TIBCO ActiveSpaces®

Security Guidelines

Version 4.9.0 | August 2023

Contents

About This Product

The TIBCO ActiveSpaces® software is a distributed in-memory data grid product. Some features of ActiveSpaces® include the use of familiar database concepts, high I/O capacity, and network scalability.

Product Editions

ActiveSpaces is available in two editions: Community Edition and Enterprise Edition.

	Community Edition	Enterprise Edition
Ideal for	Getting started with ActiveSpaces for implementing application projects, including proof of concept projects, for testing, and for deploying applications in a production environment. Production deployments running up to 5 nodes (a total of the copyset nodes or proxies in your data grid) For more information, see Terms used in Community and Enterprise Editions.	All application development projects, and for deploying and managing applications in the production environment of an enterprise. Production deployments with more than 5 nodes (a total of the copyset nodes or proxies in your data grid) For more information, see Terms used in Community and Enterprise Editions.
Features	All features of the Enterprise Edition except enterprise monitoring using dashboards.	Includes all the features presented in this documentation set.
Limitations	Run up to 5 nodes (a total of the copyset nodes or proxies in your data grid). Although the community license limits the number of production instances, you can easily upgrade to the enterprise edition as	No limitations on a total of the copyset nodes or proxies in your data grid.

	your use of ActiveSpaces expands.	
Cost	Free	Paid
Compatibility	Compatible with both the enterprise and community editions of TIBCO FTL®	Depends on the enterprise edition of TIBCO FTL for monitoring and management of data grid components and secure communication.
TIBCO Support	No access to TIBCO Support	Access to TIBCO Support

Terms used in Community and Enterprise Editions

- Node - a copyset node or proxy where each copyset node or proxy is an operating system process with a unique process ID.
- Process ID - For the purposes of the definition of Node, Process ID means a standard computer industry term that uniquely identifies each operating system process.
- Copyset - For the purposes of the definition of Node, “Copyset” means a logical grouping of nodes such that a portion of the data is shared uniformly by all the nodes that form a copyset.

Product Overview and Security Features

This document describes guidelines to ensure security within the components of ActiveSpaces and the communication between them. It also provides additional security-related guidance and recommendations for other aspects of internal and external communication. In particular, this document provides details of product connectivity and configuration of security options.

ActiveSpaces software includes the following security features that are layered above the TIBCO® FTL security features:

- Every data grid can be configured to encrypt connections
- Every process has authentication and trust file options

ActiveSpaces software leverages TIBCO FTL for the following security features:

- Secure transports for communication among data grid processes and the communication between applications and the data grid processes
- TLS to secure TCP transports
- HTTPS to secure connections to the TIBCO FTL server
- Authentication and authorization service

For more information about TIBCO FTL security features, see *TIBCO FTL® Security*.

