IBM Security
Intelligence. Integration. Expertise.

IBM

Compliance and Event Monitoring

Using the PowerSC Tools for IBM i Compliance Monitoring and Reporting Tool

Terry Ford
Senior Managing Consultant
IBM Lab Services Power Systems Delivery
taford@us.ibm.com

January 24, 2018

Security and Event Monitoring - Inhibitors

- Security setup inherited from the past - previous owners / application designers no longer are available
- For many IBM i IT departments, security is performed by an individual with multiple responsibilities – operations, administration, programming, etc.
- Security implementation “how to” is often not understood, is neglected or not monitored due to time constraints.
- Security policies/standards often do not exist. If they do, monitoring of compliance to the policy is not done or understood and deviation from the policies/standards across the enterprise is unknown.
- Gathering of security information is time consuming and scattered in multiple places on the system. The analysis of this data or monitoring of security changes is often dated by the time it is read.
- **How do you measure security? What are Key Risk Indicators (KRI) ? How do I prove due diligence to security monitoring?**

PowerSC Tools for IBM i
Compliance and Event Monitoring

Compliance Assessment and Reporting Tool - Features

The Compliance Monitoring Tool is a security and systems information Data Mart with “Real Time” event monitoring capabilities. The tool utilizes DB2 Web Query to provide a low cost web-based interface for business analytics for easy monitoring of compliance on any or all systems in an enterprise.

- A centralized view of Security Compliance status across the enterprise provides the ability to quantify and act upon several aspects of security as statistical measurable components as well as to corporate defined objectives for configuration consistency
- A federated repository of IBM i user profiles that provide cross system observability of profile administration.
- Security Event Monitoring - monitor and act on events as they happen - providing near "real time" monitoring of more than 180 of the most common security events. Additional events can be monitored through a customization utility.
- A customizable scoring mechanism for prioritization of policy by customer objectives which highlights deviations from policy, unexpected differences of policy settings between systems, and security attributes that do not adhere to corporate security objectives.
- A utility to add user-defined items for monitoring inventory, auditing, status, etc. that integrates with scoring mechanisms provided by the tool.
- A utility for deploying tool fixes or enhancements that can be leveraged for deploying customer defined fixes

Compliance Assessment and Reporting Tool - More Features

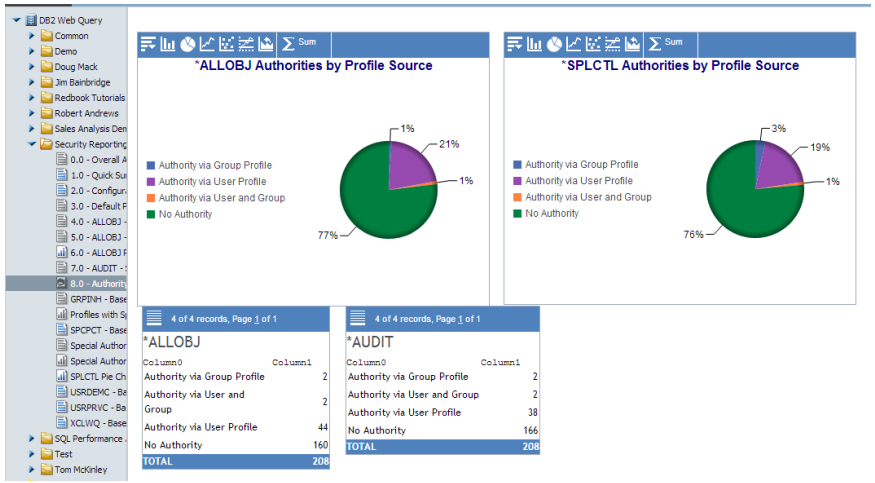
- A utility to automatically centralize and view data from configuration files and utilities that already exist or that may be created in the future. Includes creation of Web Query metadata and synonyms.
- Automated checks to the IBM PSP web for updated group PTFS. Optional checks can also be performed for individual PTFs as well as reporting of PTFs not present.
- An archive utility for selecting when to trim data and optionally save/restore data sets for future use when required.
- Automated email of individual reports to system owners.
- Automated scheduling of reports (with Web Query Standard Edition only)
- Checks of dictionary password usage. Do your users or administrators use easily guessed passwords?

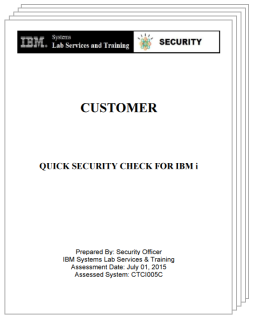
Compliance Assessment and Reporting Tool – Typical Uses

- Demonstrating to auditors that control measures are in place
- Observing and highlighting deviation from corporate security standards and policies
- Demonstrating when observed deviations have occurred
- Reporting defined security standards upon request by system or for the entire estate of systems
- Quickly observing and assessing a broad range of security attributes (commonly known and unknown to administrators)
- Quickly looking across the corporate estate for consistency in administration
- Adding customer-defined items for monitoring inventory, auditing, status, security events, etc. with incorporated scoring mechanisms provided by the tool
- Deploying fixes, enhancements or changes to individual LPARs or all LPARs for compliance or alignment with standards
- Monitoring PTF currency

