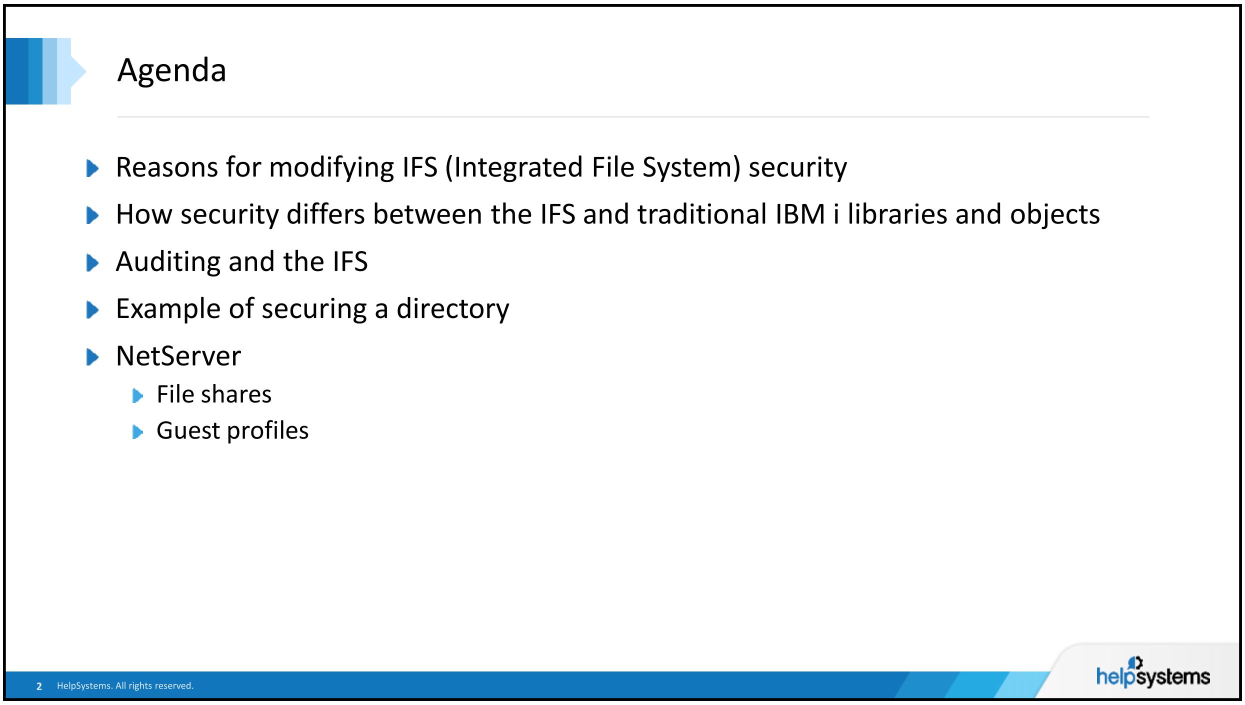
helpsystems

Coffee with Carol: Demystifying IFS Security

Carol Woodbury, CISSP, CRISC, PCIP
VP Global Security Services
carol.woodbury@helpsystems.com
@carolwoodbury
2018 IBM Champion

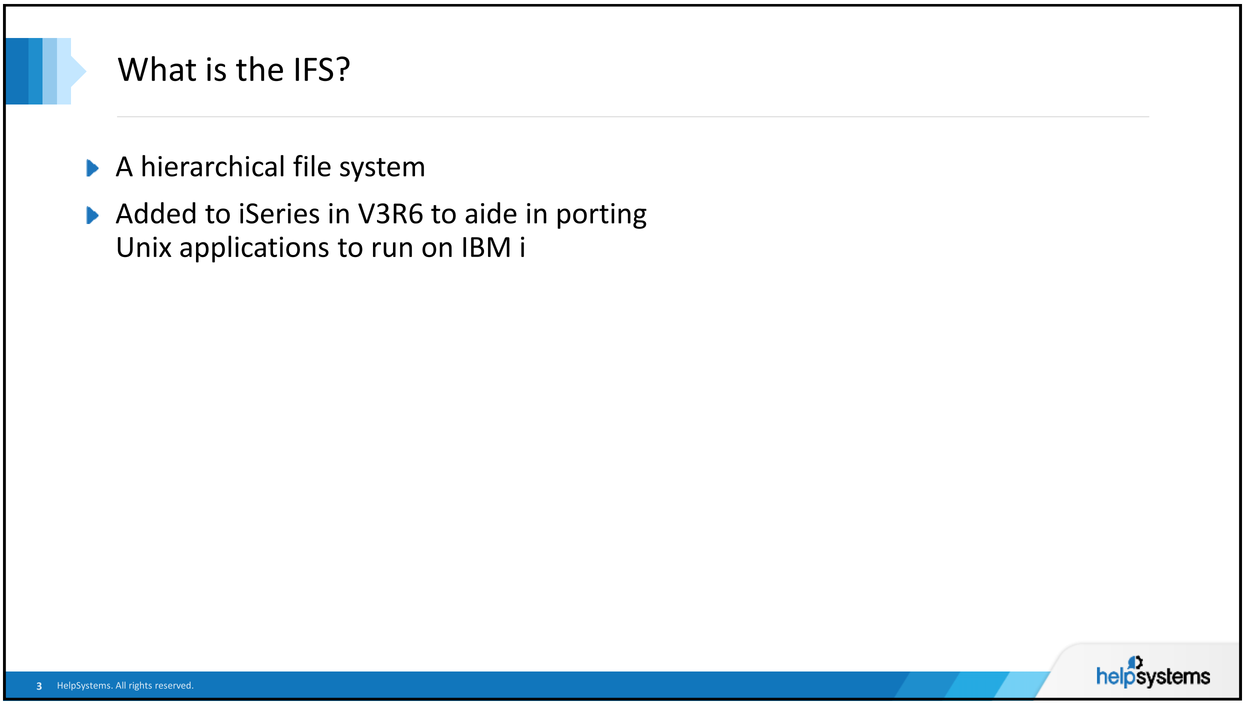
www.helpsystems.com



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
- Example of securing a directory
- NetServer
  - File shares
  - Guest profiles

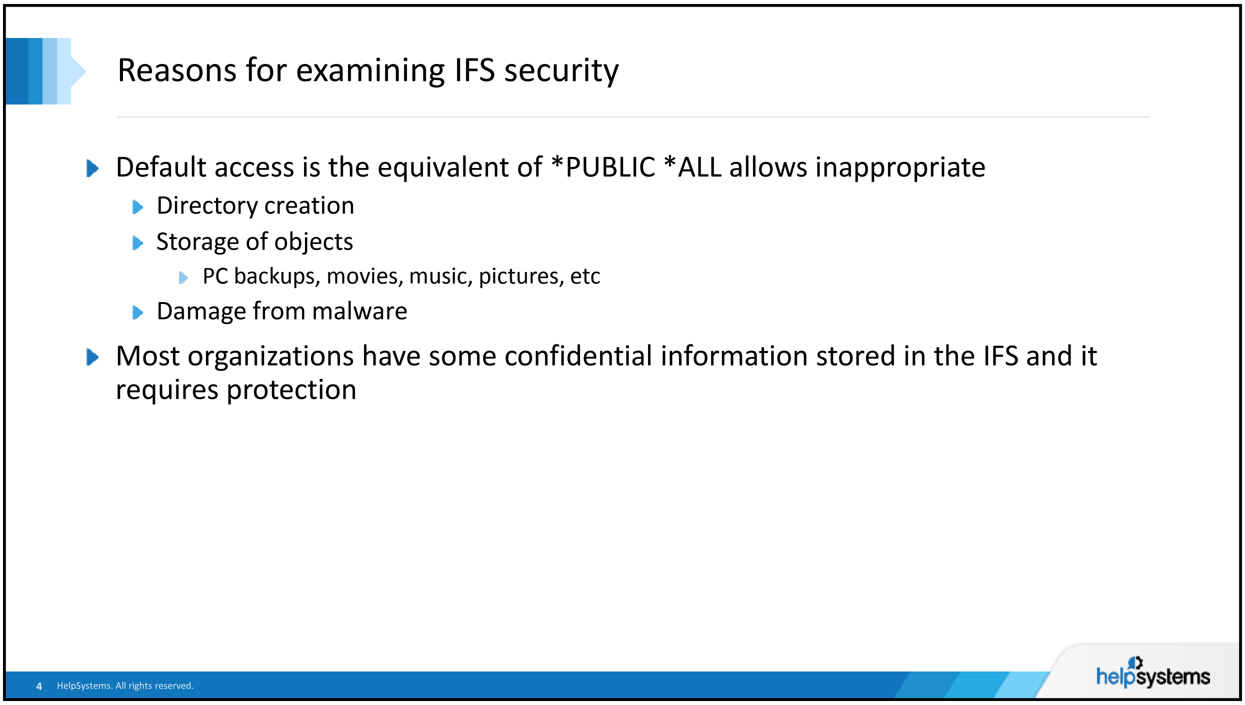
helpsystems



What is the IFS?

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

helpsystems

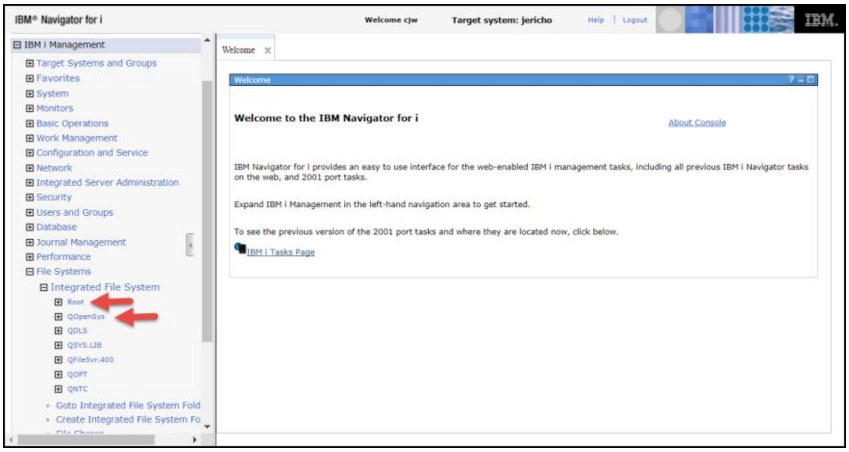


Reasons for examining IFS security

- Default access is the equivalent of *PUBLIC *ALL allows inappropriate
  - Directory creation
  - Storage of objects
    - PC backups, movies, music, pictures, etc
  - Damage from malware
- Most organizations have some confidential information stored in the IFS and it requires protection

helpsystems

Which file systems?



Welcome to the IBM Navigator for i

IBM Navigator for i provides an easy to use interface for the web-enabled IBM i management tasks, including all previous IBM i Navigator tasks on the web, and 2001 port tasks.

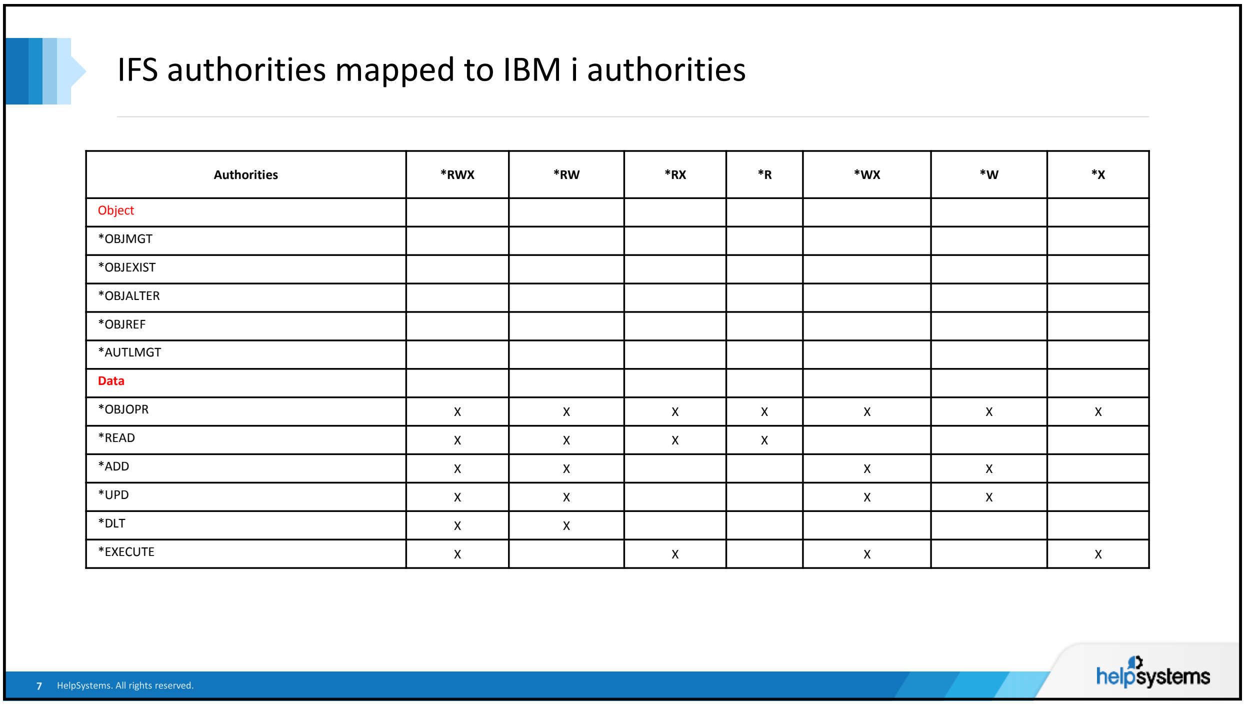
Expand IBM i Management in the left-hand navigation area to get started.

