CAC

From GFDL

Contents

Background

The Common Access Card or CAC, is the identify-proofed solution, NOAA and GFDL will use in response the the HSPD-12 directive set forth in the mid 2000's. GFDL CAC holders will use their CAC to authentic against GFDL Cyber Assets, which include, but not limited to, computers, servers, websites and any other material or equipment deemed sensitive or enforce by IT Security per policy.

Current CAC Posture

- CAC is not enforced on the GFDL workstations but it is encouraged to be used instead of username and password.
- CAC is not enforced in the R&D HPCS program but it is encouraged that users try accessing Gaea and Analysis from their GFDL Linux workstations, per the instructions below
- Technical Services is still developing the documentation and getting the licenses for home use of the Tectia Client.
- RSA and Username/Password are all still intact and nothing there has changed.
- We currently have 2 login infrastructures for authentication on both the GFDL side and R&D HPCS.

Implementation

The GFDL Account is supported by Active Directory. This system provides a trusted network to login with either your username and password or CAC and PIN. All systems that are part of the GFDL Active Directory domain (GFDL-NOAA) are enrolled and trusted. This trust is maintained with certificates. GFDL notebooks, desktops and websites (where GFDL-NOAA is specified) utilize this credential. Sometimes referred to your network password. For externally connecting into GFDL, Tectia is the product being used. When using a CAC to connect from home, or an external device, you will ssh to a CAC bastion. RSA users will continue to ssh to the RSA bastion known as ssh.gfdl.noaa.gov. Exact methods for logging in will be available below.

Why is CAC more secure?

The DoD issued CAC was chosen to meet HSPD-12 and the DoC's CITR-008 because of it's preexisting and vetted infrastructure. This smartcard qualifies as a Level of Assurance (LOA) 4 device. We are most familiar with RSA tokens at GFDL which are only an LOA-2 device. An LOA-4 device not only is 2-factor but also identifies the individual that it is assigned to. The card itself has an integrated circuit chip (ICC) that stores over a hundred KB of data. Each card contains two certificates. The Public Key Infrastructure (PKI) certificate enables users to digital sign documents and establish secure connections. These cards are resistant against brute force attacks because the PIN locks after 3 unsuccessful authentication attempts. The only way to reinstate the PIN is to physically visit a RAPIDS

site where a trained admin can identify you via ID and finger prints. This is more secure than the RSA tokens which automatically unlock after 15 minutes.

Who can use CAC

Right now, only users who have been issued a DoD CAC and who do not use a Mac can use their CAC for accessing portions of the GFDL IT infrastructure and the R&D HPC systems. Mac users will continue to use their normal way of access (RSA) until a CAC solution is ready.

Where is CAC enforced?

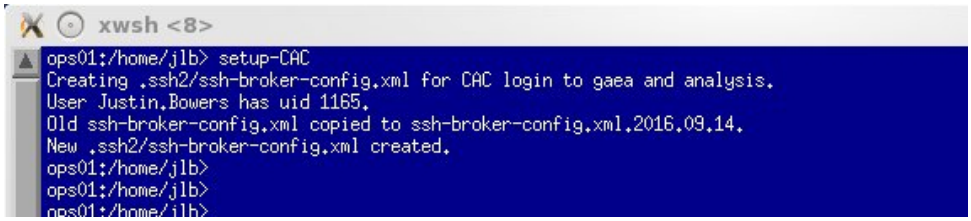
CAC is currently not enforced anywhere. For the GFDL workstations, it is extremely encouraged that you use your CAC but a technical control will not be put into place until all the issues are corrected. We do expect CAC to be enforced later this year for local login and remote connections. Users who have a CAC and are identified as not using a Mac for remote access will have their RSA tokens turned off and collected. That will not happen until major bugs are identified, corrected and our CAC infrastructure is hardened.

How to log into my Linux Workstation with CAC, locally

- insert your CAC into the CAC reader at your workstation while completely logged out. A light on the reader should blink. Some readers are imbedded into the keyboard.
  - If you do not have a reader or are unsure where it is, please call Operations or open a help desk ticket
- If you account is configured to reference your account, the login prompt for your workstation should change to your CAC identification sequence and ask for you PIN.
  - If this does not work, open a help desk ticket.
- Enter your CAC PIN and click enter
- You should be logged in now
  - If this does not work, open a help desk ticket.
- If you use Gnome, when you pull out your CAC the screen will lock. If you use KDE, it will not lock at this point in time because it's broken.
- Always lock or logout when leaving your worsktation
- When you return to your workstation, insert your card and authenticate with your PIN again.
- Everything about your session should remain the same, as it would if you logged in with your username and password.
  - If it does not, open a help desk ticket.