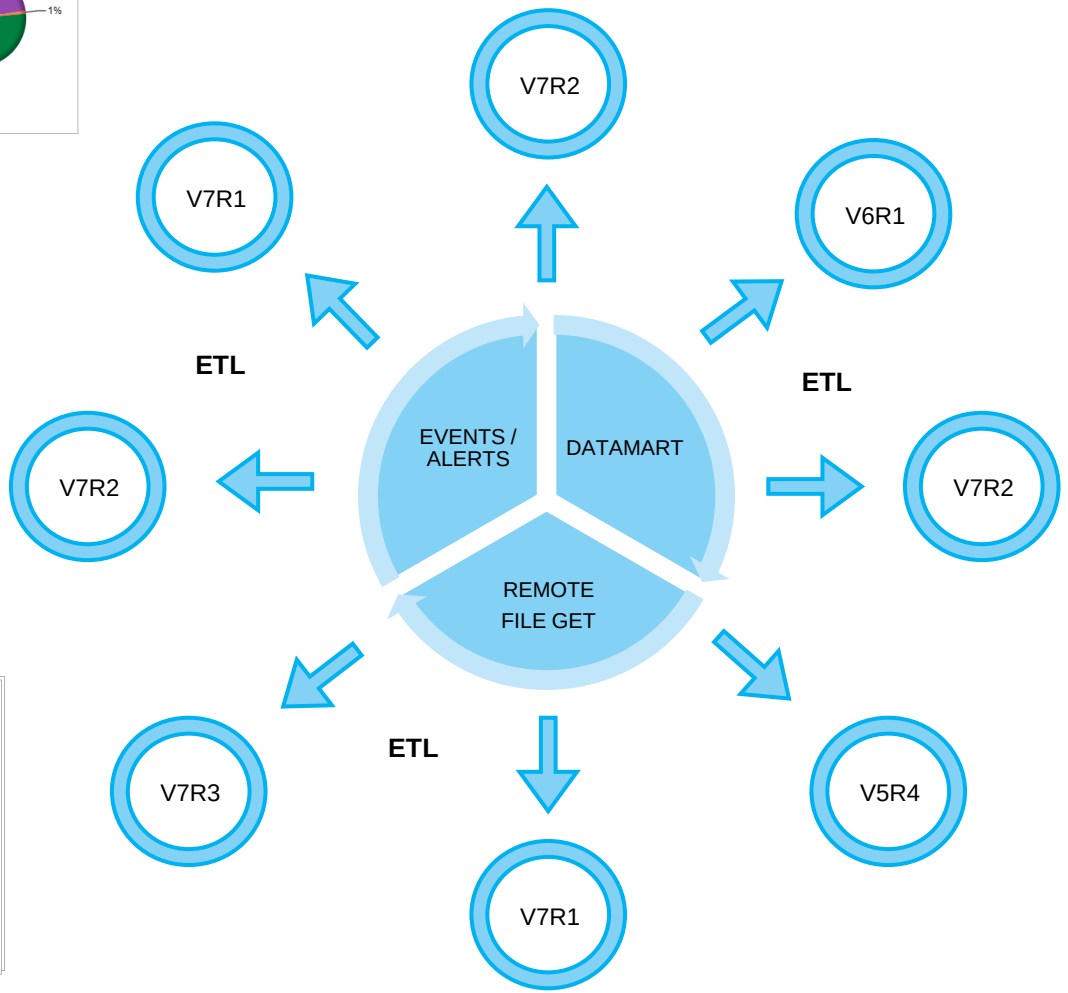
High Level Architecture

Compliance Assessment and Reporting Tool - Enterprise





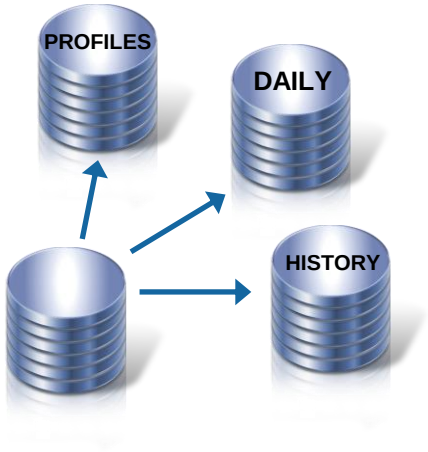
ETL - Daily on Schedule
Events - Every 3 minutes

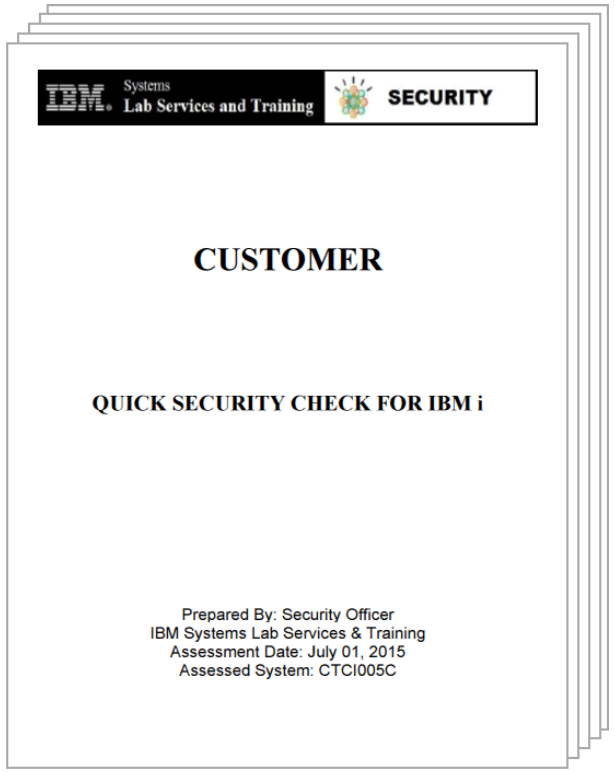


Compliance Assessment and Reporting Tool - SMB

High Level Architecture

EVENTS and DAILY Report Created by the
Compliance Assessment Tool Collection Agent





