Hardware and Software Tools for the Oracle Fusion Middleware Architect

Arijit Das, Greg Belli, Tony Kendall, Erik Lowney, Riqui Schwamm

Presentation Outline

- Who we are (our Mission)
- Our Challenge: Replace our KM Portal
- Quick overview of our current KM Portal
- Overview of the replacement KM Portal Using Oracle Beehive and Portal 11g.
- Review of the tools, tips and techniques learned in building the new KM portal.

Our Mission

- The Distributed Information Science and Experimentation (DISE) uses KM/Collaborative tools for DOD experimentation.
- Example: the annual Trident Warrior (TW) exercise.
- During the whole process (preparation, execution, reporting) collaboration and exchange of documents takes place in a web workspace.

The Challenge

- Replace an aging OCS (Oracle Collaboration Suite) with KM Portal Using Beehive and Oracle 11g Portal

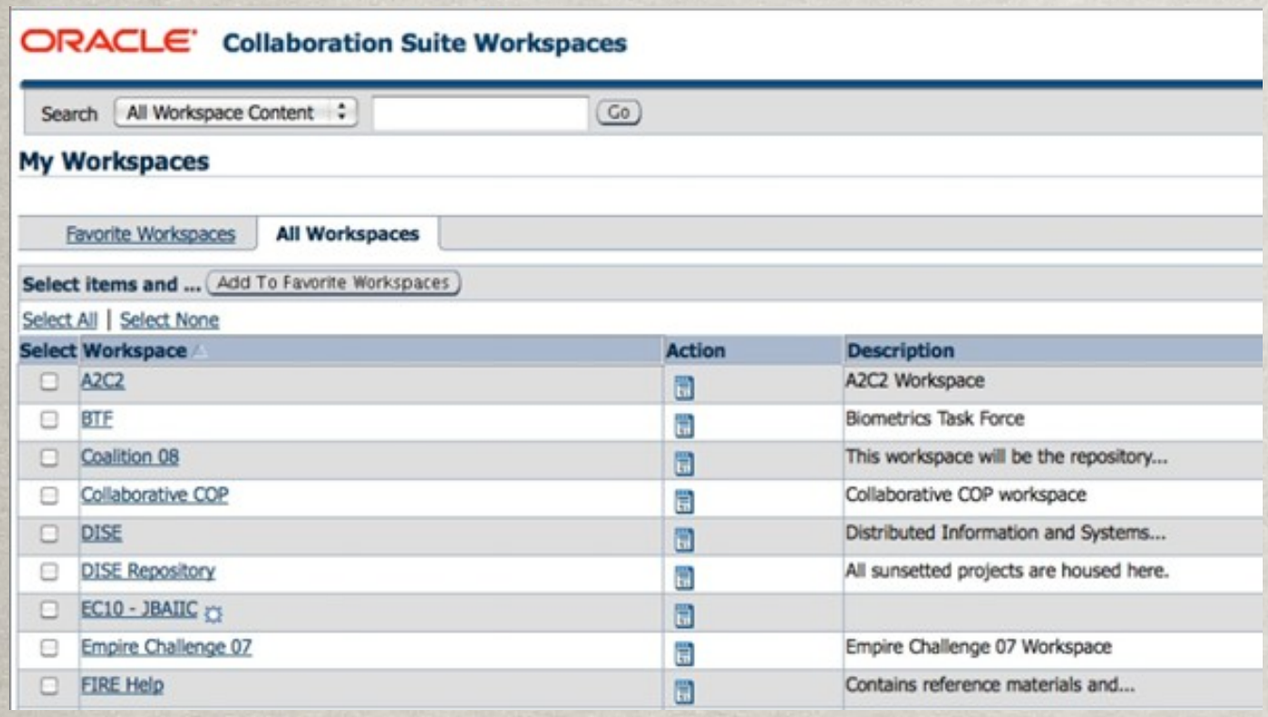
- Limited Resources
  - Small Team
  - Security and IA constraints
  - Small Budget

Beehive Licensing

- Navy has been given a site-wide license for Oracle
- DISE pays for Fusion Middleware license.
- Perpetual License $30 to $100 per user (GSA $48)
- Support costs from $11 to $22 per user.
- Tip: User 3rd party such as SEWP (Solutions for Enterprise-Wide Procurement.
- Tip: Do a cost analysis on two basic licensing options (per CPU vs. per user)

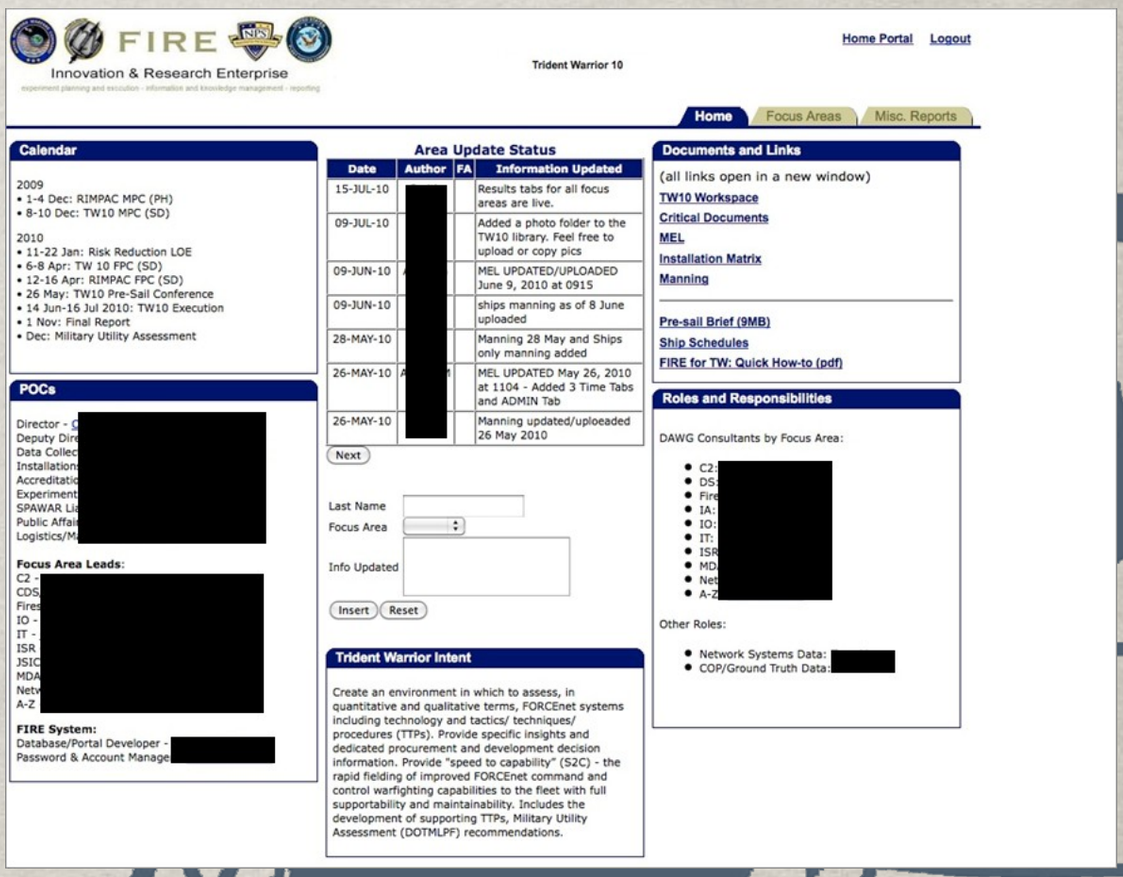
FIRE KM (Current)

Collaboration (OCS)



- workspaces
- email
- tasks and calendar
- content services (library)
- web conferencing

FIRE KM Portal (Oracle App Server)



- focus areas and forms
- reports
- other portlets (applications within the web page)

Next Generation Fire

- Two Oracle products replace the aging OCS
  - Beehive replaces the collaboration tools
  - Oracle Portal 11g/WebLogic replaces Oracle App Server (Experiment development area—the portal)

- Modular and more scalable than OCS

- Compatible with Windows 7 and Mac
- No new licensing costs. Upgrade from OCS license.

New FIRE (Portal Side)

FIRE

Forces Innovation & Research Enterprise

experiment planning, execution and analysis - program, information and knowledge management

FIRE Home Portal

FIRE Home | Account Info | Help | Logout

Links

- My Workspaces
- My Team Collaboration
- Beehive Central
- Downloads

Experiment Development Links

HAF A2Q
- BLOS
- TACPOD

Trident Warrior
- Trident Warrior 12 (other system)

JBAIIC
- EC 11 (other system)

Archived Projects

Any project that is neither current nor listed under "Experiment Development Links" has been archived. Archived projects have restricted access. If you require access to view a specific project archive, please contact your Project PI.

Notices

Help Center

For frequently asked questions and instructions for various sections and features of FIRE see the FIRE Help Center workspace.

