration Guide* in the IBM Documentation, especially the chapters on AT-TLS policies for the policy agent [3] and AT-TLS.
- *IBM Redpaper DB2® for z/OS: Configuring TLS/SSL for Secure Client/Server Communications*

Related information

IBM z Systems Integrated Information Processor (zIIP)

Prerequisites

To be able to encrypt the data traffic between a z/OS LPAR and an accelerator, specific software components are required. On the z/OS side, various components of the z/OS Communications Server must be configured. z/OS makes use of AT/TLS, whereas the accelerator uses *stunnel*. In addition, a certificate and an RSA key pair are required.

Software

The following software components on the z/OS (LPAR) side must be operational:

- Policy Agent (a component of z/OS Communications Server. Version 1.2 or higher is required.)
- Optional: SYSLOG daemon (SYSLOGD)

Certificate and keys

To encrypt the network traffic between a z/OS LPAR and an accelerator, you need:

- An RSA key pair
- Public key certificate signed by shared certificate authority, type X.509 in PKCS#12 format

The certificate is stored in a keyring on the LPAR. The keyring contains all credentials used by the AT/TLS policy configuration.. The private RSA key, as well as the certificate from the keyring (in PKCS#12 format), are required on the accelerator.

If more than one accelerator is involved: Each accelerator needs a dedicated private key signed with a certificate that was issued by the certificate authority (CA). All accelerators attached to a specific LPAR require certificates that were signed by the same CA. The following figure shows three LPARs that are connected to two accelerators.

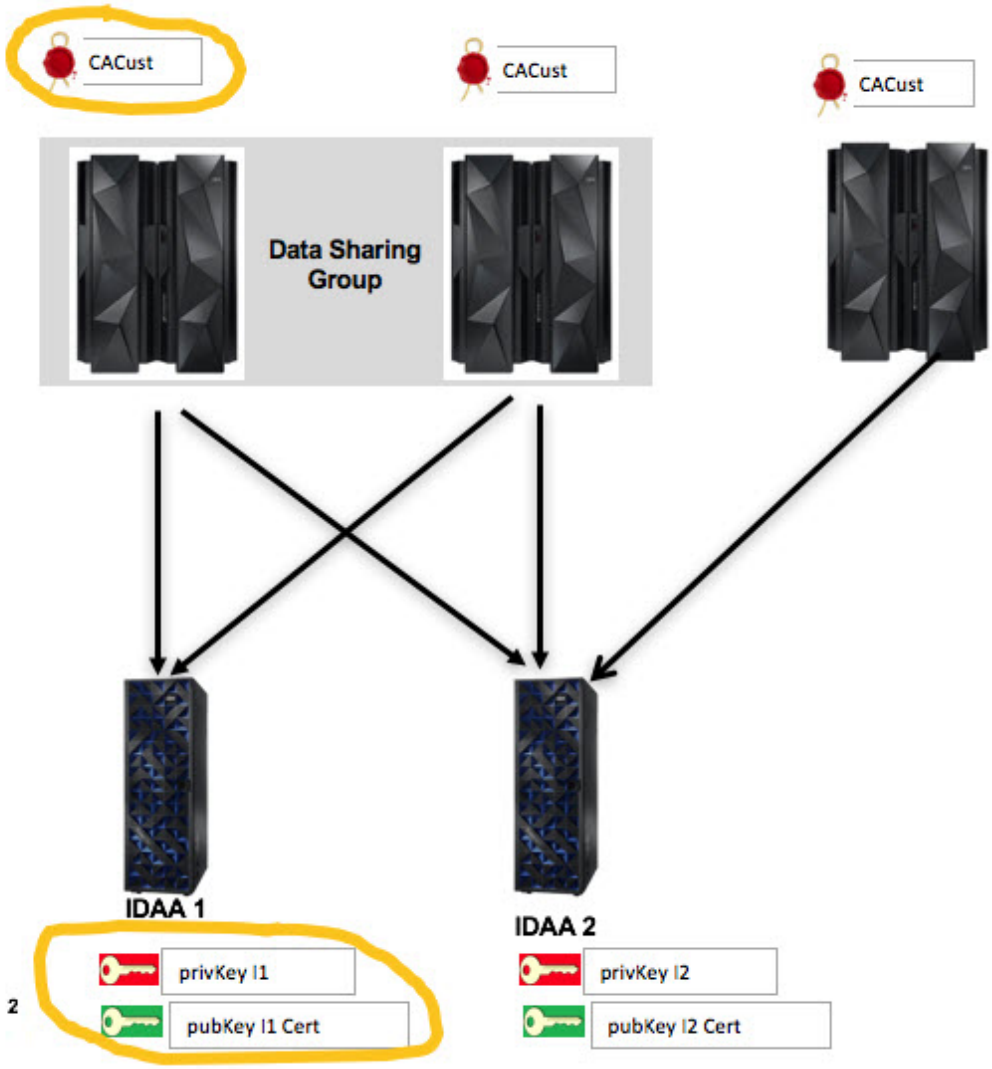

Figure 1. Distribution of certificates and keys

The following sections describe how to configure one connection from one LPAR to one accelerator (circled yellow in the previous figure).

Attention: As indicated, the resulting AT/TLS configuration will accept any certificate issued by the chosen CA. Someone with a valid certificate from the same CA could therefore run a man-in-the-middle attack. You can mitigate that risk by choosing a private CA just for IBM Db2 Analytics Accelerator, and use that CA to sign certificates for valid accelerators only.

Creating a key ring that includes the CA certificate

You start by creating a key ring to include the certificate of the certificate authority (CA). This certificate is then used to sign the certificates for each individual accelerator.

Before you begin

Make sure that the required z/OS Communications Server components are installed and operational.

About this task

The steps presented here include the creation of a self-signed certificate. You can skip this step (step “3” on page 4) if you want to use an existing certificate from an external CA.

Procedure

1. Add commands to create a RACF® profile with appropriate permissions:
   a) First add commands to define the required classes:

```
RDEFINE FACILITY   IRR.DIGTCERT.ADD        UACC(NONE)
RDEFINE FACILITY   IRR.DIGTCERT.ADDRING    UACC(NONE)
RDEFINE FACILITY   IRR.DIGTCERT.CONNECT    UACC(NONE)
RDEFINE FACILITY   IRR.DIGTCERT.GENCERT    UACC(NONE)
RDEFINE FACILITY   IRR.DIGTCERT.GENREQ     UACC(NONE)
RDEF    FACILITY   IRR.DIGTCERT.EXPORT     UACC(NONE)
RDEF    FACILITY   IRR.DIGTCERT.EXPORTKEY  UACC(NONE)
RDEF    FACILITY   IRR.DIGTCERT.DELETE     UACC(NONE)
RDEF    FACILITY   IRR.DIGTCERT.LIST       UACC(NONE)
```

   b) Grant the required permissions.

   All users that run IBM Db2 Analytics Accelerator stored procedures (this includes users of IBM Db2 Analytics Accelerator Studio), must have READ and UPDATE permissions as shown in the following example. In the example, these permissions are given to the users in group IBMGRP01:

```
PE IRR.DIGTCERT.LIST CL(FACILITY) ID(IBMGRP01) ACC(READ)
PE IRR.DIGTCERT.LISTRING CL(FACILITY) ID(IBMGRP01) ACC(UPDATE)
```

   You might want to give these permissions to all users, which can be achieved by running the following commands:

```
PE IRR.DIGTCERT.LIST CL(FACILITY) ID(*) ACC(READ)
PE IRR.DIGTCERT.LISTRING CL(FACILITY) ID(*) ACC(UPDATE)
```

   In addition, users running Db2 address spaces (Db2 started task users), such as DDF (DIST) require the UPDATE permission:

```
PE IRR.DIGTCERT.LISTRING CL(FACILITY) ID(DB11USER) ACC(UPDATE)
```

   Note:

   Granting the permission to update the IRR.DIGTCERT.LISTRING FACILITY class is not a security risk. It is true that users with this permission can read anyone’s key ring. However, that only allows these users to extract and use the certificates of the key ring. It does not allow them to use the private keys associated with the certificates. Therefore, users with an update permission for IRR.DIGTCERT.LISTRING FACILITY cannot pretend to be using somebody else´s user ID.

