IBM i Quick Security Assessment Summary
Noviembre 2023

Santiago Barú Núñez Gómez
Power IBM i Consultant – IBM Technology Expert Labs - Systems

Statement of Good Security Practices

- IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise.
- Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others.
- **No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access.**
- IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.
- IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

IBM Security

Introduction

The IBM i Quick Security Assessment is a standardized Systems Lab Services and Training offering which provides Clients with a summarized analysis of how security has been implemented across a number of aspects of their IBM i. At a high level this analysis includes:

- Profile Administration
- Networking Interfaces
- Access Controls
- System Configuration

The tool does a thorough analysis of fundamental access controls, that is:

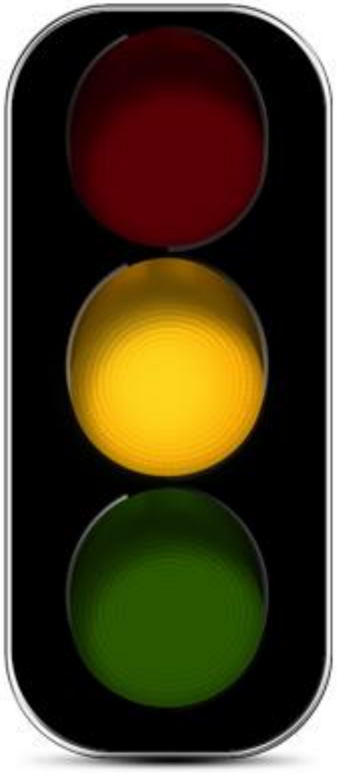
- –Authorization List (*AUTL) authorities
- –Public authorities
- –Private authorities
- –User/Group inheritance
- –Command line escapes
- –Object ownership

The results of the analysis is delivered in the form of a PDF document. The results are then reviewed with the Client at the conclusion of the engagement.

Introduction

The security assessment was conducted on the following partitions:

- ✓ **S1020F7D**



The primary focus of the assessment:

- ✓ Operating system environment
- ✓ User configuration
- ✓ General object permissions
- ✓ Application security
- ✓ Common network settings and services
- ✓ Audit and logging setup

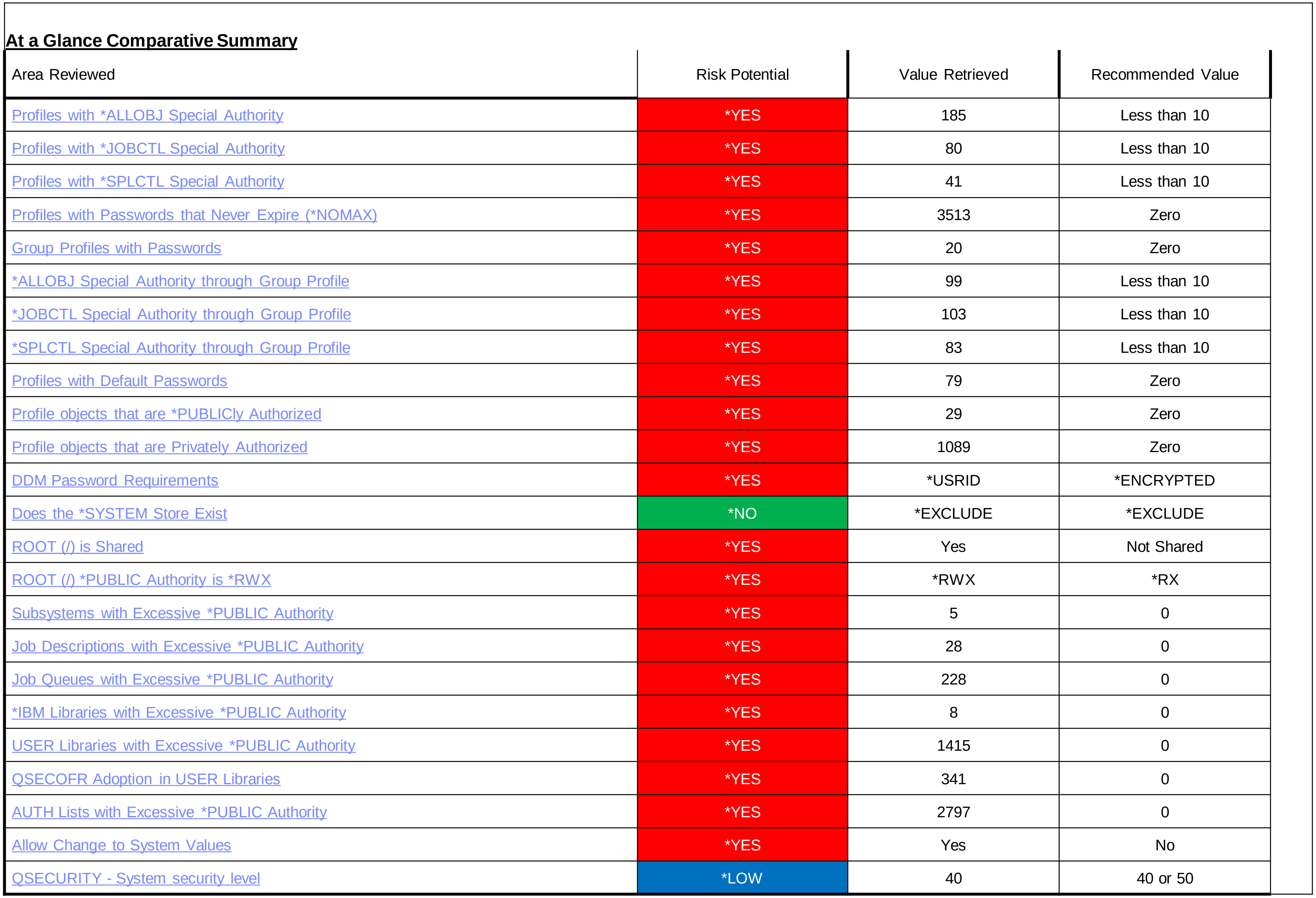
The overall Risk Rating across the partitions is HIGH.

Indicators

Findings are color coded as follows:

- 🟥 Red indicates the finding is serious or indicates a highly probable vulnerability with substantial impact to system integrity and should be corrected immediately
- 🟩 Green indicates findings that in our opinion are well done
- 🟦 Blue findings indicate low probability and/or lower impact to system integrity