To see the previous version of the 2001 port tasks and where they are located now, click below.

All statements made apply to both /Root and /QOpenSys

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

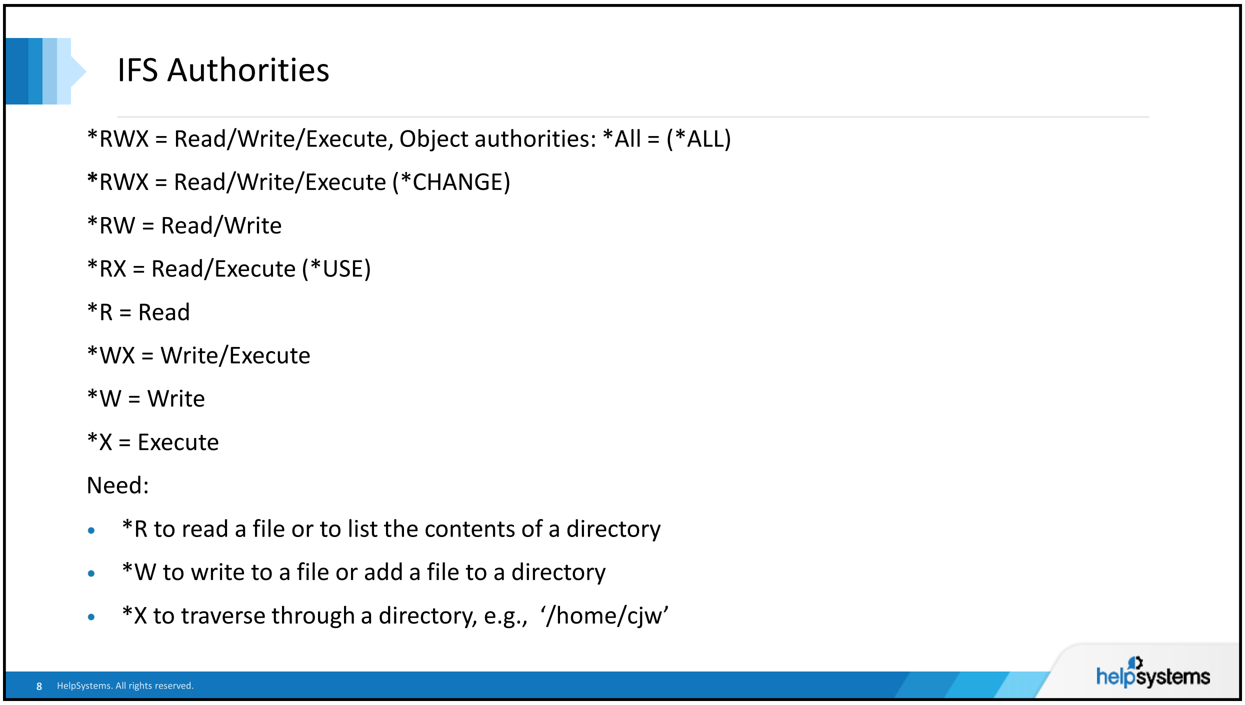
Same	Different
Authority checking algorithm	Authority names *RWX vs *CHANGE
*PUBLIC authority	Ignores QCRTAUT system value
Can use authorization lists and private authorities	Ignores ownership setting in User profile
	Ignores adopted authority
	Need to look in different audit fields



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

7 HelpSystems. All rights reserved.



IFS Authorities

*RWX = Read/Write/Execute, Object authorities: *All = (*ALL)

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

*RW = Read/Write

*RX = Read/Execute (*USE)

*R = Read

*WX = Write/Execute

*W = Write

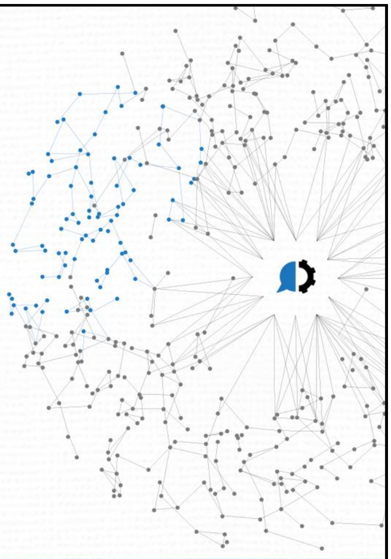
*X = Execute

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'

8 HelpSystems. All rights reserved.

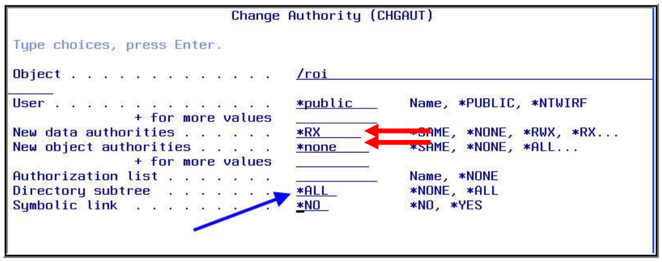
Managing Authorities and Ownership



UP NEXT

helpsystems

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
```

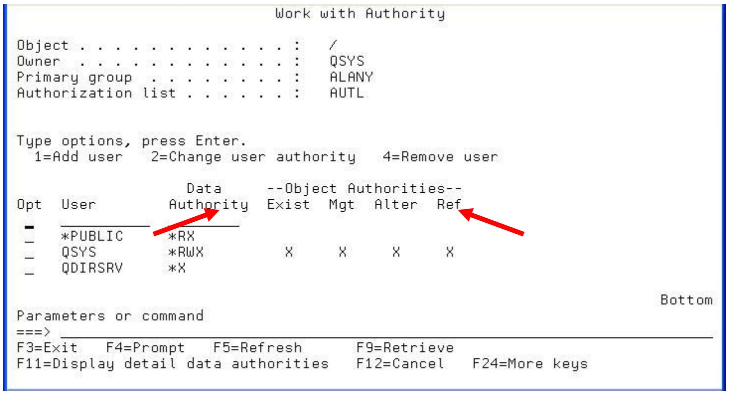
CHGAUT – Change Authority command

Must consider the appropriate authority for both the Data authorities and the Object authorities

Specifying *ALL for Directory subtree allows you to set the authorities on the entire path

helpsystems

Two sets of authority to manage



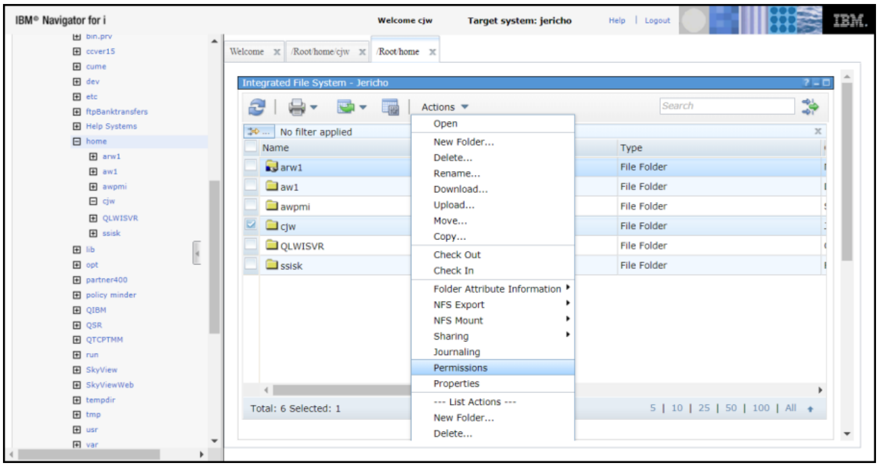
```
                           Work with Authority

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


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

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

                                                          Bottom
Parameters or command
===> ___________________________________________________________
F3=Exit   F4=Prompt   F5=Refresh      F9=Retrieve
F11=Display detail data authorities   F12=Cancel   F24=More keys
```

WRKAUT – Work with Authority command

Note: This is the recommended setting for '/'

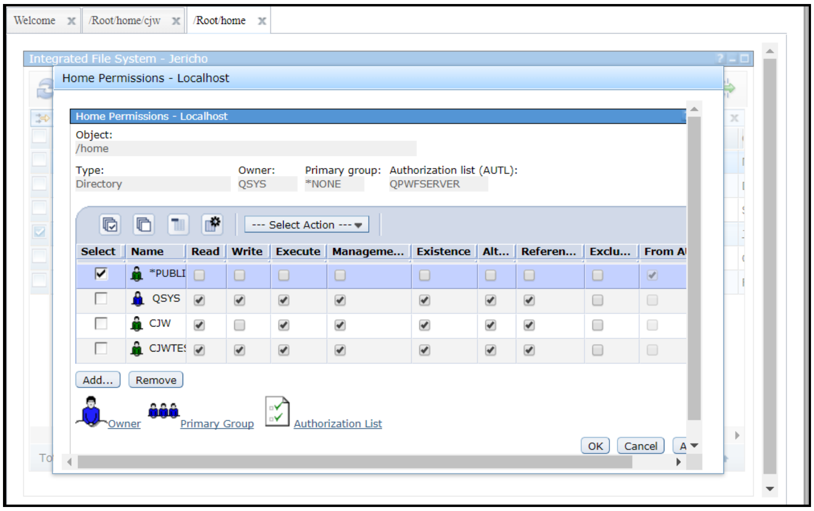
Data authorities *RX, Object authorities *NONE

Working with permissions in Navigator for i



Name	Type
arw1	File Folder
aw1	File Folder
awpmi	File Folder
cjw	File Folder
QLWISVR	File Folder
ssisk	File Folder

Permissions and Change ownership



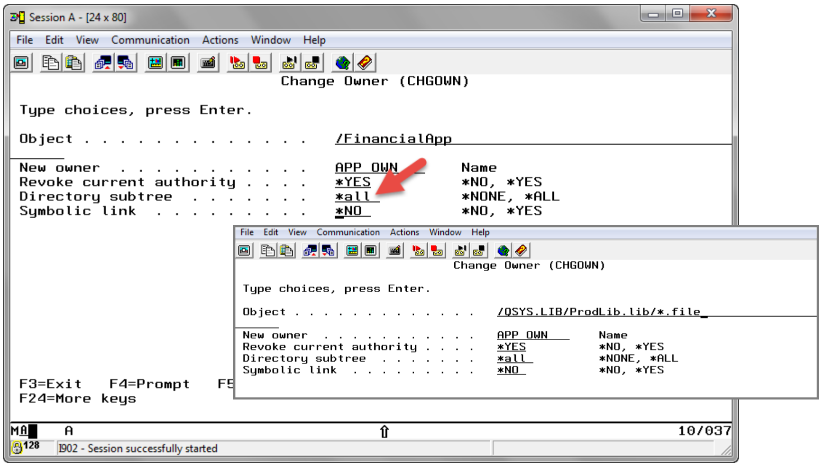
Home Permissions - Localhost

Object:
/home

Type: Directory
Owner: QSYS
Primary group: *NONE
Authorization list (AUTL): QPWFSERVER

Select	Name	Read	Write	Execute	Manageme...	Existence	Alt...	Referen...	Exclu...	From A
☑	*PUBLI	☐	☐	☐	☐	☐	☐	☐	☐	☑
☐	QSYS	☑	☑	☑	☑	☑	☑	☑	☐	☐
☐	CJW	☑	☐	☑	☑	☑	☑	☑	☐	☐
☐	CJWTE	☑	☑	☑	☑	☑	☑	☑	☐	☐

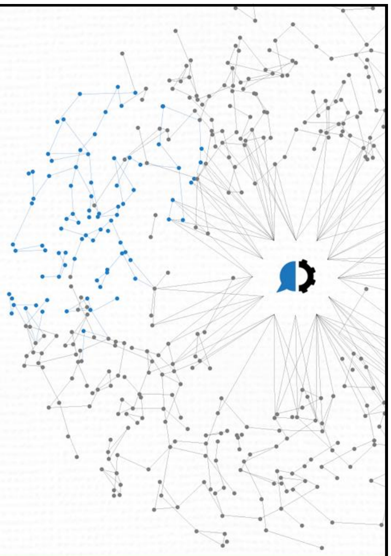
Change Owner (CHGOWN)



```
                         Change Owner (CHGOWN)

Type choices, press Enter.

