Configuration of AERS 4.5.2 environments with multiple Middle Tiers and https/SSL

Sunil G. Singh

DBMS Consulting

20 September 2006

Safety

Session 22

Acknowledgements

- Thanks to OCUG and the Saftery Focus Group for this opportunity to speak and present.
- Thanks to Brad Gallien and the OCUG planning committee for their infinite patience in accepting and reviewing this presentation.
- My sincere thanks to everyone who assisted me with this presentation whose input was invaluable.
- Thanks to the audience members for attending.

Assumptions and Scope

- Assumption: Audience is familiar with Oracle AERS
- Scope: High-level discussion of Load Balancing methods and supportability

Need for https/SSL and Multiple Middle Tier Servers for AERS

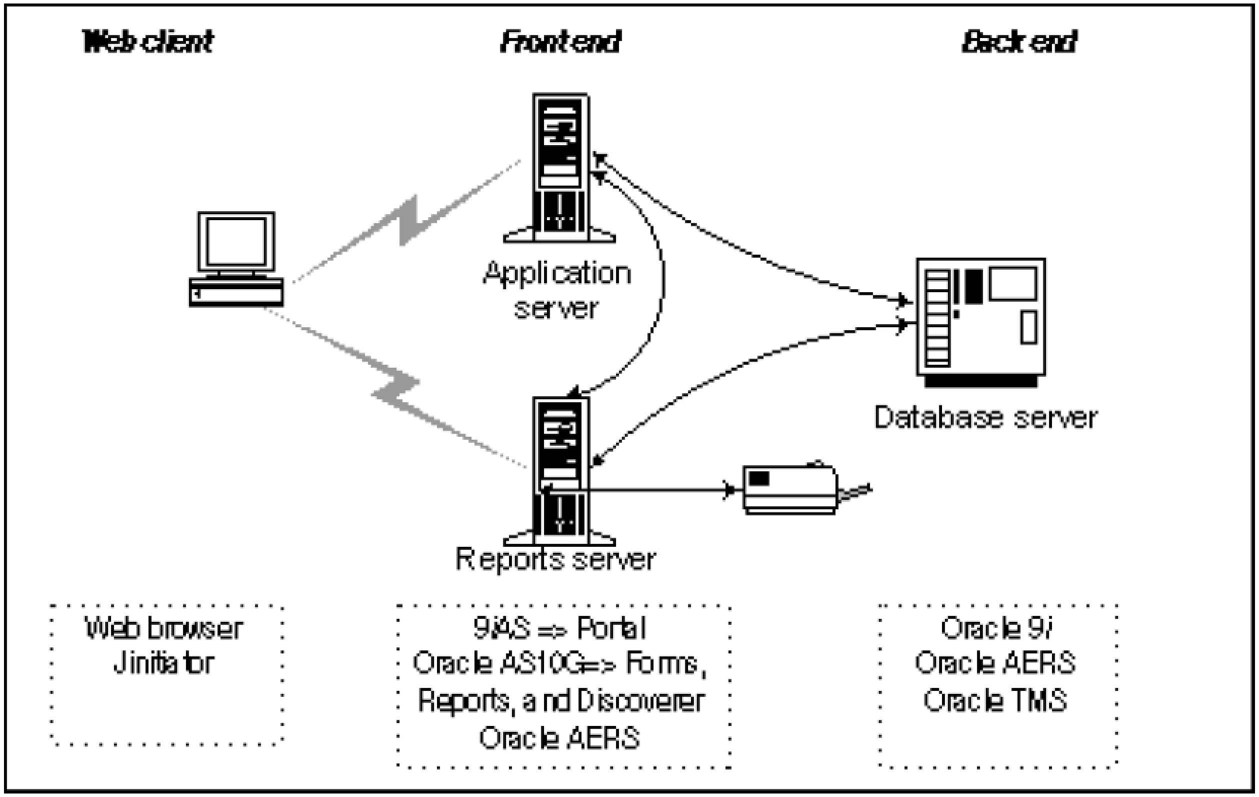
- Many AERS production environments have global utilization and contain sensitive company data.
- As a result many organizations are trying to find ways to make their production AERS environment more fault tolerant and more secure.
- This has lead to a growing need for https/SSL configurations for Oracle AERS and also multiple Middle Tier servers where possible.

Documented https/SSL, Multiple Middle Tier configurations for AERS

- There does not appear to be very much documentation available publicly on how to configure AERS specifically to use https/SSL or how to configure AERS to use multiple Middle Tiers.
- This makes it difficult to understand what configurations are technically possible and supported.
- However, it turns out that architecture of Oracle AERS is still very close to Oracle Apps 11i E-Business Suite, which may provide some insights into both of these configurations for Oracle AERS.