At a Glance…

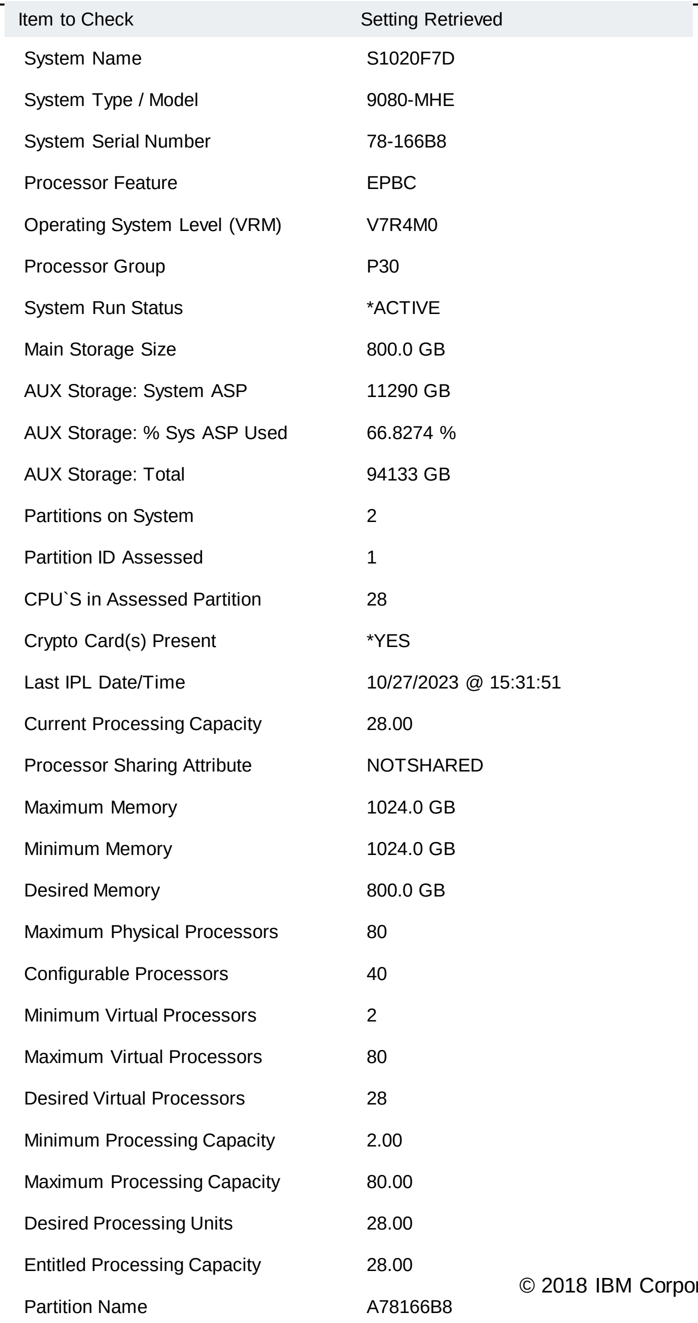


At a Glance Comparative Summary

Area Reviewed	Risk Potential	Value Retrieved	Recommended Value
Profiles with *ALLOBJ Special Authority	*YES	185	Less than 10
Profiles with *JOBCTL Special Authority	*YES	80	Less than 10
Profiles with *SPLCTL Special Authority	*YES	41	Less than 10
Profiles with Passwords that Never Expire (*NOMAX)	*YES	3513	Zero
Group Profiles with Passwords	*YES	20	Zero
*ALLOBJ Special Authority through Group Profile	*YES	99	Less than 10
*JOBCTL Special Authority through Group Profile	*YES	103	Less than 10
*SPLCTL Special Authority through Group Profile	*YES	83	Less than 10
Profiles with Default Passwords	*YES	79	Zero
Profile objects that are *PUBLICly Authorized	*YES	29	Zero
Profile objects that are Privately Authorized	*YES	1089	Zero
DDM Password Requirements	*YES	*USRID	*ENCRYPTED
Does the *SYSTEM Store Exist	*NO	*EXCLUDE	*EXCLUDE
ROOT (/) is Shared	*YES	Yes	Not Shared
ROOT (/) *PUBLIC Authority is *RWX	*YES	*RWX	*RX
Subsystems with Excessive *PUBLIC Authority	*YES	5	0
Job Descriptions with Excessive *PUBLIC Authority	*YES	28	0
Job Queues with Excessive *PUBLIC Authority	*YES	228	0
*IBM Libraries with Excessive *PUBLIC Authority	*YES	8	0
USER Libraries with Excessive *PUBLIC Authority	*YES	1415	0
QSECOFR Adoption in USER Libraries	*YES	341	0
AUTH Lists with Excessive *PUBLIC Authority	*YES	2797	0
Allow Change to System Values	*YES	Yes	No
QSECURITY - System security level	*LOW	40	40 or 50

Configuration reviewed

- During the security assessment, library QZRDQWKSEC was installed on your system and contained the commands, programs and queries used by the assessment.
- These programs and queries are the property of IBM and are provided for use during the security assessment only.
- They are provided on an as-is basis with no warranties implied.
- Library QZRDQWKDTA was produced during the assessment and contains the database files that can be queried by you and your staff to produce customized reports of the data.
- Both libraries QZRDQWKSEC and QZRDQWKDTA are *EXCLUDE from the *PUBLIC while on the system and library QZRDQWKSEC should be removed following the review.



Item to Check	Setting Retrieved
System Name	S1020F7D
System Type / Model	9080-MHE
System Serial Number	78-166B8
Processor Feature	EPBC
Operating System Level (VRM)	V7R4M0
Processor Group	P30
System Run Status	*ACTIVE
Main Storage Size	800.0 GB
AUX Storage: System ASP	11290 GB
AUX Storage: % Sys ASP Used	66.8274 %
AUX Storage: Total	94133 GB
Partitions on System	2
Partition ID Assessed	1
CPU`S in Assessed Partition	28
Crypto Card(s) Present	*YES
Last IPL Date/Time	10/27/2023 @ 15:31:51
Current Processing Capacity	28.00
Processor Sharing Attribute	NOTSHARED
Maximum Memory	1024.0 GB
Minimum Memory	1024.0 GB
Desired Memory	800.0 GB
Maximum Physical Processors	80
Configurable Processors	40
Minimum Virtual Processors	2
Maximum Virtual Processors	80
Desired Virtual Processors	28
Minimum Processing Capacity	2.00
Maximum Processing Capacity	80.00
Desired Processing Units	28.00
Entitled Processing Capacity	28.00
Partition Name	A78166B8

User administration

The following table is a high-level breakdown of the user population on the system that was reviewed. It might be worth investigating whether all users on the system need access. Also note the number of disabled users. Is there a need for these profiles to remain on the system? In the pages that follow we will dissect in great detail how these users and all users are administered.

Special authorities are used to give users the authority to perform certain system operations (e.g. save & restore, job control, security administration, etc.) on a global basis. The special authorities referred to and reported in this section represent special authority at the user and group levels.

FINDINGS

■ **Total number of profiles:**	**8,086**
✓ **Customer created:**	**8,014**
✓ **Enabled profiles:**	**3,282**
✓ **Disabled profiles:**	**4,732**

■ **Profiles with SPCAUT:**	
✓ ***ALLOBJ – All Object:**	**284**
✓ ***AUDIT – Auditing:**	**17**
✓ ***IOSYSCFG – System configuration:**	**96**
✓ ***JOBCTL – Job Control:**	**183**
✓ ***SAVSYS – Save and restore:**	**129**
✓ ***SECADM – Security administration:**	**34**
✓ ***SERVICE – Use DST/SST:**	**71**
✓ ***SPLCTL – Spool files:**	**124**
✓ ***NONE:**	**7,768**

RECOMMENDATIONS

- ✓ Examine disabled user profiles → cleanup
- ✓ Check profiles with command line access
- ✓ Check profiles with special authorities should only be granted on an exception basis
- ✓ The purpose of a group profile is to grant access to users via memberships
  - Never log in with a group profile
  - In profile specify: `PASSWORD(*NONE) INLMNU(*SIGNOFF) LMTCPB(*YES)`

Default passwords

The Analyze Default Passwords (ANZDFTPWD) command allows you to print a report of all the user profiles on the system that have a default password and to take an action against the profiles. A profile has a default password when the profile's password matches the user profile name. **Always** change vendor-supplied default passwords.

FINDINGS

🟥	**Default Passwords:**		**79**
	✓	**Enabled profiles:**	**2**
		✓ **with privileges:**	**1**
		✓ **with *ALLOBJ Forever:**	**1**

RECOMMENDATIONS

- ✓ Do NOT use default passwords
- ✓ For service or function user profiles consider a password of *NONE
- ✓ Schedule the ANZDFTPWD command with the *DISABLE option
- ✓ Analyze user creation process
  - Change CRTUSRPRF parameter default for PASSWORD
- ✓ For audit and documentation purposes, always specify a descriptive text for objects - including user profiles

Password expiration / override

Passwords are generally the weakest link in security. Forcing users to change their passwords more often increases the difficulty for a person seeking to gain entry to the system. The following table provides statistics regarding password expiration on the system. The current password expiration system value on the system analyzed is set to **30** . Take note of the number of profiles that never expire or have a password expiration greater than 90 days. Also take note of the number of profiles that override the system value QPWDEXPITV. These could represent a security exposure, especially when these profiles have special authorities and/or default passwords.

FINDINGS

🟥	**Number of profiles that never expire (*NOMAX):**	**3,513**
🟦	**Q profiles that never expire:**	**43**
🟩	**Expired but still enabled:**	**27**
🟩	**Expiration = *SYSVAL:**	**4,475**
🟥	**Not compliant with QPWDEXPITV:**	**3,611**
🟥	**Total PWD expiry not = *SYSVAL:**	**3,611**
🟥	**Profiles with no password:**	**2,093**
🟦	**Profiles PWD expiring 15 days**	**288**

RECOMMENDATIONS

- ✓ Set a password expiration value on all systems
- ✓ Investigate invalid sign on attempts
- ✓ Monitor PW audit journal entries for password conformance
- ✓ Reduce the number of profiles with passwords that do not expire

Inactive accounts

Inactive or dormant accounts are a notorious administrative weakness on any system, especially those accounts with special authorities. Once an account is known, it can become the target of an attack - whether enabled or disabled. Eliminating the inactive accounts reduces the number of targets that an attacker can use to gain access to a system.

Not Recently Used:

Never:	689
Never used with password *NONE:	386
Over 365 days:	1,349
Over 180 days:	1,248
Over 90 days:	600
Over 60 days:	217
Over 30 days:	296
Enabled:	246
Enabled with *SPCAUT:	15
Total not signed on:	4,399

Never Used:

Over 365 days:	456
Over 180 days:	61
Over 90 days:	36
Over 90 days – ALL:	553
Over 90 days – ALL & ENABLED:	59
Over 60 days:	16
Over 30 days:	16
Less than 30 days:	104
Enabled:	69
Enabled with *SPCAUT:	3
Total created not used:	689

RECOMMENDATIONS

- ✓ Archive and delete these profiles. Inactive accounts may be vulnerable to impersonation and unauthorized access if they are currently *ENABLED or later re-*ENABLED by an administrator.
- ✓ The accumulation of inactive accounts that remain on the system can make account administration difficult at best. All accounts should be carefully analyzed prior to removal to avoid application or system impact

Profiles with passwords that can signon CL access

The following table provides statistics on the count of user profiles that have command line access. Review those user profiles with command line access that can sign on. If these users have special authorities they may present a security exposure.

