Channel Access Security Lab

John Sinclair

ORNL/SNS

sinclairjw@ornl.gov

January 2019

Procedure

Summary

- Build and run the IOC application
- Note that there are no restrictions on modifying one:limit
- Reconfigure IOC application with access security, rebuild and run
- Note that only user “expert” may modify the above PV when security is enabled
- Disable access security and verify no restrictions

Details (1/4)

- Open three terminal windows
- Window 1 - build and run the IOC application
  - cd /home/training/epics-train/jwsExamples/caSecurity
  - make
  - cd iocBoot/iocasExample1
  - chmod +x st.cmd
  - ./st.cmd
- Window 2 – modify one:limit
  - caput one:limit 5
  - Note that write access succeeds
  - caget one:limit
- Window 3 – used later

Details (2/4)

- – Window 1 – reconfigure IOC with access security
  - exit
  - cd ../..
  - Edit the following files and uncomment related content – search for ACC SECURITY
    - – asExample1App/Db/one.db – 5 lines
    - – iocBoot/iocasExample1/st.cmd – 2
  - make clean uninstall
  - make

Details (3/4)

- Window 1 - start the IOC application
  - cd iocBoot/iocasExample1
  - ./st.cmd
- Window 2 – attempt to modify one:limit
  - caput one:limit 5
  - Note that write access fails
  - caget one:limit
- Window 3 – modify as user “expert”
  - sudo –s
  - su –l expert
  - caput one:limit 5
  - Note that write access succeeds
  - caget one:limit

Details (4/4)

- Window 2 – disable access security the write PV
  - caput one: accessState “Disabled”
  - caput one:limit 5
  - Note that write access now succeeds
  - caget one:limit