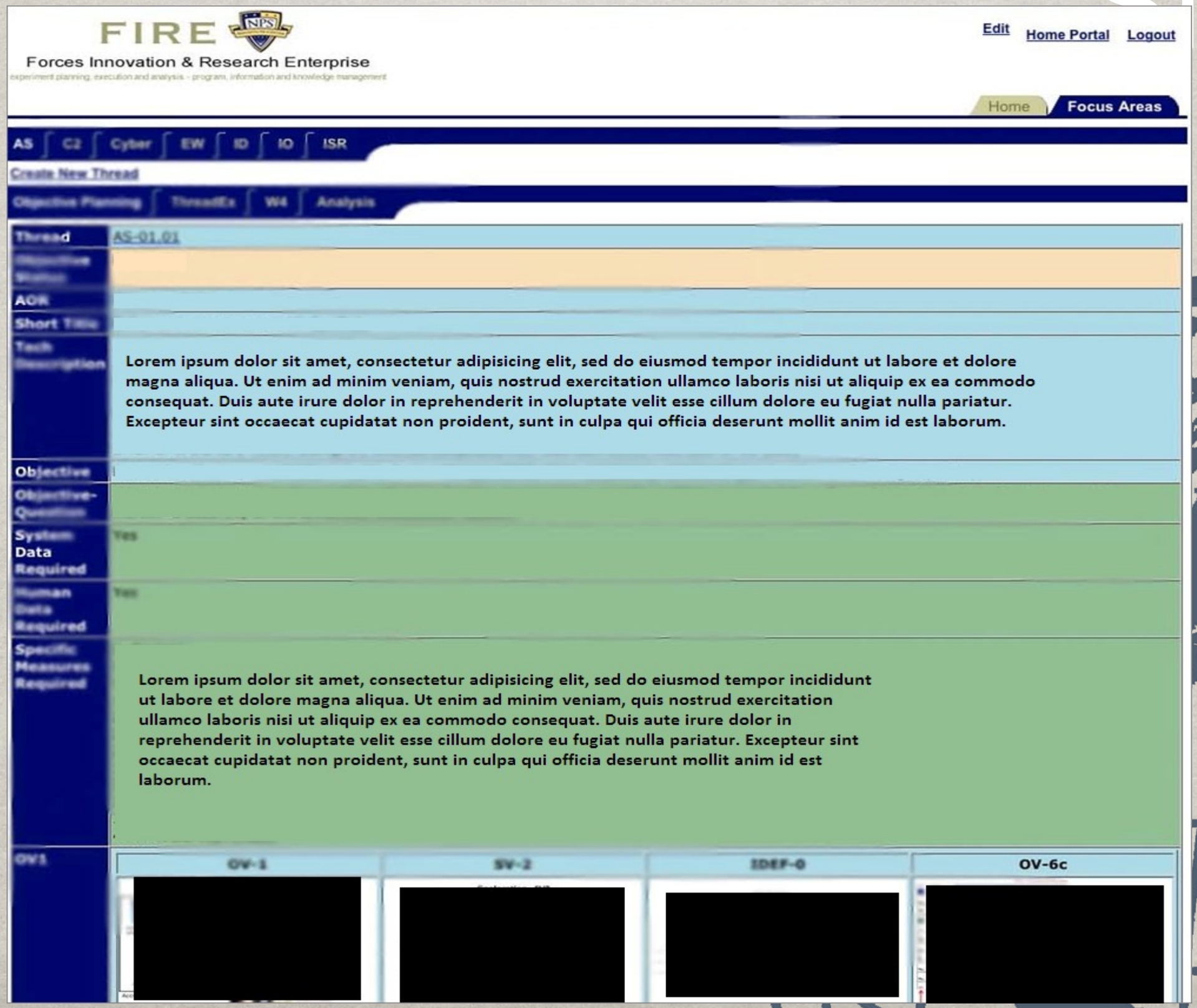
Quick Help Links
- Email the DISE Help Desk
- Submit a Trouble Ticket (a .docx file, save to your desktop)
- How to: Passwords
- Experiment Development Help

Other Links
- About FIRE
- About DISEsurveyor
- About DISE

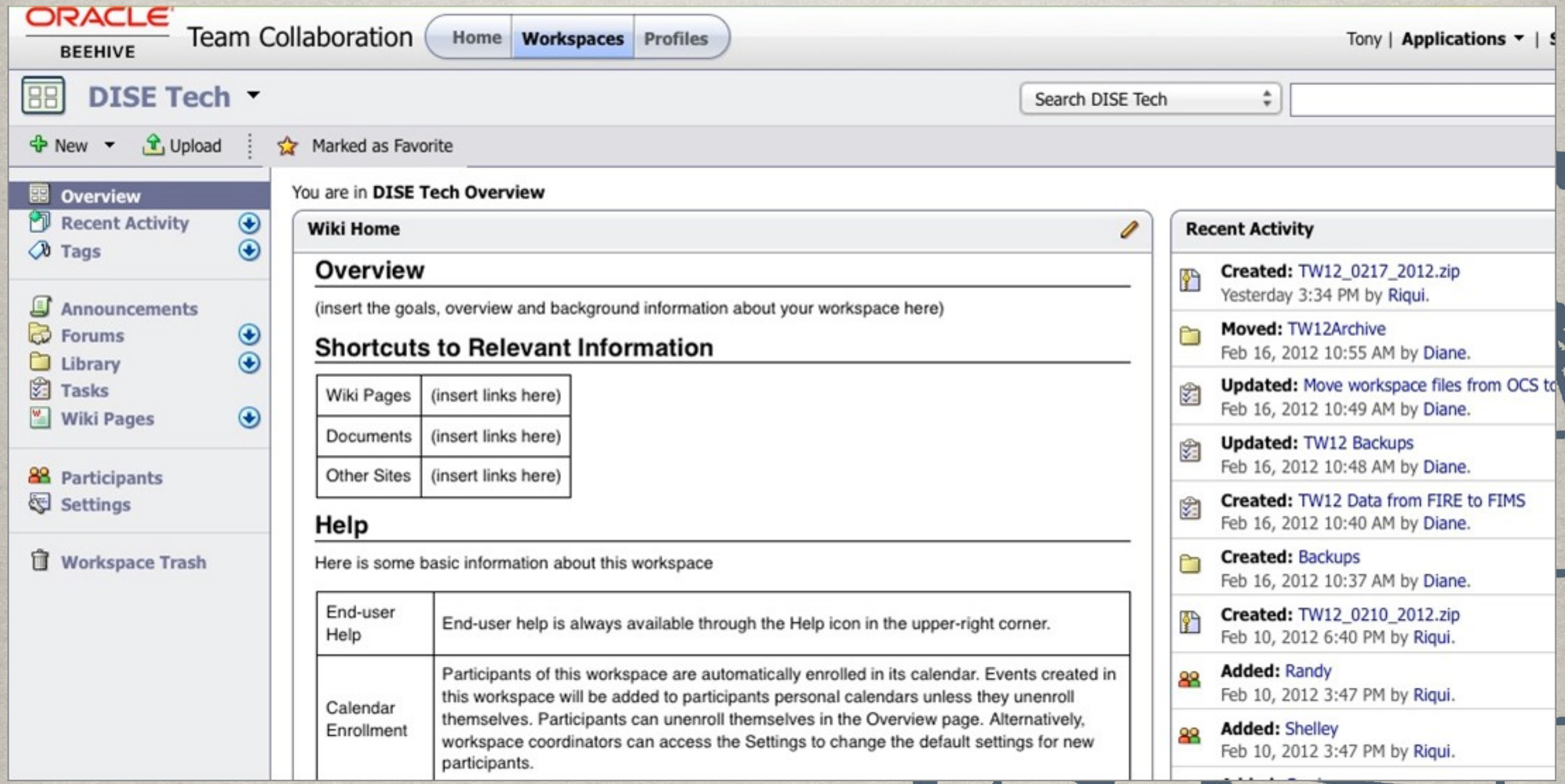
About

The Forces Innovation & Research Enterprise (FIRE) is administered by the Distributed Information Systems Experimentation (DISE) Group at Naval Postgraduate School.

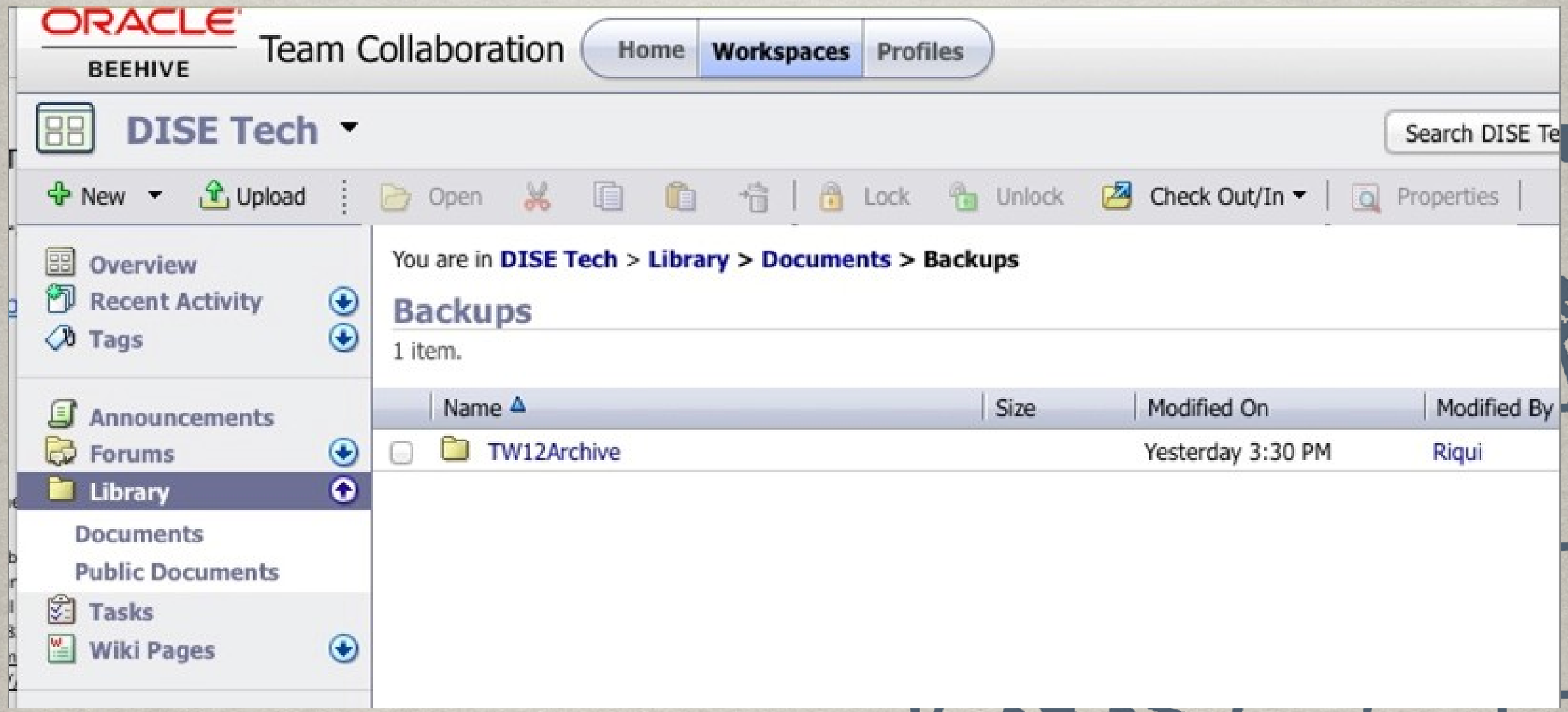
New FIRE (Portal Side)