FINDINGS

🟨	**Profiles with CL can signon:**	**57**
🟥	**Profiles with CL cannot sign-on:**	**109**
🟧	**Total profiles with CL access:**	**166**
🟧	**Limit capabilities = *NO:**	**166**
🟧	**Limit capabilities = *YES:**	**7,920**
🟧	**Limit capabilities = *PARTIAL:**	**0**

RECOMMENDATIONS

✓ Typically only the system administrators and operators require command line access.

✓ All users working on the production environment should use the Operational Assistant menu or application menus that are custom designed to provide required commands so that they do not need command line access.

Group Profiles

Group Profiles are a mechanism used to organize and control the access or permissions of its members. It defines the authority of a group of users. A Group Profile is a special type of user profile and can own objects on the system. Typically, you create a group profile for a set of users with similar system access and usage needs. For example, you might create a group profile for a set of users who need to use the same applications in the same way.

FINDINGS

🟩	**Total number of groups:**	**337**
🟥	**Groups with special authorities:**	**19**
🟨	**Group profiles with password:**	**20**
🟨	**Largest user group:**	**GRPCONS001**
🟨	**Groups with owner *GRPPRF:**	**0**
🟨	**User profiles not in a group:**	**328**
🟨	**Members in largest group**	**3,661**

RECOMMENDATIONS

- ✓ Be cautious when using multiple groups, authority inherited from multiple groups is cumulative.
- ✓ Review the groups with special authorities. Only administrative groups should have special authorities.
- ✓ Application group profiles should not require any special authorities. Group members that inherit special authorities from their groups may represent a security exposure.

Profiles that grant the *PUBLIC access

Granting *PUBLIC authority to any user created or IBM supplied profile not designed to grant *PUBLIC authority presents a security exposure by allowing any other user on the system to use these *PUBLICly authorized users to swap authority with them and run jobs as them. The following table provides a count of the *PUBLICly authorized profiles and the count of those with Special Authorities.

FINDINGS

🟥	**User profiles with *PUBLIC not *EXCLUDE:**	**10**
🟥	**User profiles with *PUBLIC not *EXCLUDE with *SPCAUT:**	**4**
🟨	**QDBSHRx, QTMPLPD *PUB NOT DFLT :**	**25**

RECOMMENDATIONS

- ✓ Granting *PUBLIC authority to any profile other than the three IBM supplied profiles (QDBSHR, QDBSHRDO, and QTMPLPD) is not recommended.
- ✓ Any authenticated user on this system can submit jobs and swap authorities with any *PUBLICly authorized profiles.
- ✓ If these profiles are *PUBLICly authorized to enable help desk personnel to manage them, a better alternative would be an adopted authority program that limits the functions that help desk personnel can perform on these profile objects.

Profiles that are privately authorized

Granting private authorities to any user created or IBM supplied profile not designed to grant a private authority to any user that is not the owner of the profile or a group member of the profile may present a security exposure by allowing those privately authorized users to use these profiles to swap authority with them and run jobs as them. The following statistical table is provided to show not just the count of privately authorized profiles (if present) but the extent to which they exist and the number of profiles that have been given authority to the profiles of others.

FINDINGS

🟥	**User profiles with private authorities:**	**1,089**
🟥	**User profiles with private auth *SPCAUT:**	**81**
🟨	**Total private authorities:**	**1,624**
🟨	**Total authorized users:**	**252**

RECOMMENDATIONS

- ✓ Granting private authority to any profile not designed to be privately authorized is not recommended unless there is a known reason for privately authorizing these profiles.
- ✓ Authenticated users on the system can submit jobs and swap authorities with any privately authorized profiles they have authority to.
- ✓ If these profiles are privately authorized to enable help desk personnel to manage them, a better alternative would be an adopted authority program that limits the functions that help desk personnel can perform on these profile objects

User profile initial programs

The following table provides statistics about the administration of initial programs in the user profiles. Make a point to investigate the users that have an initial program that adopts the authority of its owner. Specifying a program that adopts authority - especially *ALLOBJ, could pose a security risk. This risk increases if the users LMTCPB is not equal to *YES and they have access to a command line after calling these programs.

FINDINGS

🟩	**Profiles with initial program:**	**4,444**
🟥	**Profiles with initial program *NONE:**	**3,642**
🟨	**Profiles with initial program not found:**	**3**
🟨	**Profiles using *LIBL / *CURLIB:**	**9**
🟨	**Profiles that adopt:**	**2**
🟨	**Profiles that adopt with *SPCAUT:**	**2**
🟨	**Profiles that adopt with *ALLOBJ:**	**2**
🟨	**Profiles with INLPGM = QCMD:**	**0**
🟨	**INLPGM QCMD with LMTCPB *NE *YES:**	**0**
🟥	**Users with an invalid initial program:**	**4,444**

RECOMMENDATIONS

✓ Make a point to investigate the users that have an initial program that adopts the authority of its owner.

✓ Specifying a program that adopts authority - especially *ALLOBJ, could pose a security risk.

✓ This risk increases if the users LMTCPB is not equal to *YES and they have access to a command line after calling these programs.

User profile initial menus

The next table provides statistics about the administration of initial menus in the user profiles. Make a point to investigate the users with initial menus. Note that even users limited to a menu with no command line may be able to execute commands thru other mechanisms such as RMTCMD, REXEC, or FTP.

FINDINGS

🟩	**Profiles with initial menu:**	**4,599**
🟨	**Initial menu MAIN/*LIBL:**	**83**
🟨	**Initial menu *SIGNOFF:**	**3,514**
🟨	**Menu *SIGNOFF with LMTCPB *NE *YES:**	**40**
🟨	**Unique initial menus:**	**19**
🟥	**Users with an invalid initial menu:**	**4,440**

RECOMMENDATIONS

- ✓ Make a point to investigate the users with initial menus.
- ✓ Note that even users limited to a menu with no command line may be able to execute commands thru other mechanisms such as RMTCMD, REXEC, or FTP.

User profile attention programs

The following table provides statistics about the administration of attention programs in the user profiles. Make a point to investigate the users that have an initial program that adopts the authority of its owner. Specify a program that adopts authority - especially *ALLOBJ, could pose a security risk. The risk increases if the users LMTCPB is not equal to *YES and they have access to command line after calling these programs.

FINDINGS

🟨	**Profiles with attention program:**	**205**
🟨	**Profiles with ATNPGM = *SYSVAL:**	**203**
🟨	**Profiles with ATNPGM = QSCATTN:**	**2**
🟨	**Profiles with ATNPGM = QCMD:**	**0**
🟨	**Profiles with ATNPGM = QUSCMDLN:**	**0**
🟨	**ATNPGM QCMD with LMTCPB *NE *YES:**	**0**
🟨	**Profiles with QUAL/ATNPGM missing:**	**0**
🟨	**Profiles with ATNPGM using *LIBL:**	**0**
🟨	**Profiles with ATNPGM = *ASSIST:**	**0**
🟨	**Profiles with ATNPGM = *NONE:**	**7,881**
🟨	**Profiles with other ATNPGM:**	**0**
🟨	**Profiles with ATNPGM of other owner:**	**205**
🟨	**Profiles with ATNPGM ADP other owner:**	**0**
🟥	**User with an invalid ATNPGM:**	**2**

Invalid signon attempts

The following table reports statistics and details on invalid sign-on attempts. Review profiles with a large number of invalid attempts. A high number of failed sign-on attempts could indicate that an unauthorized person is trying to gain access to the system. It is very unlikely that a user would try to sign-on so many times with a wrong password.

FINDINGS

Profile with most attempts total:	**3,442**
Profile with more than 5 tries:	**144**
Total number of attempts:	**6,609**
Profile with most attempts:	**SCOR**

RECOMMENDATIONS

- ✓ Try to find the root cause of the invalid signon attempts.
- ✓ These may originate from automation programs that try to signon.
- ✓ If these users have not been used in several years and do not own any objects, you should consider deleting those profiles

System values that control passwords

Weak passwords are arguably the weakest link in IT. Potentially, a weak password gives an outsider access not only to the IBM i, but to the entire network to which the IBM i is connected. It is the foundation of your computer security, and it needs to stand up against the tools that hackers have for cracking it. There are 308 million possible letter combinations for a six letter password using all upper case or all lower case letters. Password crackers that are readily available on the Internet at no cost can check all of them in about 2 minutes.