How to log into Gaea and Analysis from a GFDL Linux Workstation

- Connection can only be done with CAC if you are physically at the workstation
- Make sure CAC is inserted to the workstation CAC reader (hopefully you used this to log into the workstation)
  - If you do not have a reader or are unsure where it is, please call Operations or open a help desk ticket
- Open a new terminal on your workstation
- For first time connecting, you much configure a new ssh broker file (similar to .ssh/config), we have a script to do this for you
  - Run the command setup-CAC



-
  - Your default configuration is now setup with the Tectia Client
  - You can now connect to Gaea and Analysis
- Run the command sshg3 gaea (to connect to Gaea). When prompted for passphrase, enter your CAC PIN.

xwsh <8>

```
ops01:/home/jlb> sshg3 gaea
Host key for the host "bastion-gaea.princeton.rdhpcs.noaa.gov" not found from database.

The fingerprint of the host public key is:
Babble: "xofic-gecik-kycoz-guvyc-nazoh-byhyk-cufom-gabiz-mesuz-ricyc-nuxyx"
RFC4716: "71:67:51:7e:e0:0f:6f:de:c7:32:16:6b:d3:fd:72:ef"


You can get a public key's fingerprint by running
% ssh-keygen-g3 -F publickey.pub
on the key file.

Please select how you want to proceed.
    cancel) Cancel the connection.
      once) Proceed with the connection but do not save the key.
      save) Proceed with the connection and save the key for future use.
Please select one (cancel, once, save): once^H^H^H
Invalid selection.
Please select one (cancel, once, save): save
*****************************************************************************
*                                WARNING!                                   *
*****************************************************************************
* This is a United States Government computer system, which may be          *
* accessed and used only for official Government business by authorized *
* personnel.  Unauthorized access or use of this computer system may        *
* subject violators to criminal, civil, and/or administrative action.       *
*                                                                           *
* All information on this computer system may be intercepted, recorded, *
* read, copied, and disclosed by and to authorized personnel for            *
* official purposes, including criminal investigations.  Access or use  *
* of this computer system by any person, whether authorized or              *
* unauthorized, constitutes consent to these terms.                         *
*****************************************************************************


Token label: BOWERS.JUSTIN.LEWIS.1386554702
Manufacturer:
Passphrase for the private key:
warning: Failed to bind address 127.0.0.1:31165: 'Address already in use'. / Local tunnel from port 31165 to localhost:31165 failed.
Authentication successful.
Welcome to the NOAA RDHPCS Infrastructure system
    bastion-gaea.princeton.rdhpcs.noaa.gov
running CentOS 6.8 x86_64 on a Red Hat KVM

This system has the following roles:
        CAC Bastion VM server
id: cannot find name for group ID 500

Welcome to the NOAA RDHPCS.

Attempting to renew your proxy certificate...Proxy certificate renewed.
Proxy certificate has 720:00:00  (30.0 days) left.

        Welcome to bastion-gaea.princeton.rdhpcs.noaa.gov
Gateway to gaea.ncrc.gov and other points beyond

HASH(0x2e92830)

The Gaea destinations are:
Hostname            Description
gaea                gaea head nodes
gaea10              c3 head node
gaea11              c3 head node
gaea12              c3 head node
gaea13              c4 head node
gaea14              c4 head node
gaea9               c3 head node

You will now be connected to OneNOAA RDHPCS: Gaea (CMRS/NCRC) system.
To select a specific host, hit ^C within 5 seconds.
Local port 31165 forwarded to remote host.
Remote port 21165 forwarded to local host.

For port forwarding instructions, see
http://wiki.gfdl.noaa.gov/index.php/Login

**********************************<<< gaea11 >>>*********************************
*                               NOTICE TO USERS                               *
*                                                                             *
*  This is a Federal computer system and is the property of the United        *
*  States Government. It is for authorized use only. Users (authorized or     *
*  unauthorized) have no explicit or implicit expectation of privacy.         *
*                                                                             *
*  Any or all uses of this system and all files on this system may be         *
*  intercepted, monitored, recorded, copied, audited, inspected, and          *
*  disclosed to authorized site, Department of Energy, and law enforcement    *
*  personnel, as well as authorized officials of other agencies, both         *
*  domestic and foreign.  By using this system, the user consents to such     *
```

```
*  interception, monitoring, recording, copying, auditing, inspection, and   *
*  disclosure at the discretion of authorized site or Department of Energy   *
*  personnel.                                                                *
*                                                                            *
*  Unauthorized or improper use of this system may result in administrative  *
*  disciplinary action and civil and criminal penalties. By continuing to    *
*  use this system you indicate your awareness of and consent to these       *
*  terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to   *
*  the conditions stated in this warning.                                    *
*                                                                            *
**********************************<<< gaea11 >>>*********************************
Last login: Sun Sep 11 20:14:42 2016 from gaea.princeton.rdhpcs.noaa.gov
gaea11 home1/Justin.Bowers> xclock
Error: Can't open display:
gaea11 home1/Justin.Bowers> echo $DISPLAY
DISPLAY: Undefined variable.
gaea11 home1/Justin.Bowers>
```