   If you use the incremental update function, the roles of client and server are reversed for the TLS handshake. That is, the Db2 subsystem acts as the server, and the accelerator as the client. Hence the user ID behind the Db2 started tasks needs access to the key ring used by AT/TLS:

```
PE IRR.DIGTCERT.LIST  CL(FACILITY) ID(DB11USER) ACC(UPDATE)
PE IRR.DIGTCERT.LISTRING  CL(FACILITY) ID(DB11USER) ACC(UPDATE)
SETROPTS RACLIST(FACILITY) REFRESH
```

2. The key ring referenced by the TTLSKeyRingParms keyword in the AT-TLS configuration must contain a certificate for the Certificate Authority. If a suitable key ring does not yet exist, create one. Include, for example, the following code in the JCL job, which creates a key ring for a TSO user named DBAUSER. If necessary, replace DBAUSER with the ID of the actual user.

```
//* add a ring

RACDCERT ID(DBAUSER) ADDRING(TLS_SHARED_RING)
```

   In addition, each Db2 subsystem that uses a different user ID for its started tasks requires a keyring for each such user. For example:

```
RACDCERT ID(DB11USER   ) ADDRING(TLS_SHARED_RING)
```

   For more information, see *IBM Redpaper DB2 for z/OS: Configuring TLS/SSL for Secure Client/Server Communications*.
3. Add commands to the JCL that will create a self-signed root (CA) certificate for each key ring. In the following example, the certificate is named CA1_ATTLS.

```
//*
//* Create a CA certificate (self-signed in TLS_SHARED_RING)
//*
//CRKEY   EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSTSIN  DD *
 RACDCERT CERTAUTH GENCERT                                  +
   SUBJECTSDN(                                              +
     CN('CACERT2')                                          +
     O('IBM DEUTSCHLAND RESEARCH & DEVELOPMENT GMBH')       +
     OU('SYSTEM Z SW TESTLAB')                              +
     C('DE'))                                               +
   NOTBEFORE(DATE(2015-08-06))                              +
   NOTAFTER(DATE(2030-12-31))                               +
   KEYUSAGE(CERTSIGN)                                       +
   WITHLABEL('CA1_ATTLS')
```

4. Append commands that add the certificate to each key ring, for example:

```
//* add the CA certificate to a key ring

/*
//* connect the CA to key ring TLS_SHARED_RING for ID DBAUSER
CONN1   EXEC PGM=IKJEFT01
SYSTSPRT DD SYSOUT=*
SYSPRINT DD SYSOUT=*
SYSTSIN  DD *
RACDCERT ID(DBAUSER) CONNECT(CERTAUTH LABEL('CA1_ATTLS') +
          RING(TLS_SHARED_RING) USAGE(CERTAUTH))
```

5. Submit the JCL job.

Generating a key pair and a certificate for an accelerator and exporting these

A further pair of keys and certificate is required for the accelerators that are supposed to participate in the encrypted network communication with a z/OS client LPAR. An accelerator requires the RSA key pair and the associated certificate in a PKCS#12 password-encrypted file. You can use a tool of choice or an external certificate authority to generate the PKCS#12 file. This chapter contains instructions how to generate the PKCS#12 file using the z/OS Security Server RACF RACDCERT command.

Before you begin

See RACDCERT GENCERT (Generate certificate) for information about the authorizations that are required to run the RADCERT command.

About this task

This step is only required for the first LPAR that needs to connect to an accelerator. The certificate can be used for all connections to the same accelerator. The steps in this section do not require or cause an outage of the system.

Procedure

1. Create a JCL job and add commands to generate a pair of keys and a certificate to contain the public key for an accelerator, so that the z/OS client LPAR can identify the accelerator as an authorized participant in the encrypted network communication. The following example is a certificate for an accelerator with the name ACC148:

```
//*
//* Create a personal certificate for the ACC148 accelerator
//* signed by the CA
//CRKEY   EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSTSIN  DD *
 RACDCERT ID(DBAUSER) GENCERT                                    +
     SUBJECTSDN(CN('ACC148')     +
     O('IBM DEUTSCHLAND RESEARCH & DEVELOPMENT GMBH')    +
     OU('SYSTEM Z SW TESTLAB')                            +
     L('BOEBLINGEN') SP('BADEN WUERTTEMBERG') C('DE'))    +
     NOTAFTER(DATE(2020-03-15))                           +
     SIZE(2048)      WITHLABEL('ACC148TTLS')              +
     KEYUSAGE(HANDSHAKE) +
     SIGNWITH(CERTAUTH LABEL('CA1_ATTLS')) +
     ALTNAME( IP(10.101.12.158))
/*
```

   In this example, a key pair and a certificate with an alias name of ACC148TTLS (`WITHLABEL('ACC148TTLS')`) are created. An alias (or X.509 friendly name) is required to refer to the certificate when you enable TLS communication. The certifcate is signed by a certificate authority (CA) named CA1_ATTLS.

2. Add commands to the JCL that will store the key pair and the certificate in a PKCS#12 file that can be transferred and read by the accelerator, for example:

```
//* run a second command
//CONN    EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSTSIN  DD *
/*
//* export the key pair and certificate into a PKCS#12 file
//* that can be transferred to the accelerator
  racdcert export(label('ACC148TTLS')) ID(DBAUSER)    +
 DSN('IDAA.CERTS.S148') FORMAT(PKCS12DER) PASSWORD('PASSWORD')
```

   Important:

   - The file type of the certificate file is PKCS#12, but the format you need to select when generating files of this type is PKCS12DER.
   - Keep the password of the PKCS#12 file secret. Everyone who has access to the file and the password can access the private key for the authentication of the TLS connection and thus use the key to run an attack on the encrypted traffic.
   - Only the following characters are allowed for the password of the PKCS#12 file:
     - a-z
     - A-Z
     - 0-9
     - Underscore (_)

3. Submit the job.

   The result is a sequential data set.

4. Download the binary PKCS#12 certificate file to a workstation on which IBM Db2 Analytics Accelerator Studio is installed. The file name `s148.p12` is used for the downloaded file in this example.

Transferring the PKCS#12 file to an accelerator

Transfer the PKCS#12 file to a connected accelerator to enable the authentication of this accelerator with the associated z/OS client LPAR.

Before you begin

In the task described here, the SYSPROC.ACCEL_UPDATE_SOFTWARE2 stored procedure is called from IBM Db2 Analytics Accelerator Studio. Hence the user who connects from the studio to the relevant LPAR must have the privilege to run this stored procedure.

On the workstation that runs IBM Db2 Analytics Accelerator Studio, you need a certificate file in PKCS#12 format containing an RSA 2048-Bit key pair (private and public key). This file must also contain a certificate issued by the same certificate authority (CA) as the root certificate on the key ring for the AT-TLS configuration of the connecting LPAR (see).

Note: The IBM Db2 Analytics Accelerator Console uses the term *certificate*, even though the entire PKCS#12 file is meant.

About this task

This step is only required for the first LPAR that needs to connect to an accelerator. The certificate can be used for all connections to the same accelerator. The steps in this section do not require or cause an outage of the system.

Procedure

1. Start IBM Db2 Analytics Accelerator Studio.
2. Open the **Accelerator** view of the accelerator that you want to transfer the certificate to.
3. Click **Encryption details** in the header of the **Accelerator** view (at the top).
4. In the **Encryption Details** window, click **Transfer new certificates**

   The **Transfer Certificates** window opens.
5. In the **Transfer Certificates** window, under the heading **Available certificates**, select the certificate file and click **Transfer certificate from client**.

   Important: If you do not see the certificate in the **Available certificates** box:

   a. Locate the certificate file in the file system of your client.

   b. Change the extension of the certificate file from p12 to `crt`. The certificate is then visible in the **Available certificates** box, so that you can transfer it.
6. Select the copied certificate file in the **Select Certificates** window and click **Add selected**.

   You return to the **Transfer Certificates** window.
7. Click **Transfer**.
8. Confirm the message in the **Transfer File** window by clicking **OK**.

What to do next

You must import the transferred file into the keystore of the accelerator. You do this from the IBM Db2 Analytics Accelerator Console.

Related tasks

Generating a key pair and a certificate for an accelerator and exporting these

A further pair of keys and certificate is required for the accelerators that are supposed to participate in the encrypted network communication with a z/OS client LPAR. An accelerator requires the RSA key pair and the associated certificate in a PKCS#12 password-encrypted file. You can use a tool of choice or

an external certificate authority to generate the PKCS#12 file. This chapter contains instructions how to generate the PKCS#12 file using the z/OS Security Server RACF RACDCERT command.

Importing the PKCS#12 file into the database of the accelerator

A certificate must be stored in the database of the accelerator before it can be used for authentication purposes.

Before you begin

You need:

- PKCS#12 certificate file that has been transferred to the accelerator
- Password of the certificate file
- Password of the IBM Db2 Analytics Accelerator Console

About this task

This step is only required for the first LPAR that needs to connect to an accelerator. The certificate can be used for all connections to the same accelerator. The steps in this section do not require or cause an outage of the system.

