

Security Considerations for the IFS (Integrated File System)

Carol Woodbury, VP Global Security Services

carol.woodbury@helpsystems.com





- 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	Х	Х	Х	Х	Х	Х	Х
*READ	Х	Х	Х	Х			
*ADD	Х	Х			Х	Х	
*UPD	Х	Х			Х	Х	
*DLT	Х	Х					
*EXECUTE	Х		Х		Х		Х

IFS Authorities



*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'



A Division of HelpSystems

Managing Authorities and Ownership



9

Two sets of authority to manage



icName, *PUBLIC, *NTWIRF
<pre> *SAME, *NONE, *RWX, *RX *SAME, *NONE, *ALL </pre>
Name, *NONE *NONE, *ALL *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 Primary group Authorization	 list	: / : QSYS : ALANY : AUTL	
Type options, 1=Add user	press Enter. 2=Change use Data	er authority 4=Remove user Object Authorities	
Opt User _ *PUBLIC _ QSYS _ QDIRSRV	 Authority *RX *RWX *X 	Exist Mgt Alter Ref	
Parameters or	command		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



Object:								
/SkyView/Policy	Minder							_
Гуре:			Owner	: Pr	imary Group:	Authorizatio	on List (AUTL):	:
Directory			Cjw	1)	Vone)	(None)		
Name	Read	Write	Execute	Managem	Existence	Alter	Reference	Exc
鶲 (Public) 🎍 Cjw	л Л	지 지	L A	Ц Ч	니 되	니 지	л Л	
4 I								
∢ Add	Remove	Customize						Þ
Add	Remove	Customize						Þ
Add Owner	Remove	Customize	horization List					ł

Navigate to the file Right click, choose Permissions

Change Owner (CHGOWN)



File Edit View Communication Actions Window He	lp	
🖻 🖹 🚔 🜉 🖩 📓 🚵 🛃 🖬 🖬 🖬 🖬 🛃 🛃 🖬	¶ 🌒 � ge Owner (CHGOWN)	
Type choices, press Enter.		
Object	/FinancialApp	
New owner	APP_OWNName*YES*NO, *YES*all*NONE, *ALL*NO*NO, *YES	
	File Edit View Communication Actions Window Help	
	o Fifi #51 200 🖬 🖬 🕹 🖉 🤌	
	Lnange Uwn	er (CHGUWN)
	Type choices, press Enter.	
	Object	S.LIB/ProdLib.lib/*.file
F3=Exit F4=Prompt F5=Refresh F24=More keys	New owner	<u>DWN</u> Name *NO, *YES _ *NONE, *ALL *NO, *YES
PILE H P128 1902 - Session successfully started		

Application authorization options



Adopted authority is ignored



- 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

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

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'
- 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 !



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



🛛 🔤 Session A - [24 x 80]	
File Edit View Communication Actions Window Help	
🖻 🗈 🕼 🔳 🔳 🖬 🛃 💩 💩	
Copy To Strea	am File (CPYTOSTMF)
Type choices, press Enter.	
From file member or save file .	
 To stream file	
Stream file option	NONE *NONE, *ADD, *REPLACE NUTO *AUTO, *TBL, *NONE FILE 1-65533, *FILE STMF 1-65533, *STMF, *PCASCII
End of line characters	CRLF *CRLF, *LF, *CR, *LFCR OFT *DFT, *INDIR, *FILE STMF 1-32767, *STMF, *PCASCII
F3=Exit F4=Prompt F5=Refresh F1 F24=More keys	Bottom 2=Cancel F13=How to use this display
MALA MW	16/037
년 ¹ I902 - Session successfully started	

IFS System Values and Exit Points



- 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/xxxx.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 <u>*all</u> *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