Area Reviewed	Risk Potential	Value Retrieved
Profiles with *ALLOBJ Special Authority	*YES	25
Profiles with *JOBCTL Special Authority	*YES	70
Profiles with *SPLCTL Special Authority	*YES	62
Profiles with Default Passwords	*YES	1
Profiles with Passwords that Never Expire (*NOMAX)	*YES	35
Group Profiles with Passwords	*NO	0
*ALLOBJ Special Authority through Group Profile	*NO	0
*JOBCTL Special Authority through Group Profile	*YES	5
*SPLCTL Special Authority through Group Profile	*NO	0
Profile objects that are *PUBLIC/y Authorized	*YES	5
Profile objects that are Privately Authorized	*YES	6
Audit Journal	*YES	Yes
DDM Password Requirements	*YES	*USRIDPWD
Does the *SYSTEM Store Exist	*EXCLUDE	*EXCLUDE
ROOT (/) is Shared	*YES	Yes
ROOT (/) *PUBLIC Authority is *RWX	*YES	*RWX
Subsystems with *PUBLIC not *USE or *EXCLUDE	*YES	13
Job Descriptions with *PUBLIC not *USE or *EXCLUDE	*YES	78
Job Queues with *PUBLIC not *USE or *EXCLUDE	*YES	13
*IBM Libraries with *PUBLIC not *USE or *EXCLUDE	*YES	3
USER Libraries with *PUBLIC not *USE or *EXCLUDE	*YES	426
QSECOFR Adoption in USER Libraries	*YES	544
AUTH Lists with *PUBLIC not *USE or *EXCLUDE	*YES	9
Allow Change to System Values	*YES	Yes
QSECURITY - System security level	*LOW	40

The Engagement

Implementation Agenda (Enterprise)

- Day 1 Tuesday:
  - Overview of the tool
  - Installation on target systems
  - Installation on central server
  - Installation of WQ application component
  - Configuration of target systems on central
- Day 2 Wednesday:
  - Walk thru the administrative functions
  - Walk thru patching tool
  - Alerts and problem determination
- Day 3 Thursday:
  - Walk thru Web Query reports for systems / user profiles
  - Scoring
  - Extending the collection (customer defined items / exit programs)
- Day 4 Friday:
  - Customizations
  - Wrap up

Pre-Engagement **(before we travel)**:

- ☑ Validate pre-requisites (TR's and LPP's)
- ☑ Validate installation and setup of WQ

Post-Engagement:

- ☑ Defect Support (If Purchased)
- ☑ Web Query workshop (Optional)
- ☑ Remediation assistance (Optional)
- ☑ Security consulting (Optional)
- ☑ Report customization (Optional)
- ☑ Enhancements (Optional)

Implementation Agenda (Single LPAR)

- One Day (Onsite or Remote):
  - Overview of the tool
  - Installation on target system
  - Walk thru the administrative functions
  - Initial Collection
  - Discussion of the findings
  - Event monitoring setup
  - Wrap up

Pre-Engagement **(before we travel)**:

☑ Validate pre-requisites (TR's and LPP's)

Post-Engagement:

☑ Defect Support (If Purchased)
☑ Remediation assistance (Optional)
☑ Security consulting (Optional)
☑ Enhancements (Optional)