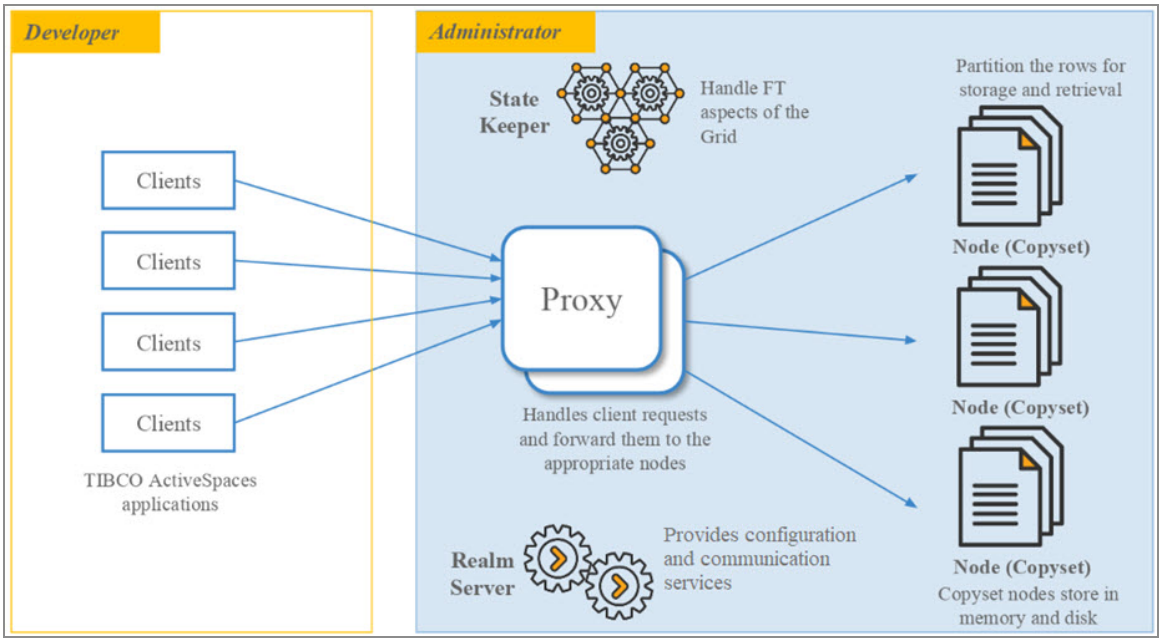
Product Connectivity

ActiveSpaces product connectivity can be broken down into the following categories:

- ActiveSpaces client application to data grid process connectivity
- ActiveSpaces data grid process to data grid process connectivity

Both client applications and data grid processes communicate with the realm service in the TIBCO FTL server. After the initial realm communication, client applications communicate with proxy processes. The proxy processes forward requests internally to the data grid and then forward replies back to the external client application. Internal grid communication happens between proxy, state keeper, and node processes at different points in time.

As an administrator, with the help of the security guidelines, you can secure both internal grid communication and external client-to-proxy communication. You can also help application developers configure a client application and connect to a secure data grid. The following high-level diagram shows the connectivity information.



Setting up a Secure TIBCO FTL Server

For a production deployment, perform the following steps:

Procedure

1. Set up the secure TIBCO FTL server. For details about securing TIBCO FTL servers, see "Securing FTL Servers" in *TIBCO FTL® Security*.
2. Set up the YAML configuration file, and configure the FTL servers to use TLS security in their configuration files.

```
globals:
        tls.secure: <keystore_password>
```

3. Run `tibftlserver --init-security` with a `keystore_password` file to generate the `.p12` keystore file and `ftl-trust.pem` file.
4. Distribute the `ftl-trust.pem` file for use in all other applications.
5. Start the TIBCO FTL server.

What to do next

To start a secure data grid, follow the steps in Setting up a Secure Data Grid.

Example Scripts

Sample scripts to secure a data grid are available at `TIBCO_HOME/as/<version>/samples/scripts`. You can also start a secure TIBCO FTL Server and a secure data grid by using `as-start` with the `-s` command-line option.

Note: The installation environment of ActiveSpaces is referenced as *TIBCO_HOME*. For example, on Microsoft Windows, *TIBCO_HOME* might be `C:\tibco`.

Setting up a Secure Data Grid

Before you begin

Ensure that a secure TIBCO FTL server is running.

Procedure

1. To configure a secure data grid in one command, create a .tibdg configuration file which can then be passed to the tibdg administration tool.
2. In the .tibdg file, when defining the data grid, set encrypted_connections=all as shown in the following code snippet:

   ```
   grid create copyset_size=2 encrypted_connections=all grid1
   ```

   This property forces all internal grid communication and all client-to-proxy communication to use TIBCO FTL secure TCP transports.
3. Configure the firewall to open ports for client-to-proxy communication.

