ORACLE®

GlassFish Secure Admin Handoff to QA and Doc

Tim Quinn

Nov 2010

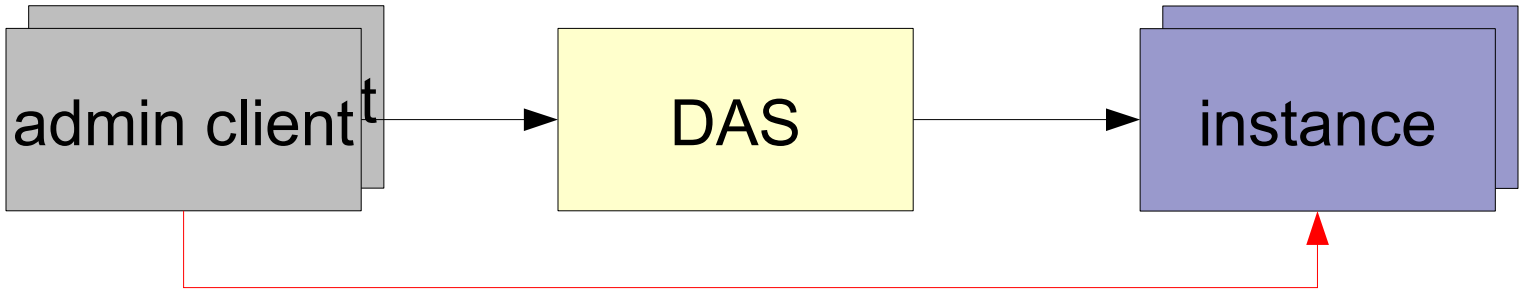
Agenda

- Overview of secure admin
- Feature description
  - SSL
  - Ways to authenticate
  - User experience
  - Upgrade support
- Demo

Secure Admin

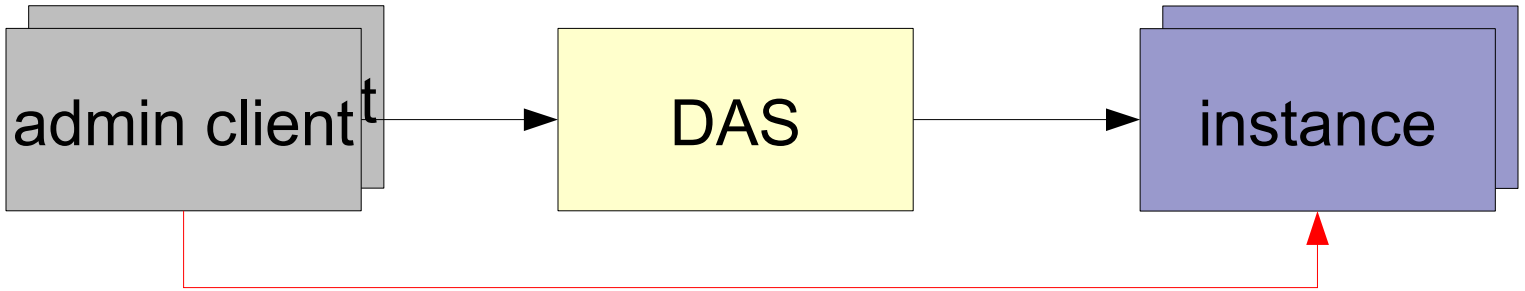
For admin traffic *anywhere* in the system maintain:

- Confidentiality – protect from snooping
- Integrity – protect from tampering
- Authentication – protect from impersonation



Secure Admin

- Secures admin traffic
  - Does NOT affect 8080, IIOP, etc.
- Permit only very limited direct client-to-instance access
- Allow administrator to enable, disable very easily
- Optional; turned off out-of-the-box



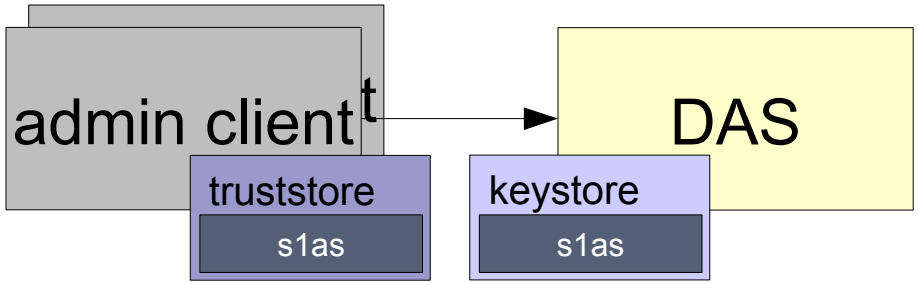
SSL

Provides much of what we need

- Confidentiality
  - Messages encrypted to prevent snooping
- Integrity
  - Participants detect message tampering
- Authentication (via certificates)
  - Each participant trusts identity of other