Procedure

1. Start and log on to the IBM Db2 Analytics Accelerator Console.

   For more information, see *Logging on to the IBM Db2 Analytics Accelerator Console* in the IBM Documentation.
2. Type the number in front of the option `Manage Encryption of Data in Motion` and press Enter to display the submenu:

```
 main -> <#>
 ------------------------------------------------------
You have the following options:
 (0) - Go back one level
 (1) - Import certificates for encrypted connections
 (2) - Delete certificates for encrypted connections
 (3) - Specify the certificate to use for the accelerator
 (4) - Display the status of encrypted connections
 (5) - Restart the encryption-of-data-in-motion service
```

3. Type 1 and press Enter:

   You see a screen similar to the following:

```
Select the PKCS#12 file to be imported:
You can transfer additional files using the Software Update
'Transfer' window in Db2 Analytics Accelerator Studio.

Files in directory '/head/dwa/transfer':
    1 : s148.p12

Select a file or enter 0 to go back:  (Default 0) > 1
```

4. Type the number in front of the PKCS#12 file name and press Enter.

   In the previous example, this is the number 1.

   You are asked to enter the password of the PKCS#12 file:

```
Enter the password for the given PKCS#12 file (in TSO, use PF3 to hide input):
```

5. Enter the password.
6. You are asked to confirm the import:

```
Import certificate from file '/head/dwa/transfer/s148.p12' (y/n) [n]: y
```

7. Type y and Press Enter.

You see a message similar to the following:

```
Certificate Name: s148
issuer= CN=CA1,OU=SYSTEM Z SW TESTLAB,O=IBM DEUTSCHLAND
RESEARCH & DEVELOPMENT GMBH,C=DE
subject= CN=SIM148,OU=SYSTEM Z SW TESTLAB,O=IBM DEUTSCHLAND
RESEARCH & DEVELOPMENT GMBH,L=BOEBLINGEN,ST=BADEN WUERTTEMBERG,C=DE
notBefore=Jan 19 23:00:00 2017 GMT
notAfter=Mar 15 22:59:59 2020 GMT
<No Alias>

Done
Press <return> to continue
```

8. Press Enter to return to the submenu.

Activating a certificate on an accelerator

An activation step is necessary before a certificate can actually be used.

Before you begin

The certificate that you want to activate must have been imported successfully on the accelerator.

About this task

Activating a new certificate might cause a temporary unavailability of existing encrypted connections to the same accelerator.

Procedure

1. Start and log on to the IBM Db2 Analytics Accelerator Console.

   For more information, see *Logging on to the IBM Db2 Analytics Accelerator Console* in the IBM Documentation.
2. Type the number in front of the option `Manage Encryption of Data in Motion` and press Enter to display the submenu:

```
 main -> <#>
 ------------------------------------------------------------
You have the following options:
 (0) - Go back one level
 (1) - Import certificates for encrypted connections
 (2) - Delete certificates for encrypted connections
 (3) - Specify the certificate to use for the accelerator
 (4) - Display the status of encrypted connections
 (5) - Restart the encryption-of-data-in-motion service
```

3. Type 3 and press Enter:

   You see a screen similar to the following:

```
Activate a new certificate for the accelerator

The following certificates are available on the accelerator:

Certificate Name: s148
issuer= CN=CA1,OU=SYSTEM Z SW TESTLAB,O=IBM DEUTSCHLAND
RESEARCH & DEVELOPMENT GMBH,C=DE
subject= CN=SIM148,OU=SYSTEM Z SW TESTLAB,O=IBM DEUTSCHLAND
RESEARCH & DEVELOPMENT GMBH,L=BOEBLINGEN,ST=BADEN WUERTTEMBERG,C=DE
notBefore=Jan 19 23:00:00 2017 GMT
notAfter=Mar 15 22:59:59 2020 GMT
<No Alias>

Currently active certificate: s148
Certificates available:
    1 : s148

Select a certificate or enter 0 to go back:  (Default 0) >
```

4. Type the number in front of the certificate name and press Enter.
   In the previous example, this is number 1.
5. You are asked to confirm the activation:
   ```
   Activate certificate 's148' (y/n) [n]:
   ```
6. Type y and Press Enter.
   You see a message similar to the following:

```
Certificate 's148' is now active.

Press <return> to continue
```

7. Press Enter to return to the submenu.

Configuring the Policy Agent on your client LPARs

z/OS Communications Server stores all configuration settings for AT-TLS in a central component called the Policy Agent. As the name suggests, this agent executes a policy, which is a set of configurable instructions. You must adapt the policy for encrypted network traffic between a client LPAR and IBM Db2 Analytics Accelerator.

About this task

The following steps show how to configure the Policy Agent for a single client LPAR and two accelerators. It is a walk-through based on examples. The following IP addresses, user ID, and key ring are used in the examples:

Table 1. IP addresses, user ID, and key ring	
Accelerator ACC1	`203.0.113.158`
Accelerator ACC2	`203.0.113.47`
TSO user ID of key ring owner	ID of Db2 started task user, for example `DBAUSER`
Key ring	`TLS_SHARED_RING`

Procedure

1. Use TSO to log on to the z/OS client LPAR that connects to the accelerator.
2. Open the Policy Agent configuration-file in an editor, such as ISPF.
3. Add an address group for the private data network on z/OS:
   For example:

```
IpAddrGroup                  StunnelAccelerators
{
    IpAddr
    {
      Addr 203.0.113.158    # ACC01
    }
    IpAddr
    {
      Addr 203.0.113.47     # ACC02
    }
}
```

4. Add a port group that contains the list of ports that the accelerator uses for encrypted connections.
   For example:

```
PortGroup                    StunnelAcceleratorPorts
{
   PortRange
   {
     Port 11400 11401        # Analytics accelerator server
   }
   PortRange
```

```
   {
     Port 11351 11399        # TLS for CDC capture engine to
                             # accelerator replication engine
   }
}
```

5. Add a `TTLSCipherParms` element that specifies the encryption algorithms to be used for the TLS connection. Specify the following CIPHERS:
   - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

   Note: AES128 is faster, but AES 256 is more secure. You can enforce the use of a specific cipher by specifying one cipher only. By default, AES128 is used if you specify both.

   The following example uses the `V3CipherSuites4Char` keyword to specify these CIPHERS by using a combination of two 4-digit hexadecimal numbers:

```
TTLSCipherParms              StunnelParms
{
   V3CipherSuites4Char       C02FC030
}
```

6. Add a TLS group action that enables AT-TLS security:

```
TTLSGroupAction              StunnelGroup
{
       TTLSEnabled                        On
}
```

7. Specify a TLS environment that includes the following information:
   - The key ring containing the root certificate
   - Use of TLS version 1.2 as the only supported protocol
   - Client authentication pass-thru (optional)
   - `CLIENT` as the handshake role
   - The `TTLSCipherParms` element defined before
   - The trace level (use different trace levels for production (`0`) and problem diagnosis (7 or 255)

   According to the example, this results in the following specification:

```
TTLSEnvironmentAction        StunnelClientEnvironment
{
       TTLSKeyRingParms
         {
           Keyring                        DBAUSER/TLS_SHARED_RING
         }
    TTLSEnvironmentAdvancedParms
       {
             SSLv2 Off
          SSLv3 Off
          TLSv1 Off
          TLSv1.1 Off
          TLSv1.2 On
          ClientAuthType PassThru

       }
       HandshakeRole                      CLIENT
       TTLSCipherParmsRef                 StunnelParms
       Trace                              7
}
```

8. Finally, add an outbound TTLS rule that combines the address group, the port range, the TTLS group action, and the TTLS environment action.
   For the current example, this rule looks as follows:

```
TTLSRule                     StunnelDWP1Sim148
{
       RemotePortGroupRef                 StunnelAcceleratorPorts
       RemoteAddrGroupRef                 StunnelAccelerators
```

```
        Direction                       Outbound
        TTLSGroupActionRef              StunnelGroup
        TTLSEnvironmentActionRef        StunnelClientEnvironment
}
```

9. Activate the changed AT-TLS policy by refreshing the Policy Agent with the following TSO command:

```
F PAGENT,REFRESH
```

Enabling encrypted network traffic for an accelerator

To enable encrypted network traffic between a z/OS client LPAR and an accelerator, all you have to do is provide the correct port number for encrypted network traffic. For a new accelerator, this can be done during the pairing process: you just specify the port for encrypted traffic rather than the standard port. Enabling encryption for an existing accelerator is less straightforward, but not very time-consuming either.

