



Srinivas Satyavaru [srs@redhat.com]
Solutions Architect, Red Hat

Agenda

- Is Flat directory structure is better than Hierarchical ?
- What are Virtual DIT views ?
- Federated Authentication ?
- Store Proximity access data into Directory Server ?
- Can OpenLDAP be used as proxy ?
- What is Fractional Replication ?
- How to use Directory Server in a Disconnect and or loosely coupled Replication cases ?
 - NIS Migration
 - Can Samba be a backend for Directory Server ?
 - What are Netgroups ?

Red Hat Identity Management Products

- Red Hat Directory Server
- Red Hat Certificate System
- Enterprise Identity Policy and Audit [IPA]

Red Hat Identity Management Products

- Red Hat Directory Server –

Is a robust, battle tested, scalable server designed to manage an enterprise-wide directory of users and resources. It is based on an open-systems server protocol called the Lightweight Directory Access Protocol (LDAP). Customers can centralizes application settings, user profiles, group data, policies and access control information into a network-based registry.

Facilitates to answer:

- Who are you ?
- What can you do ?

Red Hat Identity Management Products

- Red Hat Certificate System -

Red Hat Certificate System is an end to end, X.509 v 3 digital certificates life cycle management system that can manage issuance, revocation, CRL, publishing and directory integration. It is a component needed to handle strong authentication, single sign-on, and secure Communications between client and server.

Facilitates to answer:

Prove that you are who you say you are.

Red Hat Identity Management Products

- Enterprise Identity Policy and Audit [IPA] –

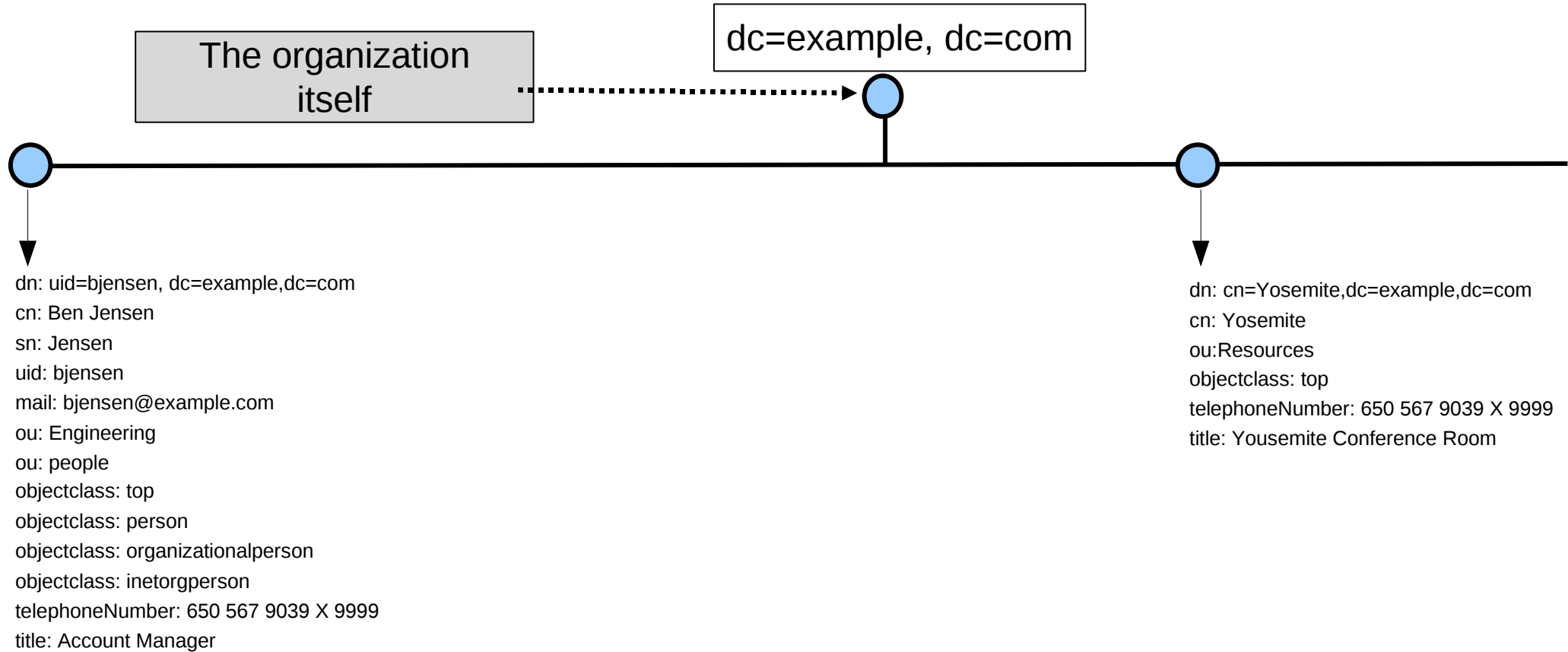
Red Hat Enterprise IPA is an integrated security information management solution combining RHEL, Red Hat Directory Server, MIT Kerberos, NTP, DNS. It consists of a web interface and command-line administration tools. It supports managing of user and resource identities today with plans to support policy and auditing management.