   For each proxy that is listening for client connections, configure the proxy_client_listen_port to the preferred port that the proxy must bind to and listen on. Example:

   ```
   proxy create proxy_client_listen_port=7771 p_01
   ```

   You can use other optional configuration options in the proxy that help configure the specific host interface. For example, you can use the proxy_client_listen_subnet_mask configuration option to configure network interfaces. You can specify this option at both the data grid and proxy level to control which network interface the proxy binds to when listening for connections from clients. For details, see "Configure Network Interfaces" in *TIBCO ActiveSpaces® Administration* .
4. Run the tibdg tool by providing the following command-line options:
   - A completed .tibdg configuration file
   - A trust file

   The following command is an example of running the tibdg tool:

```
>tibdg -r https://host1:8085 -s /home/youruser/as/init/grid1/grid1.tibdg --trust-file
/home/youruser/as/grid1/ftl-trust.pem
```

Warning: If you do not provide the trust file as a command-line option, the command fails when communicating with a secure TIBCO FTL server.

What to do next

After the data grid has been successfully configured in the TIBCO FTL server, you can start the tibdgkeeper, tibdgproxy, and tibdgnode processes. Ensure that you provide the appropriate trust file on the command-line as follows with the --trust-file option.

```
tibdgkeeper -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem -g grid1 -n k_1
```

Securing Client-to-Proxy Communication

After creating and starting a secure data grid, set the properties of the ActiveSpaces client application that are required to connect to a secure data grid and start secure communications. The properties must be passed to the DataGrid.connect() API function. The HTTPS protocol must be used in the URL parameter to connect to a secure realm service. For more information about how these properties work, see the Operations code sample at *TIBCO_HOME*\as\<*version*>\samples\src\java\Operations. The following procedure also elaborates on these properties.

Note: The installation environment of ActiveSpaces is referenced as *TIBCO_HOME*. For example, on Microsoft Windows, *TIBCO_HOME* might be C:\tibco.

Before you begin

Ensure that you have the following information from your administrator before you begin the procedure:

- The TIBCO FTL server trust file that was generated when setting up the secure TIBCO FTL server.
- The correct username and password for the ActiveSpaces client application (if the administrator set up authentication in the TIBCO FTL server).

Procedure

1. In the URL parameter passed to DataGrid.connect() function call, use https:// for each realm URL in the list.

   When specifying a list of three TIBCO FTL servers, the URL string parameter must be as listed in this example: https://ftlsvr1:8085|https://ftlsvr2:8185|https://ftlsvr3:8285.

2. To connect to a secure data grid, set a specific trust type in the properties passed to the DataGrid.connect() function call.

   a. Place the PEM trust file in the file system so that it can be accessed securely by the ActiveSpaces client application.

   b. In the ActiveSpaces client application, set the connection TRUST_TYPE property

to the enum representing USE_SPECIFIED_TRUST_FILE.

c. In the ActiveSpaces client application, set the TRUST_FILE property to the file system path of the trust file received by the administrator.

The following Java code snippet is an example:

```
Properties props = new Properties();
props.setProperty(Connection.TIBDG_CONNECTION_PROPERTY_STRING_TRUST_
TYPE, Connection.TIBDG_CONNECTION_HTTPS_CONNECTION_USE_SPECIFIED_
TRUST_FILE);
props.setProperty(Connection.TIBDG_CONNECTION_PROPERTY_STRING_TRUST_
FILE, trustFilePath);
DataGrid.connect(url, gridName, props);
```

3. If the administrator has set up authentication in the TIBCO FTL server and provided a username and password, then in the properties object passed to DataGrid.connect() function call, include the USERNAME and USERPASSWORD properties as shown in the following examples:

```
props.setProperty(Connection.TIBDG_CONNECTION_PROPERTY_STRING_
USERNAME, username);
props.setProperty(Connection.TIBDG_CONNECTION_PROPERTY_STRING_
USERPASSWORD, password);
DataGrid.connect(url, gridName, props);
```

Transport Encryption on a Data Grid

Transport encryption can be used without authentication and authorization. You can encrypt any network communication between the processes of your data grid to protect that communication from packet sniffing. For more information about encrypting a data grid, see "Enabling Transport Encryption on a Data Grid" in *TIBCO ActiveSpaces® Administration*.