Before you begin

Make sure that the following steps have already been completed:

- You have transferred and imported a PKCS#12 file for the authentication of the new connection.
- You have prepared and activated the AT-TLS policy rules in the Policy Agent.

The following cases must be distinguished:

Enabling encryption for a new accelerator
Because such an accelerator does not yet process any workload, the enablement of encryption does not cause a downtime or interruption.

Enabling encryption for an existing accelerator
For an accelerator that is in use, the switch to a different network port might lead to a situation in which a network connection with the accelerator cannot be established. In cases like these, users receive an error message when they try to submit new queries or load jobs. However, the outage does not impact jobs that were already running before the restart.

None the less, to avoid irritation, plan and communicate the outage ahead of time. You might want to stop the accelerator entirely before the restart by using the `-STOP ACCEL` command.

Enabling encryption for a new accelerator

As you attach a new accelerator to a Db2 subsystem, you can also make the necessary arrangements for encrypted network traffic.

About this task

The configuration steps are exactly the same as for adding an accelerator to a Db2 subsystem. The only difference is the port number that you specify in the **Add Accelerator**wizard.

Procedure

1. Follow the steps in the section “Obtaining the pairing code for authentication” on page 23.
   You obtain the credentials for adding an accelerator. This includes two port numbers, one for unencrypted network traffic (labeled just `Port`), and one for encrypted traffic, labeled `Port (AT-TLS)`.
2. Follow the steps in the section “Completing the authentication using the Add Accelerator wizard” on page 25 up to step 8.
   This is the point where you enter the port number. Enter the number that was labeled `Port (AT-TLS)`. By default, this is port `11400`.
3. Complete the **Add Accelerator** wizard as described.

Results

Provided that all prerequisite configuration tasks have been completed, network traffic between the Db2 subsystem and the specified accelerator will be encrypted.

Enabling encryption for an existing accelerator

To enable network encryption for an accelerator that is already in use, you must submit a SQL command to change the configured port range in the Db2 system table SYSIBM.LOCATIONS.

About this task

By default, the port range for encrypted network traffic comprises the ports 11400 and 11401. Setting the port number in SYSIBM.LOCATIONS to 11400 as described here, you specify the starting point of that port range.

Procedure

1. You want to enable network encryption for a particular Db2 subsystem/accelerator pair. From TSO, log on to the z/OS LPAR on which the Db2 subsystem is located.
2. Start an application that allows you submit SQL commands, such as SPUFI.
3. From the command line of that application, enter an UPDATE command as shown in the following example. Replace ACC01 with the name of your accelerator:

```
UPDATE SYSIBM.LOCATIONS
  SET PORT = 11400
  WHERE LOCATION = (SELECT SYSACCEL.SYSACCELERATORS.LOCATION
              FROM SYSACCEL.SYSACCELERATORS
              WHERE ACCELERATORNAME = 'ACC01');
```

Results

Provided that all prerequisite configuration tasks have been completed, network traffic between the Db2 subsystem and the specified accelerator will be encrypted.

Chapter 2. Verifying the encryption status

From z/OS , you can run several commands to monitor the policy agent AT-TLS rules and to check the details of encrypted connections.

Procedure

1. Use TSO to log on to a z/OS client LPAR that uses an encrypted connection to connect to an accelerator.
2. You have several choices to monitor the encryption status:

   - To verify the policy rules for AT-TLS, you can use the **pasearch** command. Run the command with the `-t` option to query the policy agent. The command can be run from the z/FS shell or from the Time Sharing Option Extensions (TSO/E) shell:

     ```
     pasearch -t
     ```

     The command displays all AT-TLS policy rules. See the following extract from a screen output:

     ```
     TCP/IP pasearch CS V2R1                  Image Name: TCPIP
       Date:                 01/24/2019       Time:  14:12:48
       TTLS Instance Id:     1547625735


     policyRule:             StunnelIDAARule
       Rule Type:            TTLS
       Version:              3                Status:            Active
       Weight:               1                ForLoadDist:       False
       Priority:             1                Sequence Actions:  Don't Care
       No. Policy Action:    2                ConditionListType: CNF
       policyAction:         StunnelGroup

        .
        .
        .

       TTLS Condition Work Summary:           NegativeIndicator: Off
        Local Address:
         FromAddr:           All
         ToAddr:             All
        Remote Address:
         FromAddr:           All
         ToAddr:             All

        .
        .
        .

       TTLS Action:                 StunnelGroup
         Version:                   3
         Status:                    Active
         Scope:                     Group
         TTLSEnabled:               On

        .
        .
        .

         TTLSCipherParms:
          v3CipherSuites:
            C02F  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
            C030  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
         Policy created: Wed Jan 16 09:02:15 2019
         Policy updated: Wed Jan 16 09:02:15 2019
     ```

   - You can also use the TSO command **NETSTAT TTLS** to monitor AT-TLS connections:

     NETSTAT TTLS
     Displays the number of connections per AT-TLS group. For example:

     ```
     MVS TCP/IP NETSTAT CS V2R1  TCPIP Name: TCPIP    13:36:38
     TTLSGrpAction                       Group ID    Conns
     ```

```
--------------------------- -------  ----------  -----
grp_Diagnostic                       00000047        0
grp_Production                       00000048        3
grp_StartUp                          00000049        0
DB2@SecureGrpAct                     0000004B        0
StunnelGroup                         0000004A        0
READY
```

NETSTAT ALLCONN
Displays all connection IDs.

NETSTAT ALLCONN <connid>
In conjunction with a connection ID (<connid>), the command displays the details of a specific AT-TLS connection.

See the following example, which shows a connection to an accelerator listening on port 11401 at IP address 203.0.113.158. The connection is encrypted. using the TLS 1.2 standard. The cipher TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 has been specified to select the encryption algorithm:

```
MVS TCP/IP NETSTAT CS V2R1       TCPIP Name: TCPIP
 ConnID: 000143F3
   JobName:      DB11DWA
   LocalSocket:  192.0.2.25..30199
   RemoteSocket: 203.0.113.158..11401
   SecLevel:     TLS Version 1.2
   Cipher:       C02F TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   CertUserID:   N/A
   MapType:      Primary
   FIPS140:      Off
 TTLSRule: StunnelDWP1Sim148
   TTLSGrpAction:  StunnelGroup
   TTLSEnvAction:  StunnelClientEnvironment
 ***
```

- In addition, you can view the encryption status from IBM Db2 Analytics Accelerator Studio:
  a. Open the **Accelerator** view of the accelerator that is supposed to use encrypted connections.
  b. In the header of the **Accelerator** view, click the **Encryption details** link.

  A window with the title **Encryption Details for Accelerator <name>** opens. It is devided into the following sections:

  Disk Encryption
  Shows whether disk encryption is used by your accelerator hardware.

  Network Encryption
  Shows two tables and a text box:

  Encrypted connections
  This table contains details about the encrypted connections to the selected accelerator. This includes the names of the connecting client LPARs, their IP addresses, the IP address of the accelerator, the names of the certificates that are used, and the date and time when the connections were established.

  Certificates
  This table shows details about the certificates that are used, such as the validity, the type (user or root certificate), and the distinguished name.

  Selected certificate in X.509 encoding
  Shows the content of a certificate that is selected in the table above, in (encrypted) X.509 Base64 encoding. Naturally, the displayed content does not include the private keys because these must remain secret.

What to do next

If you are facing connection problems, you might also want to check further information sources. See the links at the bottom of this topic.

Related information

Netstat TTLS/-x report

Diagnosing Application Transparent Transport Layer Security (AT-TLS)

Chapter 3. Replacing an expiring certificate

An accelerator issues repeated warnings when an encryption certificate is about to expire. You can see these warnings if you click **Encryption details** in the header section of the **Accelerator** view if the accelerator uses encrypted network connections.

About this task

A change in the configuration of the TLS service, like the replacement of a certificate, requires a restart of the TLS proxy. Such a restart ends all existing encrypted connections to the accelerator. It is therefore better to prepare for this period of unavailability beforehand.

If IBM InfoSphere® Change Data Capture for z/OS (CDC) is used for incremental updates, mind that the procedure below does not disable encryption for incrementally updated tables because this would require a cancellation of the subscription. However, tables can only be disabled and re-enabled for incremental updates if data encryption is already off. This is not the case. If you disable encryption despite the fact that there are active subscriptions, you lose all the data, and will have to reload all the tables later on.

So if CDC is your solution for incremental updates, decide carefully before you disable encryption for a Db2 subsystem. Do not delete the certificate as long as it is used by a subscription.

IBM Integrated Synchronization , on the other hand, does not depend on the encryption certificate, and is thus not affected by a restart of the TLS proxy.