Red Hat Directory Server – Deployment Scenario

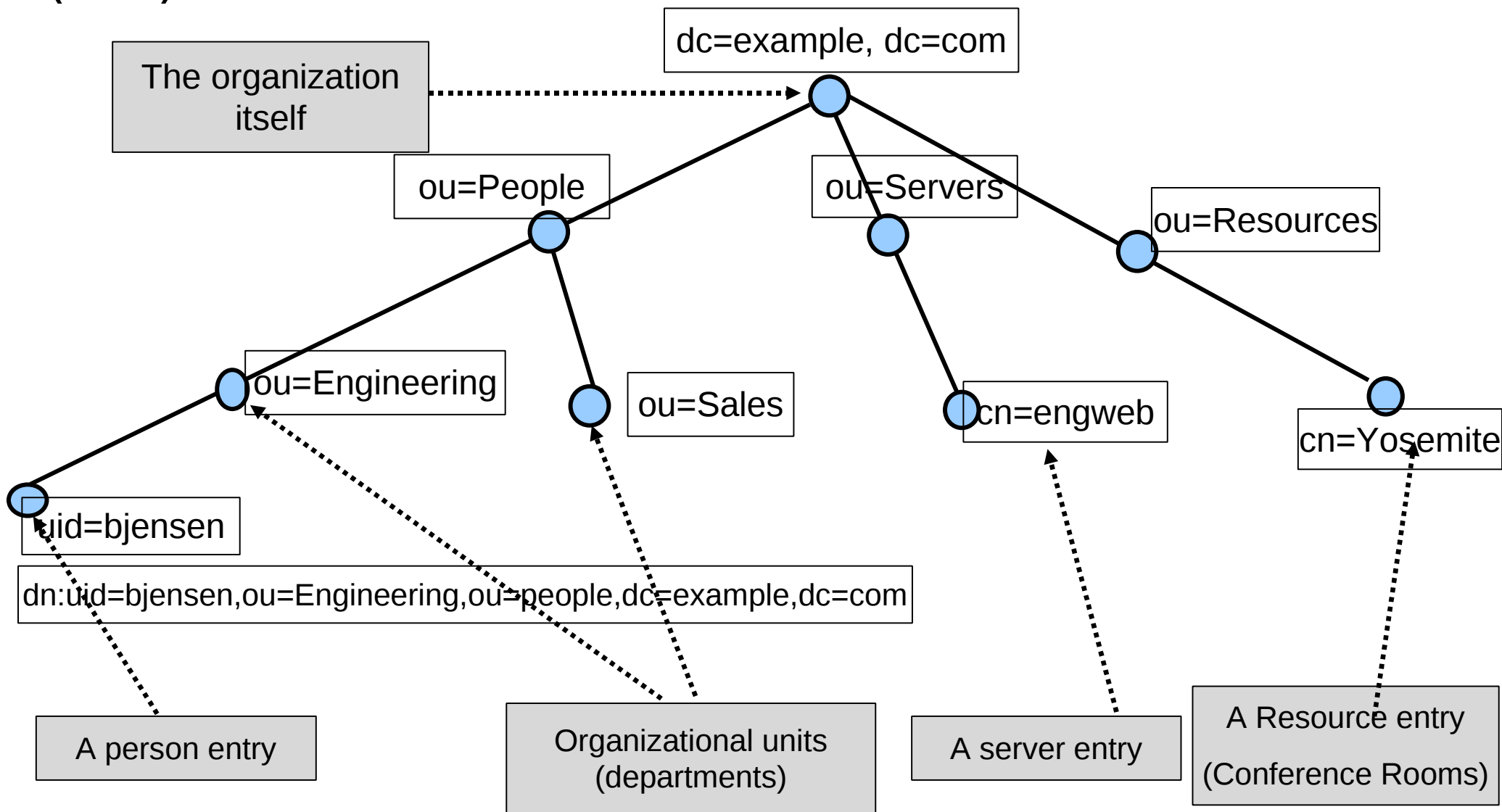
- Is Flat directory structure is better than Hierarchical ?