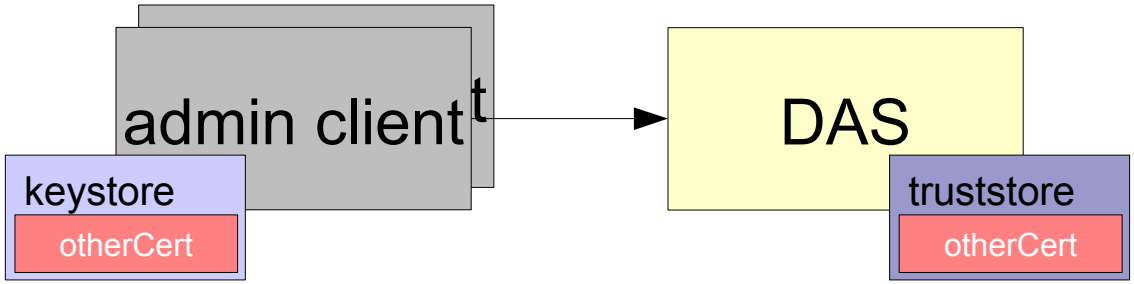
Ways to Authenticate Admin clients → DAS (as in v2.x)

- Clients include asadmin, browsers
- Valid admin user/password
  - HTTP basic authentication header
- SSL server authentication
  - DAS sends its cert to client
  - Client displays cert (if no chain to trusted authority)
  - Accepted by admin user, saved as trusted



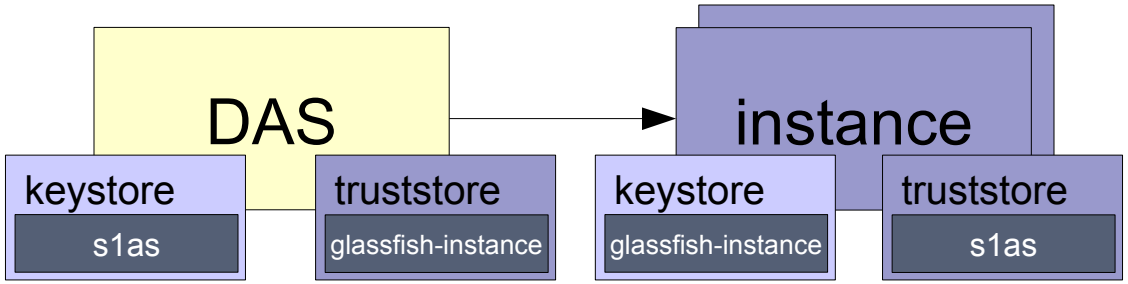
Ways to Authenticate Admin clients → DAS

- Optional and rare: Client certificate
  - Added manually to client's keystore
  - Added manually to DAS truststore
  - No automatic support by secure-admin



Ways to Authenticate DAS → Instances

- SSL client auth by DAS (as client) using DAS's certificate
- SSL server auth by instances (as servers) using instance certificate



User Experience
Enabling secure admin

- (DAS running)
- asadmin enable-secure-admin
  [--adminalias *alias-a*] (default s1as)
  [--instancealias *alias-b*] (default glassfish-instance)
  - User adds own keys and certs manually
- asadmin restart-domain
  - Restart **all** servers (DAS, instances) after a change
  - This example: only DAS is running

User Experience
Enabling secure admin

- Changes in domain.xml:
  - secure-admin (child of domain)
  - Several Grizzly config elements *for all configs*
- asadmin create-instance …
  - Will have secure-admin set up automatically (from default-config)
- Can create-instance **before or after** enable-secure-admin
  - (Currently, Grizzly bug makes before inconvenient)
  - (see demo!)

User Experience asadmin

Outwardly

Similar to GlassFish v2.x

- User runs asadmin command
- asadmin displays cert information ***regardless of --secure setting***
- User accepts/rejects
  - (Accepted: asadmin stores in ~/.asadmintruststore)
- asadmin will not prompt again for that cert

User Experience asadmin

Internally

- DAS is in control, insists on SSL
  - Redirects http → https
- asadmin automatically uses SSL if DAS says to
  - User does **not** need to specify **--secure=true**
  - asadmin now knows how to follow redirects
- **No** in-the-clear transmission of user, password
  - asadmin establishes secure connection (https)...
  - ...and only then sends user/password
- (Faster to specify --secure=true but not necessary)

User Experience
Disabling secure admin

- (DAS running)
- asadmin disable-secure-admin
- Manually restart all instances, DAS
- In domain.xml:
  - secure-admin present, empty
  - Grizzly config added by enable-secure-admin reverted

Upgrade Support

- Securing admin in v2
  - Published v2 doc on how to secure admin traffic??
  - Blogs, some relevant forum postings

- 2.x → 3.1 upgrade checks for:
  -
```
<configs>
  <config name="server-config...>
    <http-service>
      <http-listener id="admin-listener"...>
        <ssl ...>
```
  - If found, internally does enable-secure-admin

Demo

WARNING:

- If secure admin works, nearly invisible externally!
  - I'll use client and server logging (noisy)
- Grizzly bug → temporary hack of domain.xml in demo
  - I'll use vi

Demo

Steps:

- enable-secure-admin
- Stop DAS
- Hack domain.xml
- Restart DAS
- create-instance
- start-instance
- list-instances (DAS → instance message)
- Deploy (DAS → instance upload, message)
- Run

Questions

References

http://wikis.sun.com/display/GlassFish/3.1SecureAdminTraffic

ORACLE