Procedure

1. Communicate the outage to the participants ahead of time.
2. End or cancel all administrative tasks that were started from the accelerator, such as load jobs.
3. Stop incremental updates for the accelerator.
4. Run the Db2 command **-STOP ACCEL** to stop the accelerator.
5. Generate a new key pair and certificate for the accelerator.

   For instructions, see “Generating a key pair and a certificate for an accelerator and exporting these” on page 4.
6. Transfer the new certificate.

   For instructions, see “Transferring the PKCS#12 file to an accelerator” on page 6.
7. To avoid confusion later on, delete the expiring certificate from the IBM Db2 Analytics Accelerator Console.

   For instructions, see Chapter 4, “Deleting an accelerator certificate,” on page 17.
8. Import the new certificate into the accelerator database.

   For instructions, see “Importing the PKCS#12 file into the database of the accelerator” on page 7.
9. Run the Db2 command **-START ACCEL** to restart the accelerator.
10. Restart incremental updates for the accelerator.
11. If necessary, restart any administrative tasks.

Chapter 4. Deleting an accelerator certificate

It is recommended that you delete certificates from the accelerator database if these certificates are no longer used.

Before you begin

You need the password of the IBM Db2 Analytics Accelerator Console.

Procedure

1. Start and log on to the IBM Db2 Analytics Accelerator Console.

   For more information, see *Logging on to the IBM Db2 Analytics Accelerator Console* in the IBM Documentation.
2. Type the number in front of the option `Manage Encryption of Data in Motion` and press Enter to display the submenu:

```
 main -> <#>
 ------------------------------------------------------------
You have the following options:
 (0) - Go back one level
 (1) - Import certificates for encrypted connections
 (2) - Delete certificates for encrypted connections
 (3) - Specify the certificate to use for the accelerator
 (4) - Display the status of encrypted connections
 (5) - Restart the encryption-of-data-in-motion service
```

3. Type 2 and press Enter:

   You see a screen similar to the following:

```
The following certificates are available on the accelerator:

Certificate Name: s148
issuer = CN=CA1,OU=SYSTEM Z SW TESTLAB,O=IBM DEUTSCHLAND RESEARCH & DEVELOPMENT
         GMBH,C=DE
subject = CN=SIM148,OU=SYSTEM Z SW TESTLAB,O=IBM DEUTSCHLAND RESEARCH & DEVELOPMENT
        GMBH,L=BOEBLINGEN,ST=BADEN WUERTTEMBERG,C=DE
notBefore = Jan 19 23:00:00 2017 GMT
notAfter = Mar 15 22:59:59 2020 GMT
<No Alias>

Certificates available:
    1 : s148

Select a certificate or enter 0 to go back:  (Default 0) > 1
```

4. Type the number in front of the certificate name and press Enter.

   In the previous example, this is the number 1.

   You are asked to confirm the deletion:
5. Type y and Press Enter.

   The bottom of the screen looks similar to the following screen. Because only one certificate existed in the example, the actual screen output for the example is:

```
The following certificates are now available on the accelerator:

Done
Press <return> to continue
```

6. Press Enter to return to the submenu.

Chapter 5. Disabling encryption of data in motion

In case that you no longer want to encrypt network traffic between your z/OS client LPARs and your accelerators, you can, of course, undo the configuration changes and disable encryption of data in motion. In doing so, it is crucial that you observe the recommended order of steps closely to avoid losing access to a system.

Disabling encryption for an accelerator

To disable network encryption for an accelerator, you must submit a SQL command that resets the port range in the Db2 system table SYSIBM.LOCATIONS.

About this task

By default, the port range for unencrypted network traffic comprises the ports 1400 and 1401. Setting the port number in SYSIBM.LOCATIONS to 1400 as described here, you specify the starting point of that port range.

Attention: Currently, you cannot disable encryption if the incremental update function is in use. To be in a position that allows you to disable encryption, you must first disable incremental updates. That is, to return to unencrypted network traffic from a paired Db2 subsystem to a particular accelerator, you must cancel the corresponding subscription (disable incremental updates) from the IBM Db2 Analytics Accelerator Console.

In consequence, this means that you must reload all the tables involved when you re-enable incremental updates because the tables have gone out of sync during the disablement phase. Reloading all tables can be a time-consuming process. Therefore, decide carefully if you really need to disable encryption under these circumstances.

Procedure

1. You want to disable network encryption for a particular Db2 subsystem/accelerator pair. From TSO, log on to the z/OS LPAR on which the Db2 subsystem is located.
2. Start an application that allows you submit SQL commands, such as SPUFI.
3. From the command line of that application, enter an UPDATE command as shown in the following example. Replace ACC01 with the name of your accelerator:

```
UPDATE SYSIBM.LOCATIONS
  SET PORT = 1400
  WHERE LOCATION = (SELECT SYSACCEL.SYSACCELERATORS.LOCATION
              FROM SYSACCEL.SYSACCELERATORS
              WHERE ACCELERATORNAME = 'ACC01');
```

Results

Network traffic between the Db2 subsystem and the accelerator will no longer be encrypted.

Deleting the certificate

To disable encryption on the accelerator side, it is sufficient to delete the certificate.

Before you begin

You need the password of the IBM Db2 Analytics Accelerator Console.

Procedure

1. Start and log on to the IBM Db2 Analytics Accelerator Console.

For more information, see *Logging on to the IBM Db2 Analytics Accelerator Console* in the IBM Documentation.

2. Type the number in front of the option `Manage Encryption of Data in Motion` and press Enter to display the submenu:

```
 main -> <#>
 ------------------------------------------------------------
You have the following options:
 (0) - Go back one level
 (1) - Import certificates for encrypted connections
 (2) - Delete certificates for encrypted connections
 (3) - Specify the certificate to use for the accelerator
 (4) - Display the status of encrypted connections
 (5) - Restart the encryption-of-data-in-motion service
```

3. Type 2 and press Enter:

   You see a screen similar to the following:

```
The following certificates are available on the accelerator:

Certificate Name: s148
issuer = CN=CA1,OU=SYSTEM Z SW TESTLAB,O=IBM DEUTSCHLAND RESEARCH & DEVELOPMENT
         GMBH,C=DE
subject = CN=SIM148,OU=SYSTEM Z SW TESTLAB,O=IBM DEUTSCHLAND RESEARCH & DEVELOPMENT
        GMBH,L=BOEBLINGEN,ST=BADEN WUERTTEMBERG,C=DE
notBefore = Jan 19 23:00:00 2017 GMT
notAfter = Mar 15 22:59:59 2020 GMT
<No Alias>

Certificates available:
    1 : s148

Select a certificate or enter 0 to go back:  (Default 0) > 1
```

4. Type the number in front of the certificate name and press Enter.

   In the previous example, this is the number 1.

   You are asked to confirm the deletion:

5. Type y and Press Enter.

   The bottom of the screen looks similar to the following screen. Because only one certificate existed in the example, the actual screen output for the example is:

```
The following certificates are now available on the accelerator:

Done
Press <return> to continue
```

6. Press Enter to return to the submenu.

Removing accelerator-related entries from the Policy Agent configuration file

Remove entries from your Policy Agent configuration-file as shown, but do not activate the modified policy before you have removed the certificates from the connected accelerators.

Procedure

1. Use TSO to log on to the z/OS client LPAR that you want to disable.
2. Open the Policy Agent configuration-file in an editor, such as ISPF.
3. Remove the following entries from the configuration file of the Policy Agent, but only if these entries pertain to the very last accelerator that you are going to remove.

   If you still want to use encrypted connections for a subset of your accelerators, skip this step and continue with step “4” on page 21.

