TANGO Cybersecurity meeting

http://www.tango-controls.org

Tango Access Control

- TANGO access control managed by **user rights**
- User means system logon username on host where the client is running
- Two kind of users:
  - With rights defined in the ACL
  - Without any rights defined →rights fall below ”all users”

- Two kind of rights, at host **and** device level:
  - Read (+ optional per-class allowed commands)
  - Write (meaning that everything is allowed)

Advice: TANGO ACL provides **basic** access control and can be bypassed! (SUPER_TANGO)
Purpose is to avoid mistakes/mishandling.

Tango Access Control

Server (ACL) side, in the DeviceProxy constructor and command_inout call:

Get the Username
Get the host IP address
If rights defined at host level for the User/IP pair
    Give User temporary WriteAccess
If nothing specified for this User on this host
    Give temporary access right equal to host access rights of "AllUsers"
If temporary right is WriteAccess
    If something defined at device level for this User
        If access defined for this device
            Give User the defined rights
        Else
            If rights defined for "AllUsers" for this device
                Give User this rights
            Else
                Give User ReadAccess for this device
    Else
        If right defined for "AllUsers" for this device of for the device family
            Give User this right
        Else
            Give User ReadAccess for this device
Else
    Access right is ReadAccess

Then:

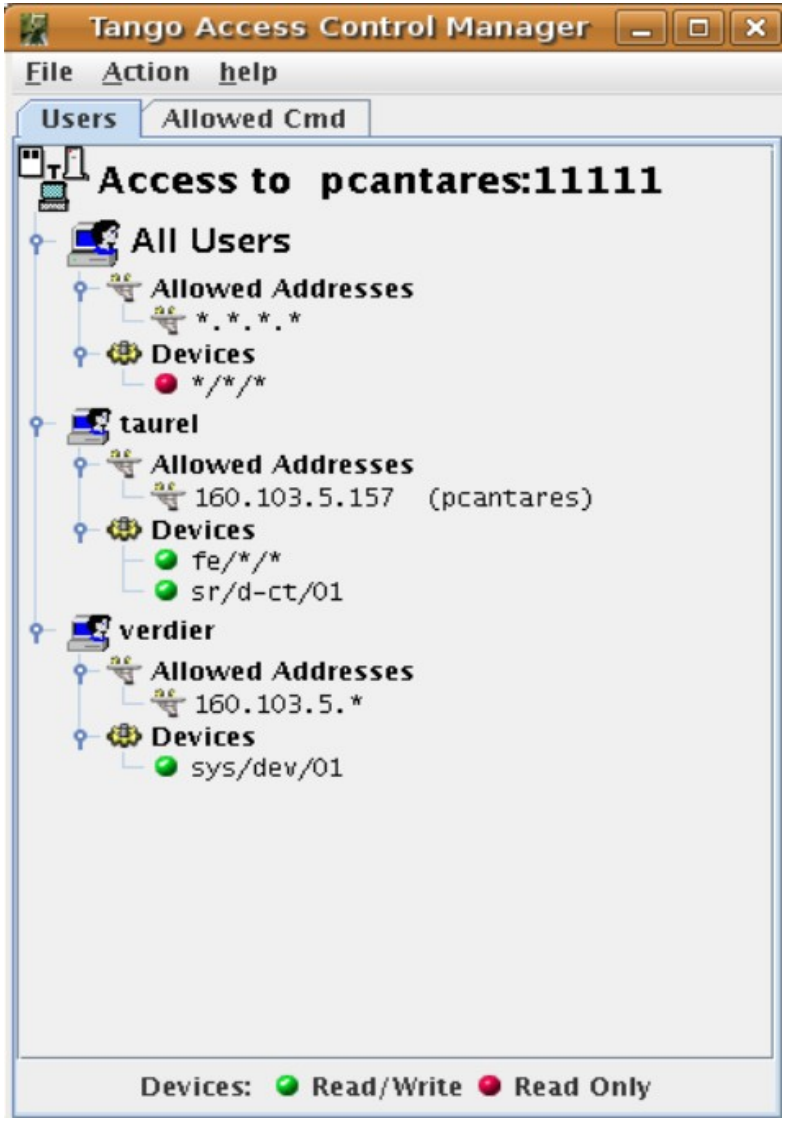
If right is ReadAccess
    If Write
        Refuse the call
    If Command
        If Command in AllowedCommands
            Send the call
        Else
            Refuse the call

Tango Access Control

taurel
- write to sr/d-ct/01 and fe/*/* only from pcantares
- read all other devices only from pcantares

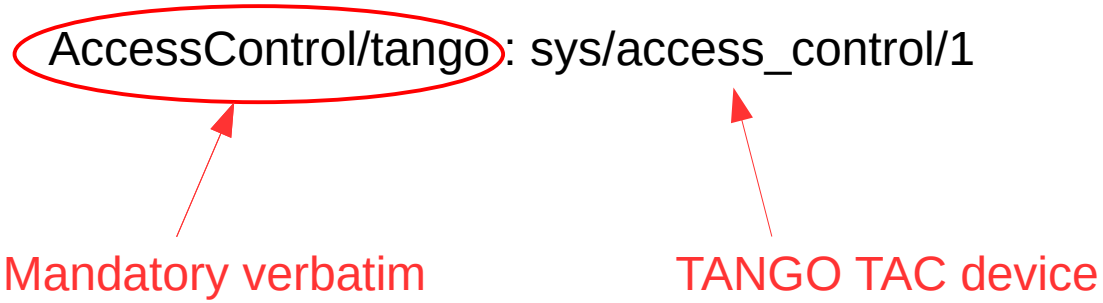
verdier
- write to sys/dev/01 from any host on 160.103.5.0/24 subnet
- read all other devices from the same subnet

all users
- read-only access from any host



Tango Access Control

- Configuration and user rights stored into two tables in the TANGO database
- Free object CtrlSystem containing the property Services
- Array of strings containing the sever/instance and the device



Tango Database Whitelist

tango.service systemd unit:

...
EnvironmentFile=/runtime/site/%H/etc/tango.conf
ExecStart=/usr/local/tango-9.3.3/bin/DataBaseds ${INSTANCE} -ORBendPoint giop:tcp:${TANGO_IP}:${TANGO_DB_PORT}
-ORBendPointPublish giop:tcp:${TANGO_IP}:${TANGO_DB_PORT}
-aclFile /runtime/site/%H/etc/${ACLFILE}

extract from ${ACLFILE}:

Databaseds.conf
#
WARNING! WARNING! WARNING!
#
This file is under revision control.
Do **NOT** edit this file! Your changes will be overwritten!
giop:tcp:192.168.231.13
giop:tcp:192.168.231.14
giop:tcp:192.168.231.15
...

And then...

- DEVELOPMENT OF NICA CONTROL SYSTEM: ACCESS CONTROL AND LOGGING
  Evgeny V. Gorbachev, Georgy Sergeevich Sedykh, JINR, Dubna, Russia
  ICALEPCS2017, Barcelona, Spain
- https://accelconf.web.cern.ch/icalepcs2017/doi/JACoW-ICALEPCS2017-TUPHA171.html
- code just made public today: https://git.jinr.ru/tango-auth/