Current AERS 4.5.2 Architecture

- As documented in the AERS 4.5.2 Installation Guide pp 1-5:



Oracle AERS consists of a back end Oracle *9i* RDBMS, middle-tier computers, and Web clients. The middle-tier computers are the 9iAS Application Server and the AS10g Reports and Forms Servers. We no longer support client/server deployments.

AERS 4.5.2 Architecture Observations

- AERS 4.5.2 still users 9iAS 1.0.2.2.2a (Release 1) as its primary connection, along with Portal 3.0.9.8.5 (same as previous versions).
- AERS 4.5.2 now uses AS 10g, but mostly for Forms, Reports and Discoverer.
- According to the AERS 4.5.2 Installation Guide, the AERS Application Server and Reports Server both have 9iAS rel 1 and AS 10g components installed. This means the Forms layer and the https layer are on the same physical servers.

Similarities between Apps 11i and AERS 4.5.2

- Apps 11i also still uses 9iAS 1.0.2.2.2a and Oracle Portal.
- Apps 11i also uses Forms 6i for its ERP applications, while AERS 4.5.2 is using Forms 9i.
- AERS 4.5.2 does not use a Forms Server by default, while Apps 11i does.
- Apps 11i has integration with Oracle Identity Management, while AERS 4.5.2 has SSO with Oracle Portal.
- By examining the documented load balancing and SSL deployment methods for Apps 11i, this would provide some insights into possible solutions for Oracle AERS.

Load Balance Methods used for Apps 11i

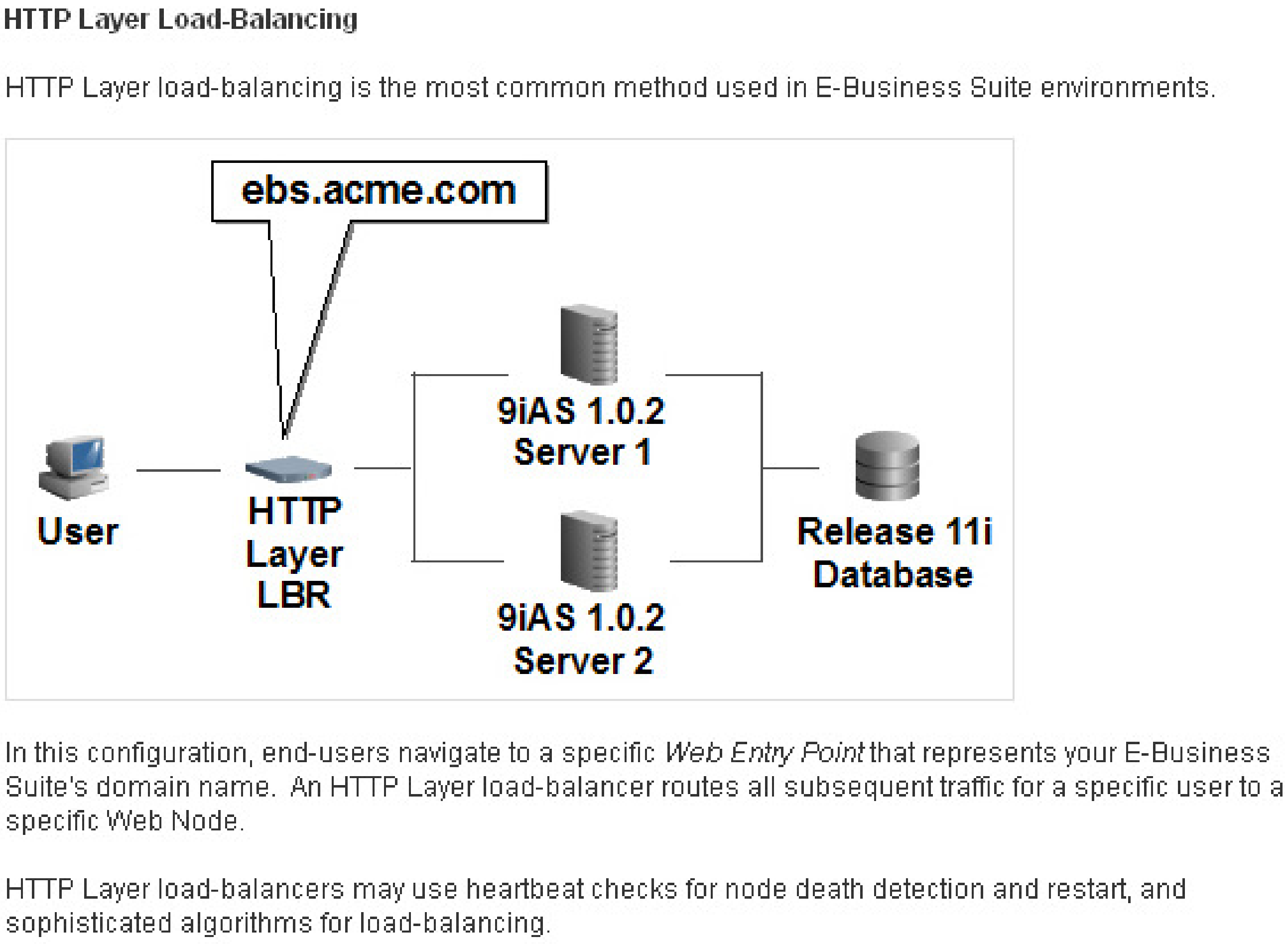
- Hardware-based HTTP Layer load-balancing
- Hardware-based DNS layer load-balancing
- Software-based JServ layer load-balancing
- Metric Server-based load balancing for Forms
- Load-balancing for concurrent processing nodes
- Load-balancing via Real Applications Clusters (RAC) for database tiers.