While you can use authentication and authorization without transport encryption, TIBCO recommends that you use transport encryption to securely use authentication and authorization.

Authentication and Authorization

Authentication and authorization uses usernames and passwords to authenticate the users of the data grid and prevent unwanted users from accessing the data grid.

When authentication and authorization is enabled, each ActiveSpaces process authenticates itself to a secure realm service by using the credentials in the password file. For more information, see "Authentication and Authorization" in *TIBCO ActiveSpaces® Administration*.

While you can use authentication and authorization without transport encryption, TIBCO recommends that you use transport encryption to securely use authentication and authorization.

Permissions

In ActiveSpaces, you can set permissions on tables to control who has access to the data in the tables. On a specific table, you can grant read or write permissions to users and roles.

For more information about how to enable permission checking in the data grid including how to grant and revoke table level permissions, see "Enabling Permission Checking when Creating or Modifying a Data Grid" in *TIBCO ActiveSpaces® Administration*.

Commands to Start a Secure Data Grid

Goal: Create a secure data grid named grid1 running across four computers and access it from a client application running on a separate computer.

Hosts: host1, host2, host3, host4, host5 (for client application)

Procedure

1. Perform the steps listed in Initial Setup to Start a Secure Data Grid.
2. Perform the steps listed in Create Directories Needed to Run the Processes.
3. Perform the steps listed in Setting Up and Starting TIBCO FTL Servers.
4. In a browser, browse to https://host1:8085 or https://host2:8185 or https://host3:8285.

   An empty realm server with a working GUI is displayed.
5. Initialize the data grid from host1.

```
>tibdg -r https://host1:8085 -s /home/youruser/as/init/grid1/grid1.tibdg --trust-file
/home/youruser/as/grid1/ftl-trust.pem
```

> **Warning:** If you do not provide the trust file as a command-line option, the command fails when communicating with a secure TIBCO FTL server.

6. Check the status after configuring the data grid (no processes are running as expected).

```
>tibdg -r https://host1:8085 --trust-file /home/youruser/as/grid1/ftl-trust.pem -g grid1 status
Grid grid1:
Grid is not functioning.
FTL healthy.  Up for 824 seconds.
Admin server is not running


PROCESSES
```

```
   TYPE  NAME     HOST  PID  REV  TXNS  REQS  COPYSET  ROLE  EST SIZE  FS USED
FS CAP  DATA DIR  MAX WRITE
   node  cs_01.n_1  NOT RUNNING
   node  cs_01.n_2  NOT RUNNING
   node  cs_02.n_1  NOT RUNNING
   node  cs_02.n_2  NOT RUNNING


   TYPE    NAME HOST  PID  REV  ROLE  STATE DIR
   keeper  k_1  NOT RUNNING
   keeper  k_2  NOT RUNNING
   keeper  k_3  NOT RUNNING


   TYPE  NAME  HOST  PID  REV  CLIENTS  REQ  TXN  ITER  STMT  QRY  LSNR  MODE
   proxy  p_01  NOT RUNNING
   proxy  p_02  NOT RUNNING
   proxy  p_03  NOT RUNNING
   proxy  p_04  NOT RUNNING
```

7. Perform the steps listed in Starting ActiveSpaces Processes.
8. Start a tibdgadmind process to accept administration commands.

```
# On host1
>tibdgadmind -r "https://host1:8085" --trust-file /home/youruser/as/grid1/ftl-trust.pem -l
localhost:7171
```