Object . . . . . . . . . . . . .   /FinancialApp

New owner  . . . . . . . . . . .   APP_OWN          Name
Revoke current authority . . . .   *YES             *NO, *YES
Directory subtree  . . . . . . .   *all             *NONE, *ALL
Symbolic link  . . . . . . . . .   *NO              *NO, *YES

F3=Exit   F4=Prompt   F5
F24=More keys

MA   A                                                      10/037
128  I902 - Session successfully started
```

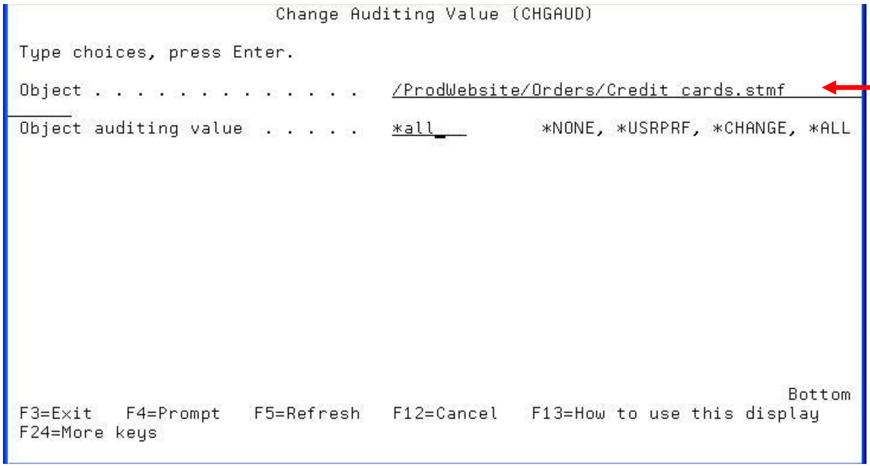
```
                         Change Owner (CHGOWN)

Type choices, press Enter.

Object . . . . . . . . . . . . .   /QSYS.LIB/ProdLib.lib/*.file_

New owner  . . . . . . . . . . .   APP_OWN          Name
Revoke current authority . . . .   *YES             *NO, *YES
Directory subtree  . . . . . . .   *all             *NONE, *ALL
Symbolic link  . . . . . . . . .   *NO              *NO, *YES
```

Auditing and the IFS



UP NEXT

Configuring auditing on an IFS object



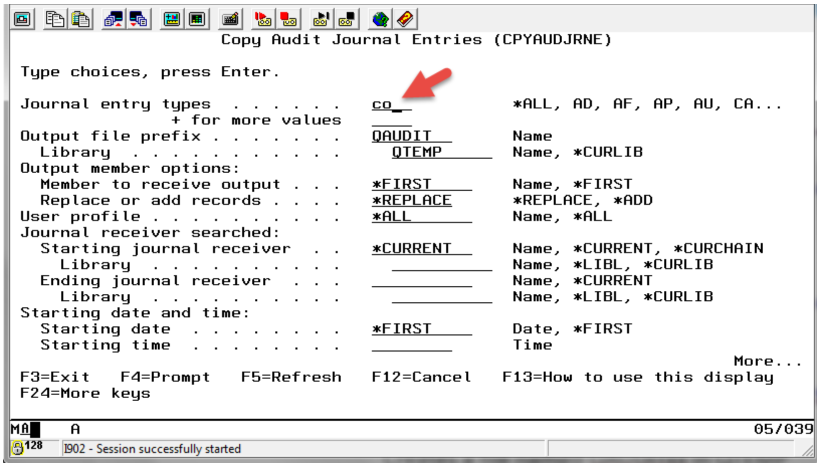
```
                    Change Auditing Value (CHGAUD)

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

IFS audit entries

- *N in the Object Name field of an audit entry 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

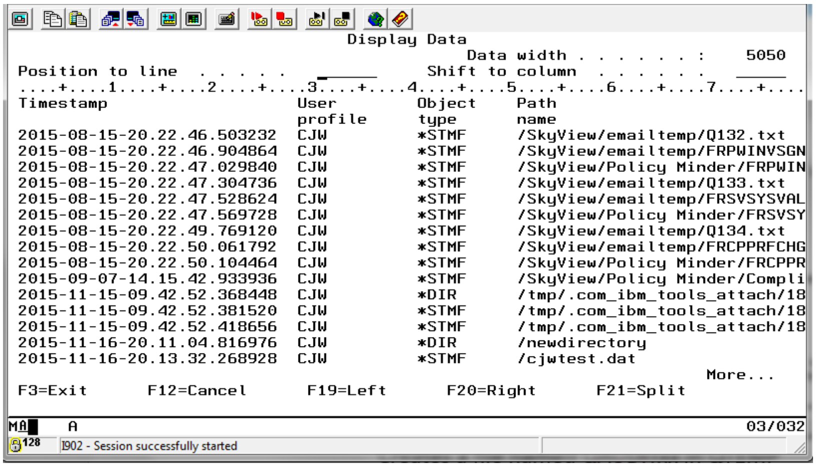
CPYAUDJRNE – Copy Audit Journal Entries



```
                    Copy Audit Journal Entries (CPYAUDJRNE)

 Type choices, press Enter.

 Journal entry types  . . . . . . .   co_            *ALL, AD, AF, AP, AU, CA...
                + for more values     ____
 Output file prefix . . . . . . . .   QAUDIT         Name
   Library  . . . . . . . . . . . .     QTEMP        Name, *CURLIB
 Output member options:
   Member to receive output . . . .   *FIRST         Name, *FIRST
   Replace or add records . . . . .   *REPLACE       *REPLACE, *ADD
 User profile . . . . . . . . . . .   *ALL           Name, *ALL
 Journal receiver searched:
   Starting journal receiver  . . .   *CURRENT       Name, *CURRENT, *CURCHAIN
     Library  . . . . . . . . . . .     __________   Name, *LIBL, *CURLIB
   Ending journal receiver  . . . .   __________     Name, *CURRENT
     Library  . . . . . . . . . . .     __________   Name, *LIBL, *CURLIB
 Starting date and time:
   Starting date  . . . . . . . . .   *FIRST         Date, *FIRST
   Starting time  . . . . . . . . .   ________       Time
                                                                         More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys

MA    A                                                                  05/039
128   I902 - Session successfully started
```

Creates a file named QAUDIT**CO** in QTEMP

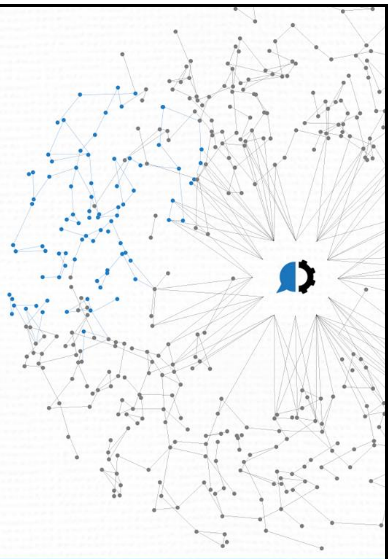
Results of query / SQL of QTEMP/QAUDITCO



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

MA     A                                                              03/032
128   I902 - Session successfully started
```

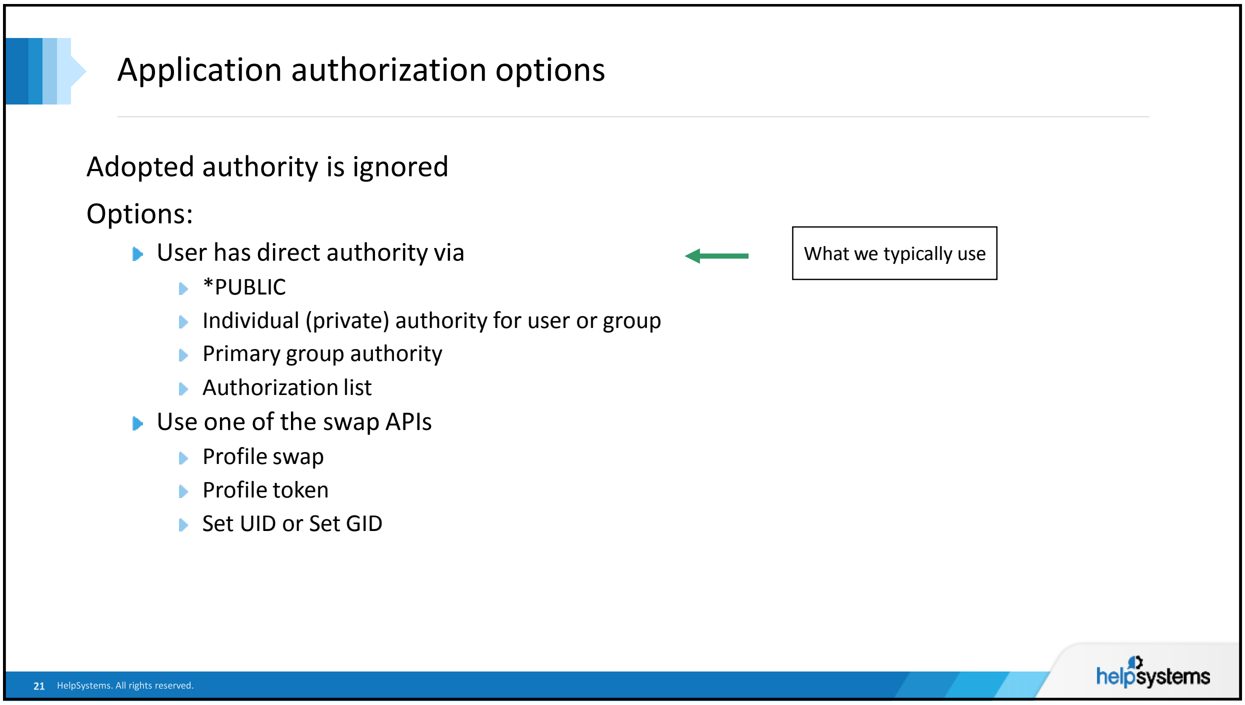
helpsystems

Changing Authorities on a Directory



UP NEXT

helpsystems



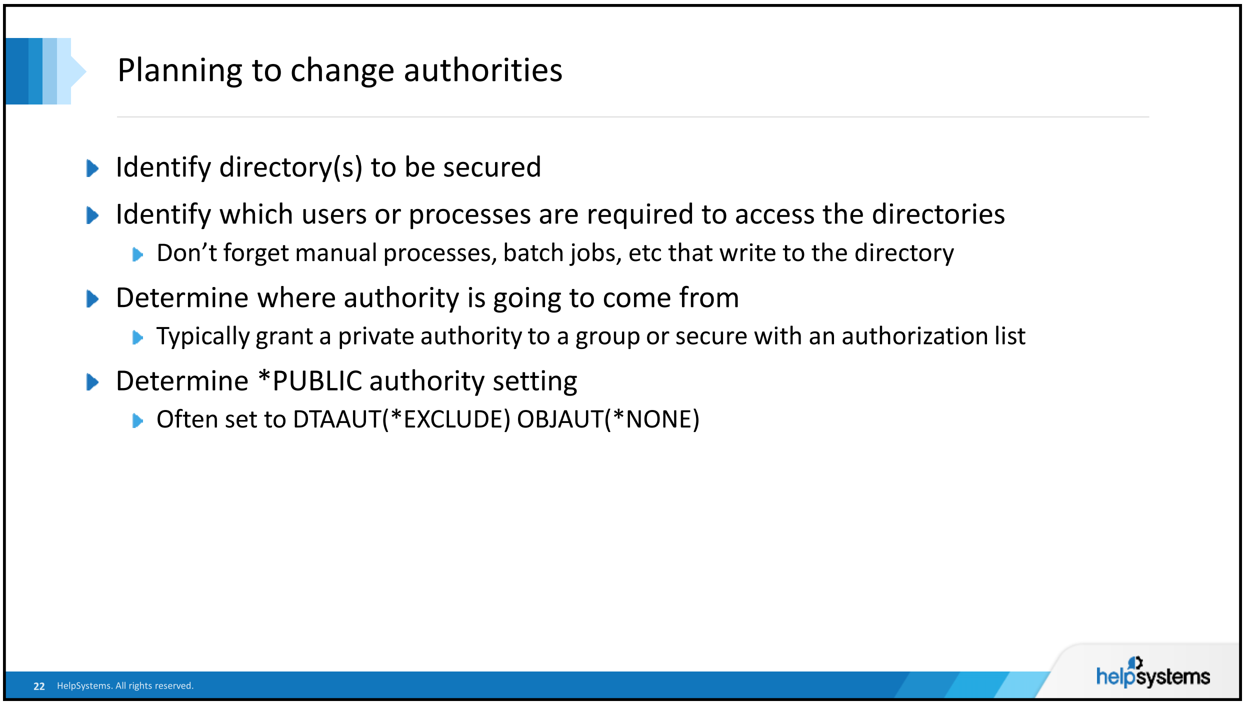
Application authorization options

Adopted authority is ignored

Options:

- User has direct authority via
  - *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

What we typically use



Planning to change authorities

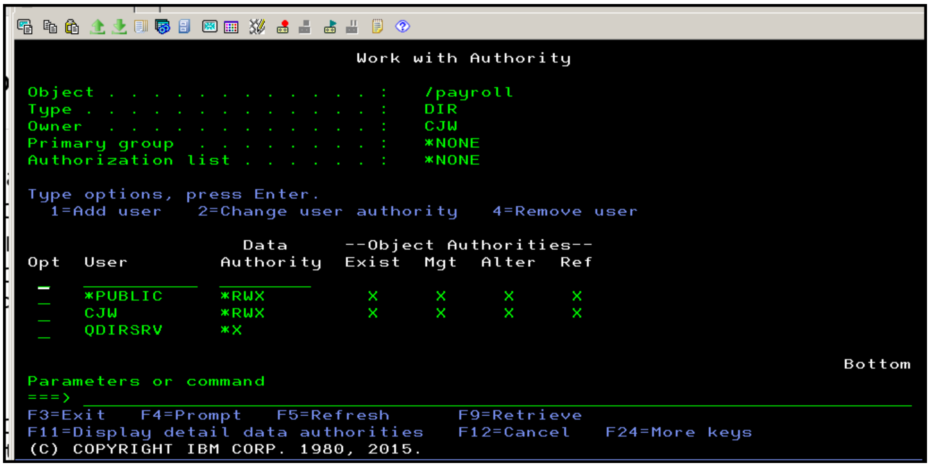
- Identify directory(s) to be secured
- Identify which users or processes are required to access the directories
  - Don’t forget manual processes, batch jobs, etc that write to the directory
- Determine where authority is going to come from
  - Typically grant a private authority to a group or secure with an authorization list
- Determine *PUBLIC authority setting
  - Often set to DTAAUT(*EXCLUDE) OBJAUT(*NONE)

Modifying authorities

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 in the directory
- OBJAUT (*OBJMGT) at the object level **to copy or rename** objects
- OBJAUT(*OBJEXIST) at the object level **to delete** objects

Example – Securing the /payroll directory

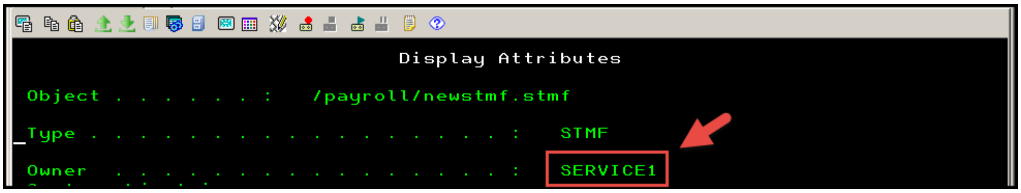