A Division of HelpSystems

	🔳 🛋 📐 🔤 🕷	8 🔌 🤌			
	ſ	Display Report			
Query : Q)SYS/QSECCO	R	eport widt	h	: 204
Position to line		Shift	to column		
Line+1	+ 2 +	3 +	4+	5+6.	+7
Entry Us	ser Object	Library	Object	Office	DLO
type pr	ofile name	name	type	user	name
034406 CO N QS	SYS *N	*N	*SOCKET		
034407 CO N QS	SYS *N	*N	*SOCKET		
034408 CO N QS	SYS *N	*N	*SOCKET		
034409 CO N QS	SYS *N	*N	*SOCKET		
034410 CO N QS	SYS *N	*N	*SOCKET		
034411 CO N QS	SYS *N	*N	*SOCKET		
034412 CO N QS	SECOFR *N	*N	*STMF		
034413 CONQS	SECOFR *N	*N	*STMF		
034414 CONQS	SYS *N	*N	*SOCKET		
034415 CO N CJ	IW TEST2	CJ₩	*DTAARA		
034416 CO N CJ	ſ⊌ ∗ N	*N	*DIR		
034417 CO N QS	SYS *N	*N	*SOCKET		
034418 CO N CJ	IU *N 🔨	*N	*STMF		
*****	End of report	*****			_
					Bottom
F3=Exit F12=	Cancel F19	=Left F20:	=Right	F21=Split	
MA A					03/033
1902 - Session successfu	illy 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



	٠	
Copy Audit Jou	rnal Entries	(CPYAUDJRNE)
Type choices, press Enter.		
Journal entry types	со 🦰	*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	<u>*FIRST</u>	Name, *FIRST
Replace or add records	<u>*REPLACE</u>	*REPLACE, *ADD
User profile	<u>*HLL</u>	Name, *HLL
Starting journal receiver	*CHDDENT	Nama *CUPPENT *CUPCHAIN
libraru	<u>+CORRENT</u>	Name, * TBL, *CURLTB
Ending journal receiver		Name, *CURRENT
Library		Name, *LIBL, *CURLIB
Starting date and time:		
Starting date	<u>*FIRST</u>	Date, *FIRST
Starting time		Time
		More
F3=Exit F4=Prompt F5=Refresh	F12=Cancel	F13=How to use this display
rz4=more keys		
MA		05/030
		037035
Boz - Session successfully started		

Creates a file named QAUDITxx in QTEMP

Results of query / SQL of QTEMP/QAUDITCO



A Division of HelpSystems

0 BB #	a 🕹 🛃 🔌 🤗	•					
Disnlay Data							
	510010	Data	width 5050				
Position to line		Shift to	column				
+ 1 + 2 + 1	3 +	4 +	5 + 6 + 7 +				
Timestamn	llser	Object	Path				
Timestamp	nrofile	tune	name				
2015-08-15-20 22 46 503232		*STME	/SkuView/emailtemn/0132_tyt				
2015-08-15-20 22 46 904864	C 14	*STME	/SkuView/emailtemp/GIO2.txt				
2015-00-15-20.22.40.504004	C 14	*STME	/SkuView/Policy_Minder/EDDUIN				
2015-00-15-20.22.47.025040	C 1U	*STME	/Skulliou/omoiltomp/0133 tyt				
		*STME	/SkyView/emailtemp/QIJJ.txt				
			/Skyview/emaillemp/FRSv5i5vHL				
	C 1U		/Skyview/Puticy Minder/FRSVSI				
			/Skyview/emailtemp/Q134.txt				
		*5100	/Skyview/emailtemp/FRLPPRFLHG				
		*SIMF	/Skyview/Policy Minder/FRLPPR				
2015-09-07-14.15.42.933936		*51MF	/Skyview/Policy Minder/Lompli				
2015-11-15-09.42.52.368448	CJW	*DIK	/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	CJ₩	*DIR	/newdirectory				
2015-11-16-20.13.32.268928	CJ₩	*STMF	/cjwtest.dat				
			More				
F3=Exit F12=Cancel	F19=Left	F20=Ri	ght F21=Split				
MA A			03/032				
128 1902 - Session successfully started			//				





Miscellaneous



Tools for managing IFS authorities - SECTOOLS



ि विमेग	Print Publicly	Auth Objects	(PRTPUBAUT)
Type choices, press	Enter.		
Object type Changed report only Directory	· · · · · · · · · · · · · · · · · · ·	<u>*DIR</u> <u>*NO</u> '/'_	*ALRTBL, *AUTL, *BLKSF *NO, *YES
Search subdirectory		<u>*N0_</u>	*NO, *YES
			Detter
F3=E×it F4=Prompt F24=More keys	F5=Refresh	F12=Cancel	Bottom F13=How to use this display