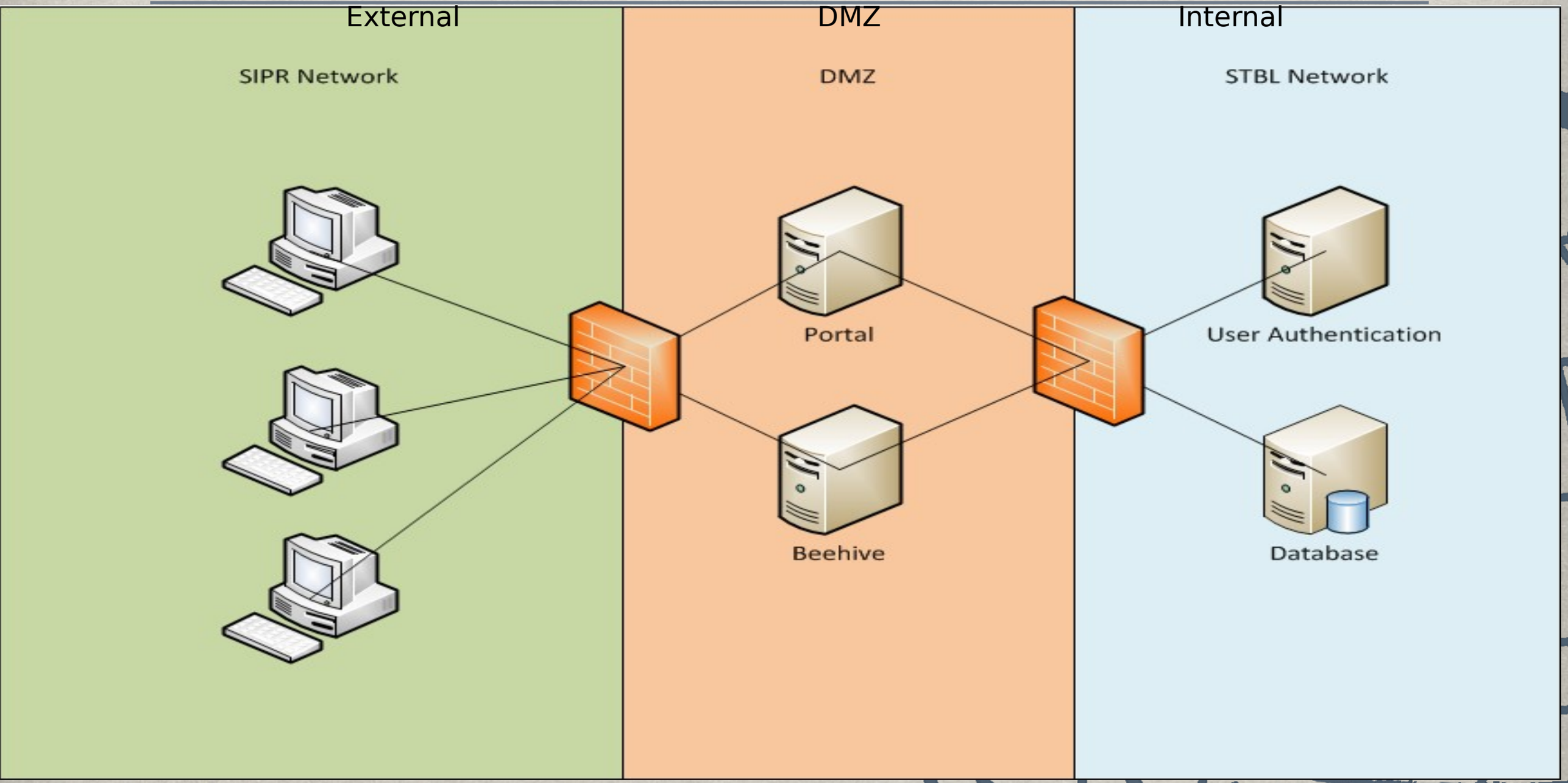
New FIRE (Beehive Side)



New FIRE (Beehive Side)