```
                              Work with Authority

 Object  . . . . . . . . . . . . . . :   /payroll
 Type  . . . . . . . . . . . . . . . :   DIR
 Owner . . . . . . . . . . . . . . . :   CJW
 Primary group . . . . . . . . . . . :   *NONE
 Authorization list  . . . . . . . . :   *NONE

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

                           Data      --Object Authorities--
 Opt  User               Authority  Exist   Mgt   Alter   Ref

  _   *PUBLIC            *RWX         X      X      X      X
  _   CJW                *RWX         X      X      X      X
  _   QDIRSRV            *X
                                                                    Bottom
 Parameters or command
 ===>
 F3=Exit    F4=Prompt   F5=Refresh      F9=Retrieve
 F11=Display detail data authorities    F12=Cancel   F24=More keys
 (C) COPYRIGHT IBM CORP. 1980, 2015.
```

Determining the profiles that need access

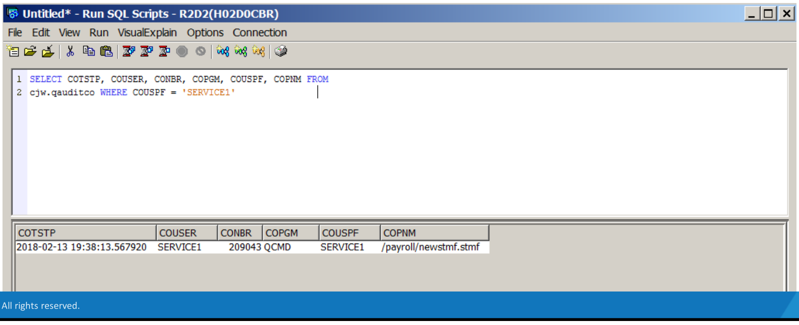
- Look at the owner of the objects in the directory
- Examine the CO and DO audit entries
  - May need to examine OM entries (object moves)
- Examine the ZR and ZC entries for objects being read/updated
- Job schedule entries (for batch jobs reading from / writing to the directory being secured)

Determining what Authority is Required



```
                              Display Attributes

 Object . . . . . . . :    /payroll/newstmf.stmf

_Type . . . . . . . . . . . . . . . . . . :    STMF

 Owner . . . . . . . . . . . . . . . . . . :    SERVICE1
```

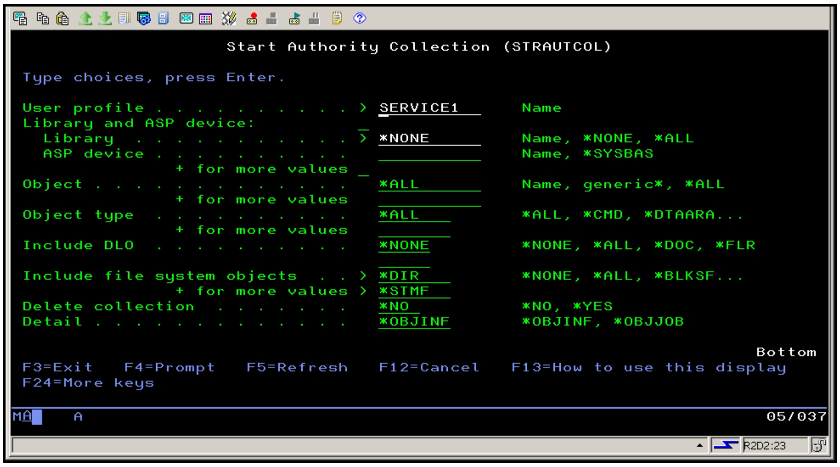
Display the owner of the objects And/Or Display the CO audit entries for the directory


Untitled* - Run SQL Scripts - R2D2(H02D0CBR)
File Edit View Run VisualExplain Options Connection

```
SELECT COTSTP, COUSER, CONBR, COPGM, COUSPF, COPNM FROM
cjw.qauditco WHERE COUSPF = 'SERVICE1'
```

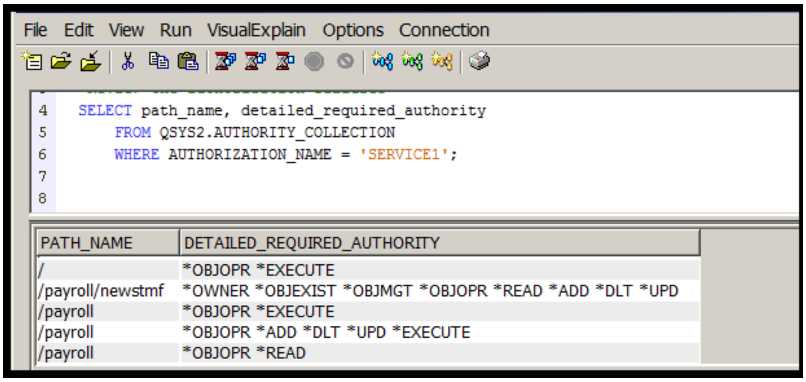
```
COTSTP                      COUSER     CONBR  COPGM     COUSPF     COPNM
2018-02-13 19:38:13.567920  SERVICE1  209043  QCMD      SERVICE1   /payroll/newstmf.stmf
```

Start authority collection for SERVICE1 – V7R3



```
                    Start Authority Collection (STRAUTCOL)

 Type choices, press Enter.

 User profile . . . . . . . . . . > SERVICE1      Name
 Library and ASP device:
   Library  . . . . . . . . . . . > *NONE         Name, *NONE, *ALL
   ASP device . . . . . . . . . .                 Name, *SYSBAS
              + for more values _
 Object . . . . . . . . . . . . .   *ALL          Name, generic*, *ALL
              + for more values
 Object type  . . . . . . . . . .   *ALL          *ALL, *CMD, *DTAARA...
              + for more values
 Include DLO  . . . . . . . . . .   *NONE         *NONE, *ALL, *DOC, *FLR

 Include file system objects  . . > *DIR          *NONE, *ALL, *BLKSF...
              + for more values > *STMF
 Delete collection  . . . . . . .   *NO           *NO, *YES
 Detail . . . . . . . . . . . . .   *OBJINF       *OBJINF, *OBJJOB
                                                                    Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys

MA      A                                                           05/037
```

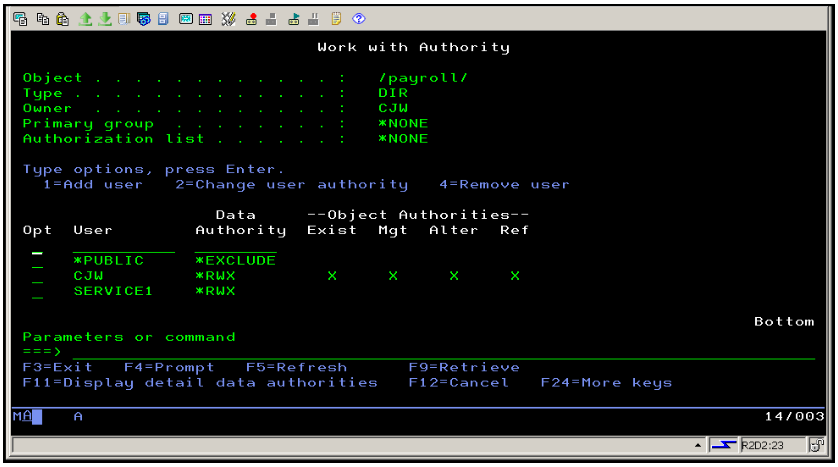
Query the collection for SERVICE1