The hierarchical DIT is useful for navigating the directory but is cumbersome and time-consuming to change. The flat DIT, while requiring little to no change, does not provide a convenient way to navigate or manage the entries in the directory.

Sample Flat Directory Information Tree (DIT)



Sample Hierarchical Directory Information Tree (DIT)

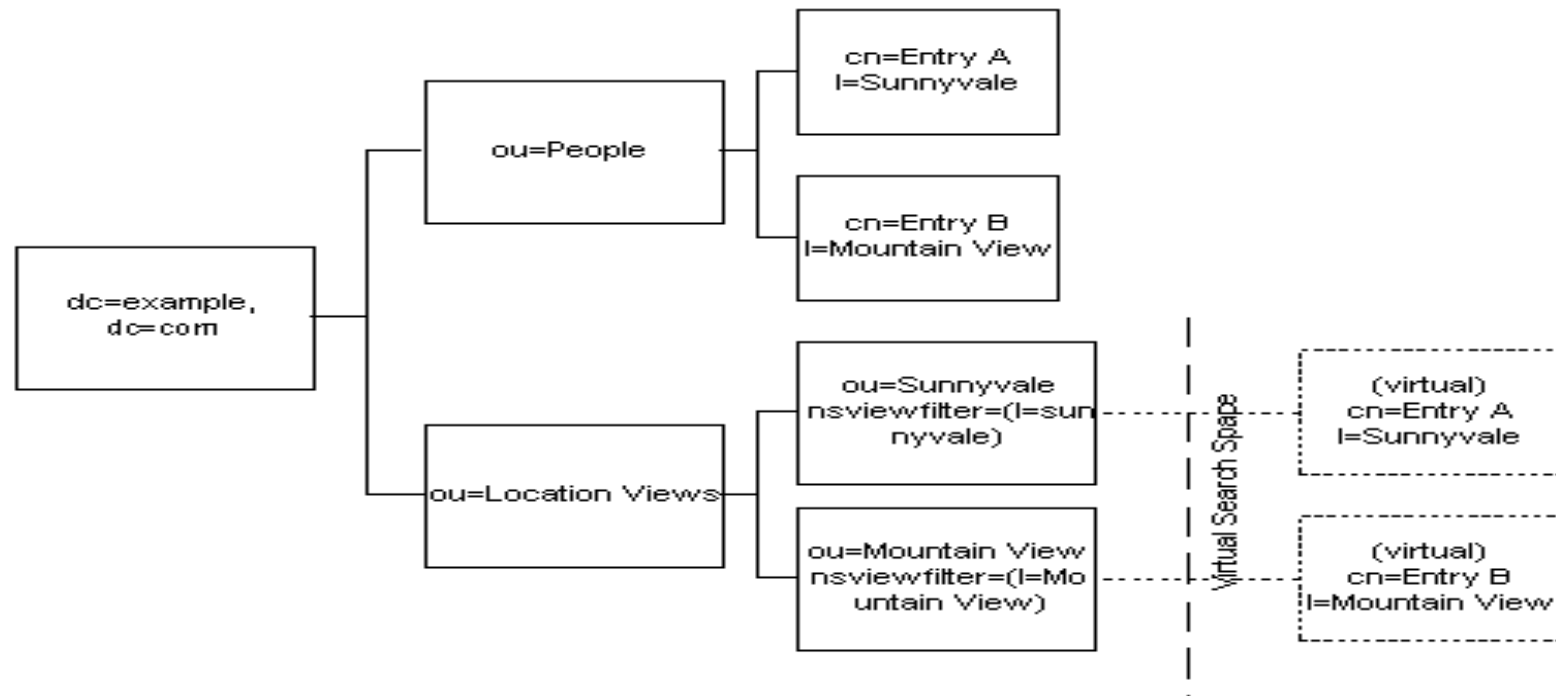


Red Hat Directory Server – Deployment Scenario

- Virtual DIT views -

Virtual DIT views are a way to navigate hierarchically entries that do not require the physical existence of those entries in any particular place. The virtual DIT view uses information about the entries to place them in the view hierarchy.