Which Load Balance methods can work with AERS Middle Tiers?

- Hardware-based HTTP Layer load-balancing
  - Yes.
- Hardware-based DNS layer load-balancing
  - Yes, similar in to HTTP Layer load-balancing
- Software-based JServ layer load-balancing
  - Not practical. The Jserv layer is already on the same node(s) as 9iAS.
- Metric Server-based load balancing for Forms
  - Not possible. Oracle AERS is not configured to call Forms Metric server and does not use the Forms listener
- Load-balancing for concurrent processing nodes
  - Not possible. The concurrent manager run all of the jobs in Apps 11i, but no equivalent process exists for Oracle AERS
- Load-balancing via Real Applications Clusters (RAC) for database tiers.
  - Not possible. Does not appear to be support for RAC for Oracle AERS.

Hardware Layer http Load Balancing

- Excerpt from Steven Chan, Director, Applications Technology Integration: "In-Depth: Load-Balancing E-Business Suite Environments"
  - http://blogs.oracle.com/schan/2006/06/16#a322
- Internally at Oracle, F5 BIG-IP is used both for E-Business Suite and Apps 11i On-Demand customers.



HTTP Layer Load-Balancing

HTTP Layer load-balancing is the most common method used in E-Business Suite environments.

In this configuration, end-users navigate to a specific *Web Entry Point* that represents your E-Business Suite's domain name. An HTTP Layer load-balancer routes all subsequent traffic for a specific user to a specific Web Node.

HTTP Layer load-balancers may use heartbeat checks for node death detection and restart, and sophisticated algorithms for load-balancing.

Hardware Layer http Load Balancing: Application Modifications

- Some configuration within Oracle AERS is required for this method to work, specifically, the external facing name of the load balancer must be entered into:
  - AERS System Parameters Control table values for:
    - ADHOC_URL
    - EXT_TERM_BROWSER
    - HELP_URL_PREFIX
    - PORTAL_PLS_URL

Hardware Layer http Load Balancing: Application Modifications

- Local registry keys of the middle tiers must be updated to refer to the external facing load balancer name
- Modification of files containing specific Middle Tier name references such as:
  - Jserv.conf
  - Httpd.conf
  - Jserv.properties
- Local host entry to make external facing load balancer name resolve to the local Middle Tier

Hardware Layer http Load Balancing: SSO and Portal Modifications

- In order to support connections from Application server multiple middle tiers internally (behind the load balancer), the Single-Sign On Portal configuration must be made aware of the **all** of the Middle Tiers which will connect to the portal.

Hardware Layer http Load Balancing: SSO and Portal Modifications (2)

- This is a complex process which is documented in Metalink ID 162044.1, using the option to Configure multiple Portal URLs with a single SSO URL.
  - Start with an single Application Middle Tier configured to connect to the Portal.
  - Create DADs and common cookies for each Application Server Middle Tier.
  - Create Partner Applications for each of the other Application Server Middle Tiers that will connect to the Portal.
  - Generate an ID, token and site Key for each additional Application server Middle Tier.
  - Execute ssodatax.cmd script once for each additional Application server Middle Tier.
  - Manually modify the wwsec_enabler_config_info$ table to update the ls_login_url.