System Value	Short Description	Recommended Setting	Observed setting
QMAXSIGN	Maximum Failed Signon Attempts Allowed	3	3
QMAXSGNACN	Action to take for Failed Signon Attempts	2 or 3	3
QPWDCHGBLK	Time Period to Block Password Changes	99	*NONE
QPWDEXPITV	Password Expiration Interval	90	90
QPWDEXPWRN	Password Expiration Warning	7	7
QPWDLMTAJC	Limit Adjacent Digits in Password	1	1
QPWDLMTCHR	Limit Characters in Password	AEIOU@$#	*NONE
QPWDLMTREP	Limit Repeating Characters in Password	2	2
QPWDLVL	Password Level	1 or 3	0
QPWDMAXLEN	Maximum Password Length	10	10
QPWDMINLEN	Minimum Password Length	7	8
QPWDPOSDIF	Limit password character positions	1	1
QPWDRQDDGT	Password requires at least one Numeric Digit	1	1
QPWDRQDDIF	Duplicate Password Control	1	4
QPWDRULES	Password Rules	*PWDSYSVAL	*PWDSYSVAL
QPWDVLDPGM	Password validation program	Validation program	*NONE

System values that control auditing

The following system values control if and/or how security is being monitored using native IBM i operating system auditing controls.

System Value	Short Description	Recommended Setting	Observed setting
QAUDCTL	Auditing Control	*AUDLVL, *OBJAUD, and *NOQTEMP	*OBJAUD, *AUDLVL, *NOQTEMP
QAUDENDACN	Auditing End (Error) Action	*NOTIFY	*NOTIFY
QAUDFRCLVL	Force Auditing Data	*SYS	1
QAUDLVL	Security Auditing Level	*AUTFAIL, *OBJMGT, *PGMFAIL, *SAVRST, *SERVICE, *SECURITY, and *SYSMGT	*AUTFAIL, *CREATE, *DELETE, *JOBDTA, *SECURITY, *PGMADP, *SAVRST, *PRTDTA, *OBJMGT
QAUDLVL2	Security Auditing Level Extension	*NONE	*NONE
QCRTOBJAUD	Create Object Auditing	*NONE	*NONE

General security system values

System Value	Short Description	Recommended Setting	Observed value
QDSCJOBITV	Time Interval before Disconnected Jobs End	60	10
QINACTITV	Inactive JOB Time-out Interval	30	10
QINACTMSGQ	Inactive Job Message Queue	*DSCJOB	*ENDJOB
QLMTDEVSSN	Limit Device Sessions	1	1
QLMTSECOFR	Limit Security Officer Device Access	1	0
QRETSVRSEC	Retain Server Security Data	0	1
QRMTSIGN	Remote Sign-on Control	*FRCSIGNON	RMTOBJ/EXPAST
QSCANFS	Scan File Systems	*ROOTOPNUD	*ROOTOPNUD
QSCANFSCTL	Scan File Systems Control	*ERRFAIL and *NOWRTUPG	*NONE
QSECURITY	System Security Level	40 or 50	40
QSSLCSL	SSL Cipher Specification List	V7R3 with TCP Group 5 and above & V7R4: *AES_128_GCM_SHA256 *AES_256_GCM_SHA384 *CHACHA20_POLY1305_SHA256 *ECDHE_ECDSA_AES_128_GCM_SHA256 *ECDHE_ECDSA_AES_256_GCM_SHA384 *ECDHE_RSA_AES_128_GCM_SHA256 *ECDHE_RSA_AES_256_GCM_SHA384 *ECDHE_ECDSA_CHACHA20_POLY1305_SHA256 *ECDHE_RSA_CHACHA20_POLY1305_SHA256 *RSA_AES_128_GCM_SHA256 *RSA_AES_256_GCM_SHA384 *ECDHE_ECDSA_AES_128_CBC_SHA256 *ECDHE_ECDSA_AES_256_CBC_SHA384 *ECDHE_RSA_AES_128_CBC_SHA256 *ECDHE_RSA_AES_256_CBC_SHA384 *RSA_AES_128_CBC_SHA256 *RSA_AES_128_CBC_SHA *RSA_AES_256_CBC_SHA256 *RSA_AES_256_CBC_SHA	*AES_128_GCM_SHA256, *AES_256_GCM_SHA384, *CHACHA20_POLY1305_SHA256, *ECDHE_ECDSA_AES_128_GCM_SHA25, *ECDHE_ECDSA_AES_256_GCM_SHA38, *ECDHE_RSA_AES_128_GCM_SHA256, *ECDHE_RSA_AES_256_GCM_SHA384, *ECDHE_ECDSA_CHACHA20_POLY1305, *ECDHE_RSA_CHACHA20_POLY1305_S
QSSLCSLCTL	SSL Cipher Control	*USRDFN	*OPSYS
QSSLPCL	SSL Cipher Supported Version	V7R3 with TCP Group 5 and above & V7R4: *TLSV1.3 *TLSV1.2	*OPSYS
QUSEADPAUT	Use Adopted Authority	Authorization List	*NONE

Other system values related to security

System Value	Short Description	Recommended Setting	Observed setting
QALWOBJRST	Allow Object Restore	*NONE or *ALWPTF	*ALL
QAUTOCFG	Autoconfigure Devices	0	1
QAUTORMT	Autoconfigure Remote Controllers	0	1
QAUTOVRT	Autoconfigure Virtual Devices	0	0
QCRTAUT	Default *PUBLIC Authority for Created Objects	*USE or *EXCLUDE	*CHANGE
QFRCCVNRST	Force Conversion on Restore	3	2
QSHRMEMCTL	Shared Memory Control	0	1
QSYSLIBL	System part of the Library List	QSYS, QSYS2, QHLPSYS, and QUSRSYS	QSYSBANES (*CHANGE) QSYS (*USE), QSYS2 (*USE), QHLPSYS (*USE), QUSRSYS (*USE), RBTSYSLIB(*USE)
QVFYOBJRST	Verify Object on Restore	3 or 5	1 1

System Service Tools (SST)

System Service Tools (SST) provide access to low level machine functions and hardware related configuration options. SST functions can also be used for debugging problems. SST access requires the permission to use the STRSST CL command as well as the *SERVICE special authority. In addition, the person who wants to use SST needs to have a SST user account with the appropriate privileges to access the various SST functions. SST user identifiers are not related to IBM i user profiles. There are three key security related settings found in (SST) and can also be listed using the **DSPSECA** command, however many more exist:

1. **Allow Change to System Values** shows whether the service tools flag is set to the shipped default value that allows changes to security system values. Use SST or Dedicated Service Tools (DST) to control whether users can change security-related system values. After properly setting and documenting system values, use either SST or DST to lock the system values.

2. The **Allow Add of Certificates** value controls whether a digital certificate can be added using the QYDOADDV API. This value also indicates whether or not you can reset the password for the IBM i Digital Certificate Manager.

3. The **Allow SST User to Change PW** value is the service tools value that determines whether a service tools user ID with an expired and default password can change its own password using the QSYCHGDS API or from the service tools change password option.

<u>FINDINGS</u>

🟥	**Allow change to System values:**	**Yes**
🟥	**Allow add of certificates:**	**Yes**
🟥	**Allow SST user to change password:**	**Yes**

Work management

Review this table and consider the remediation of the *PUBLIC authority and object ownership…

Area of Review	Subsystems	Job Descriptions	Job Queues	Output Queues	Class Objects
Total Objects	216	1,102	430	12,222	318
Objects Owned by QSECOFR	28	53	21	326	52
Objects Owned by QDFTOWN	101	212	76	2,484	61
Objects Owned by QPGMR	14	80	49	11	49
Objects Owned by QSYS	38	189	10	400	27
Objects Owned by Other Q Profiles	8	38	18	969	18
Objects Owned by Non Q Profiles	27	530	256	8,032	111
Objects Owned by a Group	16	289	146	419	59
Groups that Own these Objects	3	8	6	9	4
Owners that have a Password	35	174	98	7,195	73
Objects with a *PUBLIC Authority of *ALL	3	20	2	28	8
Objects with a *PUBLIC Authority of *AUTL	2	20	13	15	0
... *PUBLIC Authority in *AUTL of *ALL	2	8	12	6	0
... *PUBLIC Authority in *AUTL of *CHANGE	0	0	107	0	0
... *PUBLIC Authority in *AUTL of *EXCLUDE	0	4	40	6	0
... *PUBLIC Authority in *AUTL of *USE	0	8	271	3	0
... *PUBLIC Authority in *AUTL of USER DEF	0	0	0	0	0
Objects with a *PUBLIC Authority of *CHANGE	49	345	107	8,849	189
Objects with a *PUBLIC Authority of *EXCLUDE	10	208	38	14	31
Objects with a *PUBLIC Authority of *USE	152	509	270	3,316	90
Objects with a *PUBLIC Authority of USER DEF	0	0	0	0	0

Subsystem descriptions - Autostart Jobs

An Autostart job entry is a job that runs automatically when a Subsystem is started. Autostart job entries contain the name of a job description that can specify a default user profile. You should understand the function of the JOBDs contained in your Autostart job entries. The following table is a statistical breakdown of the Autostart job entries.