One Pagers

Compliance Assessment and Reporting Tool - Enterprise

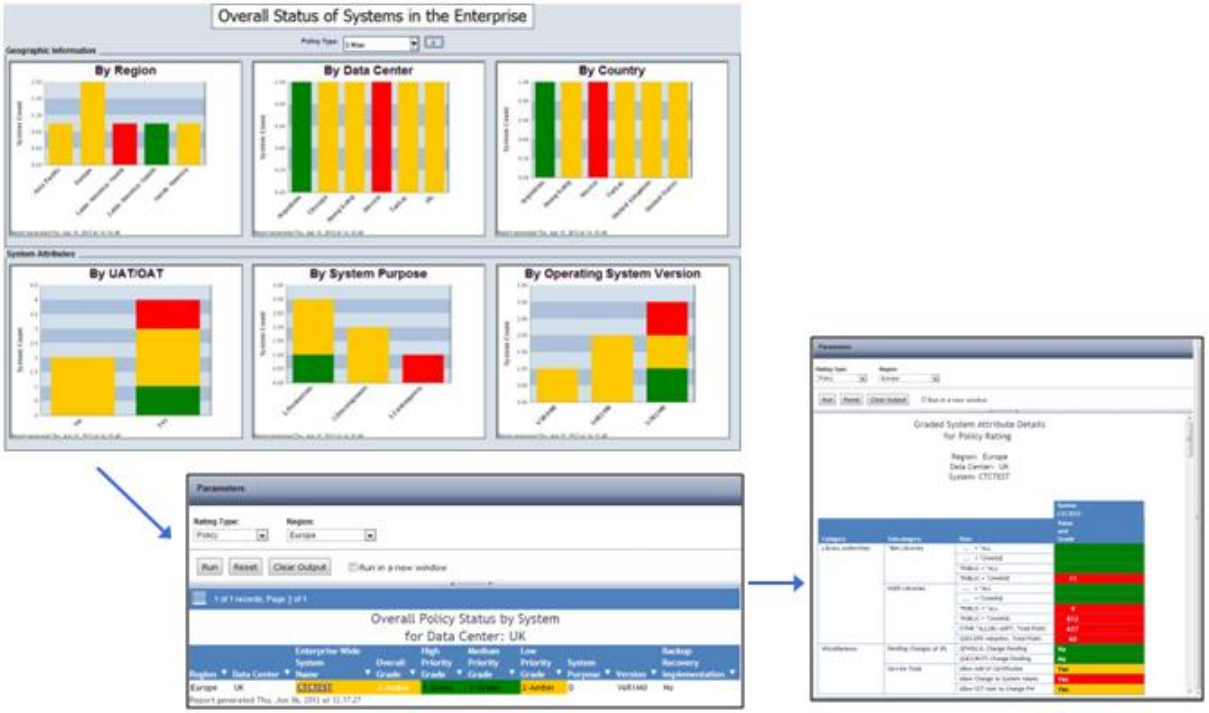
Centralized reporting of IBM i System and Security Components

- An automated collection, analysis, and reporting tool on over 1000 system and security related risks, information, statistics and demographics. All in one location and easy to use!

- **Covers:**
  - Password management
  - Profile administration
  - Special authorities
  - Group inheritance
  - Network configuration
  - NetServer attributes
  - Operational security
  - PTF currency
  - Event monitoring
  - Customer define items
  - Security risks and more

- Daily compliance dashboard reports at VM (partition), system or enterprise level

- Enables compliance officer to demonstrate adherence to pre-defined or customer-defined security polices.
- System and Security reporting made easy!



Compliance Assessment and Reporting Tool - SMB

Localized reporting of IBM i System and Security Components

- An automated collection, analysis, and reporting tool on over 1000 system and security related risks, information, statistics and demographics. All in one location and easy to use!

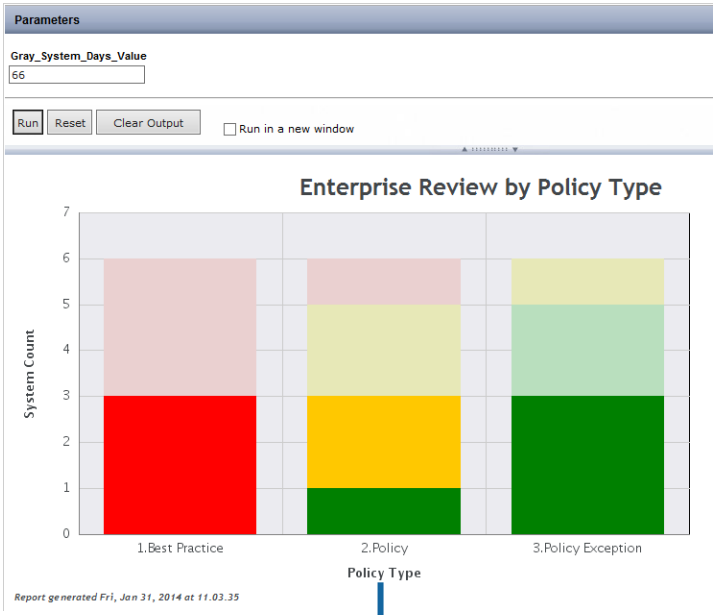
- **Covers:**
  - Password management
  - Profile administration
  - Special authorities
  - Group inheritance
  - Network configuration
  - NetServer attributes
  - Operational security
  - PTF currency
  - Event monitoring
  - Customer define items
  - Security risks and more

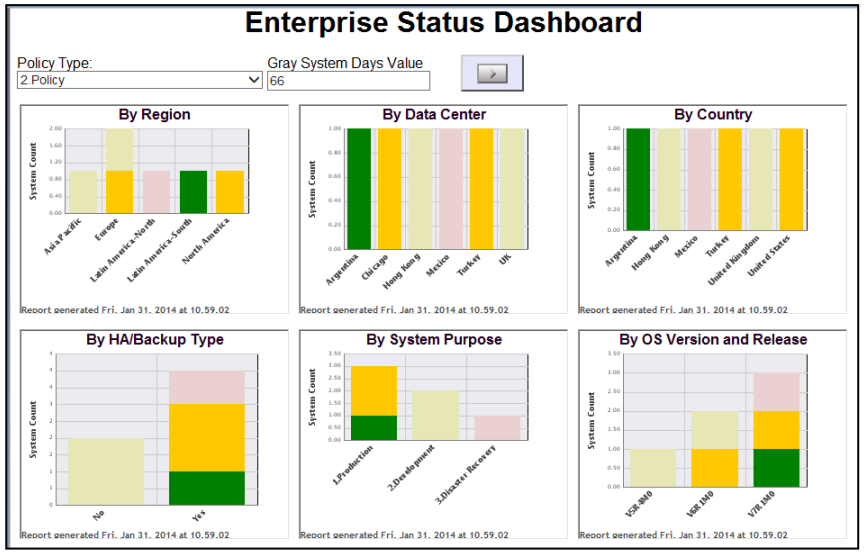
- Enables compliance officer to demonstrate adherence to pre-defined or customer-defined security polices.
- System and Security reporting made easy!