Required Load Balancer properties for http Layer Load Balancing

- Three properties of the load balancer then become key for its successful use in this configuration:
  - Persistence or “stickiness” is critical. Because the HTTP listener, Portal and AS 10g Forms or Reports are always on the same middle tier server, the connection from the client to the load balancer can not switch midstream during the AERS session. Persistence must be set for a time equal to or greater than the longest anticipated user session.
  - Given that this longer persistence is required, the load balancing occurs in the **initial connection only.** Therefore, the load balancer must use a simpler algorithm for this load balancing, such as round-robin, to achieve a balanced number of connections.
  - Ability to rewrite all URL requests consistently to the corresponding Middle Tier. AERS and Portal still generate local URL named traffic during the use of the application, and the load balancer must independently handle this situation

Hardware Layer http Load Balancing Challenges

- If AERS is configured with separate Reports and Application servers, then it can be very difficult to configure load balancing among the Report Servers:
  - If 6i compatibility mode is used to connect to the report server, then load balancing is difficult since the TNSNAMES.ORA entry for the report server must know which server it is connecting to. But the AERS application can only store the TNSNAMES.ORA report server entry for **ONE** report server, leading to a conflict.
  - If 9i compatibility is used, then the URLs generated to the Report Server must also go through a separate (logical) load balancer in order to be resolved correctly. Reports Server clustering is available in AS 10g, but it is not clear if AERS 4.5.2 can run without 6i compatibility mode.
- If using a public-facing load balancer DNS names, some external sites can present themselves with multiple IP addresses. This causes the load balancer to incorrectly switch the same source client from one Middle Tier to another, forcing a disconnection from AERS.
- A user can always connect longer than the persistency time of the load balancer, exposing possible disconnection.

Installing a Digital Certificate on SSL Accelerator or Load Balancing device

- The high-level steps for requesting and installing a Digital Certificate on any of hardware SSL Accelerator or Load Balancing devices are similar:
- Generate a private key
- Apply for a certificate
- Generate a CSR (Certificate Signing Request)
- Use the public name of the Load Balancer or SSL Accelerator (network device) server (This should be a public DNS Name if it is public facing)

Installing a Digital Certificate on SSL Accelerator or Load Balancing device

- Send CSR to the Certifying Authority (CA)
  - Usually uploaded to the CA’s website or sent via e-mail
- Receive genuine certificate from the CA
  - Usually received via e-mail from the CA
- Install genuine certificate from the Certifying Authority into Load Balancer or SSL Accelerator’s device configuration files (specific steps for each device)

Comments on https/SSL configuration for AERS 4.5.2

- It is much simpler to combine the https/SSL configuration with a load balancer than to try to deploy https/SSL on each Application server Middle Tier. Deploying https/SSL on individual Application Servers can lead to:
  - Increased maintenance for certificate management and expiration
  - Slower performance of the individual Application Server and network environment
- For the Report Server, access to the integrated Portal and Report Server is already secured in AERS 4.5.x. The passing of the passwords for the Portal and Report Server is also encrypted.

Load Balance and SSL Devices Used tested for AS 10g

- Oracle had tested the following Load Balancers and Stand-Alone SSL Accelerators:

Load Balancer

✓ BIG-IP F5	V4.5, V9
✓ Radware WSD	7.50.05,8.16.13
✓ Radware CT100c	3.03.07,3.21.07
✓ Nortel Alteon	AD4(HTTP only)
✓ Foundry Serverlron	08.1.00ct24
✓ NetScaler	NS 5.2
✓ Cisco ACE	1.0
✓ Cisco CSM	12.1

Stand Alone SSL Accelerators:

✓ Sonic Wall SSL	R3
✓ Ingrian	i220/2.9.1

Future directions for AERS load balancing/SSL configuration

- Future versions of AERS should be able support more types of load balancing and SSL configurations, which would include:
  - Load balancing Forms 9i with Web Cache
  - Support for Identity Management and load balancing of authentication against Identity Management servers
  - Returning optional use of Wallet Manager for Forms 9i SSL support
  - Support for Oracle AS 10g Portal

Question and Answers

All follow-up questions, please contact:

Sunil G. Singh
singh@clinicalserver.com
+1-860-983-5848
+1-888-463-4751
+91-98-181-34-017

Stephan Kromov
skromov@clinicalserver.com
+1-215-353-0811

Dr. Letian Liu
lliu@clinicalserver.com
+86-134-0212-4879