```sql
SELECT path_name, detailed_required_authority
    FROM QSYS2.AUTHORITY_COLLECTION
    WHERE AUTHORIZATION_NAME = 'SERVICE1';
```

PATH_NAME	DETAILED_REQUIRED_AUTHORITY
/	*OBJOPR *EXECUTE
/payroll/newstmf	*OWNER *OBJEXIST *OBJMGT *OBJOPR *READ *ADD *DLT *UPD
/payroll	*OBJOPR *EXECUTE
/payroll	*OBJOPR *ADD *DLT *UPD *EXECUTE
/payroll	*OBJOPR *READ

Set the authorities

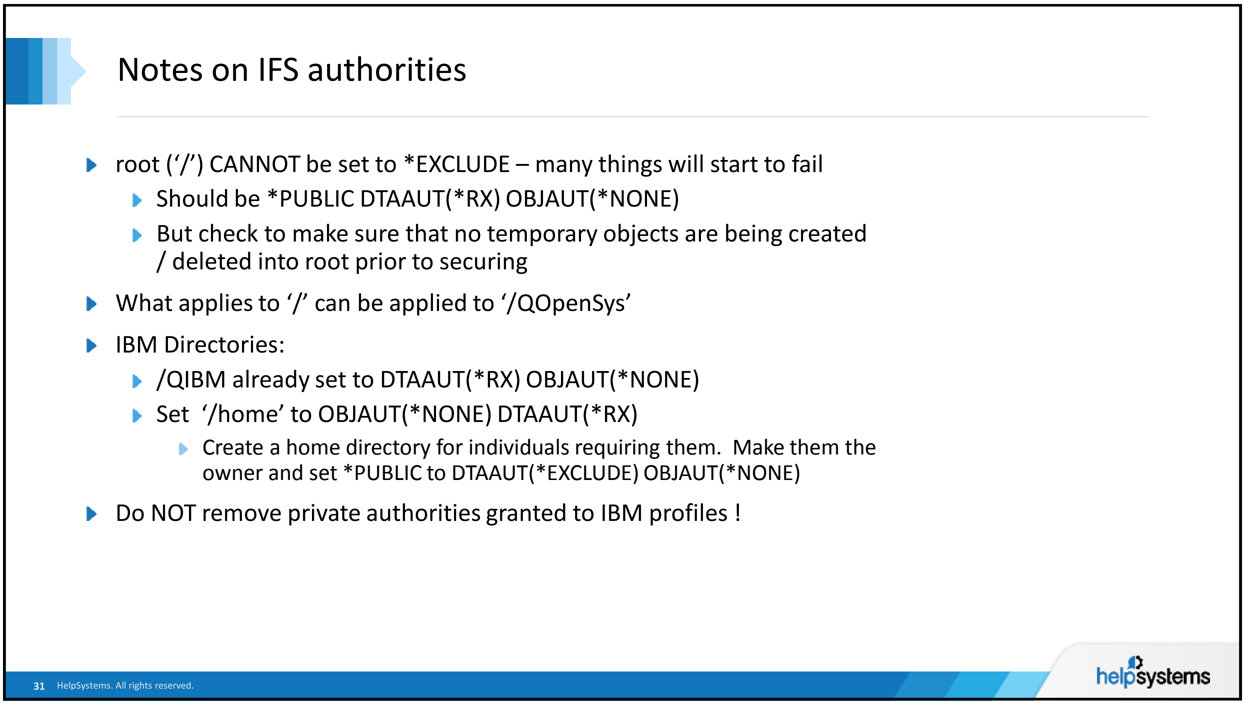


```
                              Work with Authority

Object . . . . . . . . . . . . :   /payroll/
Type . . . . . . . . . . . . . :   DIR
Owner  . . . . . . . . . . . . :   CJW
Primary group  . . . . . . . . :   *NONE
Authorization list . . . . . . :   *NONE

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

                  Data       --Object Authorities--
Opt  User         Authority  Exist  Mgt   Alter  Ref

 _   *PUBLIC      *EXCLUDE
 _   CJW          *RWX         X     X      X     X
 _   SERVICE1     *RWX
                                                              Bottom
Parameters or command
===>
F3=Exit   F4=Prompt   F5=Refresh      F9=Retrieve
F11=Display detail data authorities   F12=Cancel   F24=More keys

MA     A                                                     14/003
```

Or make SERVICE1 the owner of /payroll

More on Authorities

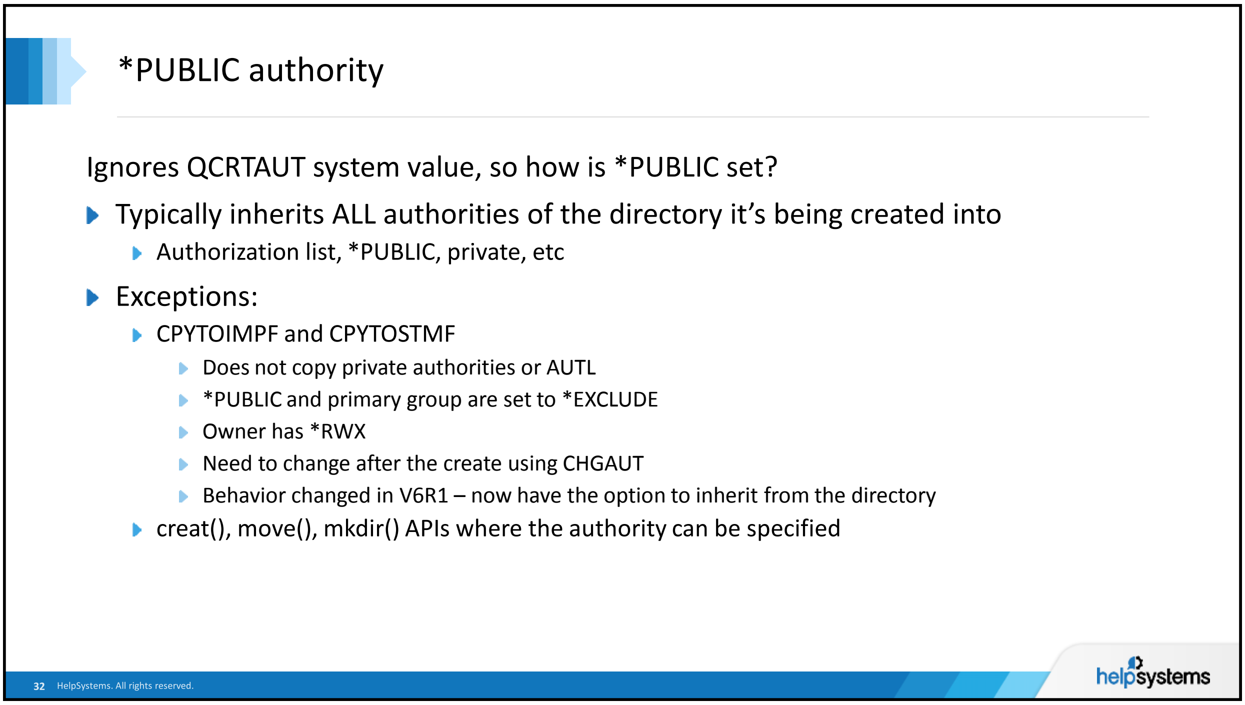
UP NEXT



Notes on IFS authorities

- 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'
- IBM Directories:
  - /QIBM already set to DTAAUT(*RX) OBJAUT(*NONE)
  - Set '/home' to OBJAUT(*NONE) DTAAUT(*RX)
    - Create a home directory for individuals requiring them. Make them the owner and set *PUBLIC to DTAAUT(*EXCLUDE) OBJAUT(*NONE)
- Do NOT remove private authorities granted to IBM profiles !

31 HelpSystems. All rights reserved.



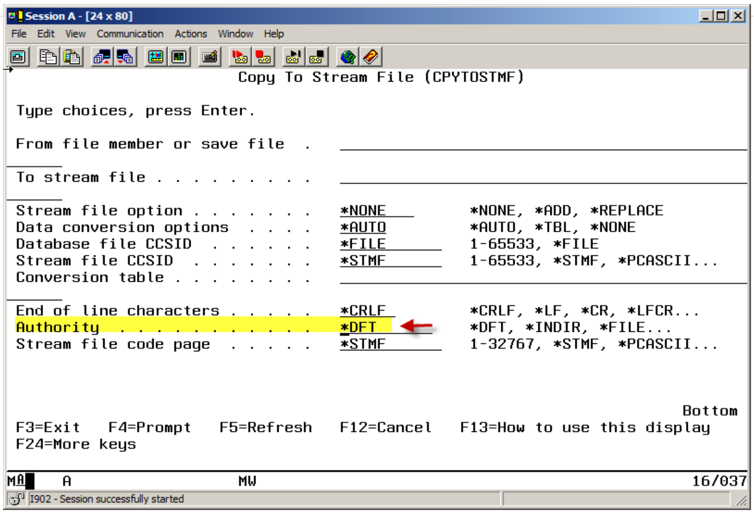
*PUBLIC authority

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

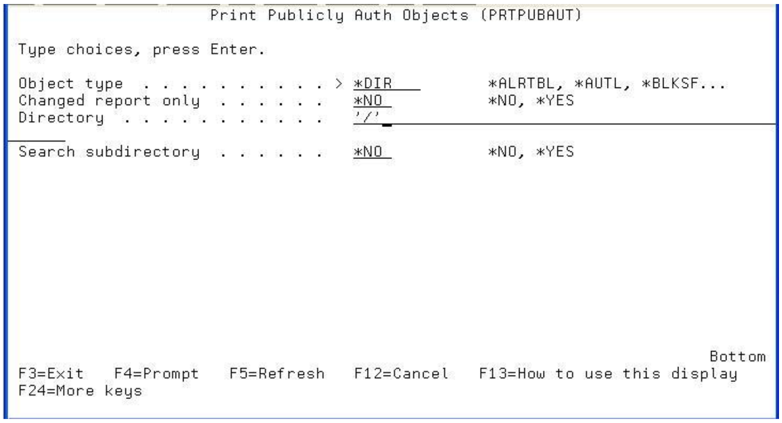
32 HelpSystems. All rights reserved.

CPYTOSTMF as of V6R1


Session A - [24 x 80]
File Edit View Communication Actions Window Help
I902 - Session successfully started

```
                          Copy To Stream File (CPYTOSTMF)

 Type choices, press Enter.

 From file member or save file  .   ____________________________________________
 ______
 To stream file . . . . . . . . .   ____________________________________________
 ______
 Stream file option . . . . . . .   *NONE         *NONE, *ADD, *REPLACE
 Data conversion options  . . . .   *AUTO         *AUTO, *TBL, *NONE
 Database file CCSID  . . . . . .   *FILE         1-65533, *FILE
 Stream file CCSID  . . . . . . .   *STMF         1-65533, *STMF, *PCASCII...
 Conversion table . . . . . . . .   ____________________________________________
 ______
 End of line characters . . . . .   *CRLF         *CRLF, *LF, *CR, *LFCR...
 Authority  . . . . . . . . . . .   *DFT          *DFT, *INDIR, *FILE...
 Stream file code page  . . . . .   *STMF         1-32767, *STMF, *PCASCII...



