

Security Considerations for the IFS (Integrated File System)

Carol Woodbury, VP Global Security Services
carol.woodbury@helpsystems.com

Agenda

- Reasons for modifying IFS (Integrated File System) security
- How security differs between the IFS and traditional IBM i libraries and objects
- Auditing and the IFS
- File shares
- NetServer

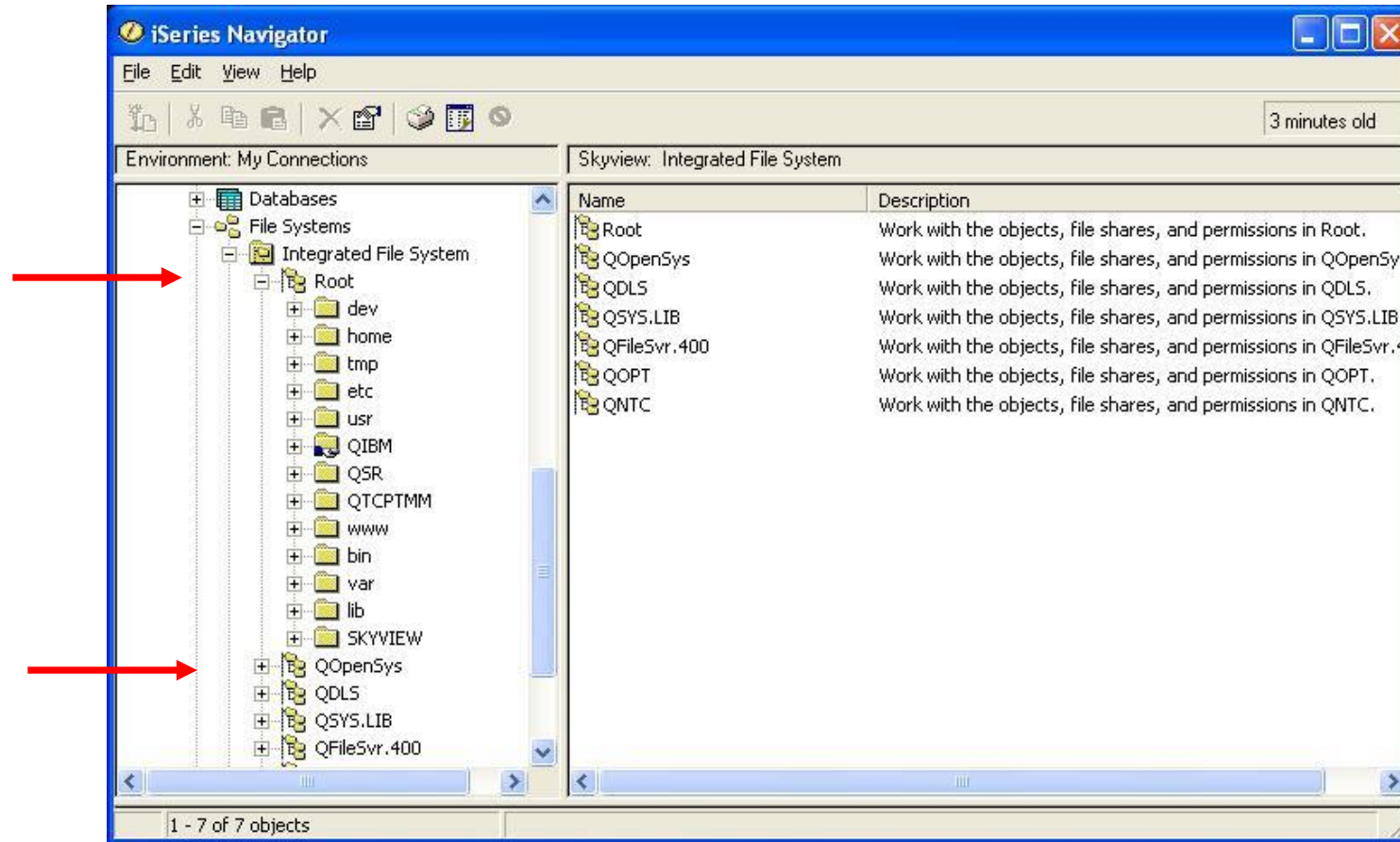
What is the IFS?

- A hierarchical file system
- Added to iSeries in V3R6 to aide in porting Unix applications to run on IBM i

Reasons for examining IFS security

- Default access is the equivalent of *PUBLIC *ALL allows inappropriate
 - Directory creation
 - Storage of objects
 - PC backups, movies, music, pictures, etc
- Uses (e.g. files containing private data are created and transmitted, images containing confidential data are stored) require protection

Which file systems?



All statements made apply to both /Root and /QOpenSys

Where they're the Same and Where they're Different

Same	Different
Authority checking algorithm	Authority names *RWX vs *CHANGE
*PUBLIC authority	Ignores QCRTAUT system value
Can use authorization lists and private authorities	Ignores ownership setting in User profile
	Ignores adopted authority
	Need to look in different audit fields

IFS authorities mapped to IBM i authorities

Authorities	*RWX	*RW	*RX	*R	*WX	*W	*X
Object							
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
*AUTLMGT							
Data							
*OBJOPR	X	X	X	X	X	X	X
*READ	X	X	X	X			
*ADD	X	X			X	X	
*UPD	X	X			X	X	
*DLT	X	X					
*EXECUTE	X		X		X		X

***RWX = Read/Write/Execute (*CHANGE)**

***RW = Read/Write**

***RX = Read/Execute (*USE)**

***R = Read**

***WX = Write/Execute**

***W = Write**

***X = Execute**

Need:

- ***R** to read a file or to list the contents of a directory
- ***W** to write to a file or add a file to a directory
- ***X** to traverse through a directory, e.g., `'/home/cjw'`

Managing Authorities and Ownership

Two sets of authority to manage

```
Change Authority (CHGAUT)

Type choices, press Enter.

Object . . . . . /roi
-----
User . . . . . *public      Name, *PUBLIC, *NTWIRF
                + for more values
New data authorities . . . . . *RX          ← *SAME, *NONE, *RWX, *RX...
New object authorities . . . . . *none       ← *SAME, *NONE, *ALL...
                + for more values
Authorization list . . . . .                Name, *NONE
Directory subtree . . . . . *ALL          *NONE, *ALL
Symbolic link . . . . . *NO             *NO, *YES
```