   For example:

4. For the accelerators that you want to disable, remove the corresponding IP address group (`IpAddrGroup`):
   For example, remove:

```
IpAddrGroup                  StunnelAccelerators
{
    IpAddr
    {
      Addr 203.0.113.158    # ACC01
    }
    IpAddr
    {
      Addr 203.0.113.47     # ACC02
    }
}
```

5. Also remove the port group (`PortGroup`). For example:

```
PortGroup                    StunnelAcceleratorPorts
{
   PortRange
   {
     Port 11400 11401        # Analytics accelerator server
   }
   PortRange
   {
     Port 11351 11399        # TLS for CDC capture engine to
                             # accelerator replication engine
   }
}
```

6. Remove the specification of the encryption algorithms.
   For example, remove:

```
TTLSCipherParms              StunnelParms
{
   V3CipherSuites4Char       C02FC030
}
```

7. Remove the group action statement or set the value to `off`:

```
TTLSGroupAction              StunnelGroup
{
       TTLSEnabled                       On
}
```

8. Remove the TLS environment settings.
   For example, remove:

```
TTLSEnvironmentAction        StunnelClientEnvironment
{
       TTLSKeyRingParms
         {
           Keyring                       DBAUSER/TLS_SHARED_RING
         }
    TTLSEnvironmentAdvancedParms
       {
              SSLv2 Off
           SSLv3 Off
           TLSv1 Off
           TLSv1.1 Off
           TLSv1.2 On
           ClientAuthType PassThru

       }
       HandshakeRole                     CLIENT
       TTLSCipherParmsRef                StunnelParms
       Trace                             7
}
```

9. Remove the outbound TLS rule.
   For example:

```
TTLSRule                     StunnelDWP1Sim148
{
```

```
        RemotePortGroupRef                StunnelAcceleratorPorts
        RemoteAddrGroupRef                StunnelAccelerators
        Direction                         Outbound
        TTLSGroupActionRef                StunnelGroup
        TTLSEnvironmentActionRef          StunnelClientEnvironment
}
```

10. To activate changes made in this way, submit the following command from TSO or the SFDF command interface:

```
F PAGENT,REFRESH
```

Results

The Policy Agent picks up the current policy configuration and data encryption for the remaining applications remains intact.

Hint: You need not refresh the SERVAUTH class to re-read the key-ring file at this point because the certificate for the accelerator is still in place. So there would be no change.

Verifying the removal of encrypted accelerator connections

Having removed the encryption settings for IBM Db2 Analytics Accelerator, verify that encrypted connections are not listed anymore.

Procedure

- Depending on the chosen verification method, make sure that:
  - When run from the z/FS command line or TSO/E shell, the **`pasearch -t`** command does not list any policy rules.
  - From TSO, the **`NETSTAT TTLS`** and **`NETSTAT ALLCONN`** commands do not display the number or the IDs of encrypted connections.
  - If you click **Encryption details** in the **Accelerator** view of a formerly participating accelerator in IBM Db2 Analytics Accelerator Studio, no information is displayed under the heading **Network Encryption**.

Deleting a certificate from a key ring

If you deleted a certificate from an accelerator, also delete its counterpart from the key ring that is stored on the client LPAR.

Procedure

1. Use TSO to log on to the client LPAR
2. Create a JCL job and add a command that will remove the certificate and the associated pair of keys from the key ring, for example:

```
RACDCERT ID(DBAUSER) REMOVE(CERTAUTH LABEL('CACERT2') RING(TLS_SHARED_RING))
```

3. Add a command to the job that will delete the certificate. For example:

```
RACDCERT ID(DBAUSER) DELETE(LABEL('CACERT2'))
```

4. Submit the JCL job.
5. If no longer needed, you can also remove the RACF profiles that you created for AT-TLS.

Obtaining the pairing code for authentication

Communication between an accelerator and a Db2 subsystem requires both components to share credentials. These credentials are generated after you submit a temporarily valid pairing code. This step is required each time you add a new accelerator. The following steps describe how to obtain the pairing code.

About this task

Note: You can renew the authentication for an existing accelerator without having to use a new pairing code. To do so, click the **Update** link in the **Accelerator** view.

The steps *Obtaining the pairing code for accelerator authentication* and (next topic) belong together, but are seldom carried out by the same person. Since the pairing code obtained from the IBM Db2 Analytics Accelerator Console is only valid for a limited time (30 minutes by default), the persons operating the console and IBM Db2 Analytics Accelerator Studio must coordinate the steps.

Procedure

1. Ask the network administrator or the person who did the TCP/IP setup for the IP address of the accelerator. Make a note of this information. You need to enter it as you complete the steps that follow.

   For IBM Db2 Analytics Accelerator on an IBM Integrated Analytics System, this is the virtual IP or wall IP address.

   For Db2 Analytics Accelerator on Z, this is the IP address of the network that you labeled DB2 in the **Appliance Installer**.
2. Log on to the IBM Db2 Analytics Accelerator Console by using **`telnet`** or **`ssh`**. The preferred method is **`ssh`**.

   For more information:

   - *Using telnet to log on to the IBM Db2 Analytics Accelerator Console* in the *IBM Db2 Analytics Accelerator for z/OS: Installation Guide*.
   - *Using ssh to log on to the IBM Db2 Analytics Accelerator Console* in the *IBM Db2 Analytics Accelerator for z/OS: Installation Guide*.
3. Press the Pause key, then Enter to display the following screen:

```
********************************************************************************
*         Welcome to the IBM Db2 Analytics Accelerator Configuration Console
********************************************************************************

You have the following options:
 (0) - (Menu) Manage Configuration Console
Users
 (1) - (Menu) Run Accelerator Functions
 (2) - (Menu) Manage Incremental Updates
 (3) - (Menu) Manage Encryption of Data in Motion
 (4) - (Menu) Manage Call Home

 --------------------------------------------------------------------
 (x) - Exit the Configuration Console
```

4. Type 1 and press Enter to display the submenu:

```
main -> accel
------------------------------------------------------
You have the following options:

(0) - Go back one level
(1) - Obtain pairing code, IP address, and port
(2) - List paired Db2 subsystems
(3) - Clear query history
(4) - Restart accelerator process
(5) - Reboot all appliance nodes
(6) - Dump extensive diagnostic information
(7) - Stop backend database
(8) - Start backend database
(9) - Transparently convert Db2 for z/OS REAL columns into DOUBLE columns when loading a table
(10) - Set the DB2 subsystem for time synchronization
(11) - Rotate key used to generate service password
(12) - Accelerator Workload Management
```

5. Type 1 and press Enter:
6. When the message `Specify for how long you want the pairing code to be valid.` is displayed, enter an appropriate integer to specify the validity period in minutes.

   The time that you choose must be sufficient for you or a coworker to go to the workstation that runs IBM Db2 Analytics Accelerator Studio, start the **Add New Accelerator** wizard, and enter the information that is returned by the console. Values from 5 to 1440 are allowed. If you just press Enter, you accept the default of 30 minutes.

```
Press <return> to accept the default of 30 minutes.
 Cancel the process by entering 0.



 Accelerator pairing information:
   Pairing code  : 6048
   IP address    : 203.0.113.8
   Port          : 1400
   Port (AT-TLS) : 11400
   Valid for     : 30 minutes

 Press <return> to continue
```

   Important: A pairing code is valid for a single try only. Furthermore, the code is bound to the IP address that is displayed on the console.
7. Make a note of the following information on the **console**:
   - `Pairing code`
   - `IP address`
   - `Port` (for unencrypted network communication). Use this port if you are not sure.
   - `Port (AT-TLS)` (for encrypted network communication).

     The use of encryption requires extra configuration steps on the accelerator and on the participating z/OS L Pars.
8. Press Enter to return to the main menu of the **console**.
9. Type x and press Enter to exit the **console** and close the telnet session.

Completing the authentication using the Add Accelerator wizard

To complete the authentication, you specify the IP address, the port number, and the pairing code in the **Add Accelerator** wizard.

Before you begin

Make sure that the following conditions apply:

- You need privileges to run Db2 administration commands and stored procedures on z/OS. If you created a power user as suggested, the power user will have the required privileges. For more information, follow the **Related information** link at the end of this topic.
- You have a valid pairing code. The pairing code, which is of temporary validity, can be obtained by using the **IBM Db2 Analytics Accelerator Console**. For more information see the **Related tasks** section at the end of this topic.

Attention: Do not give ordinary users SELECT authorization on the SYSIBM.USERNAMES table because this allows the users to see the authentication information in the SYSIBM.USERNAMES.NEWAUTHID column.

About this task

You can renew the authentication for an existing accelerator without having to use a new pairing code. To do so, click the **Update** link in the **Accelerator** view.

Attention: Making a new backup of your Db2 catalog tables is strongly recommended after each authentication update because restoration processes in your Db2 subsystem can make an accelerator unusable. This happens if you must restore your Db2 catalog and the backup of the catalog was made before the last update of the accelerator credentials. In this case, the latest authentication information will not be in the catalog tables of the backup, and so the accelerator can no longer be used.

For the completion of this task, the following stored procedures are run on your data server:

- SYSPROC.ACCEL_TEST_CONNECTION
- SYSPROC.ACCEL_ADD_ACCELERATOR

For information about the privileges that are required to run these procedures and further details, see the appropriate section in the *IBM Db2 Analytics Accelerator for z/OS: Stored Procedures Reference*. A link to this document is provided under **Related information** at the end of this section.

Procedure

1. Select the **Accelerators** folder in the **Administration Explorer**.
2. On the menu bar of the **Object List Editor**, click the downward-pointing arrow next to the green plus sign.
3. From the drop-down menu, select **Add Accelerator**.
4. In the **Name** field, type a name for the accelerator.