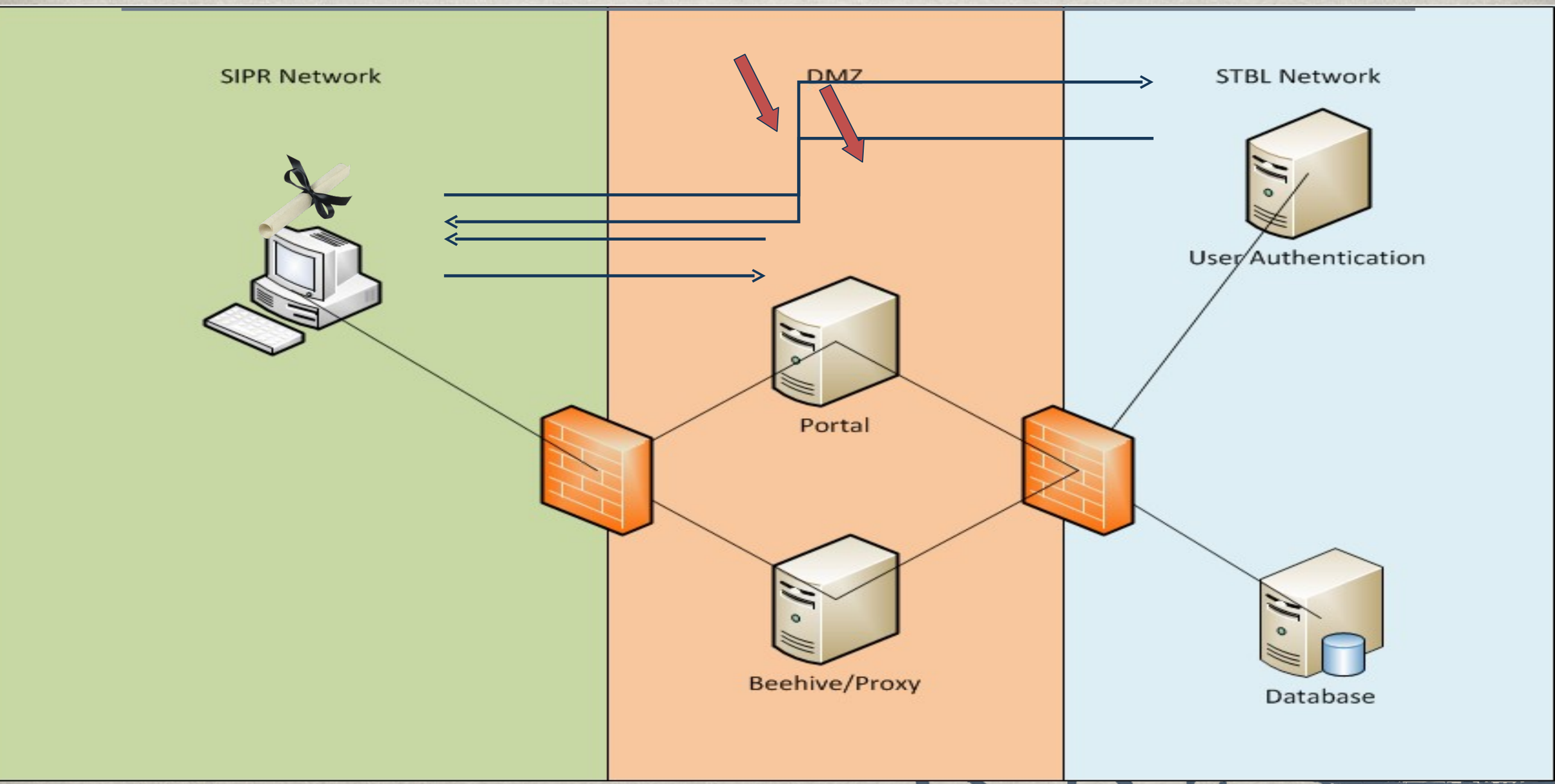


Architecture Overview



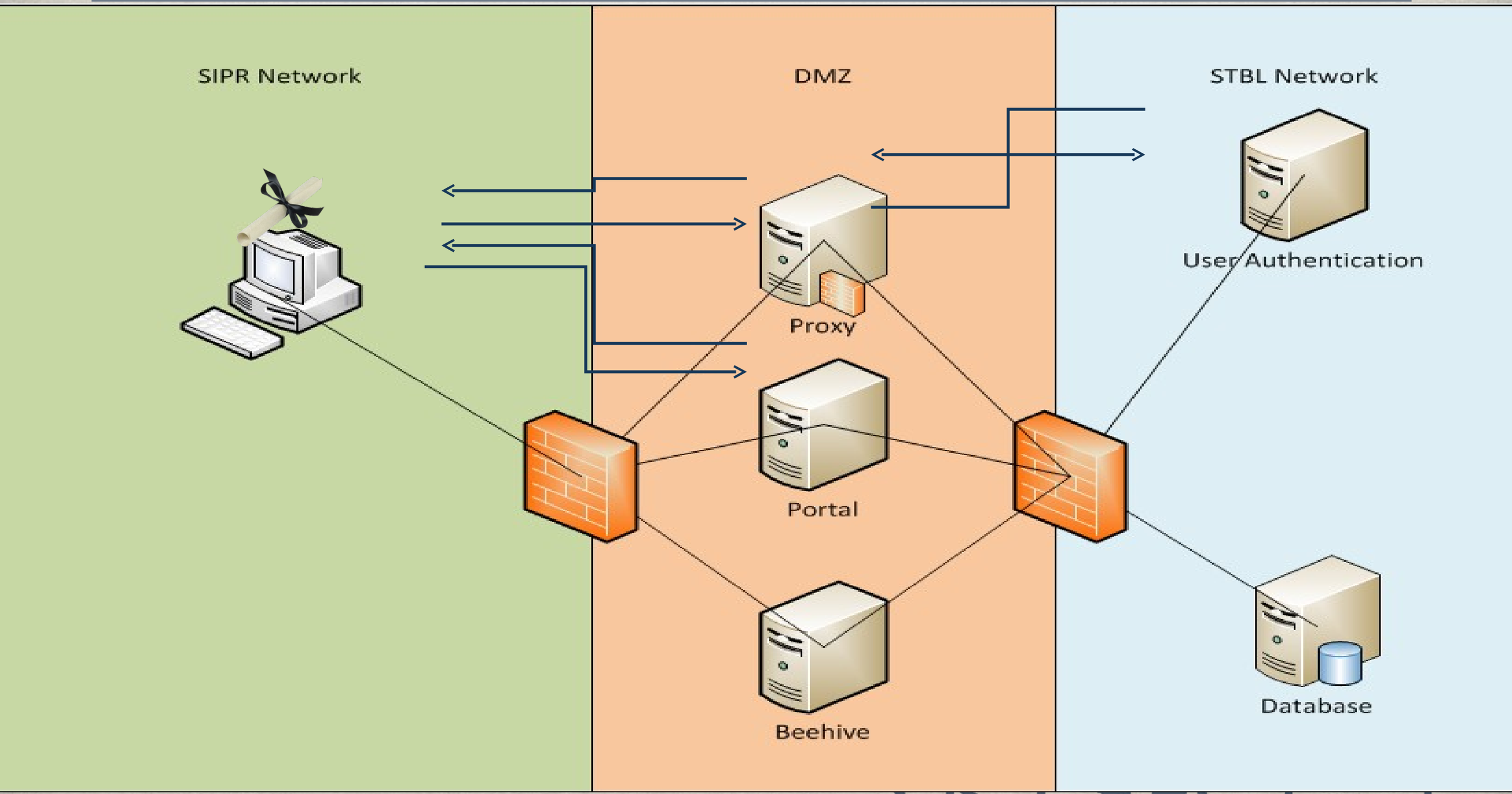
The Problem

External DMZ Internal



The Solution

External DMZ Internal



Reverse Proxy

Squid Proxy Server

Why we chose Squid

- Easy to setup
- Free
- Preapproved by DoD/IA
- Oracle options not suitable

Reverse Proxy

Squid Proxy Server

Technical Considerations

- Proxy on an existing server
- Use a default HTTPS port

Problem

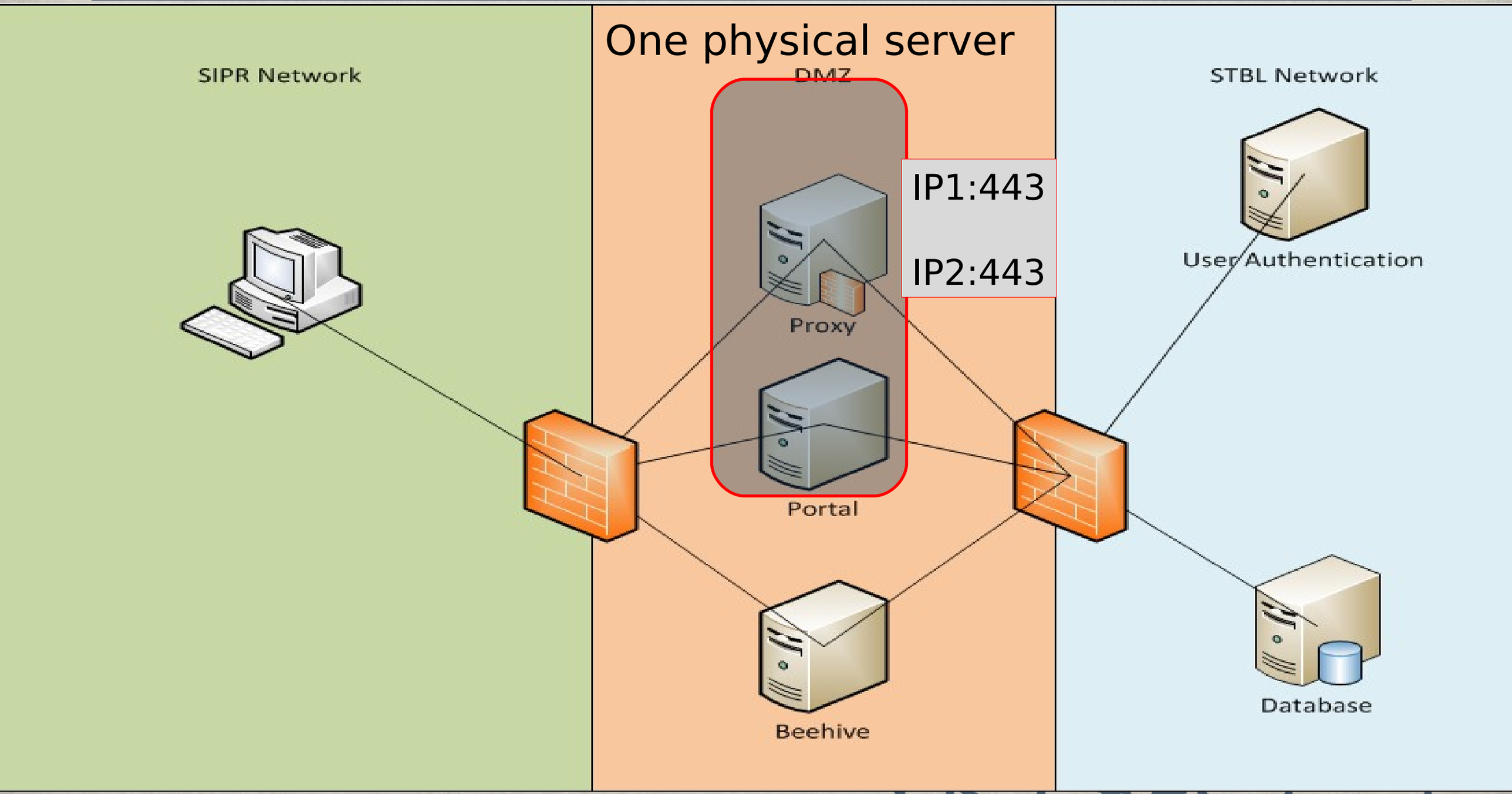
- The port is already in use

Solution

- New hostname/IP address for the reverse proxy

The Solution

External | DMZ | Internal



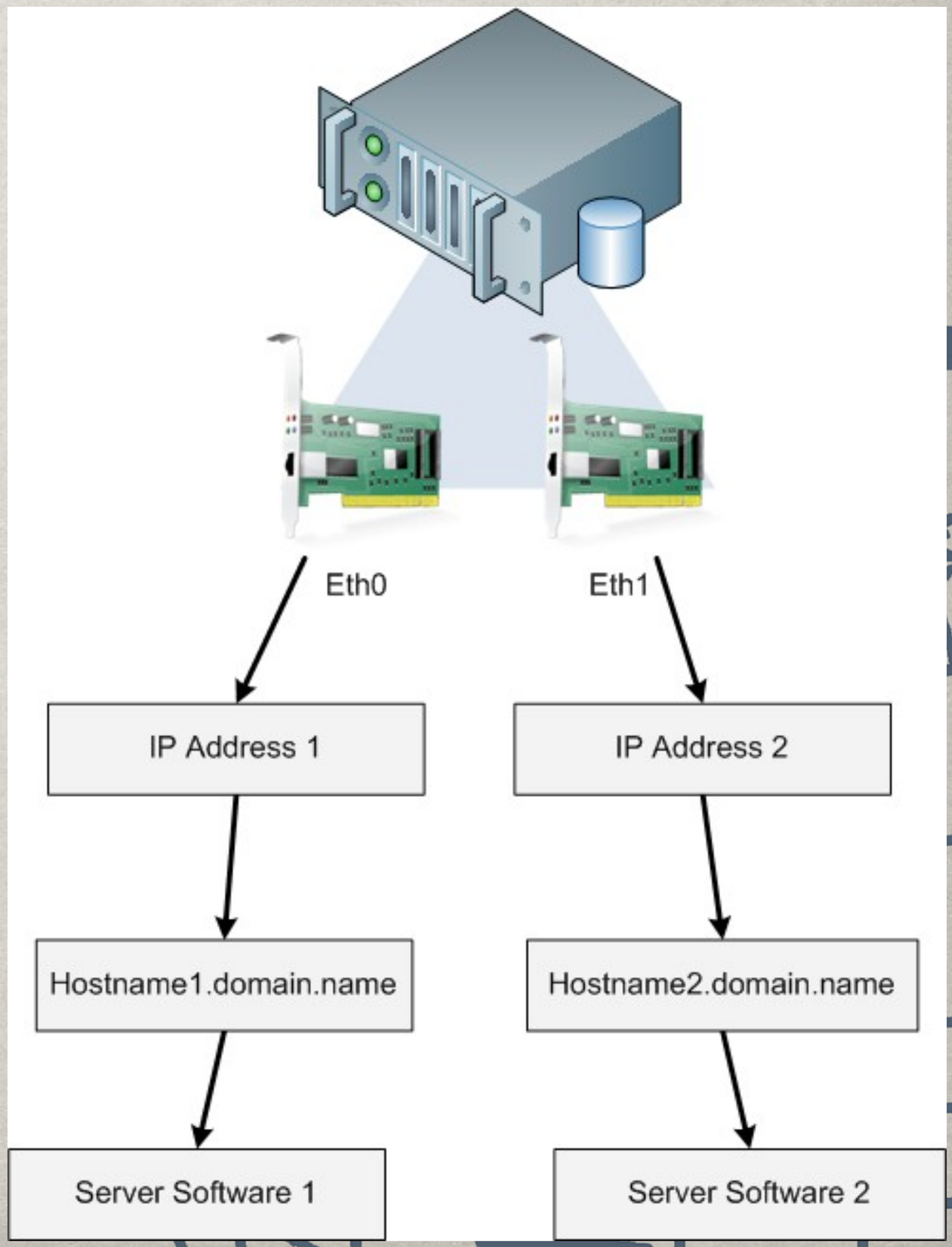
Running Simultaneous Software Systems

- Need to run several software systems.
- Hardware is limited
- Need to use one physical server for all systems
  - Limited by heat
  - Power
  - Rack space
- Hardware is fast enough to run multiple software systems
- Each software system has its own network card but share CPU and RAM

Running Simultaneous Software Systems

Each server software can run its own:

- Port number
- Domain name
- SSL certificate



Interface to IP Mapping

ssign each IP address to the appropriate physical interfac

etc/sysconfig/network-scripts/ifcfg-eth0

```
# Broadcom Corporation NetXtreme II BCM5709 Gigabit Ethernet
DEVICE=eth0
BOOTPROTO=static
DHCPCLASS=
HWADDR=18:03:33:00:11:22
IPADDR=192.168.1.1
NETMASK=255.255.255.0
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-eth1

```
# Broadcom Corporation NetXtreme II BCM5709 Gigabit Ethernet
DEVICE=eth1
BOOTPROTO=static
DHCPCLASS=
HWADDR=18:03:33:00:11:44
IPADDR=192.168.1.2
NETMASK=255.255.255.0
ONBOOT=yes
```

IP to Hostname Mapping

Assign a unique hostname to each IP address:

/etc/hosts

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
192.168.1.1     hostname1.domain.name
192.168.1.2     hostname2.domain.name
```

Kickstart Tool

Problem:

Standard Red Hat installation not IA/Oracle Compliant

Solution:

Red Hat's Kickstart tool automates the installation process to ensure IA/Oracle compliance

Benefits:

- A standard base installation to follow best practices
- Time saving
- Post install script preconfigures the system

Kickstart Tool

A kickstart file consists of three pieces:

- Red Hat Anaconda (Installation) instructions/script installs the OS
- A list of software packages to install or remove