CHGAUT – Change Authority command

Note: the command requires a pathname for the OBJ parameter

Two sets of authority to manage

```
Work with Authority

Object . . . . . : /
Owner . . . . . : QSYS
Primary group . . . . . : ALANY
Authorization list . . . . . : AUTL

Type options, press Enter.
  1=Add user   2=Change user authority   4=Remove user

Opt  User          Data Authority  --Object Authorities--
      |            |            | Exist  Mgt  Alter  Ref
-----|-----|-----|-----|-----|-----|-----|
-    *PUBLIC      *RX
-    QSYS         *RWX      X     X     X     X
-    QDIRSRV     *X

Parameters or command
===>

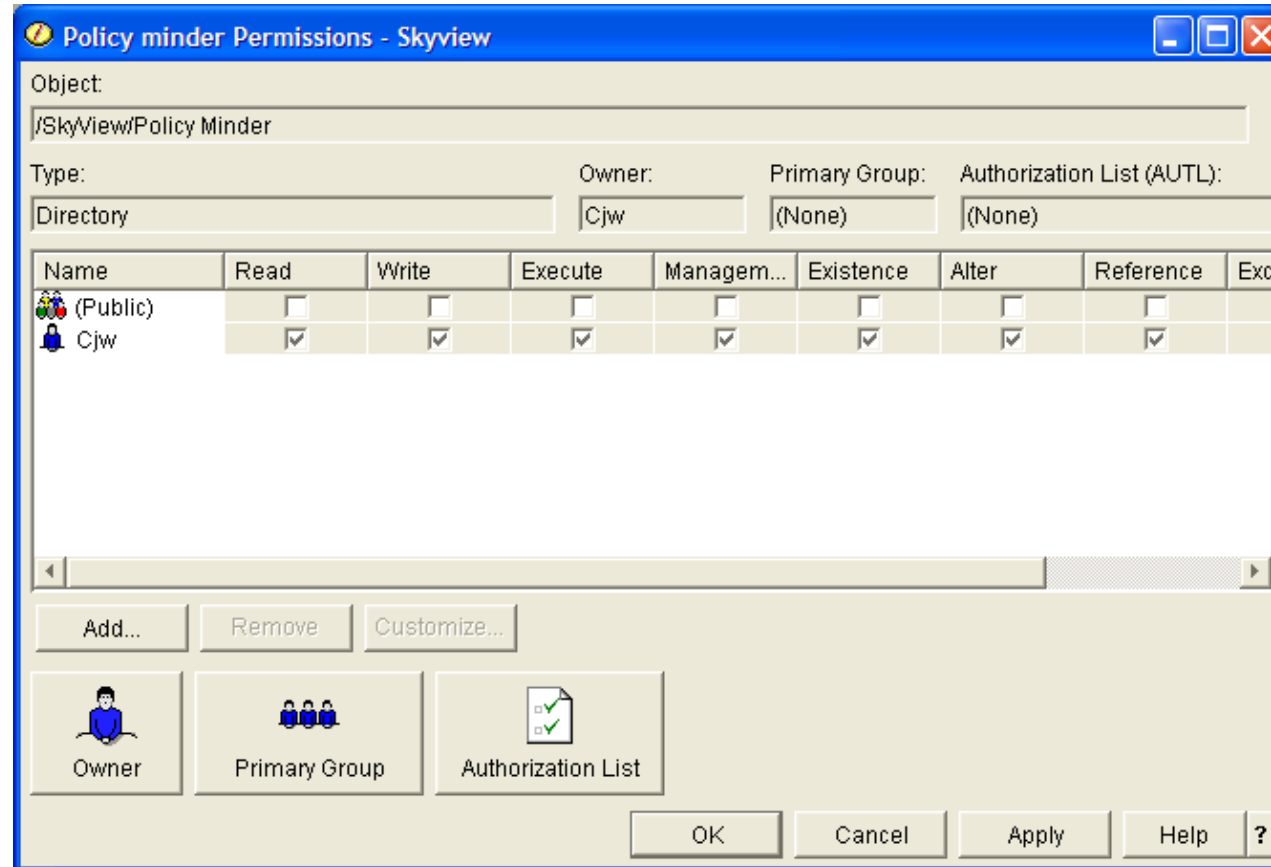
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve
F11=Display detail data authorities  F12=Cancel   F24=More keys

Bottom
```

WRKAUT – Work with Authority command

Note: This is the recommended setting for '/' Data authorities *RX, Object authorities *NONE

Working with Permissions in System iNavigator



Navigate to
the file

Right click,
choose
Permissions

Change Owner (CHGOWN)

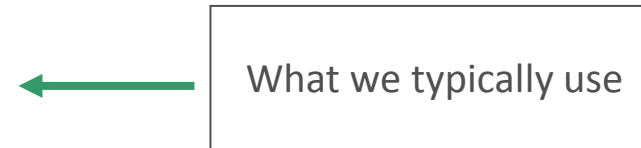
```
Session A - [24 x 80]
File Edit View Communication Actions Window Help
Change Owner (CHGOWN)
Type choices, press Enter.
Object . . . . . /FinancialApp
New owner . . . . . APP_OWN
Revoke current authority . . . . *YES
Directory subtree . . . . . *all
Symbolic link . . . . . *NO
Name
*NO, *YES
*NONE, *ALL
*NO, *YES
F3=Exit F4=Prompt F5=Refresh
F24=More keys
MA A
128 1902 - Session successfully started
```

```
Change Owner (CHGOWN)
Type choices, press Enter.
Object . . . . . /QSYS.LIB/ProdLib.lib/*.file
New owner . . . . . APP_OWN
Revoke current authority . . . . *YES
Directory subtree . . . . . *all
Symbolic link . . . . . *NO
Name
*NO, *YES
*NONE, *ALL
*NO, *YES
```

Adopted authority is ignored

Options:

- User has authorization through
 - *PUBLIC
 - Individual (private) authority for user or group
 - Primary group authority
 - Authorization list
- Use one of the swap APIs
 - Profile swap
 - Profile token
 - Set UID or Set GID



Planning to modify authorities

- Identify directory(s) to be secured
- Identify which users or processes are required to access the directories
 - Don't forget manual processes, batch jobs, etc that write to the directory
- Determine how to give them authority
 - Prefer private authority granted to a group or secured with an autl list
- Determine *PUBLIC authority setting

What authorities are needed?