   This name is automatically copied to the **Location** field.

   The location name is the unique name of the accelerator in the SYSIBM.LOCATIONS table. Mostly, this is the same name as the accelerator name.

   

   Attention:

   - If you want to connect more than one Db2 subsystem to the same accelerator, you must use a different location name for each pairing. For each IP address and port combination, the

assignment to an accelerator must be logically unique. If you disregard this rule and use the same location name, you will lose the connection to the previously paired Db2 subsystem, and the data on the accelerator will be deleted. This mechanism was implemented on purpose because it ensures that a newly added accelerator is always “clean”.

- Reuse an accelerator name only if you are absolutely sure that the accelerator was stopped before it was removed.

  Background: When an accelerator is paired with Db2 for z/OS, Db2 starts a heartbeat thread to monitor vital accelerator functions. This heartbeat thread is bound to the IP address of the accelerator. It continues to run if you remove the accelerator without stopping it before. The continuing thread is canceled only when you shut down Db2.

  Your new accelerator will take over the still running heartbeat thread of the removed accelerator if all of the following conditions are true:

  a. You did not stop the accelerator before the removal.
  b. You did not shut down and restart Db2 for z/OS after the removal.
  c. You used the name of the removed accelerator for the new accelerator.

  If thereafter problems with the new accelerator occur, and you need to check the heartbeat information, you might fail to notice that this information does not pertain to the accelerator you are scrutinizing.

5. In the **Pairing code** field, type the pairing code.
6. In the **IP address** field, type the IP address of the accelerator.
7. In the **Port** field, type `1400`. This is the fixed port for network communication between the z/OS data server and the accelerator.
8. Click **Test Connection** to check whether the accelerator with the given address can be connected to.
9. Click **OK**.

   A connection test is carried out.

Tracing encrypted accelerator connections

The **Accelerator trace information** in the **Save Trace** window of IBM Db2 Analytics Accelerator Studio includes trace information related to data encryption.. This information might prove useful as you diagnose problems.

About this task

To enable tracing for data encryption:

Procedure

1. Start IBM Db2 Analytics Accelerator Studio.
2. Open the **Accelerator** view of the accelerator that you want to collect trace information about.
3. In the header of the **Accelerator** view, click **Save**.
4. In the **Save Trace** window, select **Accelerator trace information**.
5. Click **Finish**.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd. 19-21,
Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _enter the year or years_.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux® is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

GDPR considerations

For PID(s): 5697-DA7, 5697-DA5, 5697-DAB

Notice: This document is intended to help you in your preparations for GDPR readiness. It provides information about features of IBM Db2 Analytics Accelerator for z/OS that you can configure, and aspects of the product's use, that you should consider to help your organization with GDPR readiness. This information is not an exhaustive list, due to the many ways that clients can choose and configure features, and the large variety of ways that the product can be used in itself and with third-party applications and systems.

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations.

The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

GDPR

General Data Protection Regulation (GDPR) has been adopted by the European Union (“EU”) and applies from May 25, 2018.

Why is GDPR important?

GDPR establishes a stronger data protection regulatory framework for processing of personal data of individuals. GDPR brings:

- New and enhanced rights for individuals
- Widened definition of personal data
- New obligations for processors
- Potential for significant financial penalties for non-compliance
- Compulsory data breach notification

Read more about GDPR

- EU GDPR Information Portal (https://www.eugdpr.org/)
- ibm.com®/GDPR website (https://ibm.com/GDPR)

The EU General Data Protection Regulation (GDPR) regulates data privacy in the European Union (EU). For details, see: https://www.eugdpr.org

The regulations laid out in the GDPR apply if the data controller (an organization that collects data from EU residents), or the processor (an organization that processes data on behalf of a data controller, such as a cloud service provider), or the data subject (an individual) is based in the EU (source: Wikipedia. See: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation). A violation of GDPR regulations might incur severe financial penalties (fines) and reputation damages. This documentation is intended for data controllers or processors who use Db2 for z/OS together with IBM Db2 Analytics Accelerator for z/OS with the aim of storing personal data of EU residents (individuals). As regards IBM Db2 Analytics Accelerator for z/OS, the IBM company is neither the data controller, nor the data processor. Nevertheless, the IBM company feels obliged to give such entities guidance on how to follow GDPR regulations.

Your responsibilities as a data controller or processor

If you act on behalf of a data controller or data processor, see the frequently asked questions (FAQ) on the official GDPR website to find out what your responsibilities are:

https://www.eugdpr.org/gdpr-faqs.html

Furthermore, refer to chapter 4 in the GDPR regulations:

https://www.eugdpr.org/article-summaries.html

Product Configuration for GDPR

The following sections provide considerations for configuring IBM Db2 Analytics Accelerator for z/OS to help your organization with GDPR readiness.

How to configure the offering so that it can be used in a GDPR environment

The following sections describe how personal data is stored and processed by IBM Db2 Analytics Accelerator for z/OS (called 'accelerator' in the text that follows).

If personal data is to be stored on an accelerator, the following configuration steps might help you meet your compliance objectives with regard to GDPR:

- Activate the encryption of data in motion (data that is transferred over a data network between Db2 for z/OS and the accelerator).
- Activate the encryption of data at rest (encryption of disks and other storage devices).
- Do not share passwords for the operation of the IBM Db2 Analytics Accelerator Console between multiple persons. Instead, create separate user IDs with different passwords for each console user.
- Give read access to personal data (the privilege to run queries) only to authorized Db2 for z/OS users. To this end, define appropriate Db2 authorizations (SELECT, and so on) in the Db2 for z/OS catalog.
- Restrict the right to unload data from and to create image copies in Db2 for z/OS. Give this right to authorized administrators only.
- Restrict access to the 'Save Trace' function in Db2 Analytics Accelerator for z/OS because the collected trace data might contain personal data. Access should be given to authorized administrators only.
- Restrict access to the table SYSIBM.USERNAMES in the catalog of the Db2 for z/OS communication database because this table contains authentication credentials. If these credentials are read or copied by unauthorized users, these users might obtain access to sensitive personal data.

Data Life Cycle

You can create copies of any Db2 for z/OS table on an accelerator (accelerator-shadow tables). As soon as you create a copy of a Db2 for z/OS table and load it with personal data, the GDPR regulations apply in the same way as they apply to personal data in the original Db2 for z/OS tables.

An accelerator also allows you to load and store external data outside of Db2 for z/OS, such as the data of VSAM files, in accelerator-shadow tables. Products like the Db2 Analytics Accelerator Loader can be used to this end. If the external data contains personal information, the GDPR regulations apply to the data that is trasferred to the accelerator.

What types of data?

The administrative environment of an accelerator (client and configuration software) does not store personal data, except for the user IDs and authentication tokens of its administrators. However, the GDPR regulations apply to all personal data that you store in database tables on the accelerator.

Where in the process?

An accelerator is loaded with data in the course of individual load operations or by the incremental update function (automated load of table updates). Adding a table to an accelerator does not yet copy any data. It merely defines the table's structure (metadata) on the accelerator. However, if you load the table or enable it for incremental updates, the data of the source table - which might contain personal data - is copied to the accelerator.

For what purpose?

An accelerator, like Db2 for z/OS, is a general database management system for SQL queries. Such queries are run with the aim of retrieving stored information and gaining further insights (analytical queries that uncover the dependencies or connections between sets of values). An accelerator can return the results of SQL queries to authorized and authenticated users of the system. The results usually consist of subsets or aggregations of numerous data records. All these records might include personal data.

Personal data used for online contact with IBM

IBM Db2 Analytics Accelerator for z/OS clients can submit online comments/feedback/requests to contact IBM about accelerator subjects in a variety of ways, primarily:

- Public comments area on pages in the IBM Integration community on IBM developerWorks®
- Public comments area on pages of the IBM Db2 Analytics Accelerator for z/OS product documentation in the IBM Documentation
- Feedback forms in the IBM Integration community

Typically, only the client name and email address are used, to enable personal replies for the subject of the contact, and the use of personal data conforms to the *IBM Online Privacy Statement* (https://www.ibm.com/privacy/cc/).

Data Collection

IBM Db2 Analytics Accelerator for z/OS can be used to collect personal data. When assessing your use of IBM Db2 Analytics Accelerator for z/OS and the requirements of GDPR, you should consider the types of personal data which in your circumstances are stored on an accelerator.

The use of an accelerator does not impose new requirements for the collection of personal data. It does not introduce new users or new privileges, but makes use of existing users and their privileges as defined in Db2 for z/OS. The use of an accelerator does not introduce additional obligations for the safekeeping or adminstration of data if you already observe the GDPR regulations for the storage of data in Db2 for z/OS.