- A post-install shell script to customize the installation

Kickstart Script

Sample Post Install Script

```
# Post-install script

%post --log=/var/log/kickstart.log
#!/bin/bash
groupadd oinstall
groupadd dba
useradd -g oinstall -G dba oracle
mkdir /opt/app
mkdir /opt/oracle
sed -ri 's/^#?
PermitRootLogin.*/PermitRootLogin no/'
/etc/ssh/sshd_config
```

Oracle customizations

IA compliance customizations

IA Considerations

Information Assurance is:

- The practice of managing risks related to the use, processing, storage, and transmission of information
- A challenge for a small team in a large enterprise

IA is a major factor in system design and maintenance

IA Examples

```
# GEN004000 (G633)
# This effectively prevents any non-root user from running
traceroute
echo "Locking down GEN004000"
chmod 700 /bin/traceroute
chmod 700 /bin/traceroute6
echo "GEN004000 Complete"

# GEN005400 (G656)
# Reset the permissions to a DISA-blessed rw-r-----
echo "Locking down GEN005400"
#chmod 640 /etc/syslog.conf

# Not good enough for SECSCAN, lock it down more

chown root:root /etc/syslog.conf
chmod 600 /etc/syslog.conf

echo "GEN005400 Complete"
```

IA Examples

```
# Search and replace entries in the SSHd configuration file

# Set maximum authorization retries to 1

sed -ri 's/^#?MaxAuthTries.*/MaxAuthTries 1/'
/etc/ssh/sshd_config

#  Prevent logins with blank passwords

sed -ri 's/^#?PermitEmptyPasswords.*/PermitEmptyPasswords
no/' /etc/ssh/sshd_config

# Increase the logging level from the default

sed -ri 's/^#?LogLevel.*/LogLevel INFO/' /etc/ssh/sshd_config
```

Red Hat Automated Install

Installation and configuration of Red Hat servers for Oracle software is a time-intensive task.

We developed a way to automate this process as much as possible using 3rd party multi-boot CD creation tools.

Installation options:

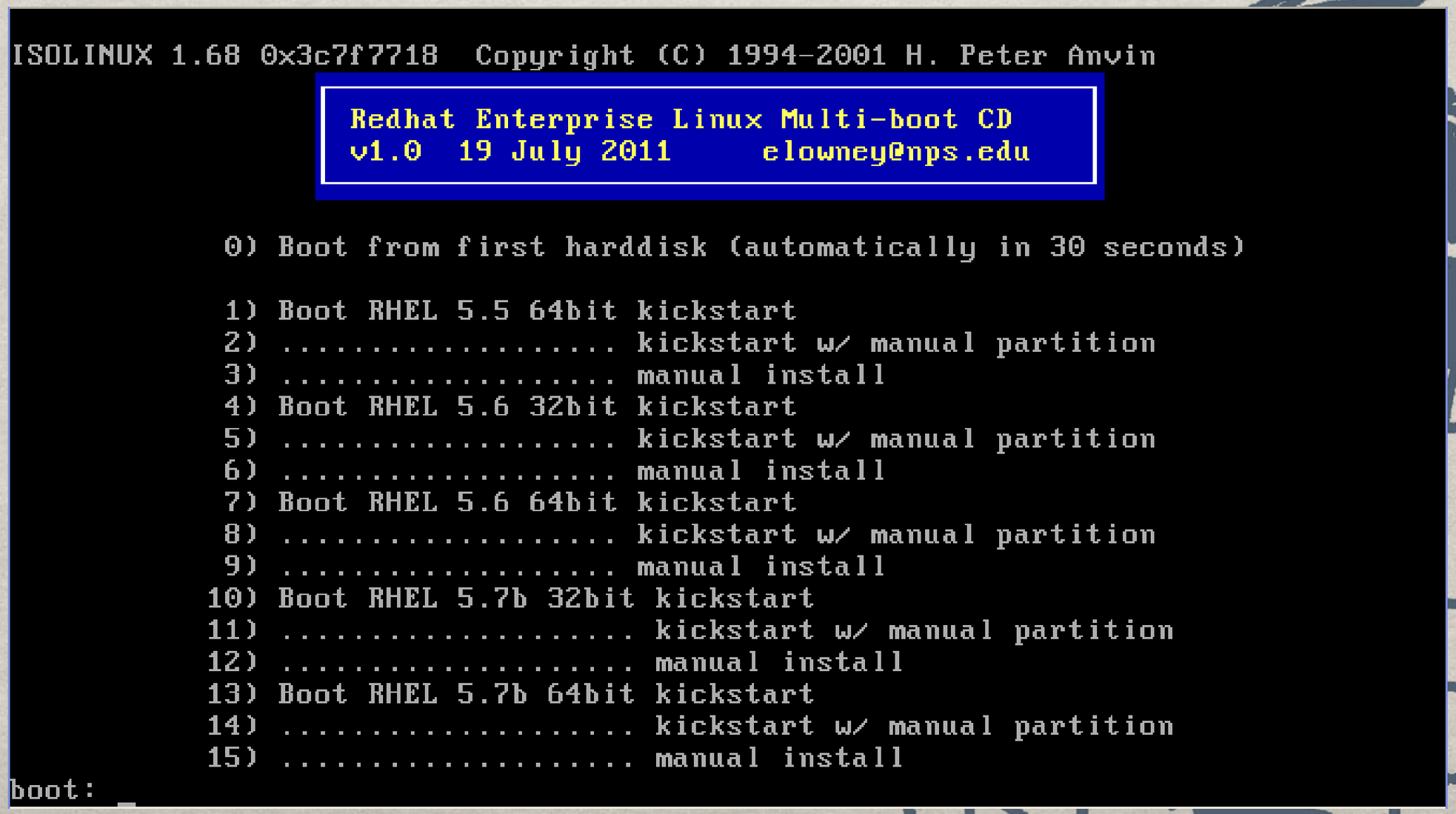
- Red Hat version (5.5, 5.6, etc).
- 32-bit vs. 64-bit
- Choice of Kickstart scripts

Automated installation reduces installation time and effort

Simple to create a standardized deployment using an

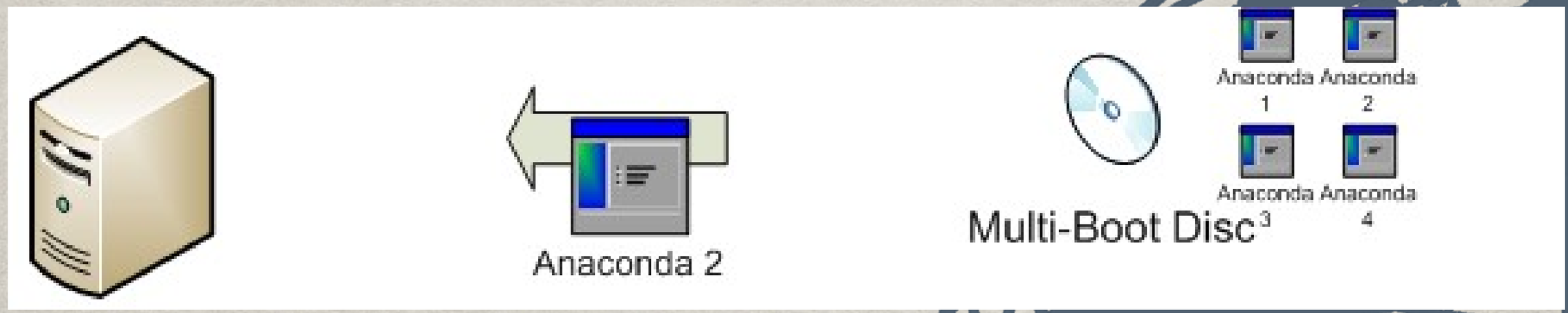
Automated Installation Process

- Step 1: User boots off customized multi-boot CD. User selects desired Red Hat and kickstart combination. This is the first and only interaction the user has during this process.