Area Reviewed	Risk Potential	Value Retrieved
Profiles with *ALLOBJ Special Authority	*YES	25
Profiles with *JOBCTL Special Authority	*YES	70
Profiles with *SPLCTL Special Authority	*YES	62
Profiles with Default Passwords	*YES	1
Profiles with Passwords that Never Expire (*NOMAX)	*YES	35
Group Profiles with Passwords	*NO	0
*ALLOBJ Special Authority through Group Profile	*NO	0
*JOBCTL Special Authority through Group Profile	*YES	5
*SPLCTL Special Authority through Group Profile	*NO	0
Profile objects that are *PUBLICly Authorized	*YES	5
Profile objects that are Privately Authorized	*YES	6
Audit Journal	*YES	Yes
DDM Password Requirements	*YES	*USRIDPWD
Does the *SYSTEM Store Exist	*EXCLUDE	*EXCLUDE
ROOT (/) is Shared	*YES	Yes
ROOT (/) *PUBLIC Authority is *RWX	*YES	*RWX
Subsystems with *PUBLIC not *USE or *EXCLUDE	*YES	13
Job Descriptions with *PUBLIC not *USE or *EXCLUDE	*YES	78
Job Queues with *PUBLIC not *USE or *EXCLUDE	*YES	13
*IBM Libraries with *PUBLIC not *USE or *EXCLUDE	*YES	3
USER Libraries with *PUBLIC not *USE or *EXCLUDE	*YES	426
QSECOFR Adoption in USER Libraries	*YES	544
AUTH Lists with *PUBLIC not *USE or *EXCLUDE	*YES	9
Allow Change to System Values	*YES	Yes
QSECURITY - System security level	*LOW	40

Compliance Assessment and Reporting Tool

"I just want to arrive in the morning, get a cup of coffee, and have a view of what systems are in compliance and which are not."



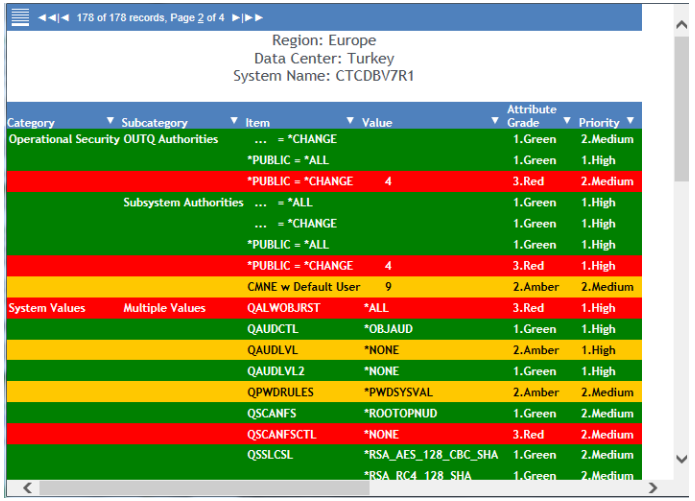


1 of 1 records, Page 1 of 1

Overall System Status by Data Center
Policy Type: 2.Policy
Data Center: Turkey

Region	Data Center	Version	System Purpose	Backup Recovery Implementation	System Operational Owner	Security Risk Owner	System Name	Overall Grade	High Priority Grade	Medium Priority Grade	Low Priority Grade
Europe	Turkey	V7R1M0	1.Production	Yes	Turkey	Turkey	CTCDBV7R1	2.Amber	1.Green	1.Green	2.Amber

Report generated Fri, Jan 31, 2014 at 11.38.17



Compliance Assessment and Reporting Tool

I want to know when security related events are occurring…

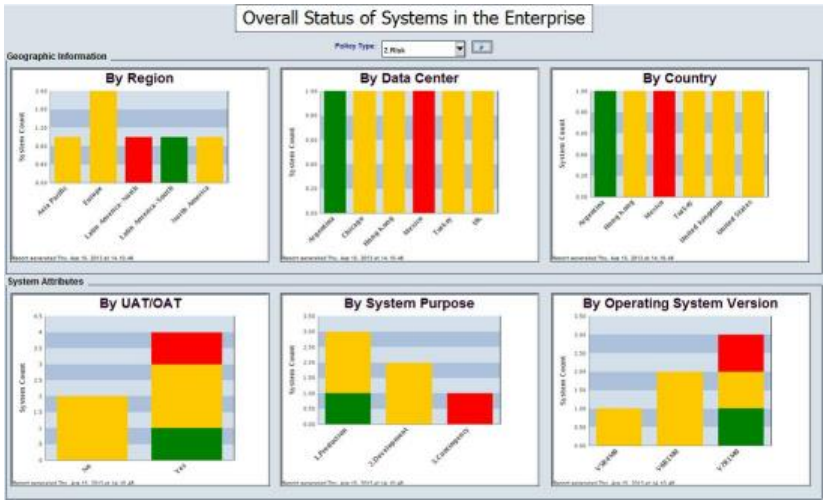
Who changed that System Value?