Red Hat Directory Server – Deployment Scenario



Red Hat Directory Server – Deployment Scenario

- Federated Authentication -

A large North American ISP stores information / relationship about domains and users within those domains, to provide users with email-ish type user-ids instead of the typical "johnny127" type names.

For e.g srs@redhat.com
srs@jboss.com

- Proximity Access –

Physical access to Bldgs. / Facilities / Data Centers etc.

Red Hat Directory Server - Deployment Scenario

- OpenLDAP as proxy
- Fractional Replication
- Disconnect and or loosely coupled Replication
- Directory Server to store profile, pictures, jpeg, digital certificates, product images, CRLs
- NIS Migration
- Samba - Samba can be configured to use LDAP as it's data store and thus authenticate windows client to Red Hat Directory Server
- Netgroups

Red Hat Directory Server – Deployment Scenario

- Use of LDAP for Kerberos data store
 - Authentication to LDAP using Kerberos ticket uses SASL/GSSAPI on client
 - Directory Server to use OS Credentials.
- LDAP and Mail client authentication and Type down search
- Active Directory - Can support Unix/Linux clients directly
- Authenticate web Applications and Services to Red Hat Directory Server for single sign on
 - memberOf attribute
- Persistent search
- Use of Directory Server for services such as SSH

Red Hat Directory Server – Deployment Scenario

- Trouble shooting Tips
 - Java Console
 - Command Line Utilities
 - Monitoring slapd process and measure performance – Cacti
 - DS uses the Agent Extensibility Protocol (AgentX) to extend SNMP and data is passed on to net-snmp.
- logconv.pl
- Cl-dump to dump and decodes the changelog
- repl-monitor (monitors repli status with a web page)
- Log (Error, Access)
- vlvindex to re-create indexes

Red Hat Directory Server – Deployment Scenario

The screenshot displays the Red Hat Management Console interface. The main window, titled "rhds.hademo.com - Red Hat Directory Server - ConfigDirectory", shows the configuration for a Directory Server. The left pane lists various configuration options under "Tasks", "Configuration", "Directory", and "Status". The right pane shows the "Replica Settings" section, which includes:

- Enable Replica
- Replica Role:
 - Single Master
 - Multiple Master
 - Hub
 - Dedicated Consumer
- Common Settings:
 - Replica ID: (Must be unique among the IDs of the master replicas)
 - Purge delay: Day(s) Never
 - Updatable by a 4.X Replica
- Update Settings:
 - Current Supplier DNs:
 - Enter a new Supplier DN:
 - Current URLs for referrals (Optional):
 - Enter a new URL:

At the bottom of the window are buttons for "Save", "Reset", and "Help".