FINDINGS

Total Autostart Job Entries:	**216**
ASJ with named JOBD:	**216**
ASJ JOBD with USER not Found:	**0**
ASJ JOBD *NE *EXCLUDE:	**93**
ASJ JOBD *NE *EXL with USER:	**92**
ASJ JOBD *NE *EXL USER *NE *EX:	**8**
ASJ JOBD *NE *EXL USER w SPCAU:	**8**

RECOMMENDATIONS

- ✓ Review the report table of Autostart job entries.
- ✓ Best practice is not to use a JOBD specifying a default user profile that is *PUBLICly authorized in an Autostart job entry.
- ✓ The job description may also contain request data (RQSDTA) that causes a program or a command to run.

Subsystem descriptions - Prestart Jobs

Prestart job entries are used to make a Subsystem ready for certain kinds of jobs so that the jobs can start more quickly. Prestart Jobs may start when the Subsystem starts or when they are needed. A Prestart Job Entry can specify a program to run, a default user profile and a job description. Prestart job entries specifying a *PUBLICly authorized profile in either the prestart job entry or the job description in the prestart job entry may provide the potential for a security exposure. You should ensure that prestart job entries perform only authorized functions.

FINDINGS

Total Prestart Job Entries:	**264**
PSJ Program compiled as *OWNER:	**69**
PSJ Start with Subsystem:	**213**
PSJ w User not Found:	**0**
PSJ w User *PUB not *EXCLUDE:	**0**
PSJ w User *PUB not *EXL w SPC:	**0**
PSJ with named JOBD:	**156**
PSJ JOBD *NE *EXCLUDE:	**153**
PSJ JOBD *NE *EXL with USER:	**57**
PSJ JOBD *NE *EXL USER *NE *EX:	**0**
PSJ JOBD *NE *EXL USER w SPCAU:	**0**

RECOMMENDATIONS

✓ Review the report table of prestart jobs. Best practice is not to use a prestart job entry with a *PUBLICly authorized user in either the prestart job entry or the job description specified in the prestart job entry.

Communications and remote locations entries

Prestart job entries are used to make a Subsystem ready for certain kinds of jobs so that the jobs can start more quickly. Prestart Jobs may start when the Subsystem starts or when they are needed. A Prestart Job Entry can specify a program to run, a default user profile and a job description. Prestart job entries specifying a *PUBLICly authorized profile in either the prestart job entry or the job description in the prestart job entry may provide the potential for a security exposure. You should ensure that prestart job entries perform only authorized functions.

FINDINGS

Total Communication Entries:	**130**
CMNE w Default User:	**58**
CMNE w Default User not Found:	**2**
CMNE w Default User w SPCAUT:	**42**
CMNE with named JOBD:	**23**
CMNE JOBD *NE *EXCLUDE:	**19**
CMNE JOBD *NE *EXL with USER:	**10**
CMNE JOBD *NE *EXL USER *NE *X:	**0**
CMNE JOBD *NE *EXL USER w SPCA:	**0**

Total Remote Location Entries:	**12**
RMTL w Default User:	**4**
RMTL w Default User not Found:	**0**
RMTL w Default User w SPCAUT:	**4**
RMTL with named JOBD:	**0**
RMTL JOBD *NE *EXCLUDE:	**0**
RMTL JOBD *NE *EXL with USER:	**0**
RMTL JOBD *NE *EXL USER *NE *X:	**0**
RMTL JOBD *NE *EXL USER w SPCA:	**0**

RECOMMENDATIONS

- ✓ Evaluate the communication and remote location entries on your system.
- ✓ Best practice is NOT to use communication and remote location entries that contain a default user profile.

Subsystems - Workstations names and types

When a Subsystem starts, it allocates all not allocated workstations that are listed (specifically or generically) in its entries for workstation names and workstations types. When a user signs on, the user is signing on to the Subsystem that has allocated the workstation. The workstation entry tells what job description will be used when a job starts at that workstation. The job description may contain request data that causes a program or a command to run. For example, the RQSDTA parameter might be CALL LIB1/PROGRAM1. Whenever a user signs on to a workstation in that Subsystem, the system will run PROGRAM1 in LIB1. The following table is a statistical breakdown of the workstation names and workstations types.

FINDINGS

Total Workstation Name Entries:	**735**	**Total Workstation Type Entries:**	**70**
WSN Allocation = *SIGNON:	**735**	**WST Allocation = *SIGNON:**	**47**
WSN Allocation = *ENTER:	**0**	**WST Allocation = *ENTER:**	**23**
WSN with named JOBD:	**0**	**WST with named JOBD:**	**5**
WSN JOBD *NE *EXCLUDE:	**0**	**WST JOBD *NE *EXCLUDE:**	**5**
WSN JOBD *NE *EXL with USER:	**0**	**WST JOBD *NE *EXL with USER:**	**0**
WSN JOBD *NE *EXL USER *NE *EX:	**0**	**WST JOBD *NE *EXL USER *NE *EX:**	**0**
WSN JOBD *NE *EXL USER w SPCAU:	**0**	**WST JOBD *NE *EXL USER w SPCAU:**	**0**

RECOMMENDATIONS

✓ A workstation entry might also specify a default user profile. For certain Subsystem configurations, this allows someone to sign on just by pressing the Enter key.

✓ If the QSECURITY system value on your system is less than 40, you should review your workstation JOBD entries for default users.

Job descriptions

The job description allows you to create a set of job properties that are saved and available for multiple uses. A job description also represents a potential security exposure. Frequently, a job description specifies a profile name for the USER parameter allowing a job to enter the system without appropriate security checking. The following table is a statistical breakdown of the job descriptions…

FINDINGS

JOBD w USER = *RQD:	**648**
JOBD w USER = USRPRF:	**454**
JOBD w USER *PUB not *EXCLUDE:	**21**
JOBD not *EXC w USER = *RQD:	**623**
JOBD not *EXC w USER = USRPRF:	**271**
JOBD w USER = NOT FOUND:	**13**
JOBD not *EXC w USER *PUB Acss:	**19**
JOBD not used in last 365 days:	**76**
JOBD never used:	**704**
JOBD w Request Data *NE *NONE:	**220**
User Created JOBDs:	**838**
***IBM Created JOBDs:**	**264**
***IBM Modified JOBDs:**	**10**

RECOMMENDATIONS

- ✓ Best practice is to have no *PUBLICly authorized job descriptions specifying a default user profile.
- ✓ Be extremely cautious with default profiles with special authorities.

Output and job queue authority

Output queues are objects that store print output, such as financial reports, payroll information, invoices, development plans, etc. Print output can contain data that is not classified or top secret information. Therefore it is very important to decide and control who has what level of access to the various output queues on the system. The following table is a statistical breakdown of the output queues.…

FINDINGS

OUTQ w Oper Control = *YES:	**12,170**
OUTQ w Display Any = *NO:	**11,422**
OUTQ w Display Any = *YES:	**791**
OUTQ w Display Any = *OWNER:	**9**
OUTQ w AUTCHK = *OWNER:	**11,570**
OUTQ w AUTCHK = *DTAAUT:	**652**

Job queues provide a mechanism to submit batch jobs on the system. Batch jobs are typically part of a business application. It is important that jobs run in the requested time and order. The following table is a statistical breakdown of the job queues…

FINDINGS

JOBQ w Oper Control = *YES:	**430**
JOBQ w AUTCHK = *OWNER:	**421**
JOBQ w AUTCHK = *DTAAUT:	**9**

IBM Libraries analysis

It is important to understand how object authorities impact the usage and functionality of your system and applications as well as how improper authorities can represent a risk to the integrity, confidentiality and usability of your system and applications. The following section details the demographics, authorities, and auditing of the *IBM Libraries.

FINDINGS

Total IBM Libraries Found:	76
IBM Libraries in ASP Groups:	0
Number of ASP Groups in Count:	0
Owned by QSECOFR:	1
Owned by QDFTOWN:	0
Owned by QPGMR:	0
Owned by QSYS:	71
Owned by Other Q Profiles:	4
Owned by Non Q Profile:	0
Owned by a Group:	1
Groups that own Libraries:	1
Owners with a Password:	1
Libraries secured by AUTL:	1

*PUBLIC = *ALL:	0
*PUBLIC = *AUTL:	1
*AUTL *PUB = *ALL:	1
*AUTL *PUB = *CHANGE:	0
*AUTL *PUB = *EXCLUDE:	0
*AUTL *PUB = *USE:	0
*AUTL *PUB = USER DEF:	0
*PUBLIC = *CHANGE:	7
*PUBLIC = *EXCLUDE:	1
*PUBLIC = *USE:	67
*PUBLIC = USER DEF:	0
Other Users = *ALL:	71
Other Users = *CHANGE:	1
Other Users = *EXCLUDE:	2
Other Users = *USE:	105
Other Users = USER DEF:	0

RECOMMENDATIONS

- ✓ Review the *PUBLIC authorities on files and other objects in excess of *CHANGE. Files and other objects should never require *PUBLIC *ALL authority. Programs should grant *USE only to prevent the use of DEBUG facilities that can change variables and run other harmful functions.

