

Installed SP base

As of April 13, 2011:

- 351 application service provider requests approved.
- 738 distinct entity IDs
- 447 distinct entity IDs with metadata installed. Most UF a few federated (NIH, ALEKS, etc)
- Avg. logon/day 253,777 for April 4-7

IdP Service Providers

Date	Logons per day	Unique credentials	Hour of peak	Logons peak hour
April 4,2011	244275	54387	13:00	18359
April 5,2011	249609	54060	13:00	18799
April 6,2011	239507	52997	13:00	17382
April 7,2011	281720	52387	10:00	*58141

* Network issue caused many logon to be reconnected during the 10am hour of 4/7
0400 - 0600 only hours under 1000 logons per hour.

0800 - 2400 regularly have over 10,000 logon per hour.

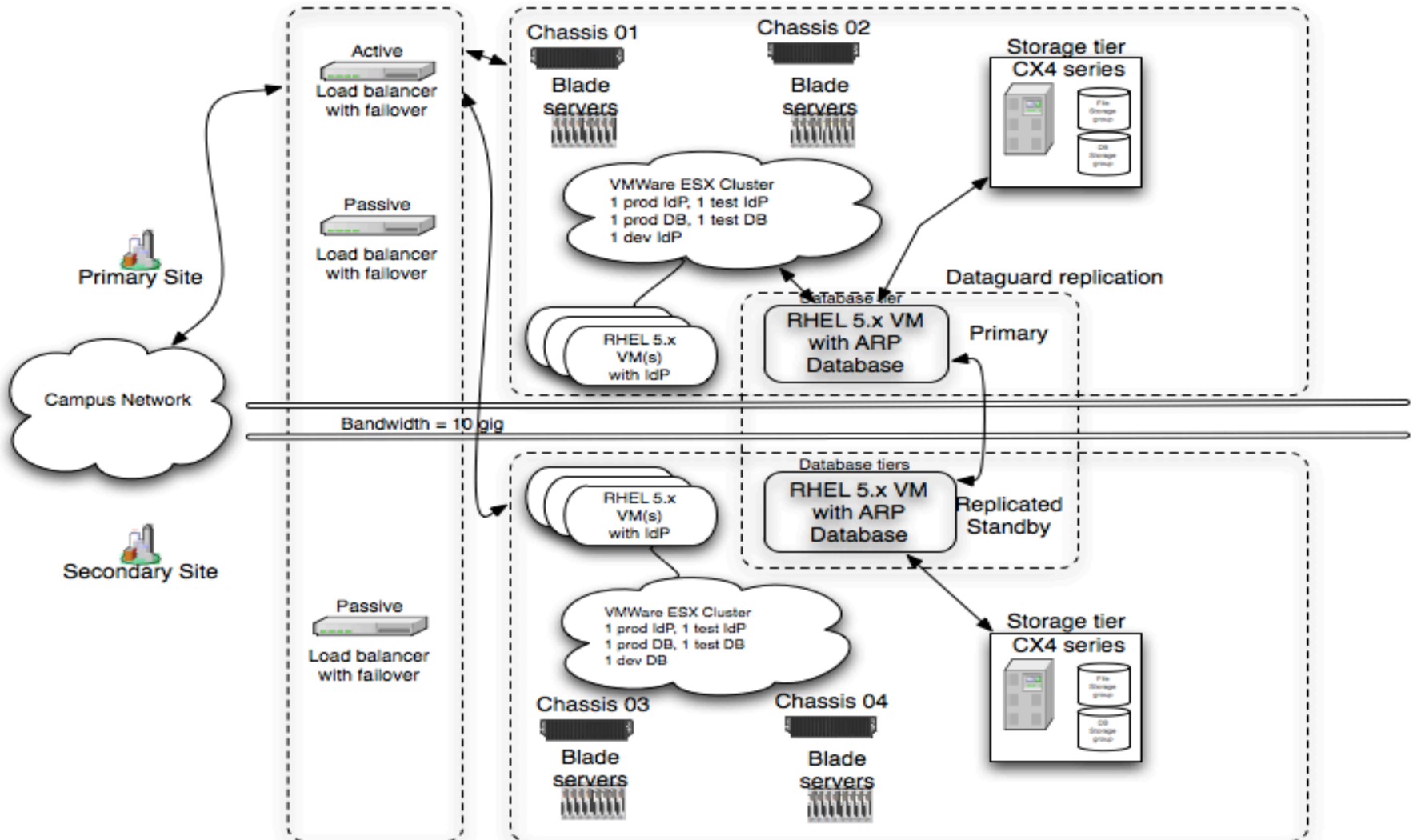
SP Setup Automation

1. Updates are made by IAM group in response to SP staff requests into a simple SP request database.
2. Approved changes are detected by IdP Management Scripts and copied to the IdP source management at 12:10pm each day.
3. Metadata Uploaded for SP
4. Process the metadata and enter into source tool
5. Recreate the Shib config files (metadata + SP db data)
6. Tag and test in Test IdP
7. Move weekly changes to Production Sunday 6am Maintenance window
8. Restart IdP 6am Sunday morning

Managing Service Providers (1)

- UF Service Provider Request starts the process.
 - Requires responsible parties to be named.
 - Requires description of service
 - Requires designation of URL(s), Server(s), and UF ARPs desired.
 - Volume of logon estimates required.
 - Received by IAM office, entered, reviewed and approved in a simple SP request database
 - Annual Certification of each SP is conducted.

IdP Technical Model



IdP Architecture

- The Shibboleth HA implementation is comprised by 3 environments with 2 clusters each:
- **prod01** RHEL 5 (64-bit), VM 7, 4 vCPU, 16 GB Memory, 2 HD 56 GB total
- **prod02** RHEL 5 (64-bit), VM 7, 2 vCPU, 16 GB Memory, 7 HD 112 GB total
 - Shibboleth IdP v 2.1.5
 - Shibboleth SP v 2.2.1
 - JRE 1.6.0-sun.x86_64
 - Terracotta 3-3.0
 - Apache Tomcat 6.0.29
 - RRDtool (monitoring/capacity)

Lessons learned

- Addition of a single SP created a load/capacity issue in Jan 2011. Make sure you review estimated load and watch capacity closely.
- Stuff Happens – Network outage April 7 caused huge peak in logon to recover.
- SPs must code applications to handle errors. IdP gets blamed for their errors.

- Helpdesk has a view of the SP database to assist when SPs have an issue.
- Helpdesk needs to understand errors that come from Shib IdP vs SP issue.
- Dreaded “dragonbird”.
- We hold monthly SP training bootcamp.
- Local Listserv for all SP techs and ISM.

Contact

Warren Curry

[Email: whcurry@ufl.edu](mailto:whcurry@ufl.edu)

<http://www.it.ufl.edu/identity/shibboleth/>