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

MA       A                  MW                                           16/037
```

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!

Proliferation of private authorities

/Images/2018/Finance/January

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

/Images/2018 – Owner: TONY, Private authority – GIBBS

/Images/2018/Finance – Owner: ZIVA, Private authorities – GIBBS, TONY

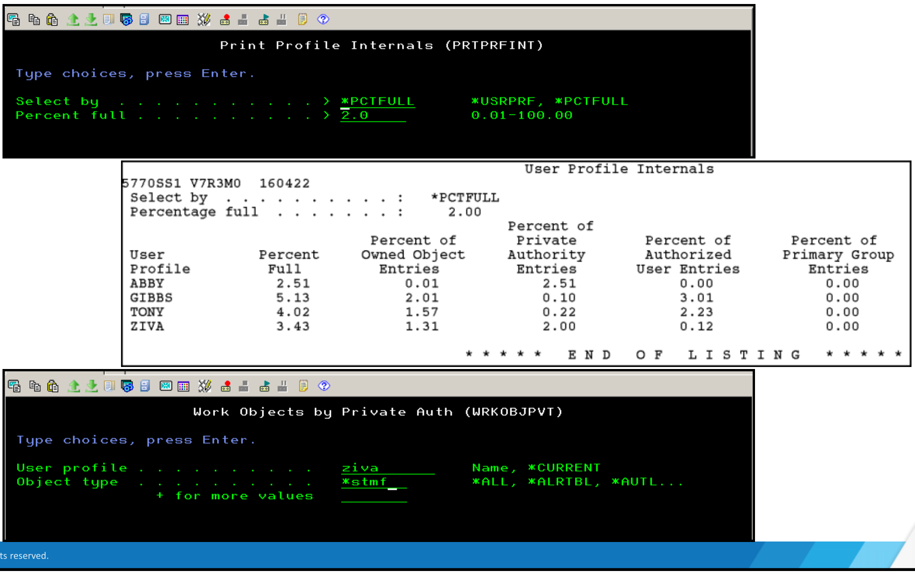
/Images/2018/Finance/January – Owner: MAGEE, Private auts – GIBBS, TONY, ZIVA

/Images/2018/Finance/January/xxxxx.doc – Owner: App_Profile

Images will be owned by App_Profile and each will have a private authority for GIBBS, TONY, ZIVA and MAGEE.

Discover which profiles have excess private authorities via PRTPRFINT (Print profile internals) and WRKOBJPVT

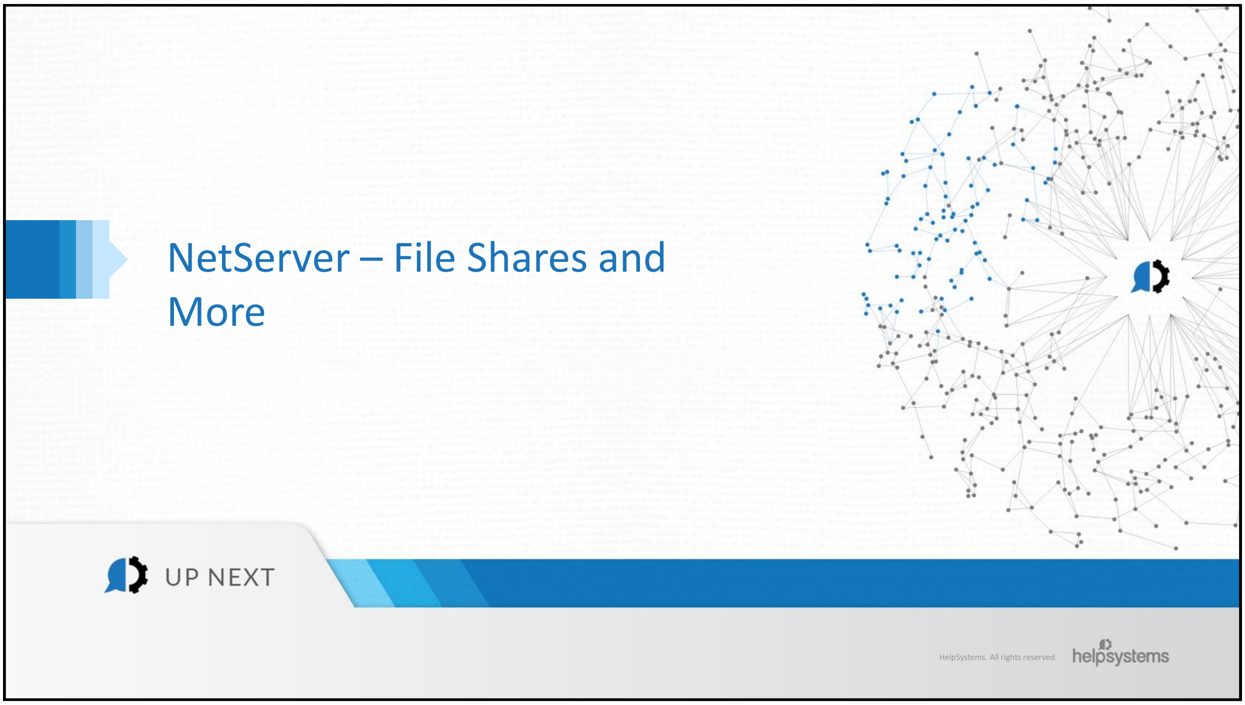
Reduce time for SAVSECDTA using PRTPRFINT



```
                    Print Profile Internals (PRTPRFINT)

 Type choices, press Enter.

 Select by . . . . . . . . . . . > *PCTFULL       *USRPRF, *PCTFULL
 Percent full . . . . . . . . . > 2.0             0.01-100.00
```

```
                                            User Profile Internals
5770SS1 V7R3M0  160422
 Select by  . . . . . . . . . . :    *PCTFULL
 Percentage full  . . . . . . . :      2.00
                                                Percent of
                              Percent of         Private        Percent of       Percent of
 User             Percent    Owned Object      Authority        Authorized      Primary Group
 Profile           Full        Entries          Entries         User Entries       Entries
 ABBY              2.51          0.01             2.51              0.00              0.00
 GIBBS             5.13          2.01             0.10              3.01              0.00
 TONY              4.02          1.57             0.22              2.23              0.00
 ZIVA              3.43          1.31             2.00              0.12              0.00

                                        * * * * *   E N D   O F   L I S T I N G   * * * * *
```

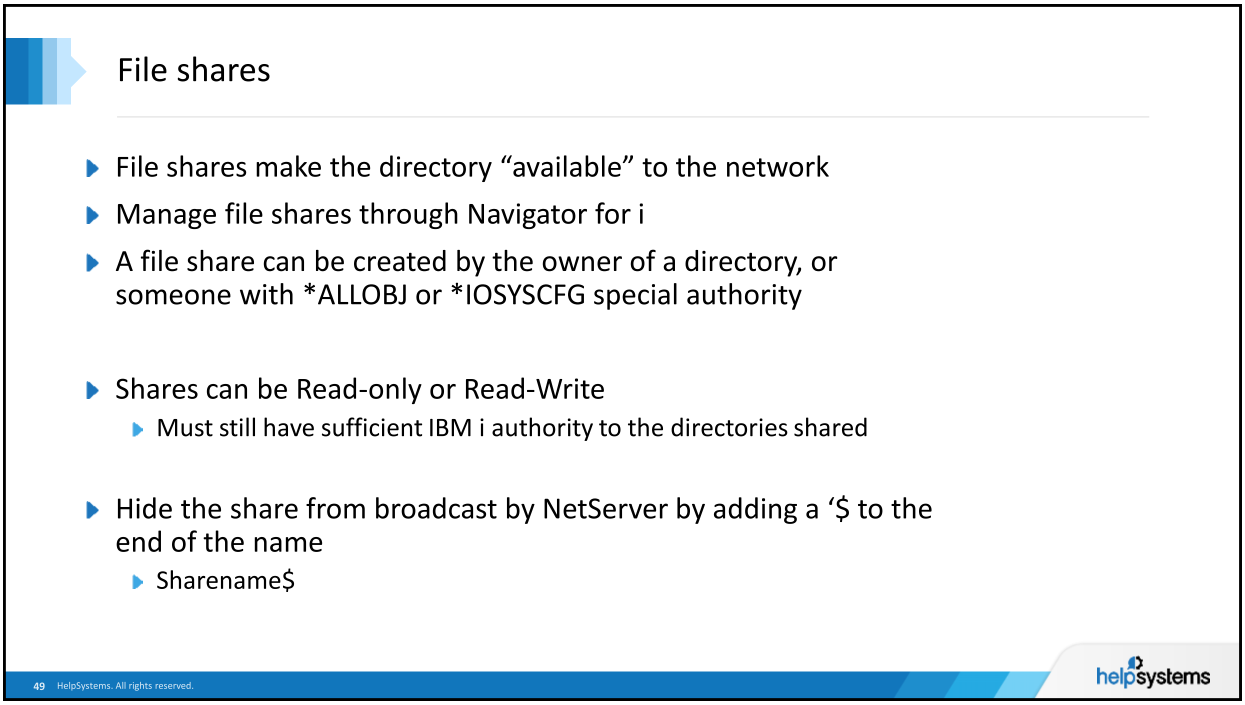
```
                 Work Objects by Private Auth (WRKOBJPVT)

 Type choices, press Enter.