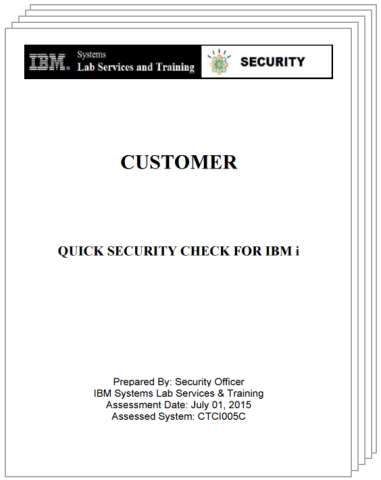
Who changed QSECOFR ?

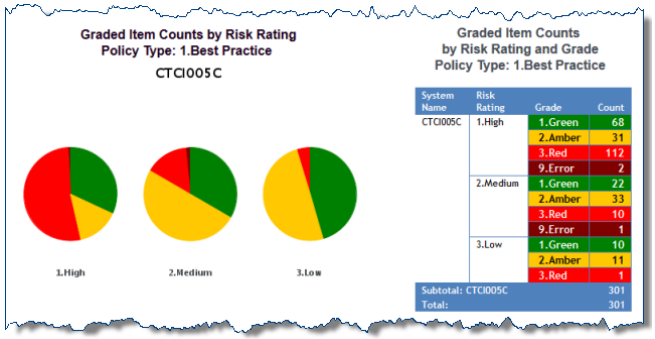
Compliance Assessment, Monitoring and Reporting Tool

Monitor enterprise security from one location …

- A Security Compliance, Assessment, Reporting and Monitoring Data Mart in one Package!
- Security analysis through a rich graphical interface that is mobile enabled
- **Contact Terry Ford (*taford@us.ibm.com*) to get started or visit ibm.biz/IBMiSecurity**







Category	Subcategory	Item Key	Item	System Name BJSYSTEM	BSTGEN	BSTGEN2	CTCDBV7R1	CTCI005C	CTCMOD	CTCSEC	CTC
User Profiles	Special Authorities	UPSA0001	*ALLOBJ	14	37	37	14	34	32	8	20
		UPSA0002	*AUDIT	15	36	36	15	30	30	8	16
		UPSA0003	*IOSYSCFG	14	37	37	14	30	30	8	16
		UPSA0004	*JOBCTL	30	40	40	30	35	35	8	19
		UPSA0005	*SAVSYS	17	40	40	17	34	33	8	20
		UPSA0006	*SECADM	14	37	37	14	37	31	8	16
		UPSA0007	*SERVICE	27	37	37	27	30	32	8	18
		UPSA0008	*SPLCTL	14	37	37	14	31	31	8	16
	Expansion of Authorities	UPEXP001	*ALLOBJ	0	1	1	0	2	0	0	3
		UPEXP002	*AUDIT	0	1	1	0	2	0	0	3
		UPEXP003	*IOSYSCFG	5	6	6	5	7	0	0	8
		UPEXP004	*JOBCTL	5	6	6	5	7	0	0	11
		UPEXP005	*SAVSYS	5	6	6	5	7	0	0	9
		UPEXP006	*SECADM	0	1	1	0	6	0	0	3
		UPEXP007	*SERVICE	0	1	1	0	2	0	0	3
		UPEXP008	*SPLCTL	5	6	6	5	7	0	0	8

Compliance Assessment and Reporting Tool

*Provides "**out of the box**" assessment of systems for security compliance and exposures*

Profile Analysis:

- Special Authorities / Inherited Privileges
- Group Profiles / Ambiguous Profiles
- Default Passwords / Password Expiration
- Inactive Accounts
- *PUBLICLY Authorized Profiles
- Privately Authorized Profiles
- Initial Programs, Menus, and Attention Programs
- Command Line Access

Administration / Configuration:

- System Values / Audit Control Settings
- Invalid Signon attempts
- Work Management Analysis
- Service Tools (SST) Security
- **PTF Currency**

- DDM Password Requirements
- Registered Exit Points / Exit Programs
- Function Usage
- Library Analysis / *ALLOBJ Inheritance
- **Customer Defined Events and Items**
- **CPU/DASD Utilization and Availability**
- **Actionable Security Events as they Happen**

Network Settings:

- Network attributes / Time Server
- NetServer Configuration
- TCP/IP servers / Autostart values
- Digital Certificate Expiration
- SNMP / SSH / SSL Configuration
- Listening ports / Network Encryption
- IP Datagram Forwarding
- IP Source Routing
- APPN Configuration (yes – for many it is still there)
- Server Authentication Entries

Cost of Compliance

Cost of Compliance

- Financial penalties being incorporated as cost of doing business
  - Fines
  - Liability cost increases
  - Greater regulatory scrutiny
  - Further pressures/increases to comply
- Costs being paid through tactical expenditures at the expense of more strategic business imperatives
  - Temporary reprioritization of business objectives
  - Impact to business continuity as audit findings are satisfied
  - Potential disruption in business as stakeholders pursue alternate lines of business (loss of confidence in reputation of business)
  - Focus on remedial efforts rather than the business