Red Hat Directory Server – What's new

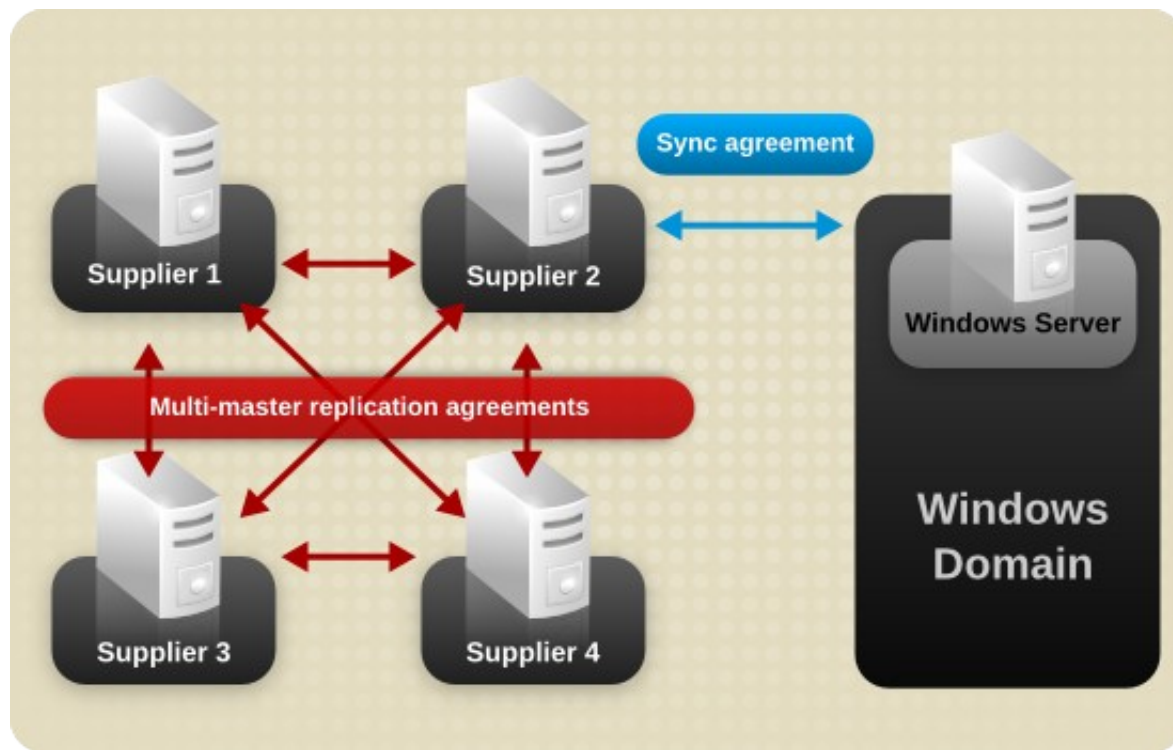
- Replaced Netscape Enterprise (Web) Server with Fortitude (Apache / mod_nss), 100% open source
- Support for 64bit x86 processors and Red Hat Enterprise Linux 5 including Virtualization [XEN]
- Basic support for IPv6
 - Server will accept incoming connections from IPv6 clients
 - IPv6 addresses in ACIs, replication agreements and chaining not yet supported
- Improved support for SASL/Kerberos
- Improved password syntax policy enforcement
- Filesystem Hierarchy Standard [FHS]

Red Hat Directory Server – What's new

- Supported Platforms for server:
 - Red Hat Enterprise Linux 3 & 4 & 5 (32-bit & 64-bit)
 - HP-UX 11i
 - Solaris 9 support (32 & 64-bit)
- Availability
 - 4-way Multi-Master over WAN
- Integration
 - DSML v2 support permits XML queries from web interface
 - SASL GSSAPI support, e.g. for Kerberos authentication and encryption
 - Identity sync with Windows 2000 Active Directory, Windows NT SAM Registry

Red Hat Directory Server – What's new

- Windows sync -
 - Directory Server Windows Sync – Red Hat Directory Server leverages the Multi-Master Replication Plug-in to synchronize user and group entries.
 - Password Sync Service - This application captures password changes for Windows users and relays those changes back to the Directory Server over LDAPS.