- OBJAUT(*NONE) and DTAAUT(*X) **to traverse** all directories in a path
/Directory/SubDir1/SubDir2/SubDir3
- OBJAUT(*NONE) and DTAAUT(*RX) to the directory **to read or list** the contents
 - Directory
 - File1
 - File2
- OBJAUT(*NONE) and DTAAUT(*RWX) to the directory **to create** objects into it
- OBJAUT(*NONE) and DTAAUT(*WX) to the directory **to rename or delete** objects
- OBJAUT (*OBJMGT) at the object level for objects **to copy or rename**
- OBJAUT(*OBJEXIST) at the object level for objects **to delete**

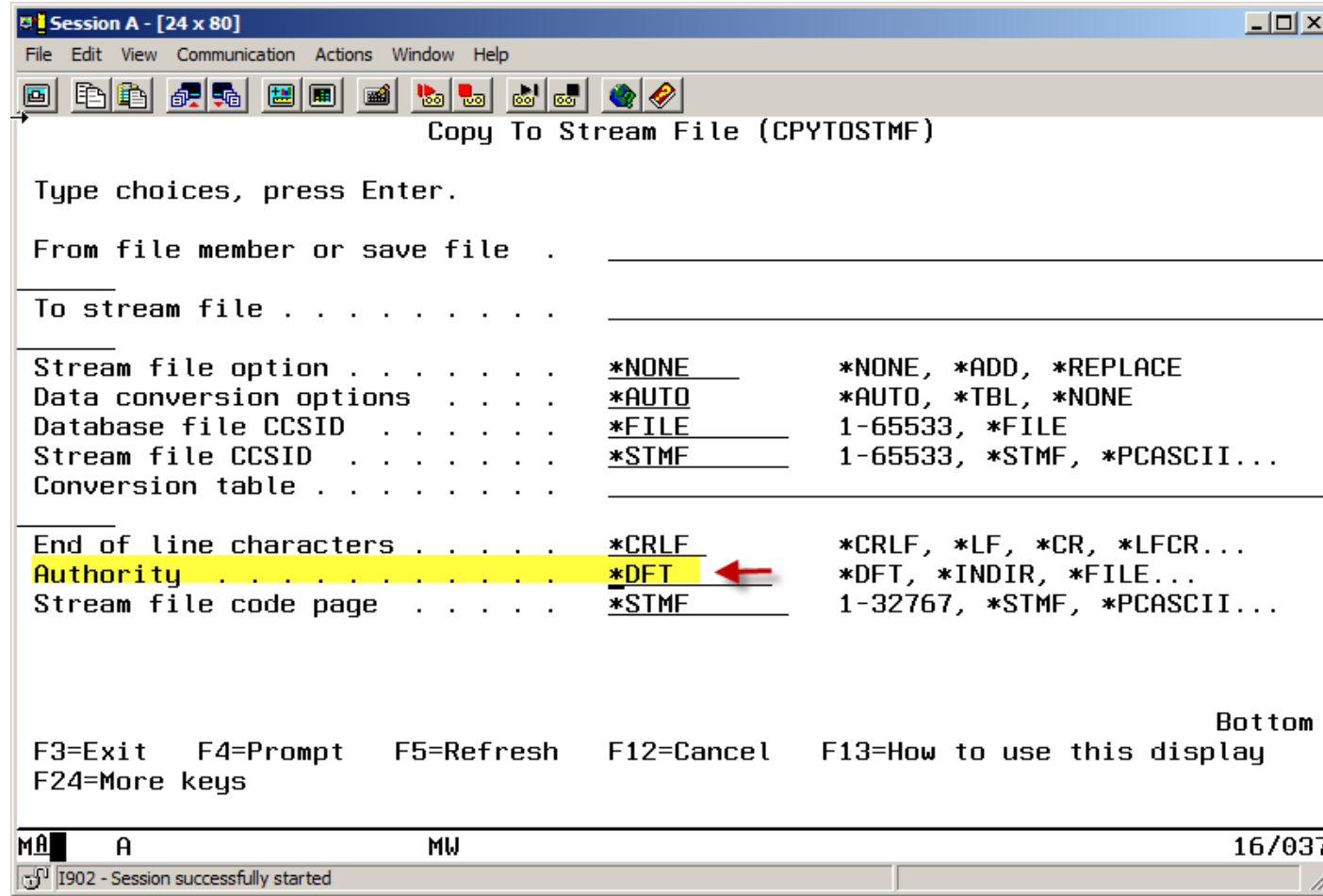
- root ('/') CANNOT be set to *EXCLUDE – many things will start to fail
 - Should be *PUBLIC DTAAUT(*RX) OBJAUT(*NONE)
 - But check to make sure that no temporary objects are being created / deleted into root prior to securing
- What applies to '/' can be applied to '/QOpenSys'
- Directories shipped by IBM are generally OK
 - May want to secure '/home' with OBJAUT(*NONE) DTAAUT(*RX) and create directories for individuals
- Do NOT remove private authorities granted to IBM profiles !

*PUBLIC authority

Ignores QCRTAUT system value, so how is *PUBLIC set?

- Typically inherits ALL authorities of the directory it's being created into
 - Authorization list, *PUBLIC, private, etc
- Exceptions:
 - CPYTOIMPF and CPYTOSTMF
 - Does not copy private authorities or AUTL
 - *PUBLIC and primary group are set to *EXCLUDE
 - Owner has *RWX
 - Need to change after the create using CHGAUT
 - Behavior changed in V6R1 – now have the option to inherit from the directory
 - creat(), move(), mkdir() APIs where the authority can be specified

CPYTOSTMF as of V6R1



- QSCANFS – Scan file system
 - *NONE or *ROOTUPOD – every stream file in '/', QOpenSys and user-defined file systems are scanned
 - Works together the QIBM_QPOL_SCAN_OPEN (Scan on Open) and QIBM_QPOL_SCAN_CLOSE (Scan on Close) exit points to define what program does the scanning.
 - Documented in the API section of the Info Center.
- QSCANFSCTL – Scan file system control parameters
 - Determines which objects and when objects within a file system are scanned (for example – scan only when the object is changed.)
 - Determines the action to take when the scan fails.
 - Works together with new attributes on *DIR (*CRTOBJSCAN) and *STMF (*SCAN)
- Originally added to enable real-time virus scanning but can also be used for encryption.