- Run the command sshg3 analysis (to connect to Analysis). When prompted for passphrase, enter your CAC PIN.

```
xwsh <13>
ops01:/home/jlb> sshg3 analysis
Saved key for the host "bastion-analysis.princeton.rdhpcs.noaa.gov" does not match.

@@
@@ WARNING: SERVER HOST IDENTIFICATION HAS CHANGED!
@@

There are many possible reasons for this:
1. The administrator of the remote host computer has changed the host key.
2. The remote host computer is part of a server cluster.
3. SOMEONE COULD BE EAVESDROPPING ON YOU RIGHT NOW (man-in-the-middle attack)!

It is NOT RECOMMENDED to connect to the remote host computer until you have
contacted the system administrator and found out why the host identification
has changed.

The fingerprint of the host public key is:
"xuriz-huzuf-sonih-gokaz-dagen-zusyz-fosit-marup-zuvep-lumag-sixyx"

You can get a public key's fingerprint by running following command
% ssh-keygen-g3 -F publickey.pub
on the key file.  You should check the validity of the host key ASAP.

If you choose to continue the connection without saving the changed
key, the following steps will be taken to ensure your privacy:
  - Agent forwarding is disabled to avoid attacks by corrupted servers.
  - X11 forwarding is disabled to avoid attacks by corrupted servers.
If you are not absolutely sure about what you are doing, choose cancel
and contact the administrator of the server system.

Please select how you want to proceed.
    cancel) Cancel the connection.
      once) Proceed with the connection but do not save the new host key.
      save) Proceed with the connection and replace the host key(s) in the
            database.
       new) Proceed with the connection and add the host key as an alternate
            identification.
Please select one (cancel, once, save, new): new
*****************************************************************************
*                                 WARNING!                                  *
*****************************************************************************
* This is a United States Government computer system, which may be          *
* accessed and used only for official Government business by authorized    *
* personnel.  Unauthorized access or use of this computer system may        *
* subject violators to criminal, civil, and/or administrative action.       *
*                                                                           *
* All information on this computer system may be intercepted, recorded,     *
* read, copied, and disclosed by and to authorized personnel for            *
* official purposes, including criminal investigations.  Access or use      *
* of this computer system by any person, whether authorized or              *
* unauthorized, constitutes consent to these terms.                         *
*****************************************************************************


Authentication successful.
Welcome to the NOAA RDHPCS Infrastructure system
    bastion-analysis.princeton.rdhpcs.noaa.gov
running CentOS 6.8 x86_64 on a Red Hat KVM

This system has the following roles:
        CAC Bastion VM server

Welcome to the NOAA RDHPCS.

Attempting to renew your proxy certificate...Proxy certificate renewed.
```

```
Proxy certificate has 720:00:00 (30.0 days) left.

        Welcome to bastion-analysis.princeton.rdhpcs.noaa.gov
Gateway to an.lb.princeton.rdhpcs.noaa.gov. and other points beyond



The GFDL Analysis host configurations are:
Hostname            Description
an001               12 cores, 192GB memory,  15TB /vftmp, NAG library
an002               12 cores, 192GB memory,  15TB /vftmp, NAG library
an003                8 cores,  96GB memory, 8.8TB /vftmp
an004                8 cores,  96GB memory, 8.8TB /vftmp
an005                8 cores,  96GB memory, 8.8TB /vftmp
an006                8 cores,  96GB memory, 8.8TB /vftmp
an007                8 cores,  96GB memory,  18TB /vftmp, 2x /vftmp speed
an008                8 cores,  96GB memory,  18TB /vftmp, 2x /vftmp speed
an009                8 cores,  96GB memory,  15TB /vftmp
an010                8 cores,  96GB memory,  15TB /vftmp
an011                8 cores,  96GB memory,  15TB /vftmp
an012                8 cores,  96GB memory,  15TB /vftmp
an013                8 cores,  96GB memory,  15TB /vftmp
an014                8 cores,  96GB memory,  15TB /vftmp
an101               16 cores, 512GB memory,  37TB /vftmp
an102               16 cores, 384GB memory,  37TB /vftmp, 3TB /ssdtmp
an103               16 cores, 384GB memory,  37TB /vftmp
an104               16 cores, 384GB memory,  37TB /vftmp
an105               16 cores, 256GB memory,  37TB /vftmp
an106               16 cores, 256GB memory,  37TB /vftmp
an107               16 cores, 256GB memory,  37TB /vftmp
an108               16 cores, 256GB memory,  37TB /vftmp

You will now be connected to the lightest-loaded analysis host.
To select a specific host, hit ^C within 5 seconds.
Local port 41165 forwarded to remote host.
Remote port 51165 forwarded to local host.

Contact your local support staff for port forwarding setup details.

Last login: Tue Sep 13 16:15:57 2016 from analysis.princeton.rdhpcs.noaa.gov
tcsh: No entry for terminal type "iris-ansi"
```