 User profile . . . . . . . . . .   ziva          Name, *CURRENT
 Object type  . . . . . . . . . .   *stmf_        *ALL, *ALRTBL, *AUTL...
                + for more values
```



NetServer – File Shares and More

UP NEXT

HelpSystems. All rights reserved.

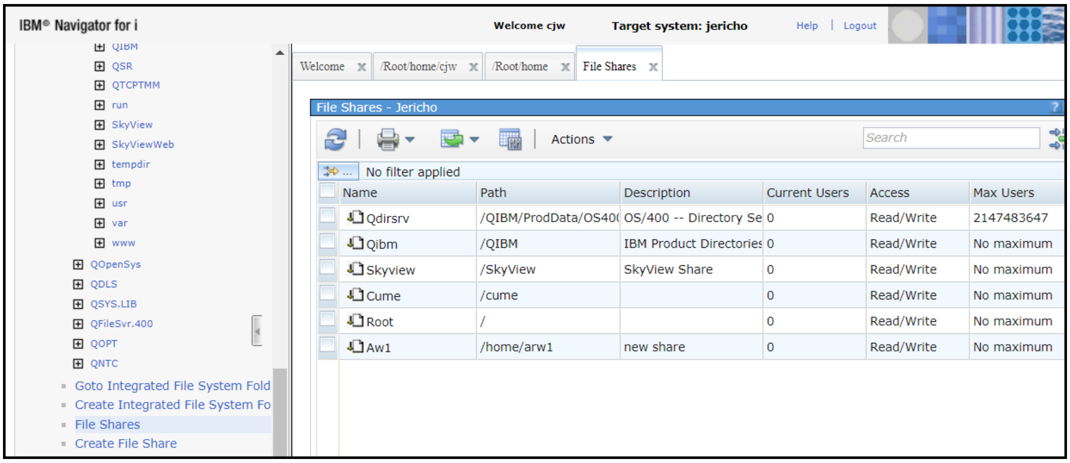


File shares

- File shares make the directory “available” to the network
- Manage file shares through Navigator for i
- A file share can be created by the owner of a directory, or someone with *ALLOBJ or *IOSYSCFG special authority
- Shares can be Read-only or Read-Write
  - Must still have sufficient IBM i authority to the directories shared
- Hide the share from broadcast by NetServer by adding a ‘$ to the end of the name
  - Sharename$

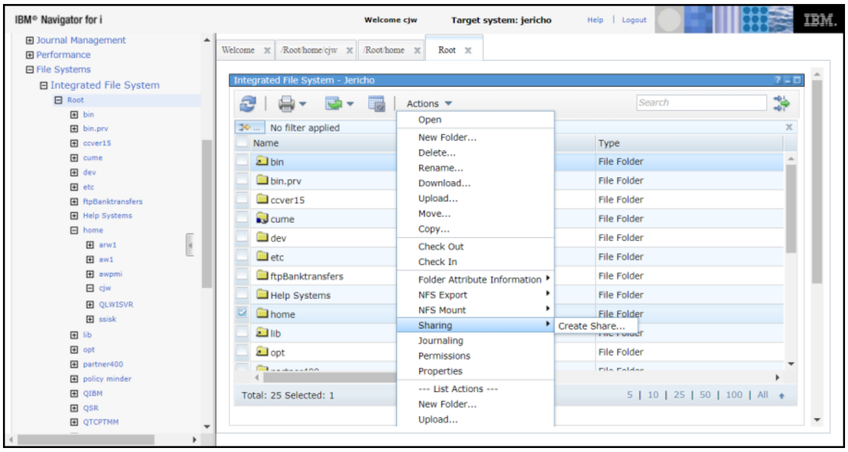
49 HelpSystems. All rights reserved.

List of file shares



Name	Path	Description	Current Users	Access	Max Users
Qdirsrv	/QIBM/ProdData/OS400	OS/400 -- Directory Se	0	Read/Write	2147483647
Qibm	/QIBM	IBM Product Directories	0	Read/Write	No maximum
Skyview	/SkyView	SkyView Share	0	Read/Write	No maximum
Cume	/cume		0	Read/Write	No maximum
Root	/		0	Read/Write	No maximum
Aw1	/home/arw1	new share	0	Read/Write	No maximum

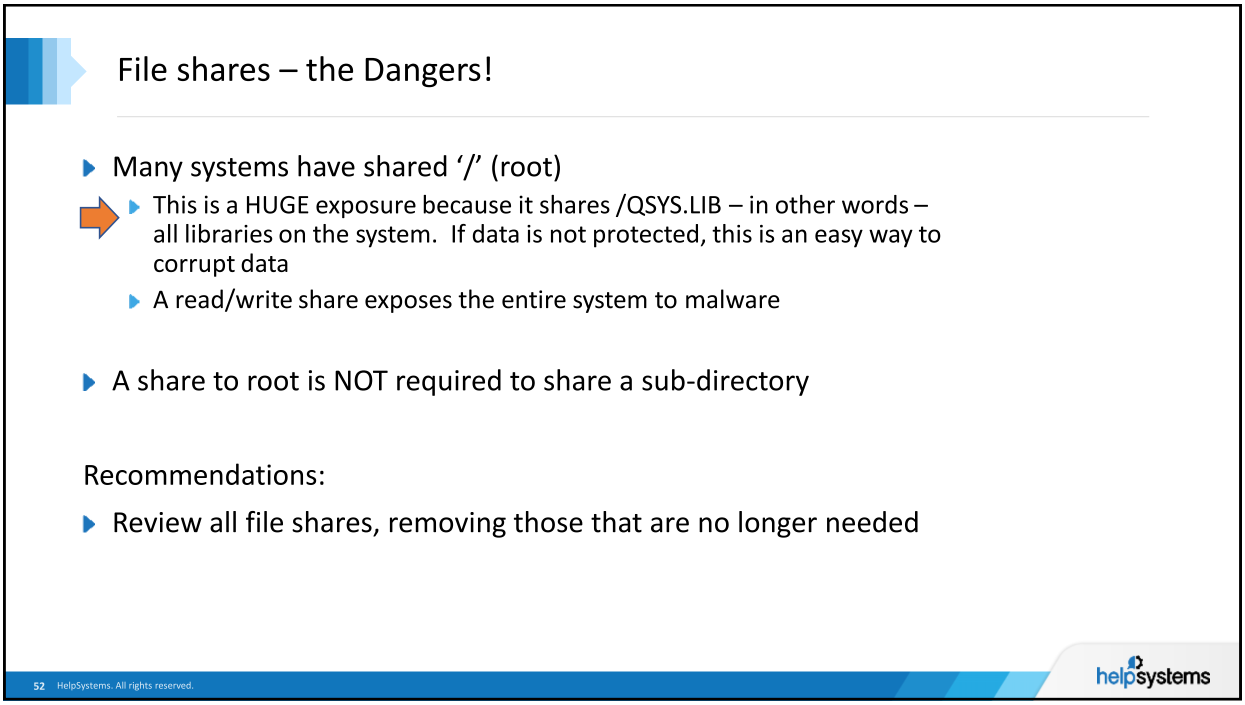
File shares



	Name	Type
□	bin	File Folder
□	bin.prv	File Folder
□	ccver15	File Folder
□	cume	File Folder
□	dev	File Folder
□	etc	File Folder
□	ftpBanktransfers	File Folder
□	Help Systems	File Folder
☑	home	File Folder
□	lib	File Folder
□	opt	File Folder

Total: 25 Selected: 1

A hand underneath the folder indicates it's shared

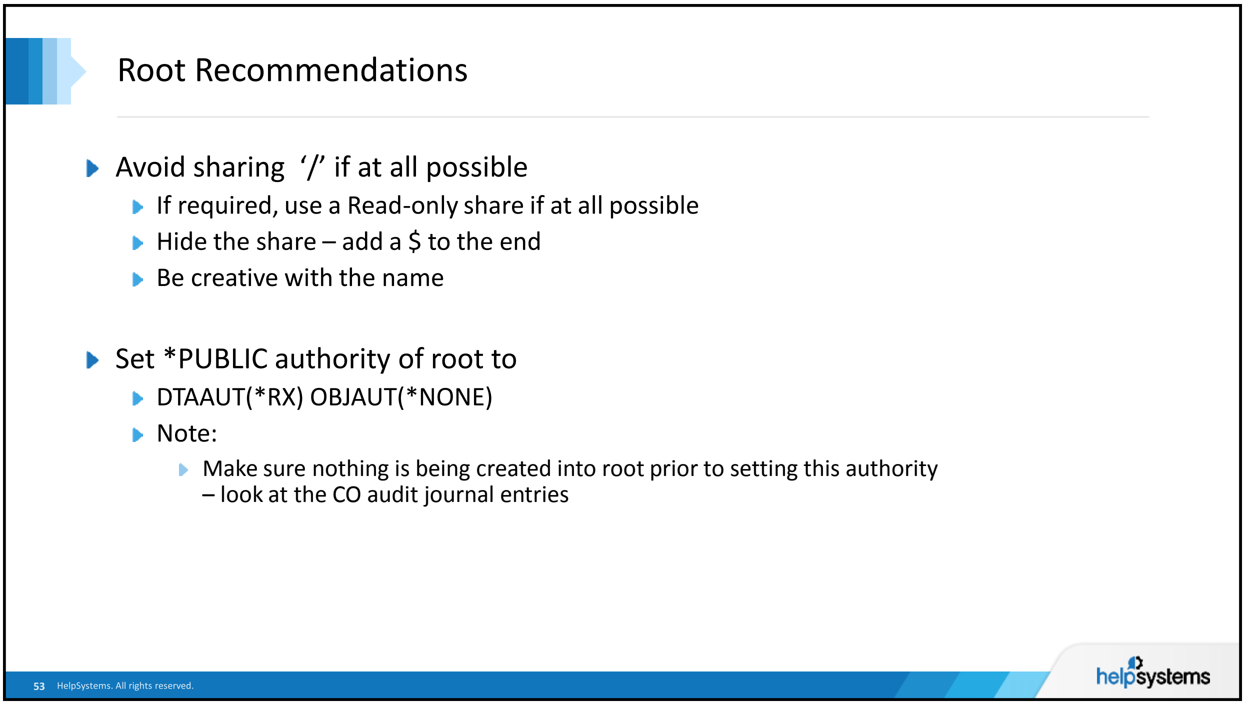


File shares – the Dangers!

- 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
  - A read/write share exposes the entire system to malware
- A share to root is NOT required to share a sub-directory

Recommendations:

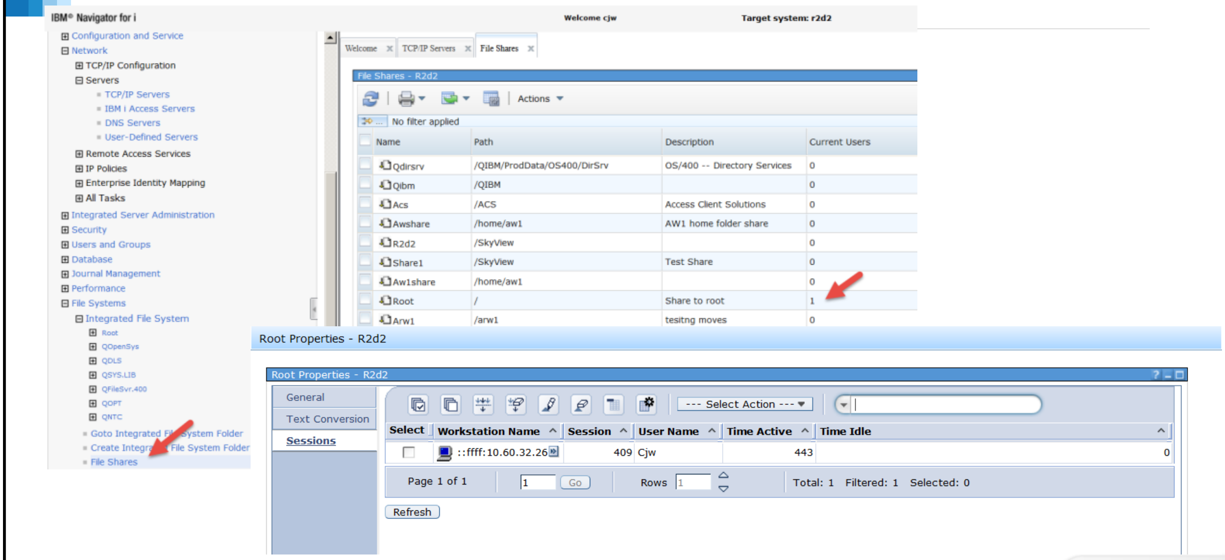
- Review all file shares, removing those that are no longer needed



Root Recommendations

- Avoid sharing ‘/’ if at all possible
  - If required, use a Read-only share if at all possible
  - Hide the share – add a $ to the end
  - Be creative with the name
- Set *PUBLIC authority of root to
  - DTAAUT(*RX) OBJAUT(*NONE)
  - Note:
    - Make sure nothing is being created into root prior to setting this authority – look at the CO audit journal entries

NetServer



IBM® Navigator for i | Welcome cjw | Target system: r2d2

- ⊞ Configuration and Service
- ⊟ Network
  - ⊞ TCP/IP Configuration
  - ⊟ Servers
    - TCP/IP Servers
    - IBM i Access Servers
    - DNS Servers
    - User-Defined Servers
  - ⊞ Remote Access Services
  - ⊞ IP Policies
  - ⊞ Enterprise Identity Mapping
  - ⊞ All Tasks
- ⊞ Integrated Server Administration
- ⊞ Security
- ⊞ Users and Groups
- ⊞ Database
- ⊞ Journal Management
- ⊞ Performance
- ⊟ File Systems
  - ⊟ Integrated File System
    - ⊞ Root
    - ⊞ QOpenSys
    - ⊞ QDLS
    - ⊞ QSYS.LIB
    - ⊞ QFileSvr.400
    - ⊞ QOPT
    - ⊞ QNTC
  - Goto Integrated File System Folder
  - Create Integrated File System Folder
  - File Shares

File Shares - R2d2

No filter applied

□	Name	Path	Description	Current Users
□	Qdirsrv	/QIBM/ProdData/OS400/DirSrv	OS/400 -- Directory Services	0
□	Qibm	/QIBM		0
□	Acs	/ACS	Access Client Solutions	0
□	Awshare	/home/aw1	AW1 home folder share	0
