Table of Contents

UNICORE Gateway Service Reference Card

Functional description

The UNICORE gateway is an authenticating web proxy service for web service requests (SOAP messages) and normal HTTP traffic.

Typically it is the only UNICORE service that must be accessible from outside the site firewall.

It consists of a web server that receives client requests, authenticates the client, adds client X509 information to the SOAP message in the form of a SAML assertion, and forwards the message to the target service. The reply from the target service is sent back to the client.

For example, if the gateway is running on myhost:8080, a request to https://myhost:8080/CLUSTER/test will be processed as follows

- the gateway checks that the client is trusted, i.e. has a certificate issued by a trusted CA
- the gateway checks its connections table for a host named "CLUSTER"
- if found (say CLUSTER is configured to be https://cluster:7700 the request will be forwarded to https://cluster:7700/test
- if it is a SOAP message, the gateway will create and insert a SAML assertion containing the X509 certificate chain of the client

Daemons running

The gateway is a single web server.

Init scripts and options (start|stop|restart|...)

The service is started and stopped using shell scripts in the bin/ folder of the installation.

If installed via a Linux distribution package, e.g. RPM or .deb, then the service can be started with /etc/init.d/unicore-gateway {start|stop|restart}.

Configuration files location with example or template

Configuration files are in the conf/ folder of the installation.

- security.properties : contains keystore/truststore locations and passwords
- gateway.properties : contains basic information such as network interface and port, and basic configuration options
- logging.properties : log4j config file for controlling the logging
- connection.properties : contains the names, hosts and ports of the target services

If installed via a Linux distribution package, e.g. RPM or .deb, then the configuration files are located in /etc/unicore/gateway.

Logfile locations (and management) and other useful audit information

Logfiles are by default placed in the logs/ directory in the installation, and rolled over daily. Details can be controlled in the logging.properties file.

If installed via a Linux distribution package, e.g. RPM or .deb, then the log files will be located in /var/log/unicore/gateway, which is writable by the unicore user created when installing the package.

Open ports

One single open port, configured in the gateway.properties file (default: 8080)

Possible unit test of the service

Unit tests are part of the build procedure and executed automatically.

Where is service state held (and can it be rebuilt)

The service is stateless.

Cron jobs

N/A

Security information

Access control Mechanism description (authentication & authorization)

Standard SSL. Optionally the gateway can be configured to accept Globus proxies. CRLs are supported.

How to block/ban a user

Revoke the certificate. CRL checking must be enabled to enforce this. As the Gateway merely authenticates users and lets anyone providing a valid certificate through, blocking users is not required at this level.

Network Usage

The gateway will connect to its configured target sites. Also target sites will connect to the gateway.

Firewall configuration

The gateway port has to be accessible from outside the firewall, i.e. the firewall must allow connections to the gateway. Also, it has to be accessible from inside the firewall.

Security recommendations

Do not run as root.

Security incompatibilities

None known.

List of externals (packages are NOT maintained by Red Hat)

n/a

Other security relevant comments

n/a

Utility scripts

n/a

This topic: EMI > UNICOREGatewaySRC
Topic revision: r3 - 2011-04-21 - unknown