

# IDC Server

The DYNES project uses the [Dell R410](#) (now discontinued) and in some cases the R420. The IDC software runs as a virtual machine on the host server.

The configuration information for this server is available [here](#).

R410 environmental specifications are:

R410: 2xE5620, 16GB (4x4GB), 2x500GB, PERC H200, Raid1				
Input Power:	259	watts	883.7	btu/h
Input Current:			2.4	amps
Sound Power Level:			6.2	bels
Airflow Rate:	16.1	l/s	34.2	CFM
Weight:	25.1	kg	55.3	lbs
Air Temperature Rise:	13.6	°C	24.6	°F

The OSCARS IDC software requires at minimum a single PC that will act as a server for processing requests. Most modern PCs should be suitable for running the software. The following specifications are the minimum requirements:

- 2 Ghz Processor
- 16 GB memory
- 500 GB hard drive
- Linux/Unix Operating System
  - Centos 5, moving to Scientific Linux 6
- Basic Internet connectivity
- System clock running the Network Time Protocol (NTP)

IDC Server monitoring and status information can be found at:

- <https://spaces.at.internet2.edu/display/dynes/Monitoring+and+Status>

This page contains information about Nagios, Rancid, alternate console access, and some useful Dell server hardware commands. The OSCARS software is run in a VM on the IDC host using either xen (at older sites) or KVM (at newer sites).

## DYNES Overview on the IDC

The IDC is typically a Dell R410 or Dell R420. In the standard configuration the IDC server runs one or more virtual machines. Each virtual machine runs an instance of the OSCARS software and other software that is used to control the DYNES switch. This software can be DRAGON, Bridge-PSS, or OESS. DRAGON is used to control non-Dell switches. Bridge-PSS is used to control Dell 8024F switches (most of the DYNES switches are this type), and OESS is used to control Dell S4810 switches, the latter being OpenFlow capable. The OESS software is the same software used by Internet2 to set up and create layer2 circuits on Internet2's AL2S backbone network.

The virtual machines are KVM VMs.

## Dell iDRAC

Every DYNES supplied IDC (Dell R410) comes equipped with Dell's iDRAC6 Enterprise. "The Integrated Dell™ Remote Access Controller6 (iDRAC6) is a systems management hardware and software solution that provides remote management capabilities, crashed system recovery, and power control functions for Dell PowerEdge™ systems." The iDRAC capability can be accessed via a web interface at the address you supplied with the configuration information for your DYNES equipment (e.g., <https://your-idrac-address> or <https://your-idrac-name.yoursite.edu>). Documentation for the iDRAC can be found [here](#). Please note that both the IDC and the FDT server supplied with DYNES are configured with iDRAC capability. If you use Firefox to access iDRAC you should be aware that you can only access one of the servers at a time. The certificate Dell supplies with their iDRAC hardware uses the same serial number and Firefox won't accept a cert with a duplicate serial number. Firefox currently does not give you the option to continue meaning that you can only view the iDRAC on the first server you access. A workaround is to remove the certs (see this [link](#) for details) or use a different browser.

## To install/replace the CERT on the IDC

The steps to import the cert and key and update the user in the OSCARS webUI.

import the cert and key to the oscar.jks and localhost.jks to overwrite the previous entry

```
[root@yourhost ~]# cd /opt/oscars/tools/bin/
[root@yourhost bin]# ./idc-importkeypair -s /etc/oscars/keystores/oscar.jks -a mykey -k /root/yourhost.edu.key
-c /root/yourhost.edu.crt -p changeit -O
[root@yourhost bin]# ./idc-importkeypair -s /etc/oscars/keystores/localhost.jks -a mykey -k /root/yourhost.edu.
key -c /root/yourhost.edu.crt -p changeit -O
```

retrive the updated subject and issuer and update the Local IDC Account (yoursite-idc) in the OSCARS webUI:

<https://yourhost.edu:8443/OSCARS/>

```
keytool -printcert -file /root/yourhost.edu.crt
```

Owner: CN=<whatever is there>, OU=Services, DC=doegrids, DC=org

Issuer: CN=DOEGrids CA 1, OU=Certificate Authorities, DC=DOEGrids, DC=org

Copy the new cert and key to the proper places

```
cp /root/yourhost.crt /etc/pki/tls/certs
```

```
cp /root/yourhost.key /etc/pki/tls/private
```

Update the new cert and key locations in the relevant places

/etc/oess/database.xml

/etc/httpd/conf.d/ssl.conf

restart OSCARS

```
/etc/init.d/oscars restart
```