9. Start a sample client to run operations.

```
>/opt/tibco/as/4.2/samples/bin/operations -r
"https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem -g grid1

AS Product Version: 4.2.0  V5

Connected to table: t1

Operations commands:
      Enter 'p'  to put a row into the table
      Enter 'g'  to get a row from the table
      Enter 'd'  to delete a row from the table
      Enter 'pm' to put multiple rows into the table
```

```
        Enter 'gm' to get multiple rows from the table
        Enter 'dm' to delete multiple rows from the table
        Enter 'i'  to iterate the rows in a table
        Enter 'l'  to listen to changes to the table
        Enter 's'  to create an SQL SELECT or DML statement and execute it
        Enter 'u'  to execute an SQL DDL update
        Enter 'md' to display metadata about the grid and tables
        Enter 'h'  to display this help menu
        Enter 'q'  to quit

Main: [p/g/d/pm/gm/dm/i/l/s/u/md/h/q]: p
Put: Enter the key (long): 1
Put: Enter the value (string): 1
Put Success

Main: [p/g/d/pm/gm/dm/i/l/s/u/md/h/q]: g
Get: Enter the key (long): 1
result: {long:key=1, string:value="1"}
```

Initial Setup to Start a Secure Data Grid

Procedure

1. Set up PATH to point to TIBCO FTL and ActiveSpaces.

```
export TIBFTL_ROOT=/opt/tibco/ftl/<version>
export TIBDG_ROOT=/opt/tibco/as/<version>
export PATH=$TIBFTL_ROOT/bin:$TIBDG_ROOT/bin:$PATH
```

2. On a computer with TIBCO FTL and ActiveSpaces, create the directories to hold the initial setup and configuration files.

```
>cd /home/youruser
>mkdir -p as
>cd as
>mkdir -p init
>cd init
>mkdir grid1
>cd grid1
>mkdir ftl_security
```

3. Initialize the files for a secure ftlserver.

```
>cd ftl_security
>vi keystore_password.txt (enter a single-line password and save file)
>tibftlserver --init-security file:/home/youruser/as/init/grid1/ftl_security/keystore_password.txt
Initializing TIBCO FTL server security.
Generating keystore 'ftl-tport.p12' and trust file 'ftl-trust.pem'.
```

4. Create the TIBCO FTL server YAML configuration file.

```
cd..
vi ftl.yaml (paste the config below)
globals:
  core.servers:
    ftl1: host1:8085
    ftl2: host2:8185
    ftl3: host3:8285
  tls.secure: file:/home/youruser/as/ftlservers/keystore_password.txt
servers:
  ftl1:
  - realm:
      ftl: host1:8088
      data: /home/youruser/as/ftlservers/ftl1/realm_data
      logfile: /home/youruser/as/logs/ftlservers/ftl1-rs-log.txt
  ftl2:
  - realm:
      ftl: host2:8188
      data: /home/youruser/as/ftlservers/ftl2/realm_data
      logfile: /home/youruser/as/logs/ftlservers/ftl2-rs-log.txt
  ftl3:
  - realm:
      ftl: host3:8288
      data: /home/youruser/as/ftlservers/ftl3/realm_data
      logfile: /home/youruser/as/logs/ftlservers/ftl3-rs-log.txt
services:
  realm: {}
```

5. Create the grid1.tibdg file. This configuration file is used to configure the data grid later after the TIBCO FTL server is running.

```
vi grid1.tibdg (paste the config below)
grid create copyset_size=2 encrypted_connections=all grid1
copyset create cs_01
```

```
copyset create cs_02
node create --copyset cs_01 --dir /home/youruser/as/grid1/cs_01.n_1_data cs_01.n_1
node create --copyset cs_01 --dir /home/youruser/as/grid1/cs_01.n_2_data cs_01.n_2
node create --copyset cs_02 --dir /home/youruser/as/grid1/cs_02.n_1_data cs_02.n_1
node create --copyset cs_02 --dir /home/youruser/as/grid1/cs_02.n_2_data cs_02.n_2
keeper create --dir /home/youruser/as/grid1/k_1_data k_1
keeper create --dir /home/youruser/as/grid1/k_2_data k_2
keeper create --dir /home/youruser/as/grid1/k_3_data k_3
proxy create proxy_client_listen_port=7771 p_01
proxy create proxy_client_listen_port=7772 p_02
proxy create proxy_client_listen_port=7773 p_03
proxy create proxy_client_listen_port=7774 p_04
table create t1 key long
column create t1 value string
```