Red Hat Directory Server – What's new

Configuring Windows Sync -

Step 1: Configure SSL on Directory Server

Step 2: Configure the Active Directory Domain

Step 3: Select or Create the Sync Identity

Step 4: Install and Configure the Password Sync Service

Step 5: Configure the Directory Server Database for Synchronization

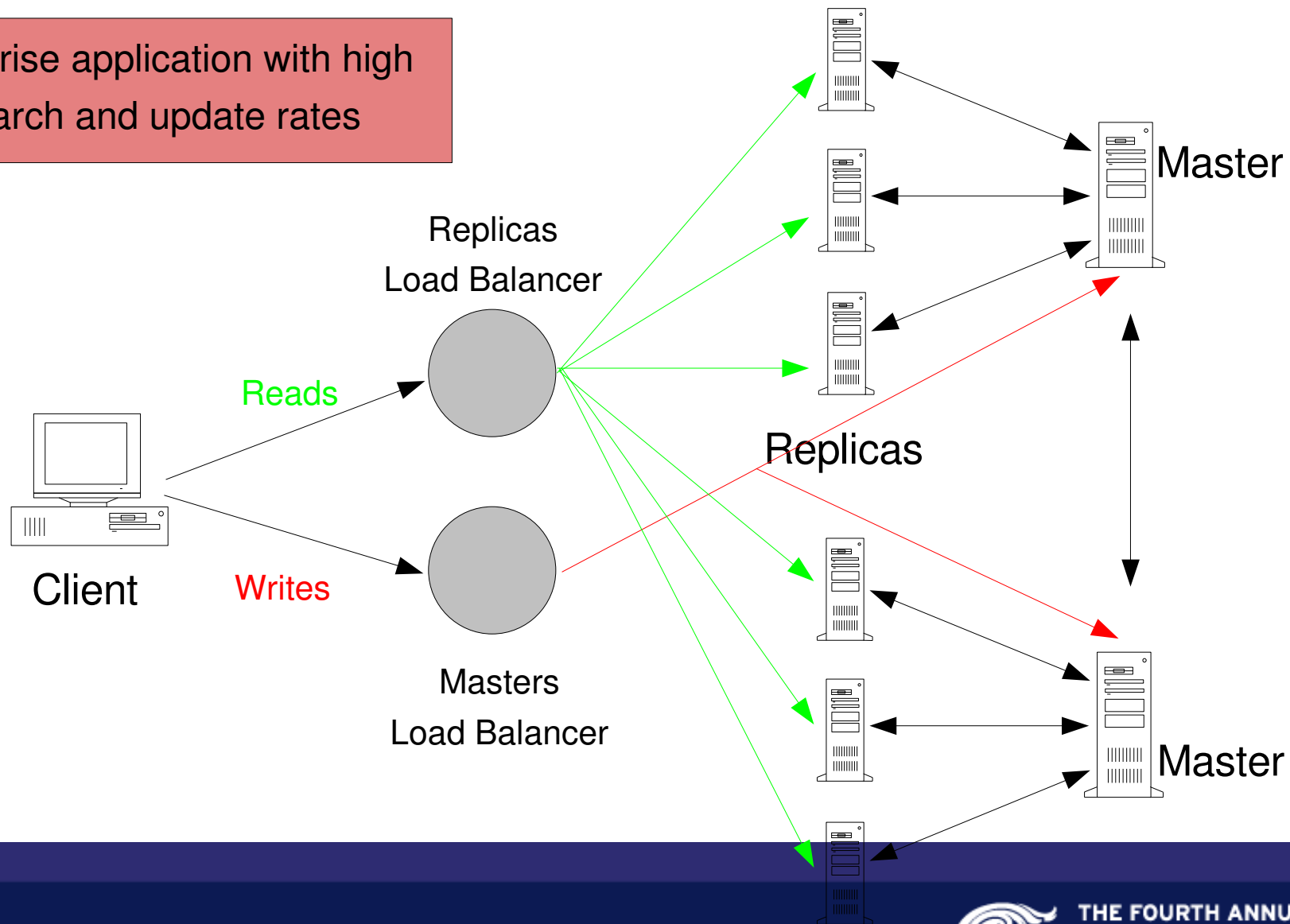
Step 6: Create the Synchronization Agreement

