Remote access implementation at GM/CA

Sergey Stepanov, Mark Hilgart, Qingping Xu, and Oleg Makarov

1. Who we are
2. History & experience of providing remote access
3. Convenience for users
4. Multi-tier cyber security
5. NX pros and cons
6. Beamline automations for remote operations

APS TWG meeting, March 18, 2021
Who we are: one of several MX facilities at APS

- GMCA works along with BioCARS, IMCA, SBC, LS, SER, NE, LRL (25% of APS)
- High degree of automation and high throughput: several user groups daily, more like Ford assembly lines.
- Mostly remote: GMCA 95% had full/partially remote even before Covid, now 100%
GM/CA computing cluster with remote access

45 workstations at two 23-ID beamlines (not all shown), ~500 cores used for data processing
GM/CA remote access history and experience

- Remote access is provided with NOMACHINE
- We have 13 years of experience with NX
- Two new groups every day (fast turnaround)
- Went through NX-3.5, NX-5, NX-6, and NX-7
- Tried NX Enterprise, opted for 10x Workstation pack (< $400 annually)
- Also tested and dropped TeamViewer, FreeNX, X2GO, Xrdp, Guacamole,...
- Using Globus for data transfers to institutions; also tried Globus over DMZ, but dropped due to lack of users interest
- Users: biologists, mostly students, postdocs and professors; many not very proficient in computing and need simplicity.

First GM/CA remote data collection with NX, March 20, 2008.
Todd Geders using dual-screen Mac workstation at U. Michigan
- 44 crystals screened
- 5 datasets collected
Simplicity for users: GM/CA remote access portal

Users navigate to https://www.gmca.aps.anl.gov/remote and then click either NX Webplayer link or download NX player template for the remote computer of their need (Collect Process or Backup)
Simplicity: video manuals and FAQ

www.gmca.aps.anl.gov/video/

Remote operations
(recorded by Mark Hilgart)

Remote connecting with Webplayer
(recorded by Sergey Stepanov)

Remote data transfers with Globus GridFTP
(recorded by Raj Kettimuthu, MCS)
Simplicity: GM/CA remote access flowchart

1. **Linux, Windows, or MacOS**
   - **Webplayer works in your browser?**
     - **YES**
       - Install Enterprise NX Player from nomachine.com
     - **NO**
       - Download & unpack NX Player package from www.gmca.aps.anl.gov/remote/players

2. **Ways to connect remotely to GMCA**
   - **Have admin rights on your OS?**
     - **YES**
       - Start NX Player by clicking desktop icon
       - Table-1: choose BL & click Collect, Process or Backup Webplayer in web browser
       - Login to Webplayer with your GMCA account
       - Method-1: NX-Webplayer
     - **NO**
       - Go to bin subdirectory and start nxplayer
       - Table-2: choose BL & save session file (Collect, Process or Backup session)
       - Open saved session file in NX Player & login with your GMCA account
       - Method-2: NX-Install
       - Method-3: NX-unpack
Simplicity: no install players

No-install NX Players

This directory contains no-install version of NX players for those GM/CA@APS users who do not have root/Administrator permissions normally required to install software on a computer and therefore unable to run the NOMACHINE Enterprise Client installer.

The players below are Copyright NOMACHINE. They are portable versions of free NOMACHINE Enterprise Player extracted from the installers without any modification to the files. These players are re-packaged and posted here solely for the convenience of GM/CA@APS users.

Download the player package for your operating system, unpack it, and start the nxplayer executable.

**On Linux:**

```
tar xzf nxplayer4linux_6.xxx_yyy.tgz
cd nxplayer4linux/bin/
./nxplayer
```

**On Windows:**

```
unzip -x nxplayer4windows_6.xxx_yyy.zip
cd nxplayer4windows\bin
nxplayer
```

**On MacOSX:**

```
tar xzf nxplayer4macosx_6.xxx_yyy.tgz
cd nxplayer4macosx/Contents/MacOS/
./nxplayer
```
Simplicity: show currently allowed connections

This is what users see when they are at ANL or have beamtime at both GM/CA beamlines

- Also automatic selection of WebRTC (x264) vs mjpegs depending on browser
Simplicity: show currently allowed connections

This is what visitors see when they are outside ANL and do not currently have beamtime at any of the GM/CA beamlines

<table>
<thead>
<tr>
<th>Beamline</th>
<th>Acquisition (blXws2)</th>
<th>Processing (blXws6)</th>
<th>Backup (blXws5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beamline-1 23ID-D (23ID-in): Launch Webplayer</td>
<td>Launch Webplayer</td>
<td>Launch Webplayer</td>
<td></td>
</tr>
</tbody>
</table>

This is what visitors see when they have beamtime at beamline 23ID-D only

*Behind the scene: PHP with SQL queries to the user accounts database*
Simplicity: remote IP controls under the hood

- Users indicating that they will work remotely are asked to provide their remote IP addresses as they are seen at GMCA. We have a webpage where they can check their IP addresses.
User account & IP management (staff tool)