Proliferation of private authorities

/Images/2014/Finance/January

/Images – Created by (therefore, owned by): Gibbs

/Images/2014 – Owner: Tony, Private authority – Gibbs

/Images/2014/Finance – Owner: Tim, Private authorities – Gibbs, Tony

/Images/2014/Finance/January – Owner: Abby, Private auts – Gibbs, Tony, Tim

/Images/2014/Finance/January/xxxxx.doc – Owner: App_Profile

Images will be owned by App_Profile and each will have a private authority for Gibbs, Tony, Tim and Abby. Discover via PRTPRFINT (Print profile internals)

Auditing and the IFS

Configuring auditing on an IFS object

```
Change Auditing Value (CHGAUD)
Type choices, press Enter.
Object . . . . . /ProdWebsite/Orders/Credit cards.stmf
Object auditing value . . . . . *all_ *NONE, *USRPRF, *CHANGE, *ALL

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
```



CHGAUD – Change Auditing command

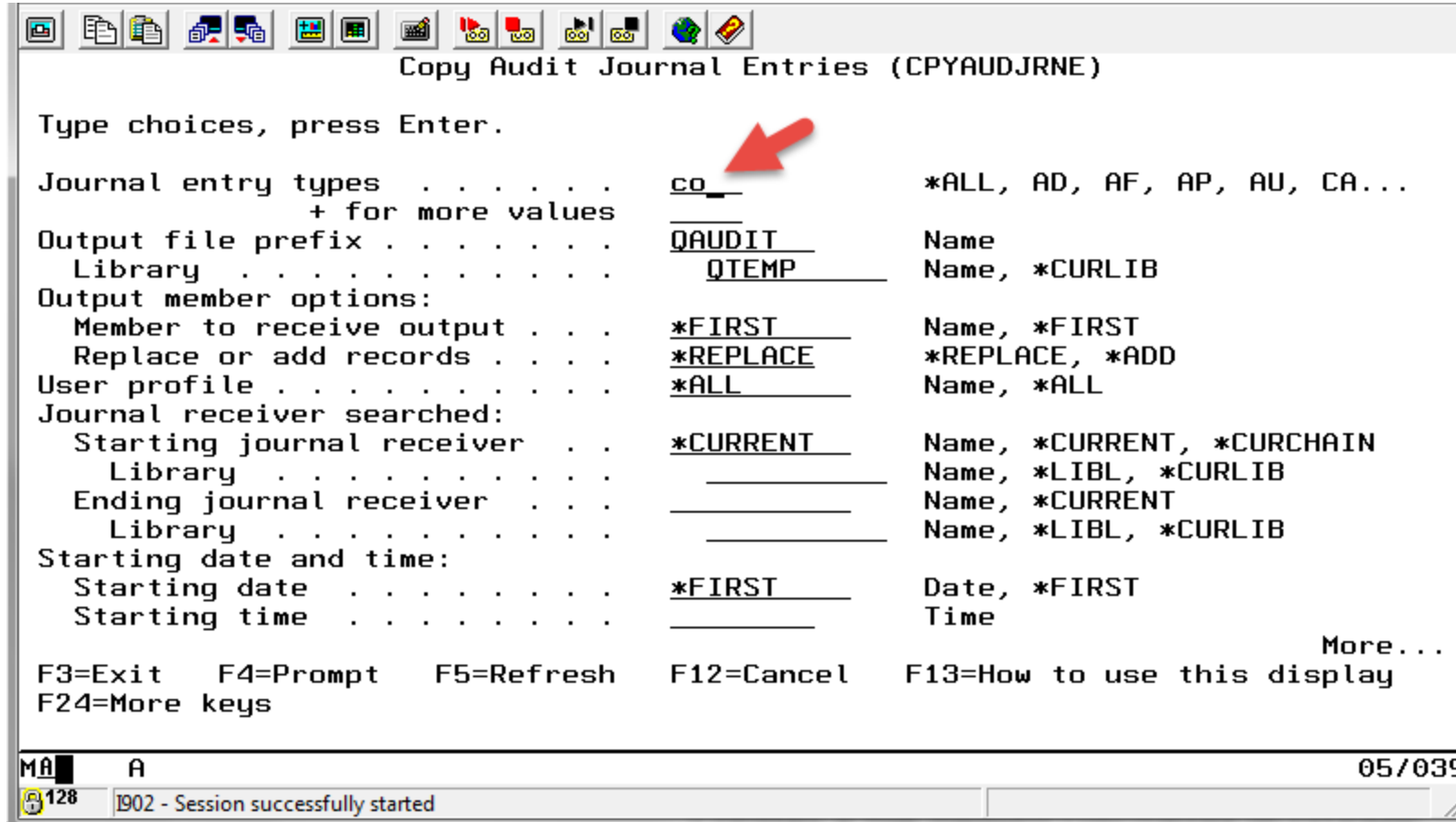
Output from DSPAUDJRNE

```
Display Report
Query . . . . : QSYS/QSECCO      Report width . . . . . : 204
Position to line . . . . .      Shift to column . . . . .
Line  . . . .+ . . . .1. . . .+ . . . .2. . . .+ . . . .3. . . .+ . . . .4. . . .+ . . . .5. . . .+ . . . .6. . . .+ . . . .7. . . .
      Entry User   Object   Library   Object   Office   DLO
      type  profile name     name     type     user     name
034406 CO  N   QSYS     *N        *N        *SOCKET
034407 CO  N   QSYS     *N        *N        *SOCKET
034408 CO  N   QSYS     *N        *N        *SOCKET
034409 CO  N   QSYS     *N        *N        *SOCKET
034410 CO  N   QSYS     *N        *N        *SOCKET
034411 CO  N   QSYS     *N        *N        *SOCKET
034412 CO  N   QSECOFR *N        *N        *STMF
034413 CO  N   QSECOFR *N        *N        *STMF
034414 CO  N   QSYS     *N        *N        *SOCKET
034415 CO  N   CJW     TEST2     CJW       *DTAARA
034416 CO  N   CJW     *N        *N        *DIR
034417 CO  N   QSYS     *N        *N        *SOCKET
034418 CO  N   CJW     *N        *N        *STMF
***** ***** End of report *****
Bottom
F3=Exit      F12=Cancel   F19=Left     F20=Right    F21=Split
MA A 03/033
128 1902 - Session successfully started
```