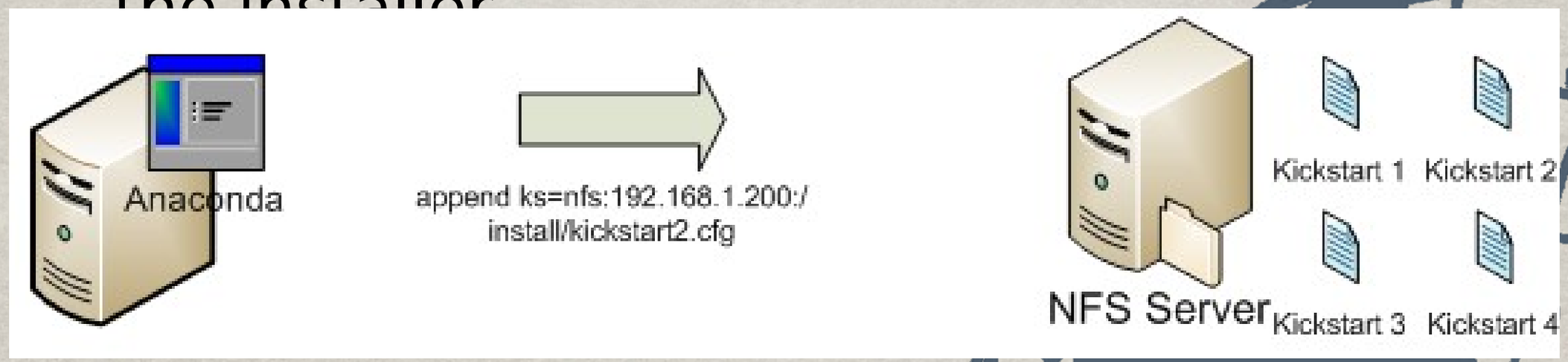
Automated Installation Process

- Step 2: The corresponding Red Hat installer is retrieved off of the Multi-boot CD and starts.



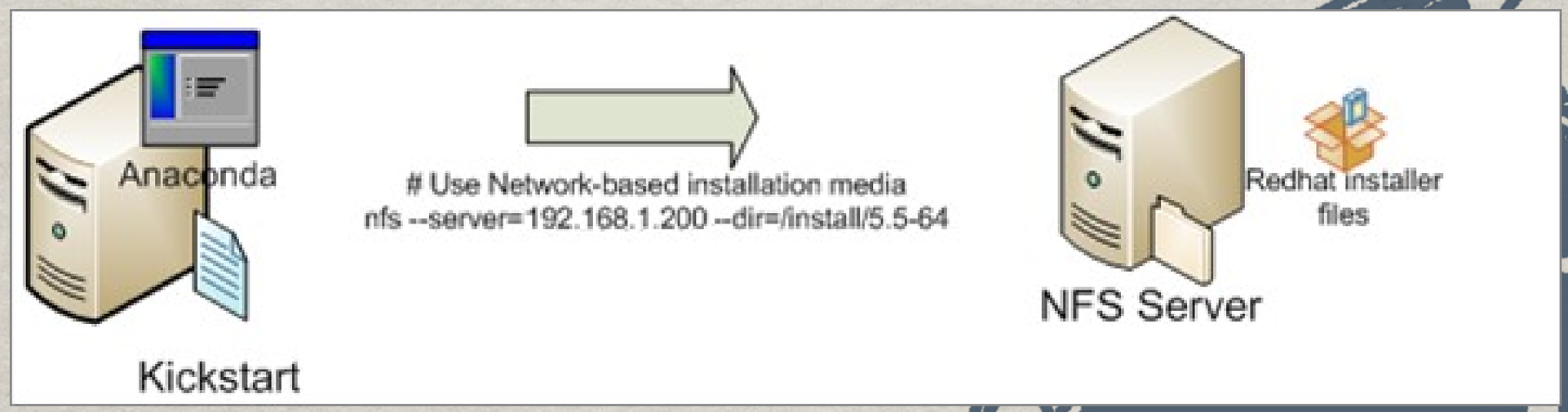
Automated Installation Process

- Step 3: The installer retrieves the appropriate kickstart file located on a NFS share – this is passed via command line to the installer



Automated Installation Process

- Step 4: The installer runs the kickstart file. The kickstart file directs the installer to retrieve the appropriate Red Hat installation media from a NFS share.



Automated Installation Process

- Step 5: Red Hat is installed according to the directives in the kickstart. After installation, a post-install script is run to customize the system.

- The end of the script directs the installer to eject the boot disc and restart the server.

Kickstart script

```
# Post-install script

%post --log=/var/log/kickstart.log
#!/bin/bash
groupadd oinstall
groupadd dba
useradd -g oinstall -G dba oracle
```

Certificates

Certificates used to secure communication

Decide what communication will be secured

- User ←→ Proxy
- User ←→ Portal
- User ←→ Beehive

Each service uses a different method for setting up SSL

- Portal uses WebCache
- Beehive uses Application Server with wallet

Certificates

Configuring Certificates for Middleware

1. Generate a Certificate Request
   - Beehive: Oracle Wallet
   - Oracle Portal: WebCache keystore
2. Submit Certificate Request to the Certificate Authority
3. Import the signed certificate into the Middleware software
   - Beehive: Oracle Wallet
   - Oracle Portal: WebCache keystore
4. Configure SSL for Portal and Beehive
   - Beehive: Quick and Easy
   - Portal: 60+ steps

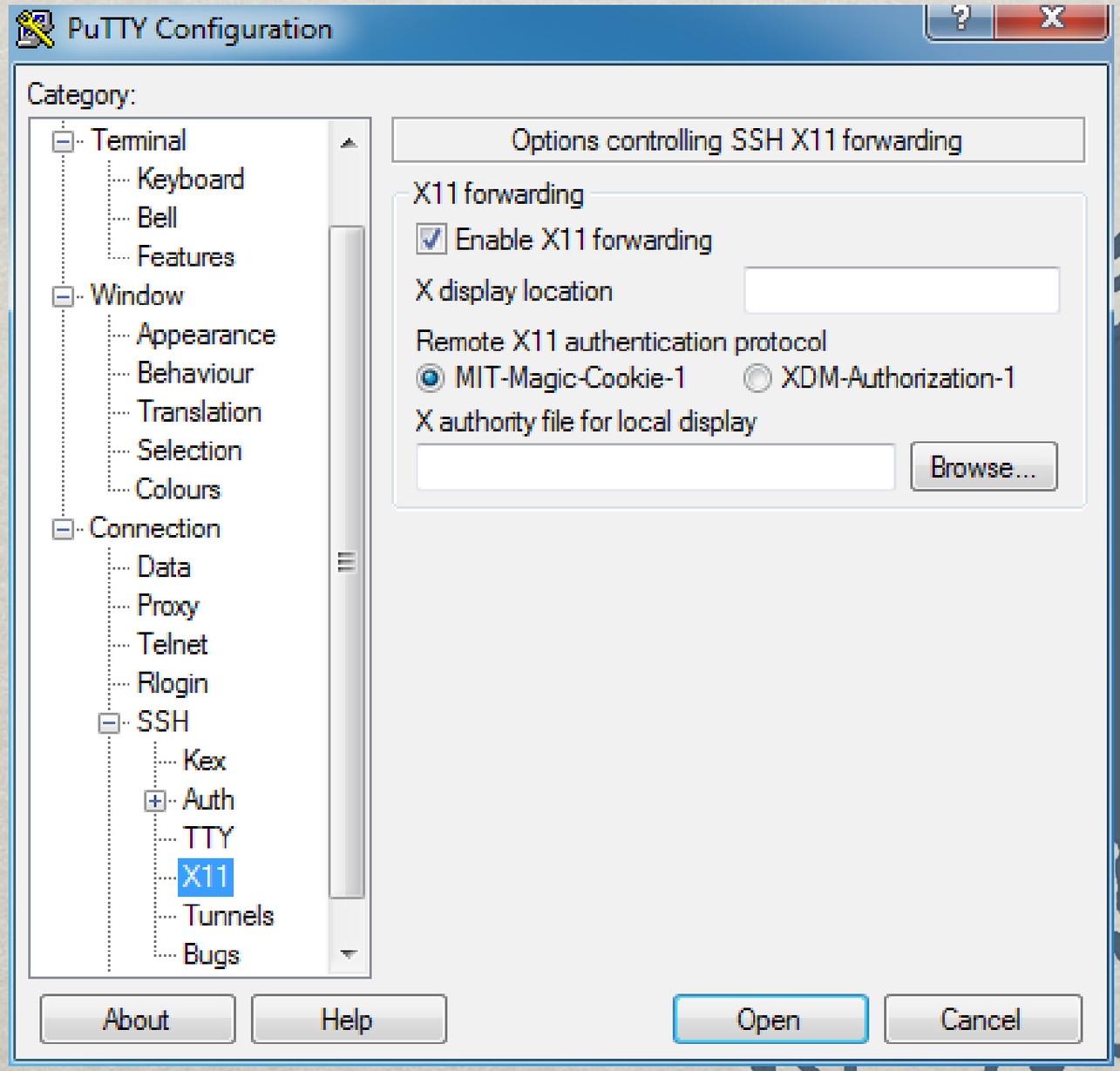
Remote Administration

PuTTY with Cygwin/X can be used to remotely run Xwindows applications such as Oracle Universal Installer and administration applications(oidadmin)