Make sure that the process of collecting data and storing it in Db2 for z/OS is GDPR-compliant. The use of an accelerator will then be equally compliant.

Data Storage

The use of IBM Db2 Analytics Accelerator for z/OS involves the storage of data in a persistent manner.

An accelerator is a general-purpose data processing and retrieval engine. It is not aware of the meaning of data or any meaning that can be inferred from it. It is thus the responsibility of the data controller or processor to classify the data as personal data - for example account data - and make sure that the collection, access and processing of this data is in accordance with the GDPR regulations.

Storage in backups:
An accelerator has no backup function. However, image copies are created in Db2 for z/OS when the accelerator's archiving function is used (high performance storage saver). If these image copies contain personal data, the GDPR rules apply. This means, for example, that if individuals request their data to be deleted, it must also be deleted from all the image copies that may exist.

Storage in archives:
The high performance storage saver deletes table data from Db2 for z/OS and stores it exclusively on an accelerator. If this data contains personal information, the GDPR regulations might require that you delete the personal information from a number of records. The current version of the accelerator software does not allow DELETE operations on archived partitions. So in case you must delete records, first restore the archived partition to Db2 for z/OS, then delete then delete the personal data from Db2 for z/OS. Finally, archive the partition again (which now does not include the personal data anymore).

Data Access

Access to data on an accelerator requires a Db2 for z/OS user ID and a password. The accelerator recognizes the privileges defined in Db2 for z/OS and does not allow a user to run functions that she or he is not entitled to use.

As long as the Db2 for z/OS authorizations, such as SELECT, INSERT, UPDATE, or DELETE privileges, are defined in accordance with the GDPR regulations, access to data on the accelerator will likewise be in accordance with these regulations.

So it is crucial that the definition of roles and access rights in Db2 for z/OS effectuates an adequate separation of duties and responsibilities.

One accelerator-specific function might provide access to personal data on the accelerator: This is the "Save Trace" function, which collects diagnostic information for troubleshooting. The resulting trace files might contain personal data because they sometimes include the code of SQL queries to which personal information has been passed in the form of query literals. Trace files can also include memory dumps that contain personal data.

It is therefore important that access privileges to data, such as SELECT privileges or superuser privileges like SYSADM and DBADM, are granted with great care. The permission to use the "Save Trace" function should be given to selected administrators only.

The privilege to create image copies in Db2 for z/OS must also be handled with care. It is required, for example, if a user wants to archive table partitions on an accelerator.

Data Processing

Privileges defined in the Db2 for z/OS catalog control data processing on an accelerator.

In addition to that, the encryption features (encryption of data in motion and encryption of data at rest) should be activated. This prevents an unauthorized person without proper privileges from gaining direct access to personal data by interferring with the network communication or by obtaining physical access to the storage devices (hard disks or solid state disks).

Encryption features and safeguarding precautions:

Encryption of data in motion:
This feature encrypts the network traffic between an IBM Z® system and an accelerator.

Encryption of data at rest:
This feature encrypts the data on an accelerator's physical storage devices (hard disks and solid state disks). Depending on the model of the hardware, the feature might already be turned on by default.

Encryption key ownership:
Restrict access to the encryption keys because the keys enable a person to read or decrypt personal data on a network or storage device. Put the safekeeping and maintenance (rotation) of the encryption keys in the hands of a trusted administrator.

Data Deletion

When data is deleted from Db2 for z/OS, it might still exist in table copies on the accelerator. To delete the data on an accelerator, you have the following options:

The data in accelerator-shadow tables is deleted:

- If the data in the original Db2 for z/OS tables has been deleted, and if the affected accelerator-shadow tables have been reloaded (with the contents of the now empty Db2 tables).
- If the accelerator-shadow tables are removed from the accelerator.
- If the incremental update function is used and the function replicates empty table content to the accelerator because the original Db2 for z/OS table data has been deleted.

The data in an accelerator-only table (AOT) is deleted:

- If the AOT is removed from the accelerator.
- If an explicit DELETE statement is submitted on the Db2 for z/OS side, which references the AOT and contains a predicate that specifies the row to be deleted.

The data in partitions archived by the High Performance Storage Saver is deleted:

- If the table partitions are removed from the accelerator.
- If an archived partition is restored to Db2 for z/OS.
- If the data is deleted from Db2 for z/OS because this means that the archived partition is reloaded or that the partition is archived again after the deletion from Db2 for z/OS (empty table content will be reloaded or archived).

Data Monitoring

Db2 for z/OS provides powerful auditing and monitoring functions that allow you to track the processing of personal data. Because IBM Db2 Analytics Accelerator for z/OS is a logical component of Db2 for z/OS, and keeps only copies of Db2 for z/OS data, the monitoring functions for data processing in Db2 for z/OS are sufficient.

Responding to Data Subject Rights

To identify an individual's data that is stored on an accelerator, you can submit SQL queries from Db2 for z/OS. These queries ought to search for the name, the account number, or for other identifying information about the subject using SQL syntax. Since an accelerator works on copies of Db2 for z/OS data, the same queries can be run to retrieve the data either from Db2 for z/OS or from the accelerator. Specific advice or examples of such queries can not be provided here because the structure and the content of the database tables, as defined by the data controller or data processor, is not known.

Does the offering facilitate being able to meet data subject rights?

Right to Access

Can the client provide individuals access to their data?
Db2 for z/OS and accelerators can process SQL queries in which an individual's ID can be specified as a search criterion. This way, all data stored about that individual can be retrieved. In Db2 for z/OS,

a client's data access can be restricted, so that the client can only search and retrieve a subset of the available data records, that is, those records that belong to a specific group of individuals. To this end, a feature called label based access control (LBAC) can be employed. IBM Db2 Analytics Accelerator provides a similar functionality, which restricts access to a selected set of rows based on the CURRENT SQLID special register.

Can the client provide individuals information about what data the client has about the individual?
Yes. To identify an individual's data stored on an accelerator, the client can submit SQL queries from Db2 for z/OS. These queries ought to search for the name, the account number, or for other identifying information about the subject using SQL syntax.

Right to Modify

Can the client allow an individual to modify or correct their data?
Db2 for z/OS allows a client to update the data that is stored about an individual. Depending on the architecture of the application, it might even be possible to authorize the individuals, so that these can update their data by themselves. After an update in Db2 for z/OS, the modified data is copied to the accelerators attached to the database during the next reload operation, which can be started manually or automatically (by the incremental update function). During that process, incorrect data will be overwritten.

Can the client correct an individual's data for them?
Yes (see the previous question *Can the client allow an individual to modify or correct their data?*).

Right to Restrict Processing

Can the client stop processing an individual's data?
Yes. In Db2 for z/OS, a client can submit DELETE statements to remove data records of individuals. The removal will be reflected in the data that is stored on an attached accelerator when the next reload operation (manual or automatic) is taking place. During that process, records previously deleted from Db2 for z/OS will also be deleted from the accelerator. Furthermore, an individual's data can be excluded from SQL queries through the use of filters in query predicates. For example, a query that reads `SELECT CUSTOMER_DATA FROM CUSTOMER_TABLE where custid NOT IN (a,b,...c)` returns only data records that are not related to (do not belong to) the users in the specified group `(a,b,...c)`.

Right to Object

Same as “Right to Restrict Processing” on page 38.

Right to Be Forgotten

Can the client delete an individual's data?
Yes.

Right to Data Portability

Can the customer provide an individual with the information that they have about the individual in a user-friendly/machine readable format?
Yes.

Glossary

Read a brief description of the terms and acronyms that are used in this document.

Policy Agent
A z/OS component that can take on various roles in connection with IP networking. The Policy Agent reads and parses policy definitions (=sets of rules) and makes these policies available to TCP/IP stacks or policy clients. The Policy Agent can be configured to start, stop, monitor, or restart dependent components, such as the Internet Key Exchange (IKE) daemon, the NSS daemon, the SYSLOG daemon, or the Traffic Regulation Management (TRM) daemon.

SYSLOG daemon
The SYSLOG daemon handles the logging of all other events that are not handled by the TRM daemon. It also controls where the log messages are written. The SYSLOG provides valuable information for troubleshooting.

TCP/IP stack
On z/OS, an addressable (named) unit or component that is responsible for the processing of network packages according to the TCP/IP set of protocols. The term is often used in a different sense in other publications, in which it means the TCP/IP set of protocols.

You can look up terms and acronyms that are not listed here in the IBM Documentation

Index

T

U

V

X

Product Number: 5697-DA7

SH12-7100-02