*N indicates an IFS object named with a pathname

- *N in the Object Name field of an audit entry using DSPAUDJRNE indicates the object is a pathname (an object in the IFS)
- Pathname is a 5002 character field at the end of the audit journal entry
- Use CPYAUDJRNE command to display and view the results in QTEMP/QAUDITxx

CPYAUDJRNE – Copy Audit Journal Entries



Creates a file named QAUDITxx in QTEMP

Results of query / SQL of QTEMP/QAUDITCO

```
Display Data
Data width . . . . . : 5050
Position to line . . . . . Shift to column . . . . .
....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....
Timestamp          User      Object   Path
                  profile   type     name
2015-08-15-20.22.46.503232 CJW      *STMF    /SkyView/emailtemp/Q132.txt
2015-08-15-20.22.46.904864 CJW      *STMF    /SkyView/emailtemp/FRPWINVSGN
2015-08-15-20.22.47.029840 CJW      *STMF    /SkyView/Policy Minder/FRPWIN
2015-08-15-20.22.47.304736 CJW      *STMF    /SkyView/emailtemp/Q133.txt
2015-08-15-20.22.47.528624 CJW      *STMF    /SkyView/emailtemp/FRSVSYSVAL
2015-08-15-20.22.47.569728 CJW      *STMF    /SkyView/Policy Minder/FRSVSY
2015-08-15-20.22.49.769120 CJW      *STMF    /SkyView/emailtemp/Q134.txt
2015-08-15-20.22.50.061792 CJW      *STMF    /SkyView/emailtemp/FRCPPRFCHG
2015-08-15-20.22.50.104464 CJW      *STMF    /SkyView/Policy Minder/FRCPPR
2015-09-07-14.15.42.933936 CJW      *STMF    /SkyView/Policy Minder/Compli
2015-11-15-09.42.52.368448 CJW      *DIR     /tmp/.com_ibm_tools_attach/18
2015-11-15-09.42.52.381520 CJW      *STMF    /tmp/.com_ibm_tools_attach/18
2015-11-15-09.42.52.418656 CJW      *STMF    /tmp/.com_ibm_tools_attach/18
2015-11-16-20.11.04.816976 CJW      *DIR     /newdirectory
2015-11-16-20.13.32.268928 CJW      *STMF    /cjwtest.dat

F3=Exit      F12=Cancel   F19=Left    F20=Right   F21=Split   More...

MA  A  03/032
128  B02 - Session successfully started
```

Miscellaneous

Tools for managing IFS authorities - SECTOOLS

```
Print Publicly Auth Objects (PRTPUBAUT)

Type choices, press Enter.


Object type . . . . . > *DIR          *ALRTBL, *AUTL, *BLKSF...
Changed report only . . . . . *NO      *NO, *YES
Directory . . . . . '/'

-----
Search subdirectory . . . . . *NO      *NO, *YES

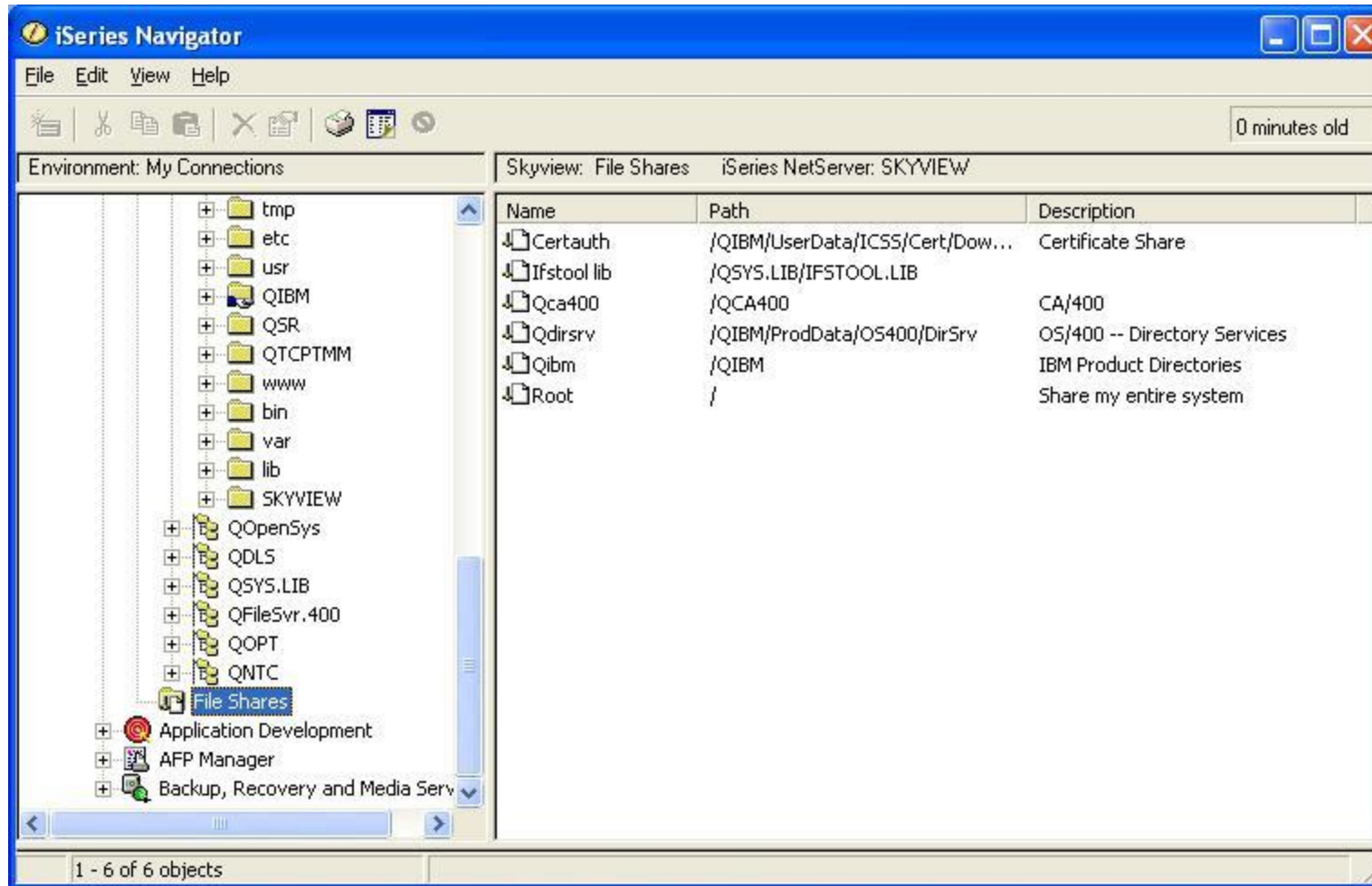
Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

SECTOOLS – PRTPUBAUT and PRTPVTAUT

Note: Use caution when specifying *YES to search subdirectory!

- File shares make the directory “available” to the network
- Many systems have shared '/' (root)
-  – This is a HUGE exposure because it shares /QSYS.LIB – in other words – all libraries on the system. If data is not protected, this is an easy way to corrupt data
- Manage file shares through System i Navigator or Navigator for i

File shares



Navigate to the directory

Right click

Choose Sharing, New sharing to define a new share

A hand underneath the folder indicates a share

- Shares can be Read only or Read/Write
- Underlying IBM i authorities on the object determine final access

Tips for controlling:

- Secure the QZLSADFS (Add file share) and QZLSCHRS (Change file share) APIs
- Add a \$ to hide the share from Windows Network Neighborhood (won't be broadcast/discoverable)
e.g., root\$
- Set authority to the QPWFSEVER authorization list to *EXCLUDE
- Create the share as Read only

- Shares can be Read only or Read/Write
- Underlying IBM i authorities on the object determine final access

Hints for controlling:

- Secure the QZLSADFS (Add file share) and QZLSCHRS (Change file share) APIs
 - Set to *PUBLIC *EXCLUDE
- Add a \$ to hide the share from Windows Network Neighborhood (won't be broadcast/discoverable)
e.g., root\$

Root (/) should not be shared

Sharing root also shared /QSYS.LIB

If share cannot be removed:

- Add a '\$' to the end of the share name, e.g., share\$
 - Prevents the share from being discoverable
- Set QPWFSERVER autl to *PUBLIC *EXCLUDE, authorizing specific users
 - Prevents access to libraries in interfaces such as Windows Explorer

Managing Access with QPWFSERVER Autl

