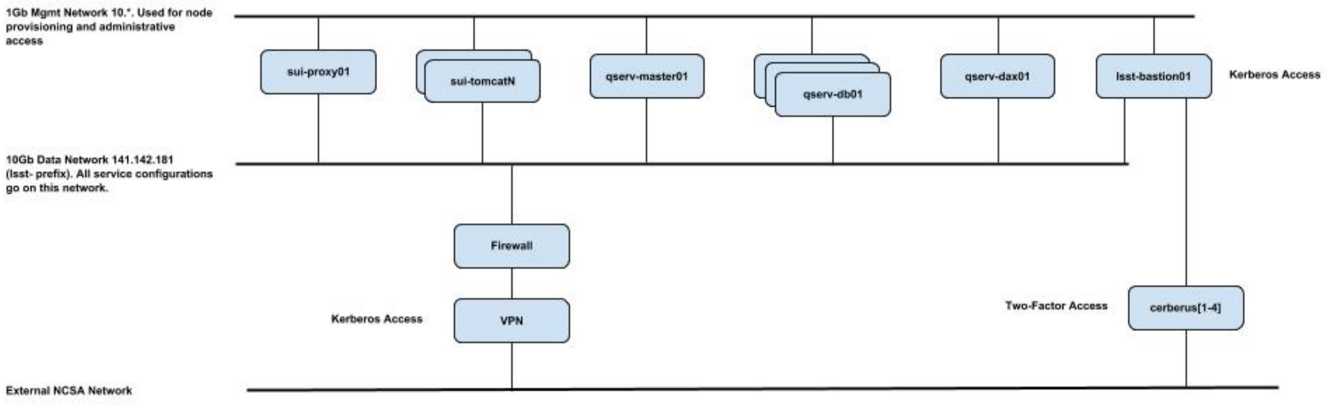
# PDAC networking and user accounts for developers

## Cluster members

- Firefly load-balancing proxy: data: lsst-sui-proxy01.ncsa.illinois.edu, management: sui-proxy01
- Firefly Tomcat server(s): data: lsst-sui-tomcat[01-02].ncsa.illinois.edu, management: sui-tomcat[01-02]
- DAX server(s): data: lsst-qserv-dax01.ncsa.illinois.edu, management: qserv-dax01
- Qserv master: data: lsst-qserv-master01.ncsa.illinois.edu, management:qserv-master01
- Qserv shard servers: data: lsst-qserv-db[01-30].ncsa.illinois.edu, management:qserv-db[01-30]

## Network connectivity


1Gb Mgmt Network 10.*. Used for node provisioning and administrative access
sui-proxy01
sui-tomcatN
qserv-master01
qserv-db01
qserv-dax01
lsst-bastion01
Kerberos Access
10Gb Data Network 141.142.181 (lsst- prefix). All service configurations go on this network.
Firewall
Kerberos Access
VPN
Two-Factor Access
cerberus[1-4]
External NCSA Network

## VPN access (for developers, intended to test what access will be available to users later on)

### Why should I use NCSA's VPN

In short, the NCSA VPN account is currently the only way to gain non-privileged end-user-type access to PDAC services. The cluster deployments within NCSA's National Petascale Compute Facility contain a 'walled garden' (ie firewalled, not related to the VPN) for staging of pre production services. Currently, access to services within the walled garden is restricted to the VPN service IP space.

So make use of the VPN when you need to access PDAC services as an end user.

### Getting a NCSA VPN Account

Any user with a valid NCSA Kerberos account, which includes all LSST members with current NCSA accounts, have a VPN access. In the future, this may be further restricted to a subset of project-approved members in order to limit access to services in the walled garden or to prevent exhausting the license limit on the VPN service. All member not directly and officially associated with the PDAC should not use the VPN service.

### Logging into the NCSA VPN

If you have the Cisco AnyConnect client installed, or have a machine capable of running the AnyConnect client, the simplest method to access the VPN environment is to point a web browser to https://sslvpn.ncsa.illinois.edu/, select the 'ncsa-vpn-default' option, and enter 'PUSH' for the 2nd Password (to trigger a NCSA Duo push). On future connects, you can just add 'sslvpn.ncsa.illinois.edu' to the AnyConnect connection window.

Failing that method, full instructions detailing alternate connection methods are listed on the NCSA wiki.

Once connected to NCSA's VPN service, you will be prompted for your NCSA username, Kerberos password, and DUO token.

If you need to reset your password, see instructions here.

A tip from Chris Walter:

Here is a tidbit if (like me) you need to use anyconnect to NCSA but also need to use if for somewhere else (Duke in my case).

You can type sslvpn.ncsa.illinois.edu in the drop down window and it works.  But if you quit the program it won't be persistent.  A did a bit of googling.  There is no way to do fix this in the UI but if you go to: (edited)
/opt/cisco/anyconnect/profile
you can put in an xml file for each connection you want.
I already had one for Duke in there.  If you add NCSA.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/">
<ServerList>
     <HostEntry>
          <HostName>NCSA</HostName>
          <HostAddress>sslvpn.ncsa.illinois.edu</HostAddress>
     </HostEntry>
</ServerList>
</AnyConnectProfile>
```

in the directory then when you start up the program next time you will see both entries in the drop down list.
Notes:
- It uses the last user name used for the user.  There used to be <user> tag but it doesn’t work anymore.  That info is stored in ~/.anyconnect
- Don’t get fooled by the presence of ncsa_anyconnect_profile.xml that you might already see in the directory.  That gets downloaded after you connect and has more connection info in it but not the host info etc.  You need the new file.

## Accessing PDAC Services from the NCSA VPN

Once connected to NCSA's VPN, the following address pairs become externally accessible:

- lsst-sui-proxy01.ncsa.illinois.edu (141.142.181.119): 80, 443
- lsst-sui-tomcat01.ncsa.illinois.edu (141.142.181.120): 80, 8080, 8100
- lsst-qserv-dax01 (141.142.181.182): 5000, 8080

# Developer administrative login

## Why is this necessary?

LSST project members associated with the initial deployment of PDAC services require administrative access to service nodes in order to perform the installation and complete the configuration. Administrative access with NCSA's NPCF requires two-factor access per security policy. VPN access is not sufficient because it neither requires two-factor authentication nor does it, in anyway, identify you to the PDAC service(s).

## Getting an administrative account

You must obtain a two-factor account by emailing lsst-account@ncsa.illinois.edu. Only approved project members will be granted two-factor accounts.

## Logging in with administrative privilege

1. SSH to cerberus[3-4].ncsa.illinois.edu and log in with your two-factor credentials.
2. SSH to lsst-bastion01 and log in with your Kerberos credentials (necessary because you just crossed an adminstrative domain)
3. SSH to any of the PDAC systems (no credentials required), omitting the "lsst-" prefix (in order to use the management network). You are now within the cluster and can move between pre-staging service nodes without credentials
4. Escalate to root: sudo su - (or similar)