-Thomas Reuters

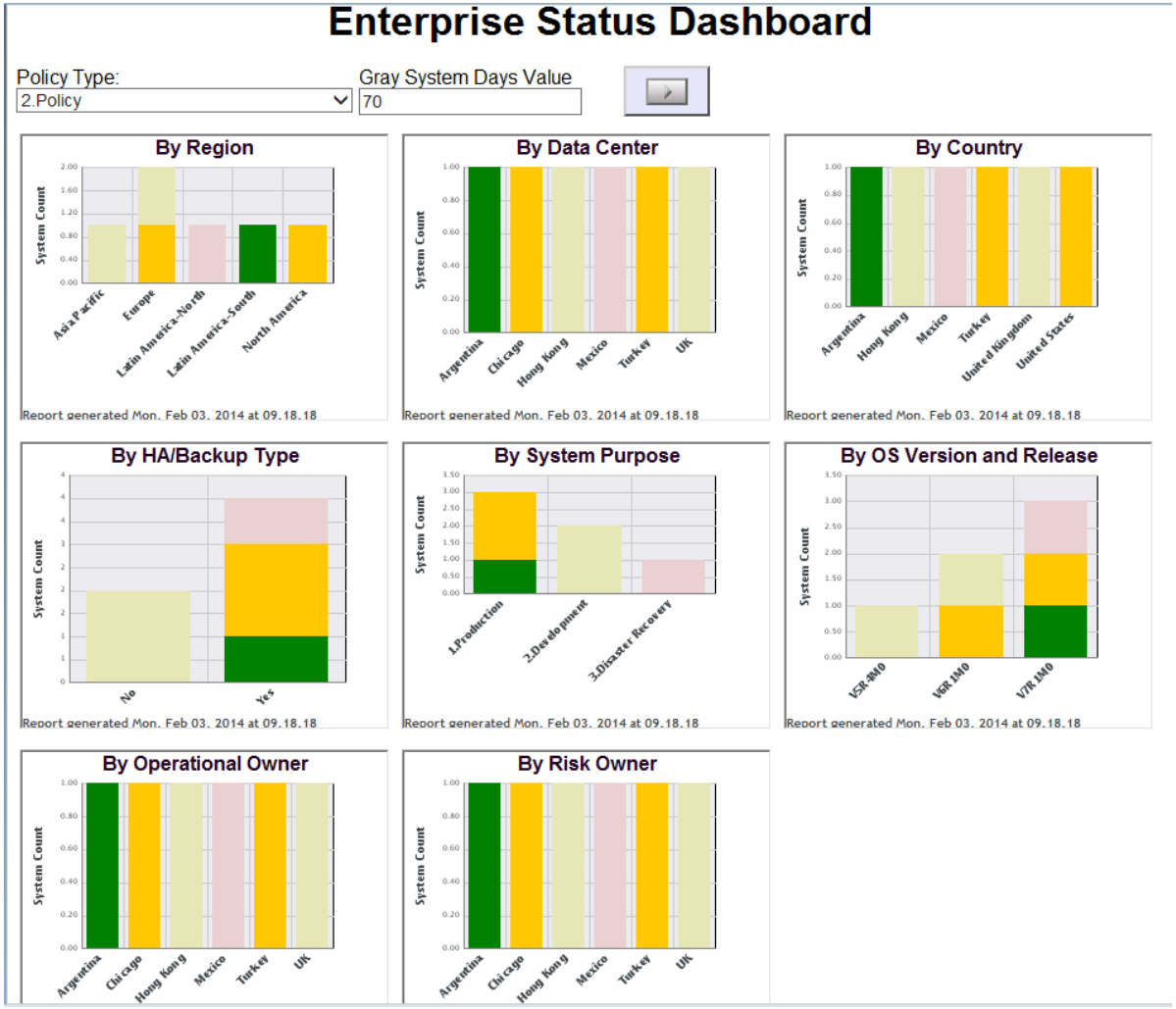
Help is always just an email or call away!

Examples and Backup

Compliance Assessment and Reporting Tool

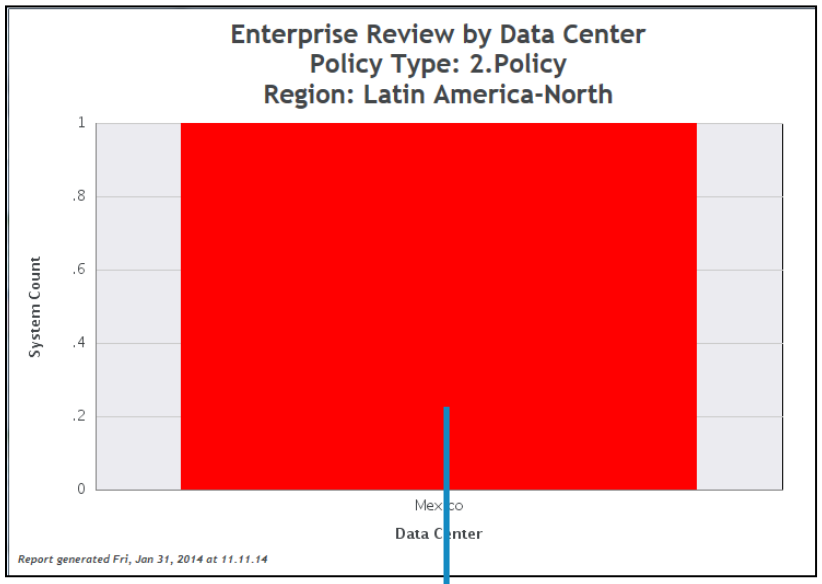
Enterprise Dashboard

- Summary of Overall System Status of all systems in the enterprise by various system attributes.
- Information is based on last successful collection for each system.



