Power of Open Source Architecture

OPEN SOURCE SYMPOSIUM 2006

Twenty Questions To Ask Yourself During A Red Hat Directory Server Deployment

Red Hat Directory Server

Satish Chetty

Technical Support Account Manager

Red Hat

What is the primary application of the Directory Server?

- Typical applications
  - NIS, Windows login, Web based phone book and authentication for Kerberos, FTP or Samba.
- You could also have the Directory Server provide information to other applications.
  - Mail servers, Calendar servers, Web servers.
- Determining the primary application up front allows you to design the deployment most appropriately
  - Will it need a modified or custom Schema?
  - What will load be?
  - How many Master/Replica servers are required?
  - How to partition the data?
  - How to construct the indexes?

Power of Open Source Architecture
OPEN SOURCE SYMPOSIUM 2006

How many Directory masters and replicas are required? (fault tolerance)

- Smallest deployment is a single Master
- Most production (non lab) instances require at least one replica to provide fault tolerance.
- More Replicas means more fault tolerance

Where are the clients located? Are they in same or different locations?

- Large deployments often have geographically dispersed sites.
- Local Replicas
  - Help distribute read load
  - Provide read availability if network connections fail
- Multiple Masters provide increased write availability

How many users will the directory deployment handle?

- Your *users* of directory server can be applications (NIS, Kerberos etc.), or users.
- Each of these clients will generate one or more requests.
  - Authentication will generate one request at a time (usually when the user logs in via the client)
  - A web portal will generate multiple request to the Red Hat Directory Server, sometimes even simultaneously.
- Knowing how many requests will help you calculate the amount of memory that will be needed to effectively set cache sizes for optimal performance.

Any firewall configurations that you should be aware?

- With the default configuration Directory server uses the following ports
  - Non SSL LDAP uses port 389
  - Secure SSL LDAPS uses port 636
- Replication information is also transmitted over these ports
- Firewalls can also be used to allow only requests from certain domains, hosts or IP addresses.
  - This is can be useful in guarding against DoS attacks

How many RHDS Masters and Replicas do I need to plan in my Directory deployment (load related)?

- Updates can only be made on the Master
  - If updates are mission critical, having multiple masters is recommended
  - Update load can also be spread across the Masters
- Masters initiate replication
  - If there are many Replica servers having multiple masters will help distribute the load during replication
- Adding Replica servers:
  - Allows Directory Servers to be placed closer to clients improving performance and availability.
  - Spreads read load

How many hubs do I need to plan in my Directory deployment?

- Large Enterprise deployments require many Replicas
- Master can get overloaded Replicating data
- Hubs can alleviate this load by acting as intermediaries.

Do you plan to have applications authenticate against LDAP?

- Understanding the number and type of read/write requests can help plan the deployment

What is the approximate load you expect?

- If your update load is high, having multiple Masters can help in load balancing.
- Multiple Read-Only Replicas may help in load-balancing read load.
- See the deployment guide for more information.

Do you plan to set up MMR?

- This feature enables multiple Master RHDS servers to synchronize information among themselves and to other replicas or hubs
- Provides fault tolerrence for large geographically dispersed enterprise deployments
- Can spread the repication load for deployments with many Replica servers

Do you plan to synchronize information with Active Directory Windows?

- Windows Sync lets you synchronize user and group information from/to RH DS with Active Directory on Windows 2000/2003.
- If userpassword attribute is part of the user information that is to be synchro nized, then a separate module needs to be installed on the Windows Active Directory Server.
  - This module is called the Password Sync.
  - If multiple Active Directory Servers are to be synchronized, password sy nc module needs to be installed on each of the Windows Servers.

How often do you want replication to happen (Scheduled or Instant)?

- Information can be replicated in real time (whenever the master gets updated) or during a particular time of day.
  - Scheduled replication is particularly useful when remote offices occasionally connect to the network and receive updates from the Master server.
- Setting up scheduled replication between masters is also possible.
  - However, there is a greater chance of replication conflict in a timed MMR.

What is the network connectivity between the Masters and Replicas?

- Understanding the bandwidth limitations between replicating servers is important for an efficient deployment.
- Bandwidth constraints may force you to set up MMR, use timed replication or distribute the data across multiple databases and multiple servers.
- Red Hat Directory Servers can handle replication efficiently even over low quality and slow networks.
- Red Hat Directory Server also supports topologies that change due to traffic shaping.

What data gets updated on the LDAP?

- What data gets updated (and replicated) will help you understand the load requirements of your directory server deployment.
- The load generated by several clients doing an email look-up is different than the load generated by an OCSP (On-line Certificate Status Protocol) application

Have you planned for fail-over or redundancy?

- Red Hat Directory Server running on an enterprise class machine (and running RHEL 4) can handle several thousand read requests and several hundred write requests per minute.
- However, you should not rely just on a single Master machine for all your LDAP needs. Having multiple Master or Replica servers will enable
  - Distributed load
  - Failover if the primary master server is unavailable (due to hardware or network failure).

What ACIs do you plan to set up?

- Access Control Instructions (ACI) are set of rules placed on the directory (or a subset of the directory).
- These rules are evaluated by the server and either allow or deny permissions to a request from a client.
- ACIs are part of the security sub system offered by the Red Hat Directory Server.

Have you planned your ACI Matrix?

- While you are in the planning phase for your directory deployment, you should define an access control strategy as an integral part of your overall security poli cy.
- An ACI Matrix is a table of all the attributes whose permissions are a ssociated by location, users and groups.
- Setting up an ACI matrix helps you understand what attributes need to be protected, how and when.
- With an ACI matrix you can set following permissions:
  - The entire directory.
  - A particular subtree of the directory.
  - Specific entries in the directory.
  - A specific set of entry attributes.
  - Any entry that matches a given LDAP search filter.

Do you want to turn on SSL on Red Hat Directory Server?

- The directory server provides security at three levels:
  - At the database level (attribute encryption)
  - At the content management level (ACI)
  - At the network level (SSL)
- To provide secure communications over the network, Red Hat Directory Server (Directory Server) includes the LDAPS communications protocol.
  - LDAPS is the standard LDAP protocol, but it runs on top of Secure Sockets Layer (SSL).
  - Red Hat Directory Server also allows "spontaneous" secure connections ove r otherwise-insecure LDAP ports, using Start TLS (Transport Layer Securit y).

Will replication be over SSL?

- Red Hat Directory Servers involved in replication can be configured for SSL so that all replication operations occur over an SSL connection.
  - This helps in securing all replication data sent between Master and Replica servers.
  - Digital certificates need to be installed on each of the Master and Replica servers.

Have you planned your indexes?

- Proper indexing is the most important thing you can do to improve read performance.
- Red Hat Directory Server uses index files to aid in searching the directory.
- The more indexes you maintain, the longer it takes the directory server to update the database.
- One other cost to maintaining index files is the increased system resources they require.
  - Index files use disk space:
  - Index files use memory:
  - Managing index files uses CPU cycles

Questions