- You will be prompted with a few options, please select the third option for saving your certificate
- You will be prompted for you CAC PIN, it will say <look at picture>
  - Depending on your previous connections, you may not be prompted for a PIN
- You should now be on a Gaea or Analysis node
- X11 Forwarding is currently not working (we are working on it)

How to install Tectia Client on my personal Windows computer

Instructions are being developed here (http://wiki.gfdl.noaa.gov/index.php/Tectia_Windows_Quick_Guide_Installation) . All users who need a license will need to open a Service Request at https://servicedesk.gfdl.noaa.gov/WorkOrder.do?reqTemplate=8402&.

Known Issues

- Remote access when host is CAC enforced must be the following:
  - ssh First.Last@ssh.gfdl.noaa.gov (w/ RSA) -> ssh public1 (username/password) -> ssh workstation (no authentication required)
  - Users cannot go from ssh directly to their workstation
  - VNC does not work with CAC enforced workstations. The work around is to use VNC with public1 or public2, then terminal to your workstation as needed.(CAC is currently not enforced on any GFDL workstation)
- X11 Forwarding is not working with CAC via sshg3 connections to R&D HPCS bastions
- Dept. of Interior PIV cards are not yet supported
- Newly issued CACs will not automatically work. The Technical Services team needs to be made aware of new CACs so we can update our databases.
- Occasionally unlock takes more than one attempt, even with correct pin on Linux hosts
- Password change notification can be too quick for reading when on Linux host.

Frequently Asked Questions

How will role accounts work? Role accounts on the Linux workstations should be sudo type accounts at this point. All users would login first as themselves then escalate to the role account. As an example, I run "dzdo su tier2" to become the tier2 user. I don't need a password or a fob because I am in the sudoers file. I believe that on the HPC side, they have a mix. Some accounts are "sudo su fms" which are based on a sudo membership list. Others have RSA tokens so a user can login with "ssh Oar.Gfdl.Tier2@analsysis". For those type of accounts, nothing will change and you will keep the RSA token.

Will CAC work on a Mac Cac will not work with Mac yet. If you have a Mac at home and need to connect remotely, you will keep your RSA token until a Mac solution is put into place.

If a user loses their CAC, will there some temporary means of granting access to GFDL computers until a replacement CAC can be generated. We will provide secondary credentials on a case by case basis. For the most part, this should not be a problem. For cases where the CAC is getting frequently forgotten or lost, there may be some sort of delay in credential issuance.

How can I log into multiple machines with a CAC You can log into your GFE device and connect to an R&D HPC System all in the same session. You cannot log into a GFE laptop and a GFE workstation with your CAC. Users who must use their CAC on both are encouraged to log into their laptop then push share their screen with the workstation monitors. From there, the user can drive their session from their laptop and log into all the needed devices, their workstation and R&D HPC Systems.