IBM Libraries analysis

Authority greater than *CHANGE is never recommended for the *PUBLIC for *IBM libraries. An authority of *ALL allows any user to change the name of a library or manage authority to the library object that could cause Denial of Service to others. An authority of *USE is better if users don't need to create files in an *IBM library and *EXCLUDE is best if the *PUBLIC should not be allowed to use the library and its objects.

FINDINGS

🟩	System CMDs that have changed:	1
🟥	*ALLOBJ Adoption, Total PGMS:	534
🟩	QSECOFR Adoption, Total PGMS:	2
🟩	QSECOFR Adoption, *PUB=*ALL	0
🟩	QSECOFR Adoption, *PUB=*CHG	0
🟩	QSECOFR Adoption, *PUB=*EXCLD	0
🟩	QSECOFR Adoption, *PUB=*USE	2
🟩	QSECOFR Adoption, *PUB=*USRDF	0
🟥	OTHR *ALLOBJ ADPT, Total PGMS	532
🟩	OTHR *ALLOBJ ADPT, *PUB=*ALL	0
🟩	OTHR *ALLOBJ ADPT, *PUB=*CHG	0
🟩	OTHR *ALLOBJ ADPT, *PUB=*EXCLD	0
🟨	OTHR *ALLOBJ ADPT, *PUB=*USE	532
🟩	OTHR *ALLOBJ ADPT, *PUB=*USRDF	0

🟩	SYSVAL QCRTAUT = *CHANGE:	0
🟩	CRTAUT = *SYSVAL:	4
🟩	CRTAUT = *ALL:	0
🟩	CRTAUT = *CHANGE:	71
🟩	CRTAUT = *EXCLUDE:	0
🟩	CRTAUT = *USE:	1
🟩	CRTAUT = Authorization List:	0
🟩	SYSVAL QCRTOBJAUD = *NONE:	0
🟩	CRTOBJAUD = *SYSVAL:	76
🟩	CRTOBJAUD = *ALL:	0
🟩	CRTOBJAUD = *CHANGE:	0
🟩	CRTOBJAUD = *USRPRF:	0
🟩	CRTOBJAUD = *NONE:	0
🟩	CRTOBJAUD = Not Available:	0

RECOMMENDATIONS

- ✓ Review any System Commands that have been changed. These could represent malicious programs or altered programs and commands that could cause an application or system failure.

User Libraries analysis

As with IBM libraries, it is important to understand how object authorities impact the usage and functionality of your system and applications as well as how improper authorities can represent a risk to the integrity, confidentiality and usability of your system and applications. The following section details the demographics, authorities, and auditing of the USER Libraries. Note that if a user needs access to objects in a library (files, programs etc.); they also require access to the library where the object exists. Even if a user has *ALL authority to a file in a library, they cannot access that file unless they have *USE or greater authority to the library that contains the object. A well planned security model includes library authority standards.

FINDINGS

Total User Libraries Found:	**1,786**
User Libraries in ASP Groups:	**1,318**
Number of ASP Groups in Count:	**1**
Owned by QSECOFR:	**65**
Owned by QDFTOWN:	**1,120**
Owned by QPGMR:	**12**
Owned by QSYS:	**63**
Owned by Other Q Profiles:	**27**
Owned by Non Q Profile:	**498**
Owned by a Group:	**307**
Groups that own Libraries:	**13**
Owners with a Password:	**235**
Libraries secured by AUTL:	**336**
Owners AUTH = *ALL:	**1,757**
Owners AUTH = *CHANGE:	**2**
Owners AUTH = *EXCLUDE:	**2**
Owners AUTH = *USE:	**1**
Owners AUTH = USER DEF:	**0**

***PUBLIC = *ALL:**	**147**
***PUBLIC = *AUTL:**	**330**
***AUTL *PUB = *ALL:**	**23**
***AUTL *PUB = *CHANGE:**	**78**
***AUTL *PUB = *EXCLUDE:**	**211**
***AUTL *PUB = *USE:**	**18**
***AUTL *PUB = USER DEF:**	**0**
***PUBLIC = *CHANGE:**	**1,166**
***PUBLIC = *EXCLUDE:**	**65**
***PUBLIC = *USE:**	**76**
***PUBLIC = USER DEF:**	**1**
Other Users = *ALL:	**867**
Other Users = *CHANGE:	**44**
Other Users = *EXCLUDE:	**196**
Other Users = *USE:	**1,387**
Other Users = USER DEF:	**7**

User Libraries analysis

Authority greater than *CHANGE is never recommended at a library level for *PUBLIC. An authority of *ALL allows any user to change the name of a library or manage authority to the library object that could cause Denial of Service to others. An authority of *USE is better if users don't need to create files in a library and *EXCLUDE is best if the *PUBLIC should not be allowed to use the library and its objects.

FINDINGS

🟩	**SYSVAL QCRTAUT = *CHANGE:**	**0**
🟩	**CRTAUT = *SYSVAL:**	**1,481**
🟩	**CRTAUT = *ALL:**	**2**
🟩	**CRTAUT = *CHANGE:**	**23**
🟩	**CRTAUT = *EXCLUDE:**	**25**
🟩	**CRTAUT = *USE:**	**5**
🟩	**CRTAUT = Authorization List:**	**249**
🟩	**SYSVAL QCRTOBJAUD = *NONE:**	**0**
🟩	**CRTOBJAUD = *SYSVAL:**	**1,769**
🟩	**CRTOBJAUD = *ALL:**	**0**
🟩	**CRTOBJAUD = *CHANGE:**	**0**
🟩	**CRTOBJAUD = *USRPRF:**	**0**
🟩	**CRTOBJAUD = *NONE:**	**16**
🟩	**CRTOBJAUD = Not Available:**	**0**

🟥	***ALLOBJ Adoption, Total PGMS:**	**10,177**
🟨	**QSECOFR Adoption, Total PGMS:**	**341**
🟨	**QSECOFR Adoption, *PUB=*ALL:**	**42**
🟨	**QSECOFR Adoption, *PUB=*CHG:**	**40**
🟨	**QSECOFR Adoption, *PUB=*EXCLD:**	**191**
🟨	**QSECOFR Adoption, *PUB=*USE:**	**68**
🟨	**QSECOFR Adoption, *PUB=*USRDF:**	**0**
🟥	**OTHR *ALLOBJ ADPT, Total PGMS:**	**9,836**
🟨	**OTHR *ALLOBJ ADPT, *PUB=*ALL:**	**840**
🟨	**OTHR *ALLOBJ ADPT, *PUB=*CHG:**	**267**
🟨	**OTHR *ALLOBJ ADPT, *PUB=*EXCLD:**	**2,316**
🟨	**OTHR *ALLOBJ ADPT, *PUB=*USE:**	**6,354**
🟨	**OTHR *ALLOBJ ADPT, *PUB=*USRDF:**	**59**

RECOMMENDATIONS

✓ Review the *PUBLIC authorities on files and other objects in excess of *CHANGE. Files and other objects should never require *PUBLIC *ALL authority. Operations such as Clear Physical File Member (CLRPFM) and Create Duplicate Object (CRTDUPOBJ) require User Defined authorities greater than *CHANGE but less than *ALL. Programs should grant *USE only to prevent the use of DEBUG facilities that can change variables and run other harmful functions.

NetServer configuration

The IFS can also be used as a file share server - sometimes referred to as NetServer, it allows the configuration of Guest User Profile support. Enabling Guest User Profile support allows users without a valid IBM i user ID and password to map to shared resources anonymously. Best practice is not to configure NetServer for Guest User Profile support. Therefore, processes must be put in place to secure the IFS and NetServer. The following table reports the key settings for the Integrated File System (IFS) and NetServer.

