Configuring the Administration Service under UNIX

The Administration Service controls the processes of the local brokers. The brokers are started or stopped. The local brokers connect with the Administration Service and provide it with their status and other information at an interval of 60 seconds. The Administration Service always has information on the current status of all local brokers.

The Administration Service also collates the status and other information of any known remote brokers and provides an interface with which these can be accessed.

This chapter covers the following topics:

- Requirements
- Introduction
- Saving the Data of Administration Service in a Flat File (Default)
- Saving the Data of Administration Service in LDAP
- Changing the Configuration of a Running Administration Service

See also *Starting or Restarting the Administration Service*.

Requirements

The Administration Service is provided in a fully functional state and is started by the installation. It needs access to the local port 57707, and to port 57708 for remote connections. The connections to port 57708 are SSL only. If this port is to be used, the client requires the respective SSL certificate. If no remote access to the Administration Service is required, you can deactivate this port. To deactivate the port, change the transport from "TCP-SSL" to "TCP". See `TRANSPORT`. The attribute file is in the working directory of the Administration Service, config/etb/ETBSRV.

Introduction

It is not normally necessary to change the configuration of the Administration Service. The log file, configuration file and SSL certificates are delivered in the EntireX directory *config/etb/ETBSRV*. If an error occurs, the log file of the Administration Service can provide information on the cause of the error. On UNIX, the log file is called *etbfile*.

The Administration Service requires SSL certificates to create brokers with SSL ports. During installation, the Administration Service copies the SSL certificates from the EntireX "etc" directory to the EntireX *config/etb* directory if this directory does not already contain any certificates. These certificates are for test purposes only and constitute a security risk. If you want to use SSL, replace the certificates in the *config/etb* directory with your own SSL certificates.

When a broker is created, the Administration Service copies the required certificates from the EntireX "config/etb" directory to the working directory of the newly created broker.

If the certificates are to be replaced after the installation, you also need to replace the certificates in the working directories *ETBSRV* (Administration Service) and *ETB001* (Default Broker) in the EntireX directory *config/etb*.

The Administration Service stores data in a directory service. The name of the corresponding data file is stored in file *xds.ini* in the EntireX directory *config*. You can also store the data of the Administration Service in LDAP. For this you need to adapt the entries in file *xds.ini* accordingly. The section for Administration Service is headed "[CIS Management]".

Saving the Data of Administration Service in a Flat File (Default)

This is the default definition in file *xds.ini*:

```
[CIS Management]
dirservice=FLATDIR
file=C:\SoftwareAG\EntireX\etc\flat
```

Saving the Data of Administration Service in LDAP

Modify default definition in file *xds.ini* to match your enviroment.

```
[CIS Management]
dirService=LDAPDIR
baseDN=<DN>
host=<host>
port=<port>
protocol=<protocol>
authDN=<user>
authPass=<ldap_password>
```

where	*<DN>*	is the base distinguished name of the directory object that is the root of all objects for authorization rules; <*DN*> must not be empty
	<host>	is the host of the LDAP server.
	<port>	is the port of the LDAP server. Default is 389 for TCP communication; default port for SSL is 636
	<protocol>	is is either "`ldap`" (default) for TCP communication, or "`ldaps`" for SSL

For authenticated access to the LDAP server, use the keywords `authDN` and `authPass`,

where	*<user>*	is the DN of the user
	<ldap_password>	is the password of this user

Warning:
The password is not encrypted in *xds.ini*

For unauthenticated access to the LDAP server, do not include these keywords `authDN` and `authPass` in the *xds.ini*.

Example

```
dirService=LDAPDIR
host=myHost.myDomain
baseDN=dc=myCompany,dc=de
port=389
protocol=ldap
authDN=cn=admin,dc=myCompany,dc=de
authPass=myLdapPassword
```

Changing the Configuration of a Running Administration Service

If the configuration of a running Administration Service is changed from flat file to LDAP, the Administration Service recognizes this and stores its data in LDAP without any further intervention.

The status of the configuration file *xds.ini* is checked every 60 seconds. This means it can take up to 60 seconds for the changes to the configuration file are activated.