Create Directories Needed to Run the Processes

Procedure

1. Create the directories needed to run the processes on host1:

```
>cd /home/youruser/as
>mkdir -p logs/ftlservers
>mkdir -p logs/grid1
>mkdir -p ftlservers/ftl1/realm_data
>mkdir -p grid1
>mkdir -p grid1/k1_data
>mkdir -p grid1/cs_01.n_1_data
```

2. Create the directories needed to run the processes on host2:

```
>cd /home/youruser/as
>mkdir -p logs/ftlservers
>mkdir -p logs/grid1
>mkdir -p ftlservers/ftl2/realm_data
>mkdir -p grid1
>mkdir -p grid1/k2_data
>mkdir -p grid1/cs_01.n_2_data
```

3. Create the directories needed to run the processes on host3:

```
>cd /home/youruser/as
>mkdir -p logs/ftlservers
>mkdir -p logs/grid1
>mkdir -p ftlservers/ftl3/realm_data
>mkdir -p grid1
>mkdir -p grid1/k3_data
>mkdir -p grid1/cs_02.n_1_data
```

4. Create the directories needed to run the processes on host4:

```
>cd /home/youruser/as
>mkdir -p logs/ftlserver
>mkdir -p logs/grid1
>mkdir -p grid1
>mkdir -p grid1/cs_02.n_2_data
```

Setting Up and Starting TIBCO FTL Servers

This procedure lists how to set up the TIBCO FTL environment and then start the TIBCO FTL server.

Procedure

1. Copy the TIBCO FTL files that are needed to start the TIBCO FTL servers.

```
# FTL yaml file to start the ftlserver
>scp /home/youruser/as/init/grid1/ftl.yaml
youruser@host1:/home/youruser/as/ftlservers/ftl.yaml
>scp /home/youruser/as/init/grid1/ftl.yaml
youruser@host2:/home/youruser/as/ftlservers/ftl.yaml
>scp /home/youruser/as/init/grid1/ftl.yaml
youruser@host3:/home/youruser/as/ftlservers/ftl.yaml
```

2. Copy the TIBCO FTL keystore password to start ftlserver securely

```
>scp /home/youruser/as/init/grid1/ftl_security/keystore_password.txt
youruser@host1:/home/youruser/as/ftlservers/keystore_password.txt
>scp /home/youruser/as/init/grid1/ftl_security/keystore_password.txt
youruser@host2:/home/youruser/as/ftlservers/keystore_password.txt
```

```
>scp /home/youruser/as/init/grid1/ftl_security/keystore_password.txt
youruser@host3:/home/youruser/as/ftlservers/keystore_password.txt
```

3. Copy the TIBCO FTL keystore file to start ftlserver securely. For more information on keystore files, see "Secure FTL Servers" in *TIBCO FTL® Administration*.

```
>scp /home/youruser/as/init/grid1/ftl_security/ftl-tport.p12
youruser@host1:/home/youruser/as/ftlservers/ftl1/realm_data/ftl-tport.p12
>scp /home/youruser/as/init/grid1/ftl_security/ftl-tport.p12
youruser@host2:/home/youruser/as/ftlservers/ftl2/realm_data/ftl-tport.p12
>scp /home/youruser/as/init/grid1/ftl_security/ftl-tport.p12
youruser@host3:/home/youruser/as/ftlservers/ftl3/realm_data/ftl-tport.p12
```

4. Copy the TIBCO FTL public trust file needed by TIBCO FTL servers (in realm_data directory)

```
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host1:/home/youruser/as/ftlservers/ftl1/realm_data/ftl-trust.pem
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host2:/home/youruser/as/ftlservers/ftl2/realm_data/ftl-trust.pem
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host3:/home/youruser/as/ftlservers/ftl3/realm_data/ftl-trust.pem
```