FINDINGS

🟩	**ROOT (/) is Shared:**	**Yes**
🟩	**ROOT (/) Permissions:**	***R**
🟨	**ROOT (/) *PUBLIC Authority:**	***RWX**
🟩	**Total Number of Shares Present:**	**43**
🟩	**Allow GUEST Support:**	**No**
🟩	**GUEST Profile:**	**N/A**
🟩	**Allow LANMAN Passwords:**	***NO**
🟩	**MSG Authentication/Signing:**	***NONE**
🟩	**Browsing Interval (ms):**	**720000**
🟩	**SMB1 Current Setting:**	***ENABLED**
🟩	**SMB1 Setting at Next Restart:**	***ENABLED**
🟩	**SMB2 Current Setting:**	***ENABLED**
🟩	**SMB2 Setting at Next Restart:**	***ENABLED**
🟩	**SMB3 Current Setting:**	***ENABLED**
🟩	**SMB3 Setting at Next Restart:**	***ENABLED**
🟩	**Is NetServer Started:**	**Yes**
🟩	**Encrypted Connection Enforced:**	***NEGOTIATE**
🟩	**QSYS.LIB is Shared:**	**No**
🟩	**QSYS.LIB Permissions:**	**N/A**
🟩	**QSYS.LIB *PUBLIC Authority:**	***RX**
🟩	**QOpenSys is Shared:**	**No**
🟩	**QOpenSys Permissions:**	**N/A**
🟩	**QOpenSys *PUBLIC Authority:**	***RWX**
🟩	**QPWFSERVER *PUBLIC Authority:**	***USE**
🟩	**ROOT (/) Ownership:**	**QSYS**

RECOMMENDATIONS

- ✓ If not already done, consider changing the *PUBLIC authority to the root directory ('/') to *RX to prevent users from creating objects or additional directories at the root of the IFS. This change requires careful consideration however, since any newly created objects at the root level will need to be manually changed to *PUBLIC *RWX authority if these objects including directories need to allow write access.
- ✓ Review all file shares and ensure that they are properly configured and provide the correct permissions

TCPIP Server autostart values

Auto Start Servers are those servers that automatically start each time that TCP/IP is started. The cardinal rule for TCP/IP security is this: Unless you need a particular server or function, don't start the server. Be sure you understand the servers and functions that are being started with TCP/IP. The following table reports all of the servers and whether they start automatically when TCP/IP is started.

Server Name	Start Command	Server Description
*CIMOM	CIMOM	Common Information Model Object Manager (CIM
*DDM	QSYS/STRTCPSVR SERVER(*DDM)	Distributed Data Manager (DDM) server
*DIRSRV	QSYS/STRTCPSVR SERVER(*DIRSRV)	Lightweight Directory Access Protocol (LDAP)
*FTP	QSYS/STRTCPSVR SERVER(*FTP)	File Transfer Protocol (FTP) server
*INETD	QSYS/STRTCPSVR SERVER(*INETD)	Internet Daemon (INETD) server
*ITMI5OS	IBM ITM I5OS AGENT	Description Not Available
*LPD	QSYS/STRTCPSVR SERVER(*LPD)	Line printer daemon (LPD) server
*MGTC	QSYS/STRTCPSVR SERVER(*MGTC)	Management Central (MGTC) server
*NETSVR	QSYS/STRTCPSVR SERVER(*NETSVR)	NetServer (NETSVR) server
*NTP	QSYS/STRTCPSVR SERVER(*NTP)	Simple Network Time Protocol (SNTP) services
*OBJC	OBJECTCONNECT SERVER	Description Not Available
*OMPROUTED	QSYS/STRTCPSVR SERVER(*OMPROUTED)	OMPROUTE Daemon (OMPROUTED) server. Handles
*REXEC	QSYS/STRTCPSVR SERVER(*REXEC)	Remote Execution (REXEC) server
*SLP	IBM SLP SERVER	Service Location Protocol
*SMTP	QSYS/STRTCPSVR SERVER(*SMTP)	Simple Mail Transfer Protocol (SMTP) client

TCPIP Server autostart values

Server Name	Start Command	Server Description
SNMP	QSYS/STRTCPSVR SERVER(*SNMP)	Simple Network Management Protocol (SNMP) ag
*TELNET	QSYS/STRTCPSVR SERVER(*TELNET)	TELNET server
*TFTP	QSYS/STRTCPSVR SERVER(*TFTP)	Trivial File Transfer Protocol (TFTP) server
*VPN	QSYS/STRTCPSVR SERVER(*VPN)	Virtual Private Network (VPN) server
HOSTCENTRAL	QSYS/STRHOSTSVR SERVER(*CENTRAL) RQDPCL(*TCP)	Central Server
HOSTDATABASE	QSYS/STRHOSTSVR SERVER(*DATABASE) RQDPCL(*TCP)	Database Server
HOSTDTAQ	QSYS/STRHOSTSVR SERVER(*DTAQ) RQDPCL(*TCP)	Data Queue Server
HOSTFILE	QSYS/STRHOSTSVR SERVER(*FILE) RQDPCL(*TCP)	File Server
HOSTNETPRT	QSYS/STRHOSTSVR SERVER(*NETPRT) RQDPCL(*TCP)	Network Print Server
HOSTRMTCMD	QSYS/STRHOSTSVR SERVER(*RMTCMD) RQDPCL(*TCP)	Remote Command Server
HOSTSERVERS	QSYS/STRHOSTSVR SERVER(*ALL) RQDPCL(*TCP)	iSeries Host Server
HOSTSIGNON	QSYS/STRHOSTSVR SERVER(*SIGNON) RQDPCL(*TCP)	TCP Signon Server
HOSTSVRMAP	QSYS/STRHOSTSVR SERVER(*SVRMAP) RQDPCL(*TCP)	TCP Server Mapper

RECOMMENDATIONS

- ✓ Review those servers that are set to start automatically and ensure that the servers are being used.
- ✓ Change the autostart value for any that are not needed to *NO.
- ✓ Then, use the Change Command Default (CHGCMDDFT) command to set up the STRTCPSVR command to start the specific server, *AUTOSTART. This does not prevent users from starting other servers. However, by changing the command default, you make it less likely that users will start all servers by accident.

Listening ports

The following table provides information about the TCP/IP ports that were in a listening status at the time of the collection and it's a statistical sampling of the most common ports and the number of connections present

FINDINGS

🟨	Total All Connections:	62,461
🟨	Total TCP Ports:	62,330
🟩	Total UDP Ports:	131
🟩	TCP Listening Ports:	103
🟩	TCP Established Connections:	3,929
🟩	FTP:	4
🟩	FTP (Secure):	0
🟩	TELNET:	1,887
🟩	TELNET (Secure):	1
🟩	POP:	0
🟩	POP (Secure):	0
🟩	SQL Services:	0
🟩	NETBIOS:	4
🟩	Host Server:	59
🟩	Net Server:	9
🟩	REXEC:	1
🟩	Central Server:	942
🟩	Central Server (Secure):	1
🟩	DB Server:	154
🟩	DB Server (Secure):	0
🟩	DTAQ Server:	88
🟩	DTAQ Server (Secure):	0
🟩	File Server:	8
🟩	File Server (Secure):	1
🟩	Remote Command:	295
🟩	Remote Command (Secure):	0
🟨	User Defined:	58,788
🟩	All Others:	219

RECOMMENDATIONS

✓ Any port that is active for a service that is not being used is a potential entry point into the system that can be used to perform intrusion attempts or denial of service attacks. The risk is to allow an intruder to break into the system or render parts of the system unusable. Ensure that these listening ports should be open for incoming connections on your system and that they meet your security requirements. Consider using TCP Port Restrictions (ADDTCPPORT) to restrict port access to specific users on specific ports and protocols. Additionally, use exit programs and/or IP filtering between hosts on your network and these open ports.

Network attributes

Network attributes control how your system communicates with other systems. Some network attributes control how remote requests to process jobs and access information are handled. The following table lists the key network attributes and their settings on your system. Four of these attributes are of particular importance - they are: ALWADDCLU, JOBACN, PCSACC and DDMACC.

FINDINGS

System Name (SYSNAME):	**S1020F7D**
Operating System Level:	**V7R4M0**
APPN Node Type (NODETYPE):	***ENDNODE**
Network Job Action (JOBACN):	***FILE**
DDM/DRDA Req Access (DDMACC):	**EXDDM – in lib RMTOBJ**
Client Req Access (PCSACC):	***REGFAC**
Allow Cluster Add (ALWADDCLU):	***ANY**

RECOMMENDATIONS

- ✓ Review the requirement for DDM communications on the system, if no DDM communication is required, set the DDM/DRDA request attribute (**DDMACC**) to *REJECT for better security.
- ✓ Review your network job tables to determine what user profile name SNA distribution jobs will run under and what actions will be taken for input streams received through the SNADS network by the system. Use the WRKNETJOBE command. If no SNADS input streams are used you can change the Network Job Action (**JOBACN**) to *REJECT for better security.
- ✓ Allow Add To Cluster (ALWADDCLU): Specifies whether to allow the system to be part of an IBM i cluster definition. This is used to enhance application availability, but could also represent a security exposure if there is a setting other than *NONE. Leave this setting at *NONE unless you are participating in a cluster, then set to *ANY but consider *RQSAUT for tighter security.

DDM Password Required Attribute (CHGDDMTCPA)

The DDM (Distributed Data Management) password required attribute (PWDRQD parameter of CHGDDMTCPA command) controls the minimum level of password security required to connect to the system.