```
                                Edit Authorization List
Object . . . . . : QPWFSERVER      Owner . . . . . : QSYS
Library . . . . . : QSYS          Primary group . . . : *NONE

Type changes to current authorities, press Enter.

User      Object      List
Authority Authority Mgt
*PUBLIC   *EXCLUDE  -
QSYS      *ALL      X
GRP_OPER  *USE      -

                                Bottom

F3=Exit   F5=Refresh  F6=Add new users
F11=Display detail object authorities  F12=Cancel  F24=More keys
(C) COPYRIGHT IBM CORP. 1980, 2003.
```

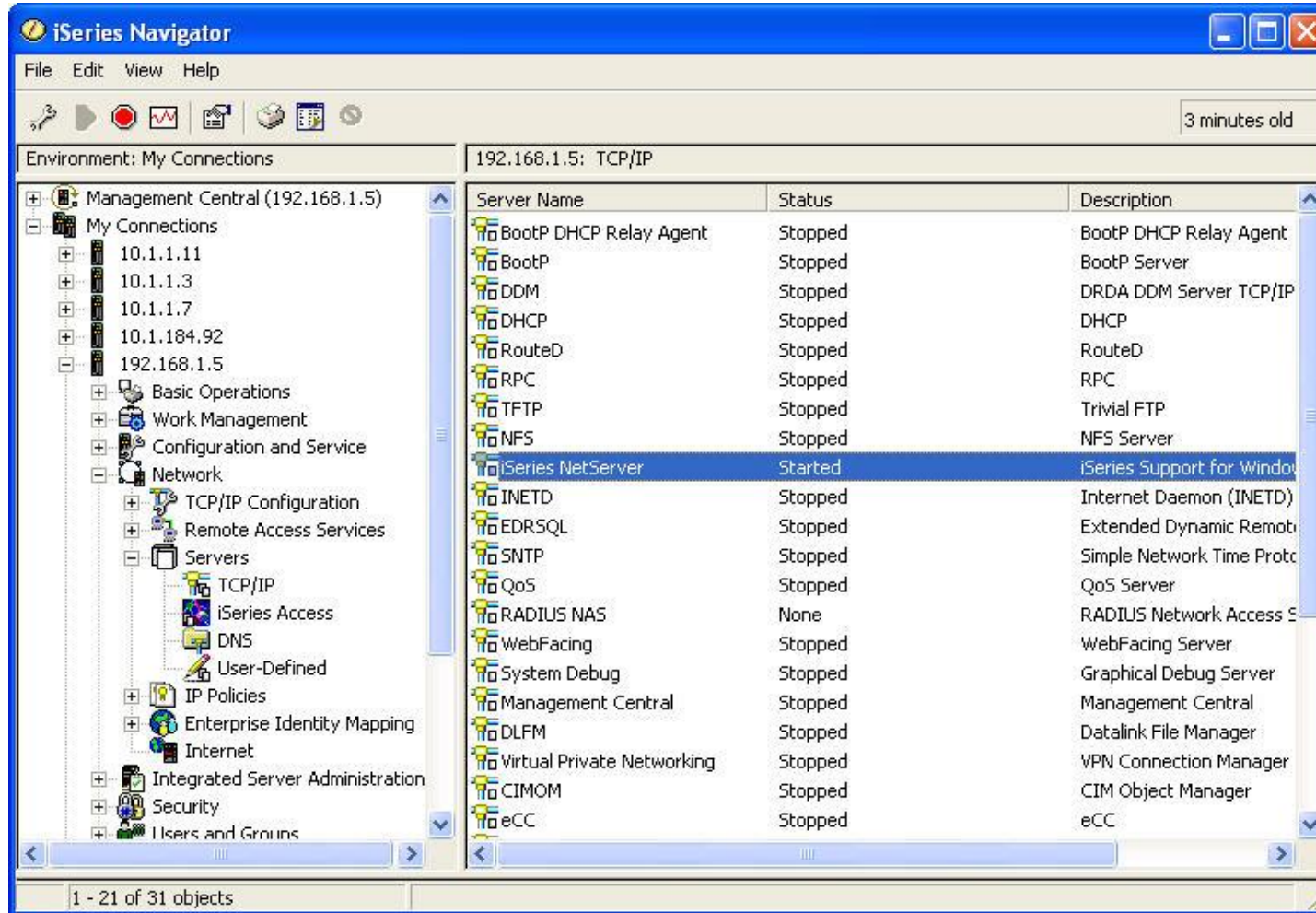
No authority – no access to QSYS.LIB file system using Explorer or System i Navigator.

Ignored when using other interfaces, e.g., FTP or ODBC

Ships with *PUBLIC *USE

Consider *EXCLUDE when root is shared

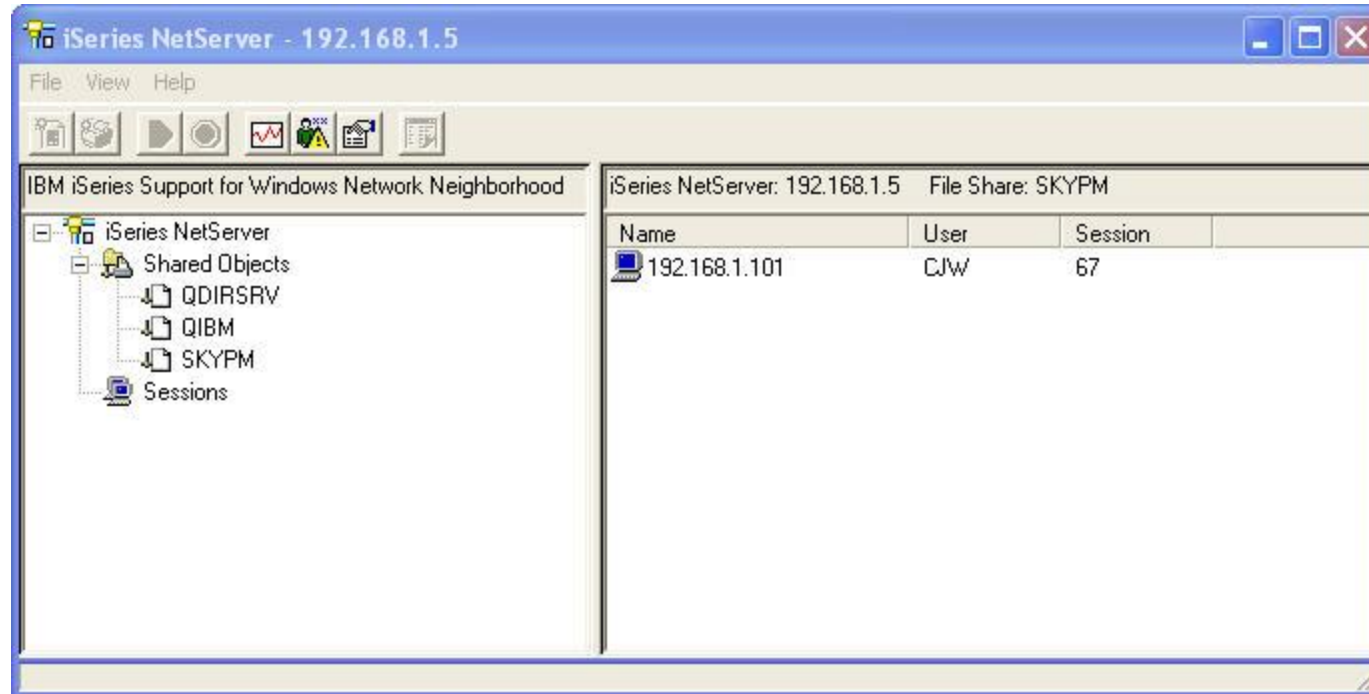
NetServer



Open the
system
name->
Network->
Servers->
TCP/IP

Right click on
iSeries
NetServer
choose
Properties