Benefits:

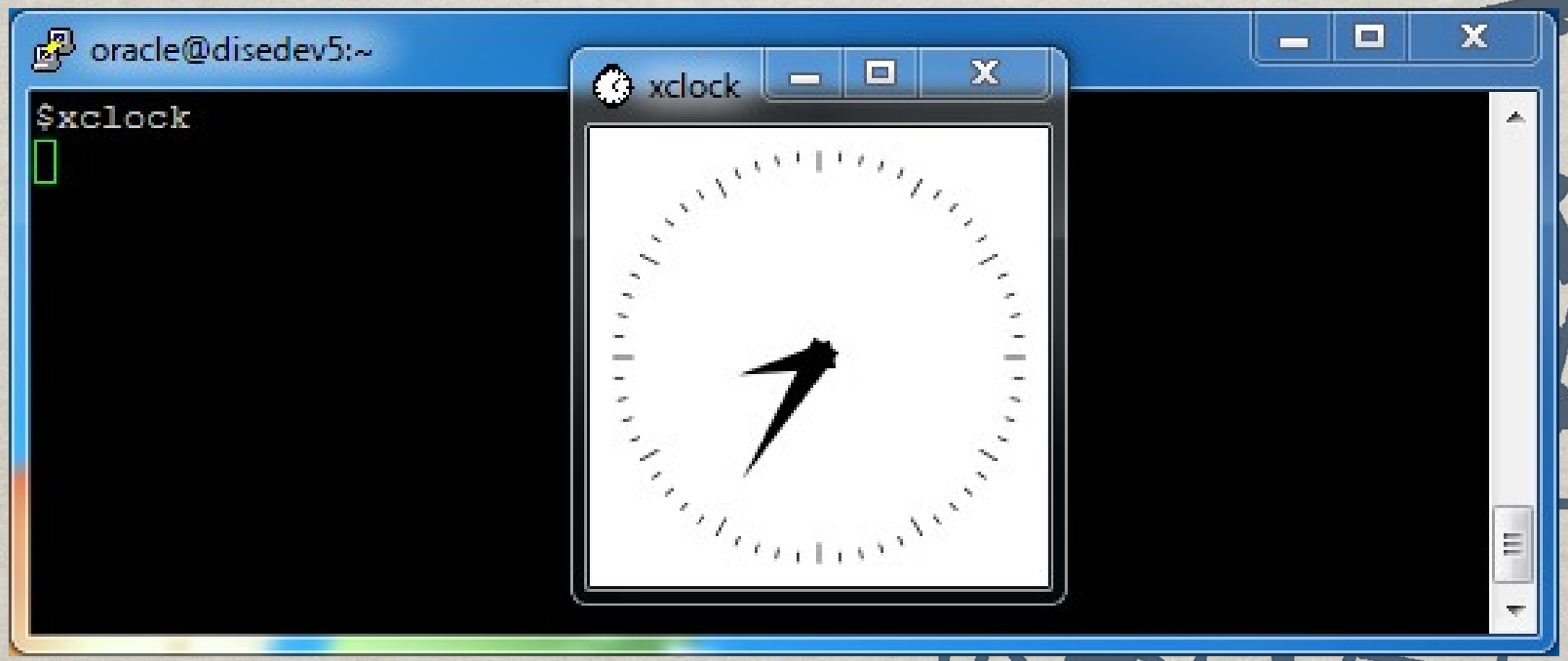
- Free and easy to use
- Works with any SSH client and Xserver software
- Can remotely setup and administer the system

PuTTY Setup


PuTTY Configuration
Category:
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Tunnels
Bugs
Options controlling SSH X11 forwarding
X11 forwarding
Enable X11 forwarding
X display location
Remote X11 authentication protocol
MIT-Magic-Cookie-1
XDM-Authorization-1
X authority file for local display
Browse...
About
Help
Open
Cancel

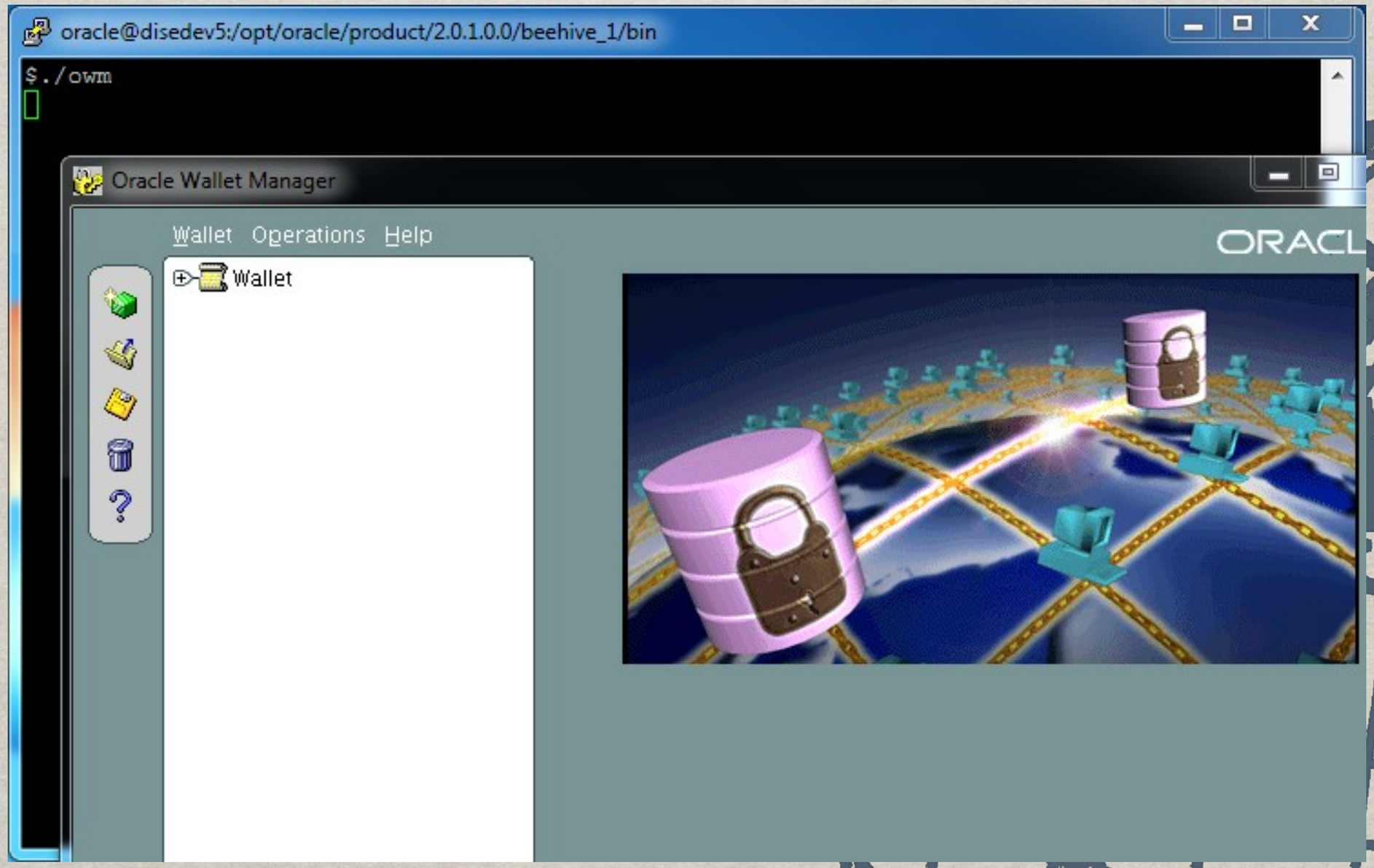
Remote Administration

xclock displaying on the MS Windows desktop



Remote Administration

Oracle Wallet Manager displaying on MS Windows



Quick Tips

- Beehive/Database Memory Tuning
  - Our servers have large amounts of RAM (32GB+)
  - Software doesn’t use all this RAM.
  - Memory settings can be tuned to utilize the physical RAM.
  - Two issues with memory tuning
    - Localizing the problem
    - Remedy

=== ODM Solution / Action Plan ===
increase the Java settings for the BEECORE, BEECLIENT and BEEAPP by running the following command
1.) Change the settings for the BEECLIENT container:

beectl modify_property --component BEECLIENT_<replace_by_beehive_instance_name>:StartJavaExecutionArguments --name MaximumHeapSizeInMB --value 1024

beectl modify_property --component BEECLIENT_<replace_by_beehive_instance_name>:StartJavaExecutionArguments --name InitialHeapSizeInMB --value 1024

beectl modify_property --component BEECLIENT_<replace_by_beehive_instance_name>:StartJavaExecutionArguments --name MaximumPermanentGenerationSizeInMB --value 1024