Step 7: Begin Synchronization

Directory Server deployment scenario - MMR

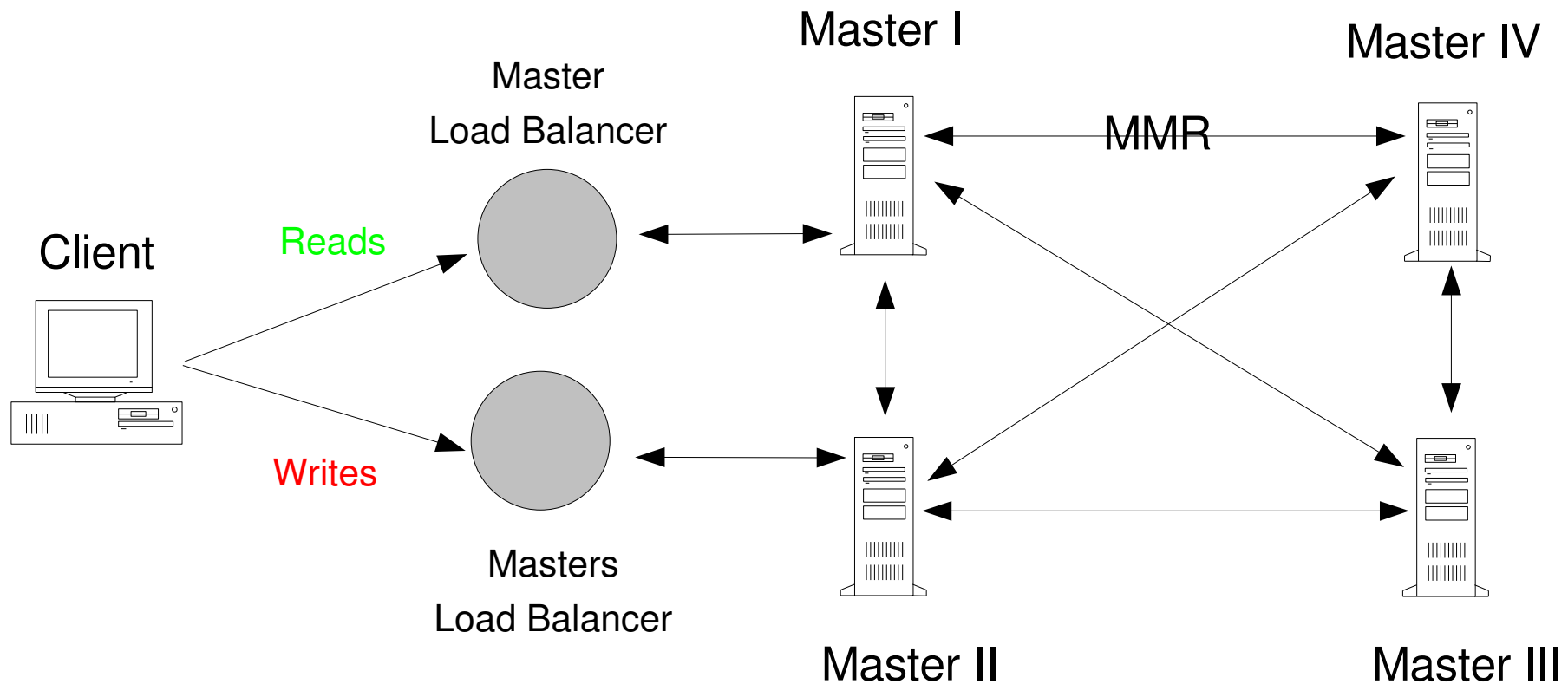
Example: Frequent Searches/Updates

Enterprise application with high search and update rates



Directory Server deployment scenario - MMR

Example: Frequent Searches/Updates



Red Hat Certificate System - Main Components

- **Certificate Authority (CA):** Issues X.509 digital certificates and CRLs
- **Token Management:**
 - **Token Processing System (TPS) & Token Key Service (TKS)**
 - Supports Global Platform smartcards
 - Makes smartcards as easy to use as an ATM
 - Manages symmetric keys for securing communication to tokens

Red Hat Certificate System - Main Components

- **Data Recovery Manager (DRM):**
 - Secure repository for backup/recovery of user's private keys
 - Configurable multi-person approval for recovery
- **Online Certificate Status Protocol (OCSP) Responder:**
 - Responds to OCSP requests to verify certificate validity in real time
- **Enterprise Security Client (ESC):**
 - Multiplatform middleware package
- **Registration Manager / Authority**

Red Hat Certificate system deployment scenario

- VPN certificates
- Code signing certificates
- Signing and encryption of email
- Secure Partner / Customer login to portal
- Health Care
 - Technical and operational PKI interoperability between healthcare providers, partners, affiliates, and patients.
 - Privilege management in healthcare
 - Long-term storage of electronic medical records.