5. Copy the TIBCO FTL public trust file needed by ActiveSpaces processes in grid1:

```
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host1:/home/youruser/as/grid1/ftl-trust.pem
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host2:/home/youruser/as/grid1/ftl-trust.pem
>scp /home/youruser/as/init/grid1/ftl_security/ftl-trust.pem
youruser@host3:/home/youruser/as/grid1/ftl-trust.pem
```

6. Start the TIBCO FTL servers

```
# On host1
>cd /home/youruser/as
>tibftlserver -c ftlservers/ftl.yaml -n ftl1
# On host2
>cd /home/youruser/as
>tibftlserver -c ftlservers/ftl.yaml -n ftl2
```

```
# On host3
>cd /home/youruser/as
>tibftlserver -c ftlservers/ftl.yaml -n ftl3
```

Starting ActiveSpaces Processes

Before you begin

Complete the steps 1 to 6 from the procedure listed in Commands to Start a Secure Data Grid.

Procedure

1. Start the data grid state keeper processes.

```
# On host1
>cd as
>tibdgkeeper -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem --logfile /home/youruser/as/logs/grid1/k_1-log.txt -g
grid1 -n k_1

# On host2
>tibdgkeeper -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem --logfile /home/youruser/as/logs/grid1/k_2-log.txt -g
grid1 -n k_2

# On host3
>tibdgkeeper -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem --logfile /home/youruser/as/logs/grid1/k_3-log.txt -g
grid1 -n k_3
```

2. Start the data grid proxy processes.

```
# On host1
>tibdgproxy -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem --logfile /home/youruser/as/logs/grid1/p_01-log.txt -g
grid1 -n p_01

# On host2
```

```
>tibdgproxy -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem --logfile /home/youruser/as/logs/grid1/p_02-log.txt -g
grid1 -n p_02

# On host3
>tibdgproxy -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem --logfile /home/youruser/as/logs/grid1/p_03-log.txt -g
grid1 -n p_03

# On host4
>tibdgproxy -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem --logfile /home/youruser/as/logs/grid1/p_04-log.txt -g
grid1 -n p_04
```

3. Start the data grid node processes.

```
# On host1
>tibdgnode -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem --logfile /home/youruser/as/logs/grid1/cs_01.n_1-
log.txt -g grid1 -n cs_01.n_1

# On host2
>tibdgnode -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem --logfile /home/youruser/as/logs/grid1/cs_01.n_2-
log.txt -g grid1 -n cs_01.n_2

# On host3
>tibdgnode -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem --logfile /home/youruser/as/logs/grid1/cs_02.n_1-
log.txt -g grid1 -n cs_02.n_1

# On host4
>tibdgnode -r "https://host1:8085|https://host2:8185|https://host3:8285" --trust-file
/home/youruser/as/grid1/ftl-trust.pem --logfile /home/youruser/as/logs/grid1/cs_02.n_2-
log.txt -g grid1 -n cs_02.n_2
```

TIBCO Documentation and Support Services

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product.

Product-Specific Documentation

The following documentation for TIBCO ActiveSpaces® is available on the TIBCO ActiveSpaces® Product Documentation page:

- TIBCO ActiveSpaces® *Release Notes*
- TIBCO ActiveSpaces® *Installation*
- TIBCO ActiveSpaces® *Concepts*
- TIBCO ActiveSpaces® *Administration*
- TIBCO ActiveSpaces® *API Reference*
- TIBCO ActiveSpaces® *Security Guidelines*
- TIBCO ActiveSpaces® *ActiveSpaces4-Sizing-Guide*

How to Contact TIBCO Support

Get an overview of TIBCO Support. You can contact TIBCO Support in the following ways:

- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support website.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to TIBCO Support website. If you do not have a user name, you can request one by clicking **Register** on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the TIBCO Ideas Portal. For a free registration, go to TIBCO Community.

Legal and Third-Party Notices

Cloud SG software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the “readme” file for the availability of a specific version of Cloud SG software on a specific operating system platform.

This and other products of Cloud SG may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.tibco.com/patents.