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

🥙 iSeries Navigator				
<u>File E</u> dit <u>V</u> iew <u>H</u> elp				Navigate to
~ X ┗ € X ☎ ♥ 👿 ♥			0 minutes old	the directory
Environment: My Connections	Skyview: File Share	es iSeries NetServer: SKYVIEW		Right click
🗄 🛄 tmp 🔝	Name	Path	Description	
etc usr usr QIBM QSR QTCPTMM QTCPTMM www bin var lib Ib SKYVIEW QOpenSys	JCertauth JIfstool lib JQca400 JQdirsrv JDQibm JCRoot	/QIBM/UserData/ICS5/Cert/Dow /QSY5.LIB/IFSTOOL.LIB /QCA400 /QIBM/ProdData/OS400/DirSrv /QIBM /	Certificate Share CA/400 OS/400 Directory Services IBM Product Directories Share my entire system	Choose Sharing, New sharing to define a new share
GOLS GOLS GSYS.LIB GOPT GOP				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 QPWFSERVER authorization list to *EXCLUDE
- Create the share as Read only

File shares



- 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\$



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



1.000		Edit Authori	zation List		
Object Library		QPWFSERVER QSYS	Owner Primary gro		QSYS *NONE
Type changes	s to current	authorities, pr	ess Enter.		
User *PUBLIC QSYS GRP_OPER	Object Authority <u>*EXCLUDE</u> <u>*ALL</u> <u>*USE</u>	List Mgt <u>X</u> —			
F3=Exit F F11=Display (C) COPYRIG	5=Refresh detail obje HT IBM CORP.	F6=Add new users ct authorities 1980, 2003.	F12=Cancel	F24=More kei	Bottom ys

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

🥙 iSeries Navigator					
File Edit View Help					
,2 🕨 🕙 🖆 🗇 🗊 🛇			3 minutes old		
Environment: My Connections	192.168.1.5: TCP/IP				
🕀 📵 Management Central (192.168.1.5)	Server Name	Status	Description		
E 📓 My Connections	Relay Agent	Stopped	BootP DHCP Relay Agent		
⊥ 10.1.1.11	RebootP	Stopped	BootP Server		
	The DDM	Stopped	DRDA DDM Server TCP/IP		
	The DHCP	Stopped	DHCP		
10.1.184.92	RouteD	Stopped	RouteD		
E Q Pacis Operations	TERPC	Stopped	RPC		
	TFTP	Stopped	Trivial FTP		
	The NFS	Stopped	NFS Server		
	ToiSeries NetServer	Started	iSeries Support for Windov		
TCP/IP Configuration	TINETD	Stopped	Internet Daemon (INETD)		
Remote Access Services	The EDRSQL	Stopped	Extended Dynamic Remoti		
🖃 🗍 Servers	To SNTP	Stopped	Simple Network Time Proto		
TCP/IP	The QoS	Stopped	QoS Server		
- 😽 iSeries Access	RADIUS NAS	None	RADIUS Network Access S WebFacing Server Graphical Debug Server Management Central Datalink File Manager VPN Connection Manager		
- 🙀 DNS	📅 WebFacing	Stopped			
🔄 🔏 User-Defined	System Debug	Stopped			
🕀 😰 IP Policies	Ranagement Central	Stopped			
🕀 👧 Enterprise Identity Mapping	R DLFM	Stopped			
Internet	📅 Virtual Private Networking	Stopped			
Integrated Server Administration		Stopped	CIM Object Manager		
🖽 🛗 Security	Recc .	Stopped	eCC		
C Hereiter Lisers and Grouns	2				
	J				

SKY VIEW A Division of HelpSystems

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

Right click on iSeries NetServer choose Properties

11/19/2015

NetServer – Connections and Shares





Right click on NetServer.

Choose Open

Use this to discover sessions connecting through various file shares

NetServer – Disabled Profiles



A Division of HelpSystems



- 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/gusrtool.html

NetServer Guest Profile - Properties



i5/OS NetServer Properties - Skyview3		
General Advanced Security WINS Con	figuration Subsystems	
Guest user ID:	GUEST	
Authentication method:	Encrypted passwords	
Allow authentication with LAN Manager pas	sword hash: No	
Require clients to sign requests:	No	
	Next Start	
	i5/OS NetServer Security Next Start - Skyview3	
	i5/OS Support for Windows Network Neighborhood	
	Guest user ID: GUEST	1
	Authentication method: Encrypted passwords	I
	🗖 🗖 Allow authentication with LAN Manager password hash	
	Require clients to sign requests: No	I
	Reset to Current	
	OK Cancel Help ?	

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.

Notes on Viruses and IBM i



• 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