- Users accounts are managed by web-based User Account Program (UAP) developed by Mark Hilgart
- Accounts are active for 2-3 days (data collection plus 1-2 days for processing and backup)
- UAP creates cron jobs to enable/disable accounts in LDAP and modify iptables, NX and SSH configs, and PAM at the time when accounts are enabled and disabled.
- If users indicate they will work remotely, their IP addresses are stored in SQL
- User sessions are killed after their beamtime is expired (a good number of users close NX window instead of logout and their session may continue to run)
- UAP uses Saltstack to push tasks to remotre workstations
Redundant cyber security: catch me if you can

Examples of what is modified by UAP

# /etc/ssh/sshd_config
   AllowUsers jsmith@127.0.0.1 jsmith@141.211.182.*

# /usr/NX/etc/htd.conf
   Require ip 141.211.182.0/24

# /etc/sysconfig/iptables
   -A INPUT -s 141.211.182.0/24 -j ACCEPT_GMCA

# GeoIP: allow connections from US, Canada and Puerto Rico only:
   -A INPUT -m state --state NEW -m geoip ! --source-country US,CA,PR -j DROP

# Allow 4 ssh or nxhtd (via localhost) connections in 120 seconds, then ban for 120 seconds
   -A INPUT -p tcp -m state --state NEW --dport 22 -m recent --name NXHTD --set
   -A INPUT -p tcp -m state --state NEW --dport 22 -m recent --name NXHTD --update --seconds 120 --hitcount 4 -j DROP

# PAM: /etc/login_groups.conf
   staffGroup
   bl1-first-day
   bl1-first-day-remote

Users are assigned a group where they can only login three remote access workstations on 1st day and only one 2nd day workstation on the other days. No logins to all cluster workstations.
More cyber security: APS/ANL blocking

# /etc/rsyslog.conf
  kern.warning @apsloghost.aps.anl.gov
  authpriv.info @apsloghost.aps.anl.gov

Login attempts and the iptables firewall messages are logged to APS/ANL and then an IP may be automatically blocked in case of multiple errors.

**Problem:** persistent users, obsolete passwords saved in NX players, attempts to log in to wrong beamline or outside allocated time window sometimes cause APS blocks. Now we receive blocking notification (thanks to Dave Leibfritz), but unblocking may be a problem after hours and on weekends. We try to warn users, but it still happens.
More cyber security: staff troubleshooting tool

```bash
# Mate Terminal

File Edit View Search Terminal Help

Temp: jsacchettini@127.0.0.1 (localhost)
j sacchettini@128.194.145.* (tamu.edu)
j sacchettini@128.194.47.* (tamu.edu)  <-- Expiration: 2021-03-13 08:00:00
(corcoran/scorcoran)

## Allowed external SSH/NX/NXHTD IPs in /etc/sysconfig/iptables:
none

## No today's SSH/NXHTD logins blocked by iptables (incl. hacks).

## Today's rejected ssh logins due to invalid user (incl. hacks):
Mar 12 09:23:02 jsacchettini from 128.194.145.245
Mar 12 09:50:35 sacchettini from 128.194.145.245

## Today's rejected ssh logins due to incorrect password:
Mar 12 09:27:05 jsacchettini from 127.0.0.1
Mar 12 09:35:06 jsacchettini from 127.0.0.1
Mar 12 09:39:16 jsacchettini from 128.194.145.245
Mar 12 09:39:25 jsacchettini from 128.194.145.245
Mar 12 09:55:07 jsacchettini from 128.194.145.245
Mar 12 09:55:32 jsacchettini from 128.194.145.245
Mar 12 09:59:37 jsacchettini from 127.0.0.1
```

The AllowedRemote tool shows:
- AllowUsers in sshd_config
- Allowed external SSH/NX/NXHTD IPs in iptables
- Today's SSH/NXHTD logins blocked by iptables
- Today's rejected ssh logins due to invalid user
- Today's rejected ssh logins due to incorrect password
- Today's rejected ssh logins due to user not listed in AllowUsers
- Today's rejected NX WebPlayer logins due to IP not allowed
- Today's closed NX sessions
- Today's failed NX sessions
- Currently running sessions with connected NX users
- Currently running sessions with disconnected NX users
NX Pros & Cons and NX version control

**NX Pros:**
- Full desktop experience
- Efficient compression providing good responsiveness even a slow networks
- Clients for most OS
- Relatively inexpensive license
- Reasonable cyber security

**NX Cons:**
- Buggy, basically permanent beta
- Support tickets may take many weeks and require a lot of effort; some tickets are never resolved
- No respect to legacy: some features you rely on may be dropped or replaced without notice
- Server-client version compatibility is not guaranteed

Our workarounds for NX cons:
- Use the simplest configuration. That is why we abandoned NX Enterprise and considering to drop WebRTC. We also disable audio and recording.
- Be conservative with major updates introducing new features. Give them at least 3 months to settle.

We control NX client version at login and do not allow old NX players and old browsers

```
# /usr/NX/etc/node.cfg
DefaultDesktopCommand anl_mate_session.sh
```
Beamline automations for remote operations

- All motions are motorized with absolute positions per motor via automated homing.
- Sample robotics (288 samples capacity).
- Four webcams per beamline including on-axis visualization and pan/tilt webcam.
- Automated beamline setup and commissioning allowing staff to setup beamline remotely.
- All-in-one data acquisition GUI (jBlulce) and automated data processing on cluster.