Composed February 22, 2011

◆ ◆ ◆ CHAPTER 4

Administering Security in Cluster Mode

This chapter describes important information about administering security in a cluster.

The following topics are described:

This chapter assumes that you are familiar with security features such as authentication, authorization, and certificates. If you are not, see Chapter 1, "Administering System Security."

Instructions for accomplishing the tasks specific to GlassFish Server by using the Administration Console are contained in the Administration Console online help.

Configuring Certificates in Cluster Mode

The sections "Certificates and SSL" on page 24 and "Administering JSSE Certificates" on page 42 describe the relevant concepts and use of certificates in GlassFish Server.

By default, GlassFish Server uses self-signed certificates. The self-signed certificates that GlassFish Server uses might not be trusted by clients by default because a certificate authority does not vouch for the authenticity of the certificate.

You can instead use your own certificates, as described in "Using Your Own Certificates" on page 90.

Dynamic Reconfiguration

Administrative commands that you execute on the domain administration server (DAS) must either be replicated on the effected server instances, or on all server instances that are part of the cluster. GlassFish Server replicates the commands by sending the same administration command request that was sent to the DAS to the server instances. As a result of replicating the commands on the DAS and the individual instances, the DAS and the instances make the same changes to their respective copies of the domain's configuration.

Note – Oracle recommends that you enable secure admin as described in Chapter 5, "Managing Administrative Security," so that GlassFish Server securely transfers these files on the network.

Dynamic reconfiguration refers to using the `--target` operand to CLI subcommands to make a change to a server instance (if the user-specified target is a server instance), or all server instances that are part of the cluster (if the user-specified target is a cluster). For example: `asadmin create-jdbc-resource some-options --target some-target`.

The --target operand allows the following values:

- `server` – Performs the command on the default server instance. This is the default value.
- *configuration_name* – Performs the command in the specified configuration.
- *cluster_name* – Performs the command on all server instances in the specified cluster.
- *instance_name* – Performs the command on a specified server instance.

If a command fails for a cluster, the status shows all server instances where dynamic reconfiguration failed, and suggests corrective next steps.

The command status also shows when a restart is required for each server instance.

The --target operand is supported for the following security-related CLI subcommands:

- create-jacc-provider
- delete-jacc-provider
- list-jacc-providers
- create-audit-module
- create-auth-realm
- create-file-user
- delete-audit-module
- delete-auth-realm
- delete-file-user
- update-file-user
- create-message-security-provider
- delete-message-security-provider
- list-audit-modules

- list-file-groups
- list-file-users
- login

Enabling Dynamic Configuration

Dynamic configuration is enabled by default and no additional action is required.

Use the following command to enable dynamic configuration from the command line:

```
asadmin set --user user --passwordfile password-file
cluster-name-config.dynamic-reconfiguration-enabled=true.
```

To enable dynamic configuration from the Administration Console, perform the following steps:

1. Expand the Configurations node.
2. Click the name of the cluster's configuration.
3. On the Configuration System Properties page, check the Dynamic Reconfiguration Enabled box.
4. Click Save

Understanding Synchronization

As described in "Resynchronizing GlassFish Server Instances and the DAS" in *Oracle GlassFish Server 3.1 High Availability Administration Guide*, configuration data for a GlassFish Server instance is stored in the repository of the DAS and in a cache on the host that is local to the instance. The configuration data in these locations must be synchronized. The cache is synchronized only when a user uses the administration tools to start or restart an instance.

See "Resynchronizing GlassFish Server Instances and the DAS" in *Oracle GlassFish Server 3.1 High Availability Administration Guide* for information about default synchronization for files and directories, for the steps required to resynchronize an instance and the DAS, and for additional synchronization topics.

Composed February 22, 2011