NetServer – Connections and Shares

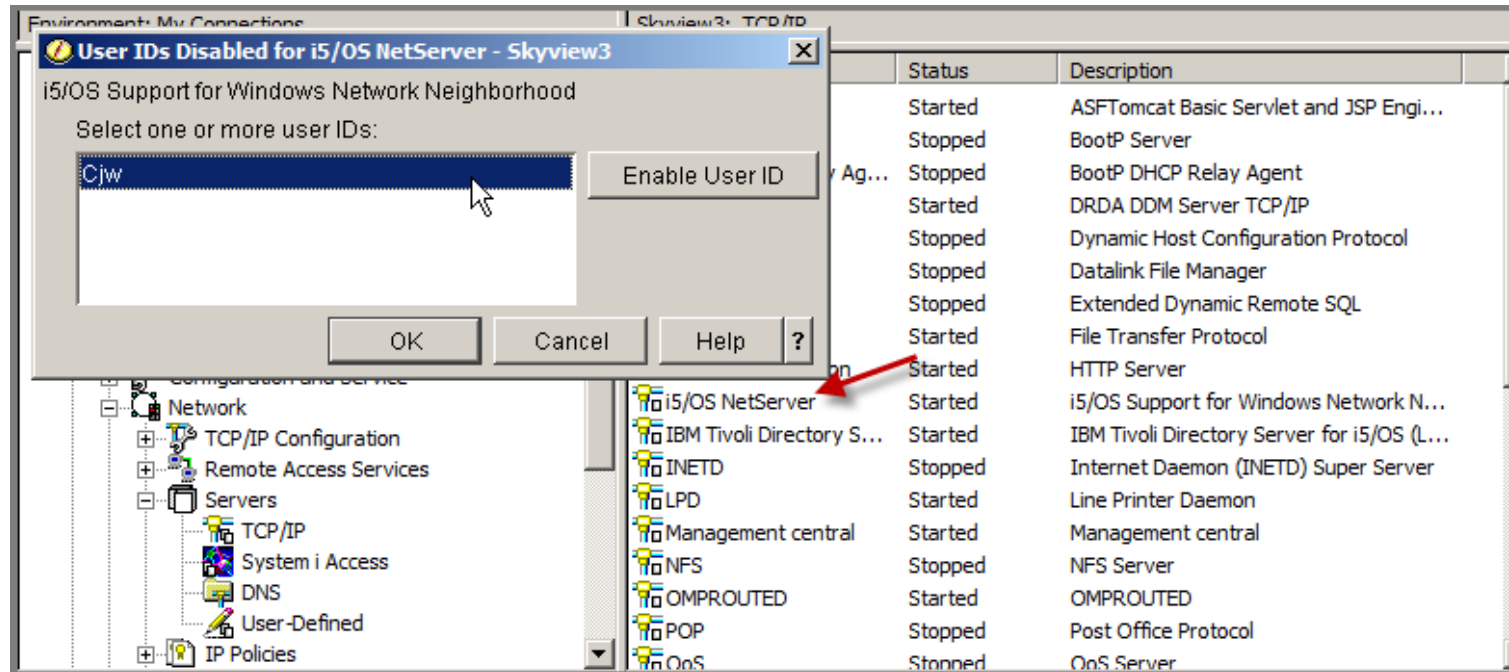


Right click on
NetServer.

Choose
Open

Use this to discover sessions connecting through various file shares

NetServer – Disabled Profiles



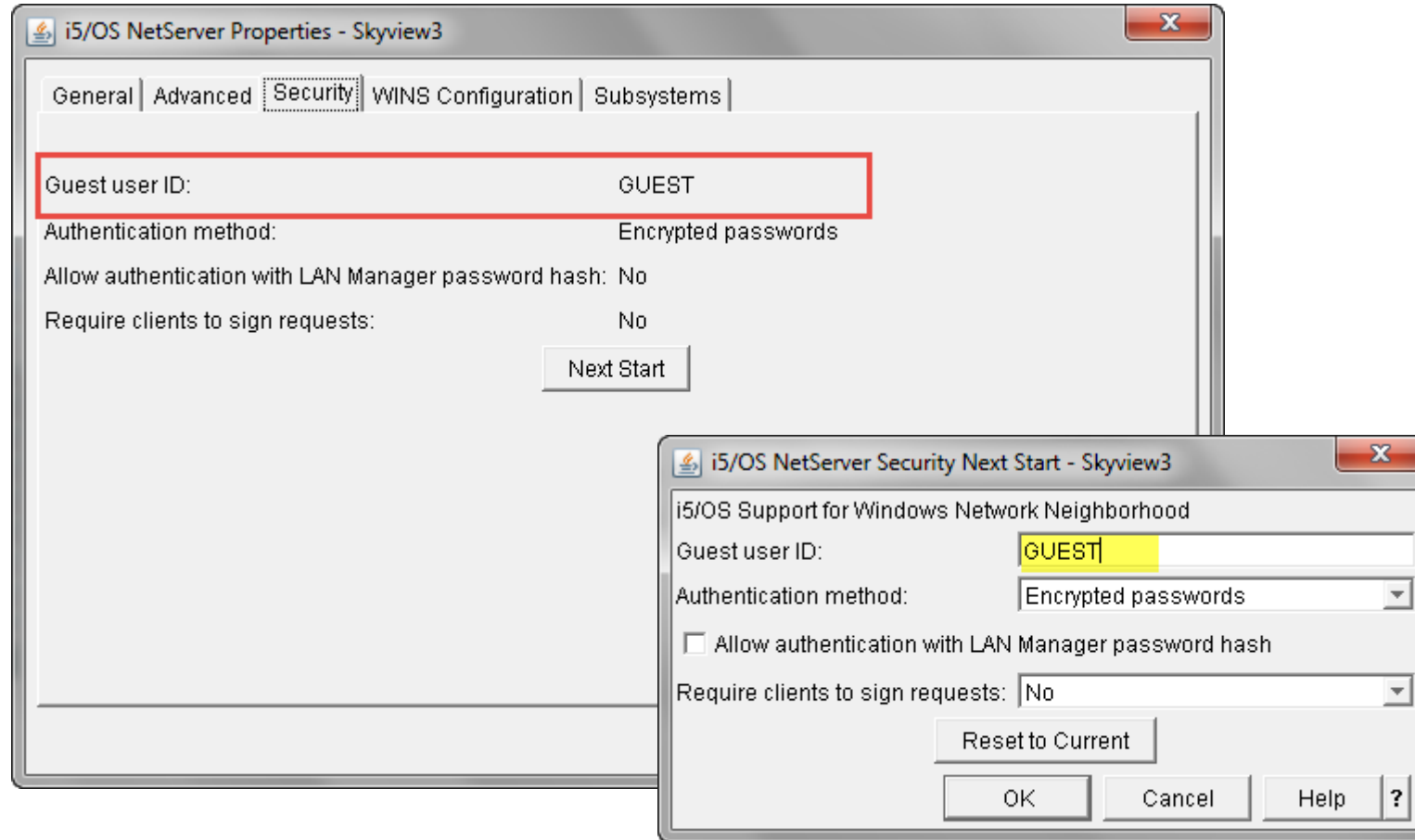
Right click on
NetServer.

Choose
Disabled
User IDs

- Only disabled NetServer profile NOT IBM i profile.
- Message CPIB682 sent to QSYSOPR for disabled NetServer users
- Enable through i Navigator or NetServer commands

<http://www-03.ibm.com/systems/i/software/netserver/qusrtool.html>

NetServer Guest Profile - Properties



Click on the Security tab

Click on Next Start

Wipe out the profile
named, click OK

Stop / Start the server

To hide the i5/OS NetServer from Windows Network Neighborhood:

- Open iSeries navigator system -> Network -> Servers->TCP/IP->Right click on NetServer, select Properties.
- Click on Advanced -> Next Start
- Specify 0 for "Browsing announcement interval."
- Go to the Advanced page, and click Next Start.

This stops all host announcements to the network.

- IBM i is 'virus resistant'
 - Not affected by most viruses currently available
 - In theory can be affected via PASE (Portable Application Solutions Environment) because it runs UNIX (AIX) executables
 - When a drive is mapped to the IFS can be affected by malware such as CryptoLocker
- IBM i is the perfect host
- Can have a 'wide-spread' virus only if written specifically for IBM i
- No virus scanner for IBM i proper, virus scanners for IFS only
 - Bytware (MacAfee signatures)

For More Information ...



- Contact us for more information on our services:
 - Managed Security Services (MSS)
 - SkyView Security Check-up
 - Remediation Services
 - Penetration (Pen) testing

info@helpsystems.com

[**www.helpsystems.com/professional-security-services**](http://www.helpsystems.com/professional-security-services)