The current setting for the DDM password required attribute is ***USRID**

A setting of ***NO** (or ***USRID** on V6R1+) indicates that the connection on the target system will be made as the User ID specified. The connection will **not** require a password and ignore one if present. This is the most open and vulnerable setting for the DDM server. If users have access to the Add Server Authentication Entry (ADDSVRAUTE) command, they can choose to use a privileged profile such as QSECOFR with which to establish connections on target systems. With a setting of *NO, there is little control over the profiles under which DDM connections are made allowing users on remote systems to submit remote commands anonymously and with elevated privileges.

Recommendation:

✓ Review all DDM files and programs that connect to this system and consider changing the DDM Password Required attribute to require passwords for secure communications. Consider using stored procedures, kerberos authentication or identity tokens as an alternative. In addition, consider a change to users who have authority to run the ADDSVRAUTE command.

Warning: The values of ***NO**, ***USRID** and ***VLDONLY** can pose significant security risks. The only exception to the server authentication entry requirement is with the use of SQL. SQL will allow a connection whether server authentication entries exist or not. SQL does honor the CHGDDMTCPA password required attribute, however.

IP Datagram forwarding and Source routing

The IP datagram forwarding attribute (IPDTGFWD) of the CHGTCPA command specifies whether the IP layer forwards Internet Protocol (IP) datagrams between different networks. It essentially specifies whether the IP layer can act as an IP router or gateway. Careful security considerations should be reviewed prior to enabling IP forwarding. The IP datagram forwarding attribute (IPDTGFWD) on this system is set to ***NO.**

Recommendation

✓ You should review the IP datagram forwarding attribute (IPDTGFWD) on this system and determine if it should allow this system to act as an IP router. You can change this attribute with the CHGTCPA command.

An IP header may contain the Loose Source and Record Route (LSRR) option traditionally used by ***traceroute*** to map out a network's topology. This option has been used by network administrators to determine why two hosts on a network are not communicating, or to specify alternate routes to relieve network congestion. A hacker may try to use LSRR to get through firewalls. By specifying LSRR and a hop that is reachable both by the hacker and private IP addresses, the hacker may reach what was previously thought to be a protected IP address.

On the IBM i, the TCP attribute IPSRCRTG (IP source routing) may be set to either *ON or *OFF through the CHGTCPA command. If IPSRCRTG is *ON, the packet is forwarded if it can be. If IPSRCRTG is *OFF and the system is not the destination of the packet, the packet is discarded. Any datagrams with IP options are signaled by the TCP/IP stack to the IBM i Intrusion Detection System as possible suspicious events. The IP source routing attribute (IPSRCRTG) on this system is set to ***YES.**

Recommendation

✓ Evaluate your need for IP source routing on this system and for your network. You can change this attribute with the CHGTCPA command.

Recommendation Summary

H - Require using encrypted passwords for DDM/DRDA server authentication entries

H - Consider requiring secure telnet access on an encrypted port using telnet over TSL.

H - Review/reduce/eliminate objects defined with *PUBLIC *ALL *CHANGE access

H - Set *PUBLIC authority of IFS Root (‘/’) to *RX

H - Default Passwords - ANZDFTPWD ran daily via job scheduler

H - Password expiration of *NOMAX reduced or eliminated

H - Security related system values synchronized and locked in SST

H - Reduction of all privileged users - examine requirement for *JOBCTL

H - Validate that Exit Programs on all network interfaces are set to block

H - Ensure consistent settings across all systems based on corporate approved policy aligned with industry standards and best practices

M - *PUBLIC authorities on objects changed to *EXCLUDE as you are able

M - Users with privileges audited - logs reviewed periodically by knowledgeable staff

M - Security auditing/monitoring enhanced - Monitoring resources and staff assigned

L - Attention Programs, initial programs, menus housekeeping

L - SST passwords changed

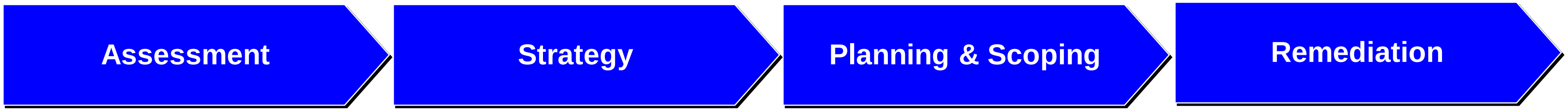
L - System Values for Password Rules enhanced

L - Review/reduce/eliminate private authorities on objects

L - Regular testing and validation of network interfaces (Exit Points) to ensure they are providing the protection intended

L - Command line access by users with initial menu of *SIGNOFF cleaned up

Information Security and Risk Management



Assessment

Strategy

Planning & Scoping

Remediation

Assessment

Consider deeper analysis

- Identify many high impact security risks on IBM i Systems

Strategy

8-24 Weeks

- Initiate budget & planning estimates
- Create Security Team
- Create Vulnerability list with description, impact, complexity and severity levels
- Determine applications & system impacts
- Develop IBM i hardening strategy
- Create work breakdown structure with high-level tasks and timeline

Planning & Scoping

32-64 Weeks

- Application design & specifications
- Detailed project planning
- Implementation planning
- Confirm capital and expense budget

Remediation

32-64 Weeks

- Test counter-measures in QA or test environments (planned fixes)
- Deploy counter-measures in production systems and applications

Information Security and Risk Management

- **Who’s In Charge**
  - Many companies put IT or Security in charge of their data assets
  - Ultimately, the business owners are also the owners of these assets and their protection
  - IT administrators and Security are only the custodians of the assets, not the owners
- **The Top Down Approach (Correct)**
  - Puts the company owners and managers in charge
  - As the owners of the data asset house, they are the ones who should drive the process
- **The Bottom Up Approach (Incorrect)**
  - If IT and Security are charged with owning security, 100 people may be running off in different directions trying to secure assets
  - The data asset house may be built with windows and doors in the wrong places and a weak foundation may be the result
  - Generally, the company may end up with a disjoined heap of flawed security products
- Every Employee is responsible for data security, ensuring information is safe, and reporting any newly discovered vulnerabilities to management

Roles and Responsibilities

IBM

Responsible for providing guidance, training, education, direction and IBM i hardening assistance.

Customer

Responsible for Defining Access Control Requirements, Testing, Implementation, Verification and Maintenance

General recommendations

- Define user roles
  - A role defines the tasks a user has to perform and the access he/she needs to objects
  - Try to keep the number of roles low, i.e. two or three roles per organization
  - Avoid “extra” authorities
  - Use one group profile per role
- Eliminate *SECOFR profiles as much as possible
  - No programmer needs *ALLOBJ
  - No programmer has all-time access to the production environment
  - When necessary, create utility programs for functions that require higher authorities
- Secure network communications
  - Encrypt passwords for Telnet, FTP, DDM and other communication protocols
- Document the requirements

General recommendations

- **Recommend Lab Service Senior Security Consultant Engagement**
  - Provide root cause and dependency analysis
  - Recommendations, guidance and education on risk mitigation and process
  - Risk mitigation planning and work plans
  - Setup exception reporting and sustaining controls
    - Facilitated by lab services tooling and assets
  - Successful engagements and experience has shown that rush to remediate without proper guidance and experience can have negative results
  - Recommend enough hours contract with possible extension if necessary

Closing entries into the system

- Use existing system controls to close ways into the system
- Start only required servers and protocols (ports)
- Purchase or write your own exit programs and register them via registered exit points to secure ubiquitous remote servers (ODBC, FTP etc.)
- Define roles (group profile) for users that need a specific function, such as ODBC access
  - Allow only the ODBC group to access your system via ODBC using exit programs

Additional information

- Security section in
  - iSeries InformationCenter
    - http://pic.dhe.ibm.com/infocenter/iseries/v7r1m0/index.jsp
    - IBM ITSO Redbooks (http://www.redbooks.ibm.com)
    - IBM System i Security Guide for IBM i5/OS, SG24-7680
    - IBM Implementation and Practical Use of LDAP on the IBM eServer iSeries Server, SG24-6193
    - IBM eServer iSeries Wired Network Security, OS/400 V5R1 DCM and Cryptography Enhancements, SG24-6168
    - AS/400 Internet Security: Developing a Digital Certificate Infrastructure, SG24-5659
  - iSeries Security Reference, SC41-5302 available in InfoCenter
  - Encryption whitepaper
    http://www-03.ibm.com/servers/enable/site/education/wp/efbe/efbe.pdf

- Or visit our websites at:

  https://www.ibm.com/it-infrastructure/services/lab-services/

  https://www.ibm.com/support/pages/ibm-i-security/

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM

IBM **Security**

Intelligence. Integration. Expertise.

© Copyright IBM Corporation 2015. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.