□	R2d2	/SkyView		0
□	Share1	/SkyView	Test Share	0
□	Aw1share	/home/aw1		0
□	Root	/	Share to root	1
□	Arw1	/arw1	tesitng moves	0

Root Properties - R2d2

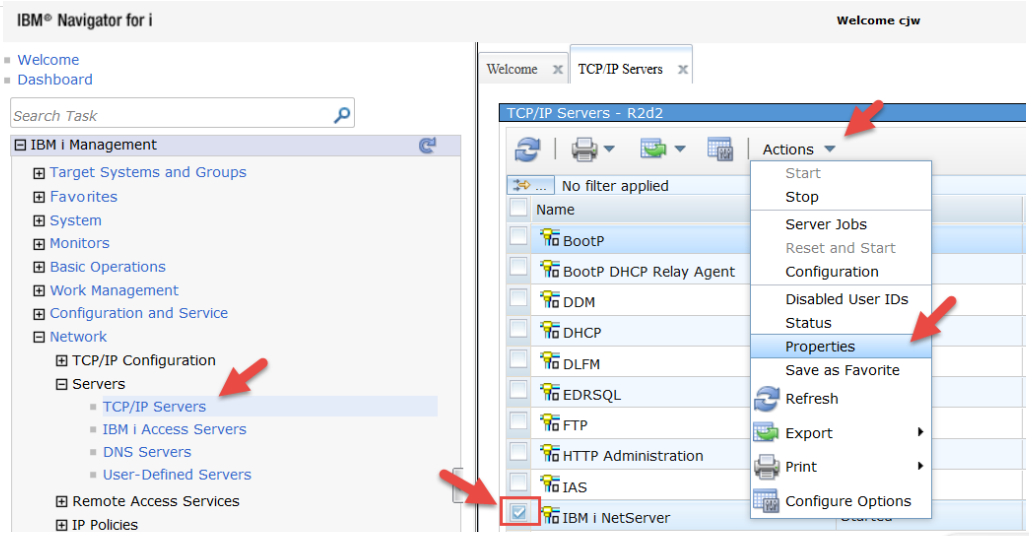
Root Properties - R2d2

Select	Workstation Name	Session	User Name	Time Active	Time Idle
□	::ffff:10.60.32.26	409	Cjw	443	0

Page 1 of 1 | 1 Go | Rows 1 | Total: 1 Filtered: 1 Selected: 0

58 HelpSystems. All rights reserved.

NetServer



IBM® Navigator for i | Welcome cjw

- Welcome
- Dashboard

- ⊟ IBM i Management
  - ⊞ Target Systems and Groups
  - ⊞ Favorites
  - ⊞ System
  - ⊞ Monitors
  - ⊞ Basic Operations
  - ⊞ Work Management
  - ⊞ Configuration and Service
  - ⊟ Network
    - ⊞ TCP/IP Configuration
    - ⊟ Servers
      - TCP/IP Servers
      - IBM i Access Servers
      - DNS Servers
      - User-Defined Servers
    - ⊞ Remote Access Services
    - ⊞ IP Policies

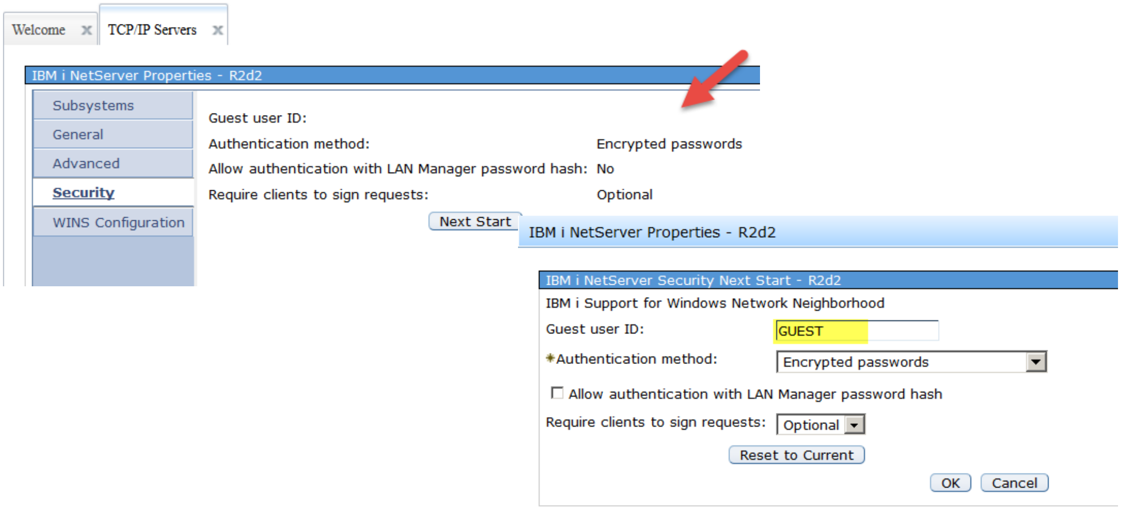
TCP/IP Servers - R2d2

No filter applied

□	Name
□	BootP
□	BootP DHCP Relay Agent
□	DDM
□	DHCP
□	DLFM
□	EDRSQL
□	FTP
□	HTTP Administration
□	IAS
☑	IBM i NetServer

59 HelpSystems. All rights reserved.

NetServer Guest Profile - Properties



IBM i NetServer Properties - R2d2

Guest user ID:
Authentication method: Encrypted passwords
Allow authentication with LAN Manager password hash: No
Require clients to sign requests: Optional

IBM i NetServer Properties - R2d2

IBM i NetServer Security Next Start - R2d2

IBM i Support for Windows Network Neighborhood

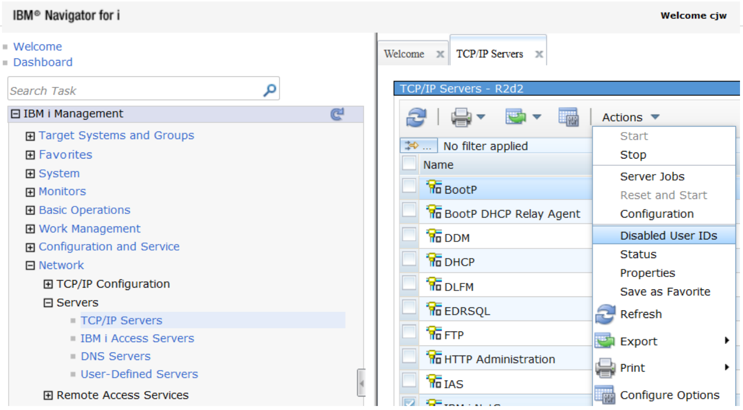
Guest user ID: GUEST

*Authentication method: Encrypted passwords

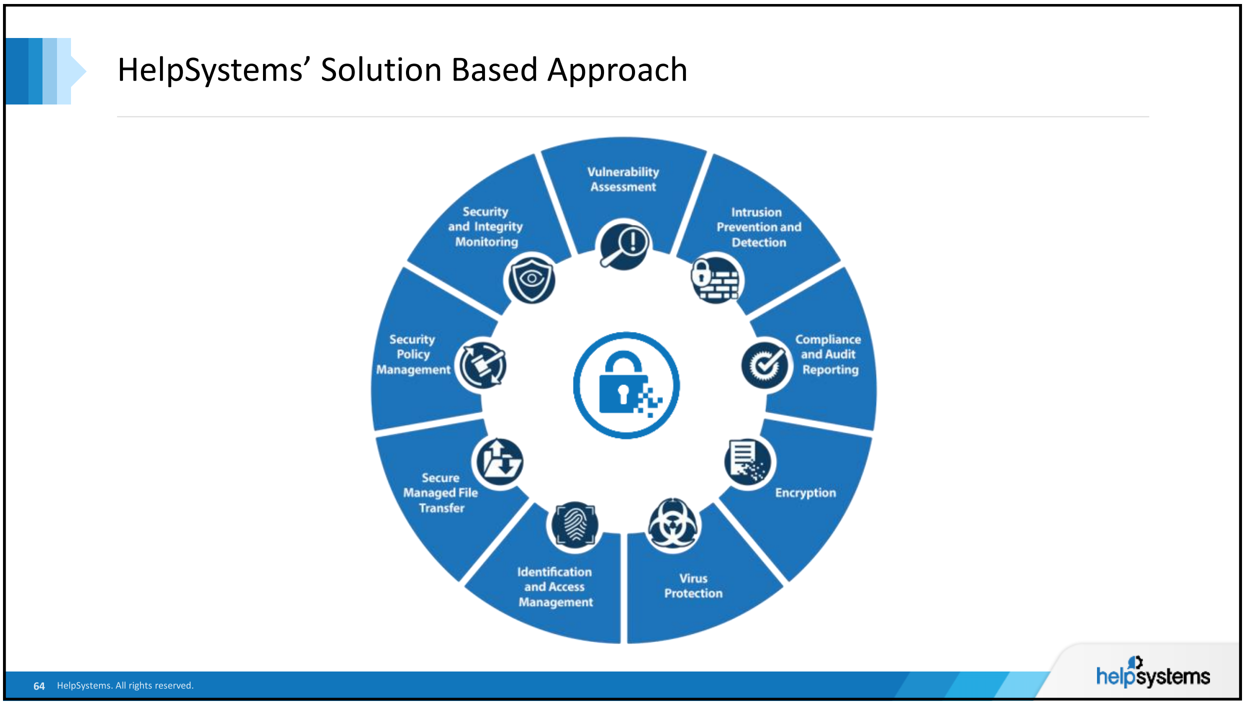
☐ Allow authentication with LAN Manager password hash

Require clients to sign requests: Optional

NetServer – Disabled Profiles



- Only disabled NetServer profile NOT IBM i profile.
- Message CPIB682 sent to QSYSOPR for disabled NetServer users



HelpSystems’ Solution Based Approach

Vulnerability Assessment

Intrusion Prevention and Detection

Compliance and Audit Reporting

Encryption

Virus Protection

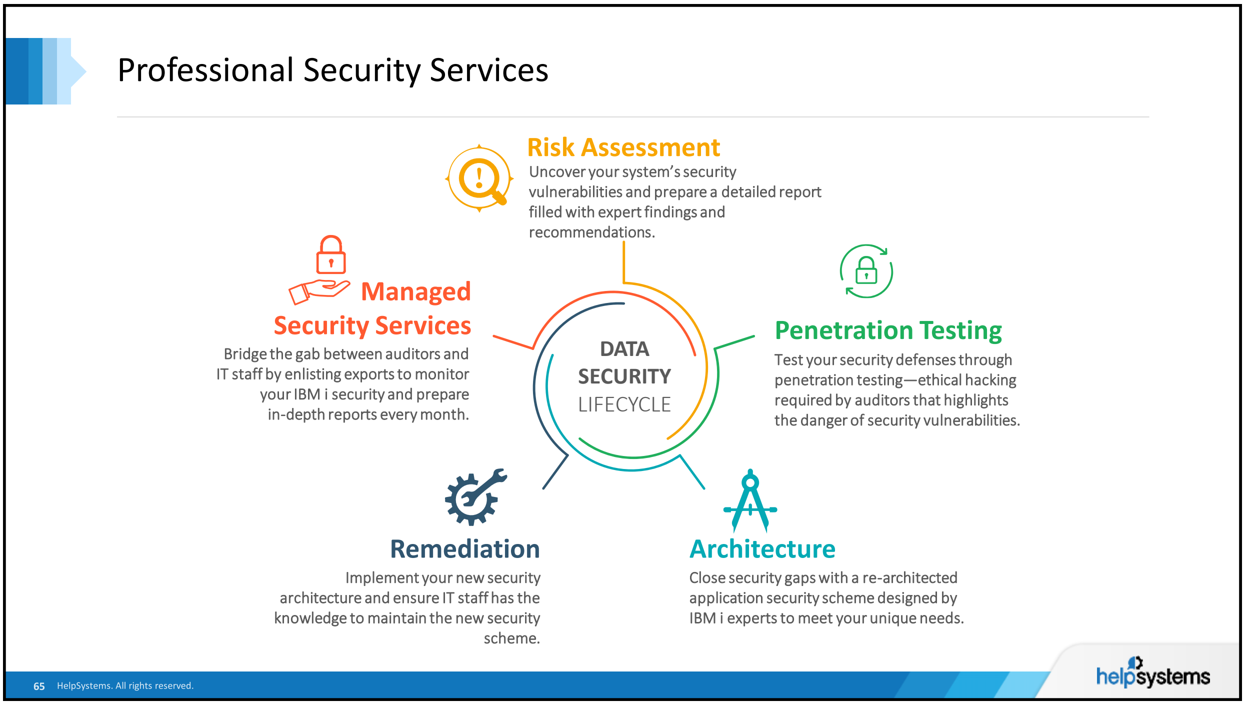
Identification and Access Management

Secure Managed File Transfer

Security Policy Management

Security and Integrity Monitoring

helpsystems



Professional Security Services

DATA SECURITY LIFECYCLE

Risk Assessment
Uncover your system’s security vulnerabilities and prepare a detailed report filled with expert findings and recommendations.

Penetration Testing
Test your security defenses through penetration testing—ethical hacking required by auditors that highlights the danger of security vulnerabilities.

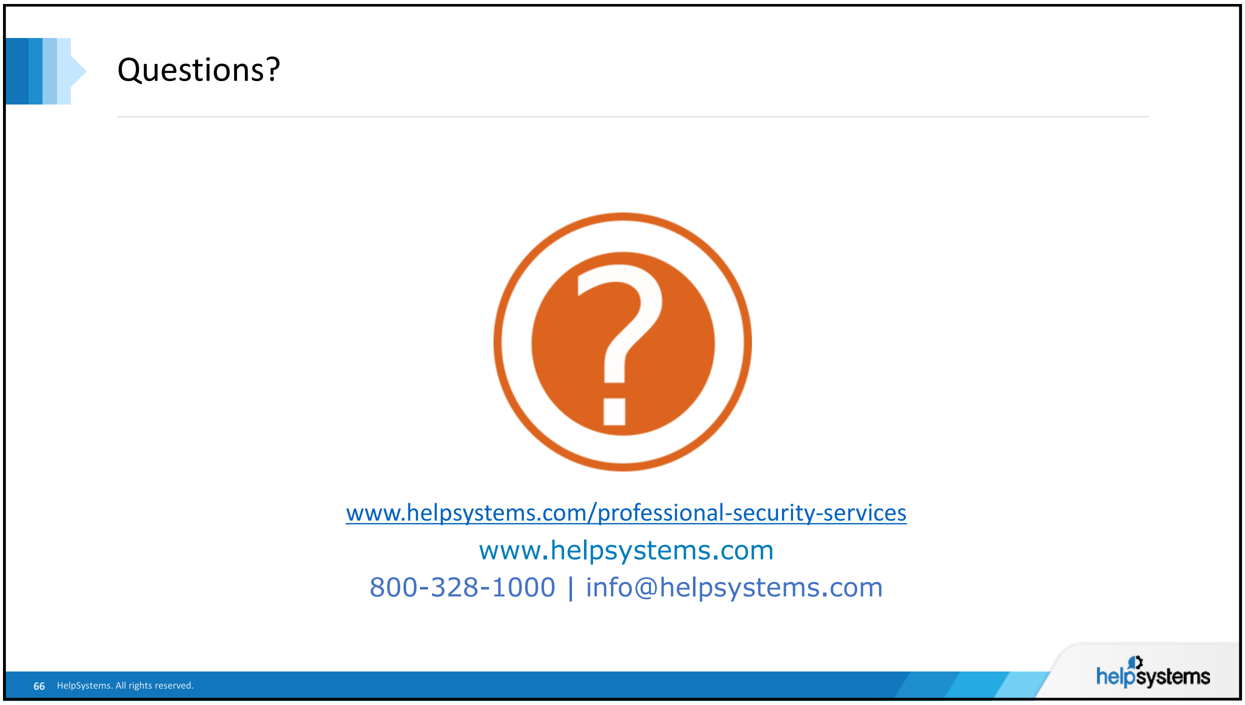
Architecture
Close security gaps with a re-architected application security scheme designed by IBM i experts to meet your unique needs.

Remediation
Implement your new security architecture and ensure IT staff has the knowledge to maintain the new security scheme.

Managed Security Services
Bridge the gab between auditors and IT staff by enlisting exports to monitor your IBM i security and prepare in-depth reports every month.

helpsystems

www.helpsystems.com/professional-security-services



Questions?

www.helpsystems.com/professional-security-services

www.helpsystems.com

800-328-1000 | info@helpsystems.com

66 HelpSystems. All rights reserved.