2.) Change the settings for the BEEAPP container:

beectl modify_property --component BEEAPP_<replace_by_beehive_instance_name>:StartJavaExecutionArguments --name MaximumHeapSizeInMB --value 1024

beectl modify_property --component BEEAPP_<replace_by_beehive_instance_name>:StartJavaExecutionArguments --name InitialHeapSizeInMB --value 1024

beectl modify_property --component BEEAPP_<replace_by_beehive_instance_name>:StartJavaExecutionArguments --name MaximumPermanentGenerationSizeInMB --value 1024

3.) change the setting for BEECORE:

beectl modify_property --component BEECORE_<replace_by_beehive_instance_name>:StartJavaExecutionArguments --name MaximumHeapSizeInMB --value 1024

beectl modify_property --component BEECORE_<replace_by_beehive_instance_name>:StartJavaExecutionArguments --name InitialHeapSizeInMB --value 1024

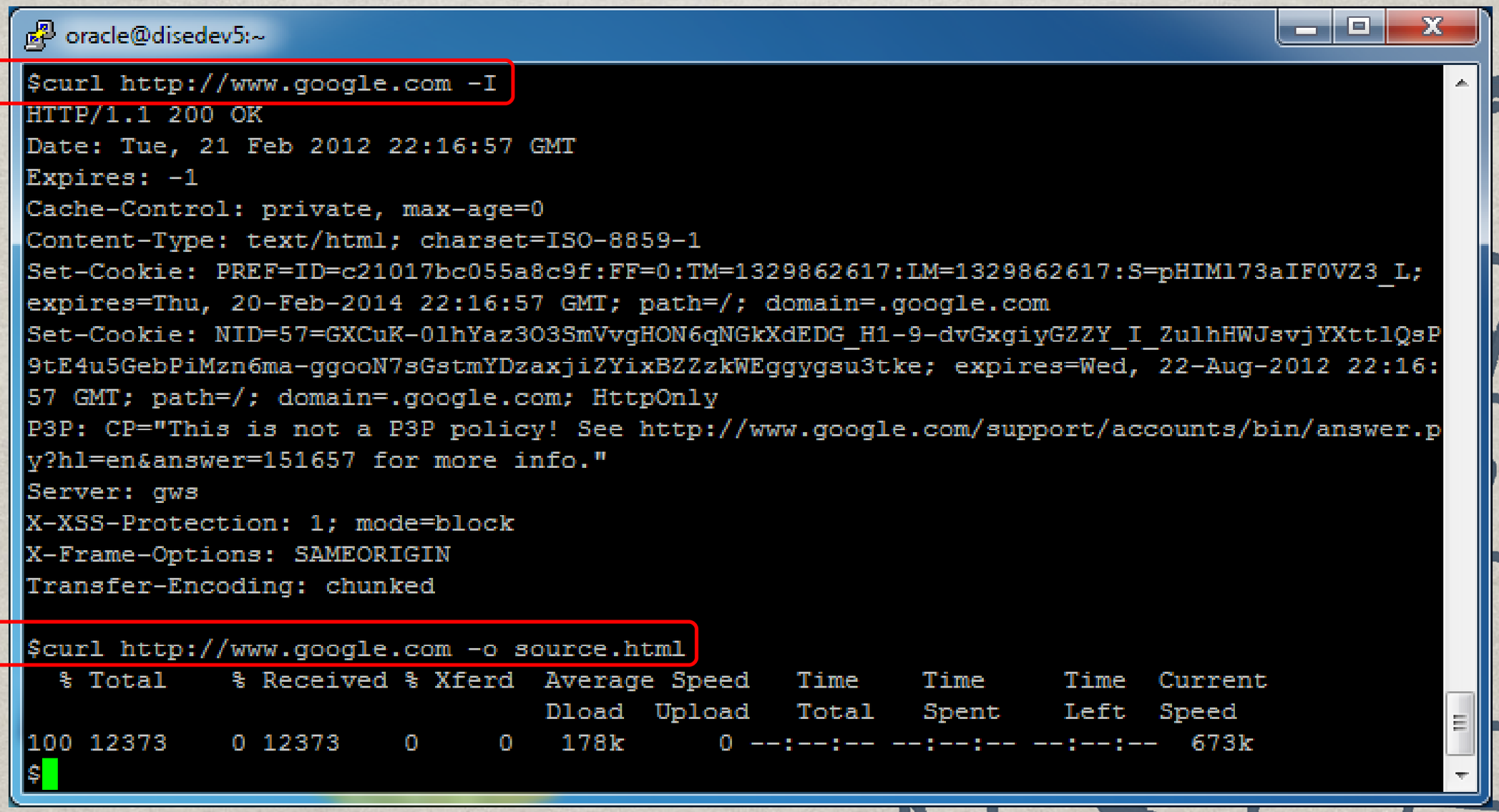
beectl modify_property --component BEECORE_<replace_by_beehive_instance_name>:StartJavaExecutionArguments --name MaximumPermanentGenerationSizeInMB --value 1024

4. After any of the above steps, apply the changes:

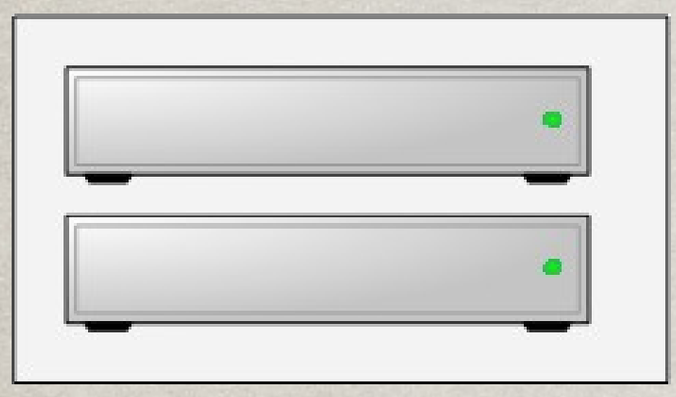
beectl activate_configuration
beectl modify_local_configuration_files

Quick Tips

Use cURL or wget as a minimal web browser

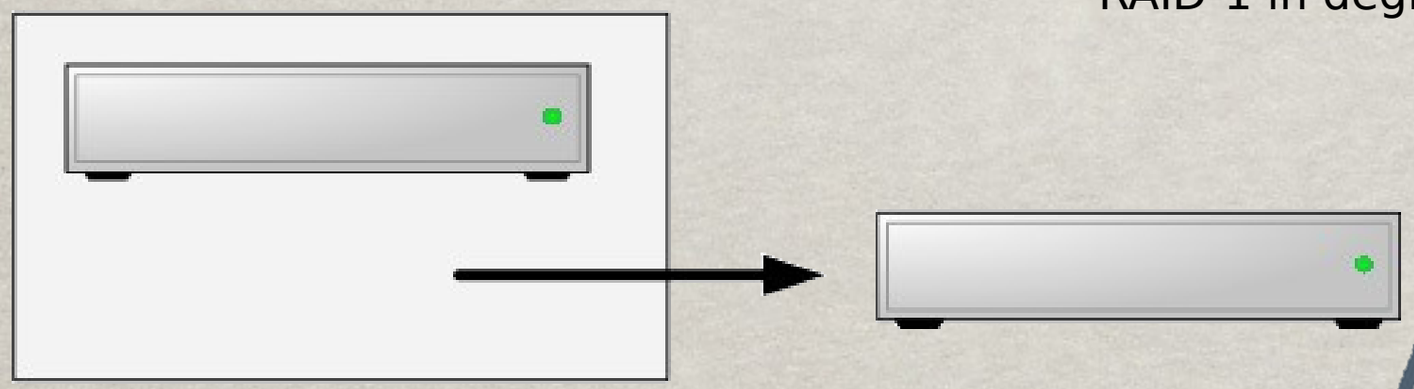


Quick Tips

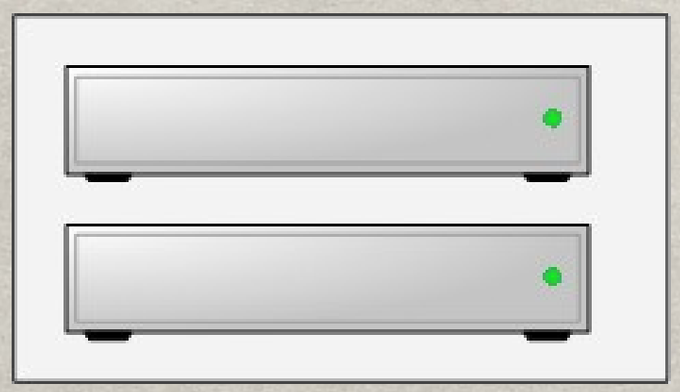


Two hard drives in a
RAID 1 Array (Mirror)

RAID-1 in degraded mode



Backup



Reconstruct array from backup

Quick Tips

Simple script to start DB, Listener and EM

```
#!/bin/bash

echo "Creating SQL script..."

echo "startup" > script.sql
echo "exit;" >> script.sql

chown oracle:oinstall script.sql
chmod 755 script.sql

mv script.sql /home/oracle

echo "Running SQL script..."

su oracle -c 'source /home/oracle/.bash_profile; $ORACLE_HOME/bin/sqlplus / as sysdba @/home/oracle/script.sql'
su oracle -c 'source /home/oracle/.bash_profile; $ORACLE_HOME/bin/lsnrctl start'
su oracle -c 'source /home/oracle/.bash_profile; $ORACLE_HOME/bin/emctl start dbconsole'
```

Contact information

Arijit Das – adas@nps.edu

Tony Kendall – wakendal@nps.edu

Greg Belli – gfbelli@nps.edu

Erik Lowney – eslowney@nps.edu

Riqui Schwamm – rschwamm@nps.edu

Questions?