Red Hat Certificate system deployment scenario

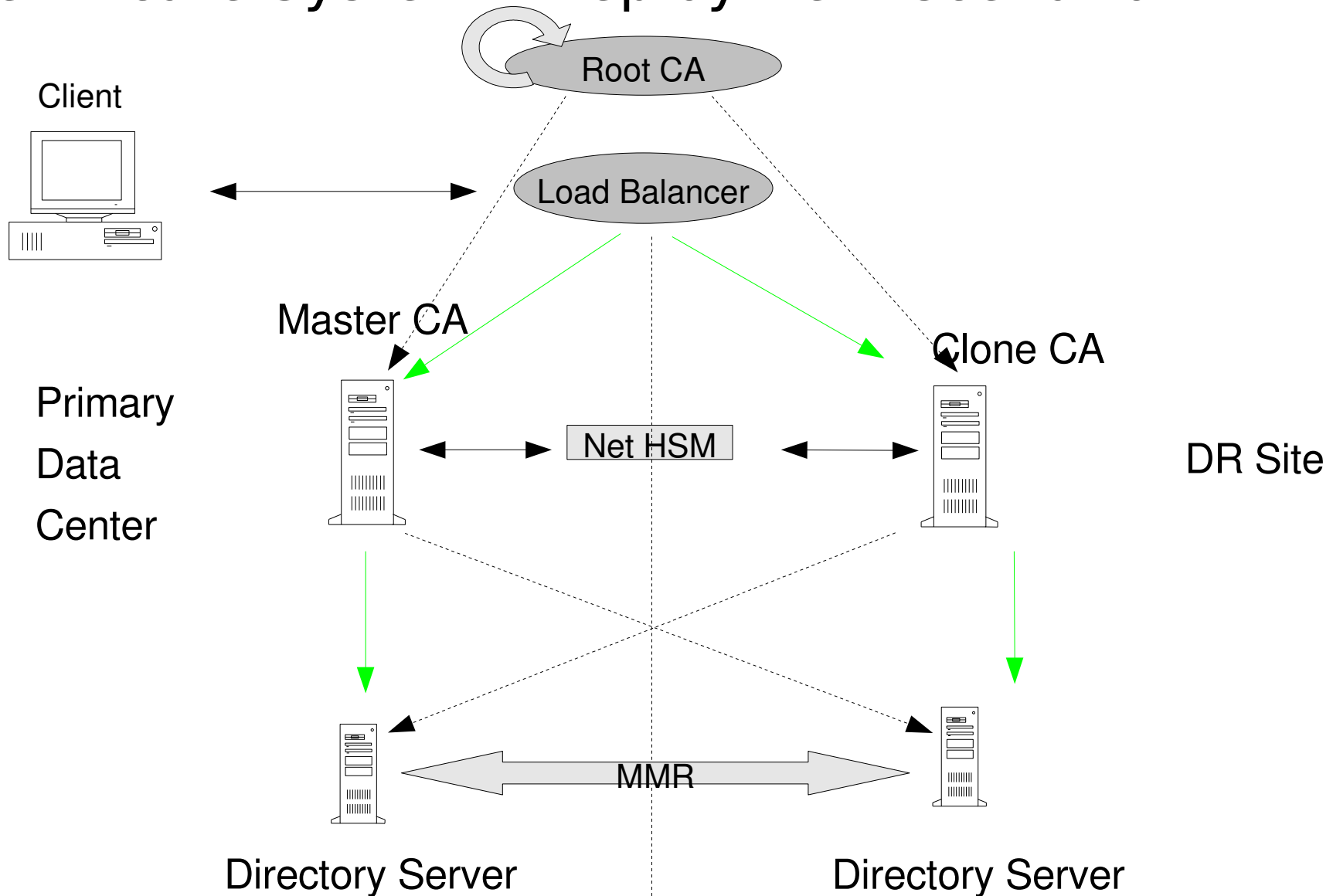
- Certificates to Routers and other devices
- Stock Exchange
- Single Sign on [SSO]
- Network Login
- US Dept of Defense [<http://iase.disa.mil/pki/>]
 - Portals, Applications, CAC cards

Red Hat Certificate system deployment scenario

- Regulations driving use of PKI
 - HIPAA healthcare
 - HSPD#12 / FIPS 201 federal government
 - Sarbanes Oxley: - Track Information about how significant transactions are initiated & authorized
Controls over safeguarding of assets.
- Gramm-Leach-Bliley:

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information

Certificate System - Deployment scenario



Questions



- You can contact me at srs@redhat.com
- Thanks for your time !!

HEADLINE | LIBERATION SANS BOLD | Size 28

- Bullet 1 | Liberation Sans | Size 24
- Bullet 2
- Bullet 3
- Bullet 4