Compliance Assessment and Reporting Tool

Regional Review (Drill down to overall grading and details)



181 of 181 records, Page 1 of 4 ▶|▶▶

Graded System Attribute Details
for 2.Policy
Region: Latin America-North
Data Center: Mexico
System Name: BSTGEN

Category	Subcategory	Item	Value	Attribute Grade	Priority
Library Authorities	*IBM Libraries	... = *ALL		1.Green	1.High
		... = *CHANGE		1.Green	1.High
		*PUBLIC = *ALL		1.Green	1.High
		*PUBLIC = *CHANGE	3	3.Red	1.High
		CRTAUT = *ALL		1.Green	2.Medium
		Owners with a Password		1.Green	2.Medium
		OTHR *ALLOBJ ADPT, *PUB=*ALL		1.Green	1.High
		OTHR *ALLOBJ ADPT, *PUB=*CHG		1.Green	2.Medium
		System CMDs that have changed		1.Green	1.High
	USER Libraries	... = *ALL		1.Green	1.High
		... = *CHANGE		1.Green	1.High
		*PUBLIC = *ALL		1.Green	1.High
		*PUBLIC = *CHANGE	80	3.Red	1.High
		CRTAUT = *ALL		1.Green	2.Medium
		Owners with a Password	112	3.Red	2.Medium
		OTHR *ALLOBJ ADPT, *PUB=*ALL		1.Green	1.High
		OTHR *ALLOBJ ADPT, *PUB=*CHG		1.Green	2.Medium

1 of 1 records, Page 1 of 1

Overall System Status by Data Center
Policy Type: 2.Policy
Data Center: Mexico

Region	Data Center	Version	System Purpose	Backup Recovery Implementation	System Operational Owner	Security Risk Owner	System Name	Overall Grade	High Priority Grade	Medium Priority Grade	Low Priority Grade
Latin America-North	Mexico	V7R1M0	3.Disaster Recovery	Yes	Mexico	Mexico	BSTGEN	3.Red	1.Green	2.Amber	3.Red

Report generated Fri, Jan 31, 2014 at 11.28.14

Compliance Assessment and Reporting Tool

System Dashboard

Key System and data collection information
- Status of last collection attempt (Success or Fail)
- Key System attributes – VRM, Location, etc.
- Overall and detailed system grading based upon last successful collection.

System Details Dashboard

System Name: CTCMOD | Policy Type: 2.Policy | Gray System Days Value: 70

Current Event Log Status for CTCMOD

Event Date	Event Type	Event Description	System Name	Region	Data Center	Coded System Purpose	Version
2013/11/27	SUCCESS	SUCCESSFUL COLLECTION FOR SYSTEM CTCMOD	CTCMOD	North America	Chicago	P	V6R1M0

System Attributes

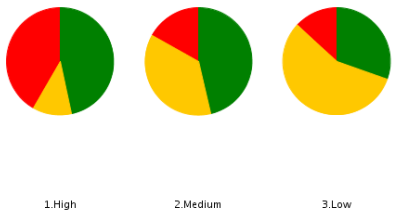
Enterprise System Name		
CTCMOD	Remote System Name	CTCDBMOD
	Serial Number	10-40F40
	System Purpose	1.Production
	UAT/OAT	Yes
	Version	V6R1M0
	Region	North America
	Data Center	Chicago
	Country	United States
	State	Illinois
	City	Chicago
	Postal Code	60606
	Local System Run Date	2013/11/27
	Remote System Run Date	2013/11/27

Overall System Status
Policy Type: 2.Policy

System Name	Overall Grade	High Priority Grade	Medium Priority Grade	Low Priority Grade
CTCMOD	2.Amber	1.Green	1.Green	2.Amber

Report generated Mon, Feb 03, 2014 at 09.25.02

Grading Counts by System and Priority
Policy Type: 2.Policy
CTCMOD



Grade System Attribute Counts
by Priority and Grade
Policy Type: 2.Policy

System Name	Priority	Grade	Count
CTCMOD	1.High	1.Green	28
		2.Amber	7
		3.Red	25
	2.Medium	1.Green	44
		2.Amber	35
		3.Red	16
	3.Low	1.Green	7
		2.Amber	13
		3.Red	3
Subtotal: CTCMOD			178
Total:			178

Report generated Mon, Feb 03, 2014 at 09.25.02

Graded System Attribute Details - 2.Policy
System Name: CTCMOD

Attribute Grade	Priority	Category	Subcategory	Item	Value
3.Red	1.High	Library Authorities	*IBM Libraries	*PUBLIC = *CHANGE	3
				System CMDs that have changed	1
			USER Libraries	*PUBLIC = *ALL	4
				*PUBLIC = *CHANGE	307
				OTHR *ALLOBJ ADPT, Total PGMS	264
				QSECOFR Adoption, *PUB=*CHG	15
				QSECOFR Adoption, Total PGMS	29
		Miscellaneous	Service Tools	Allow Change to System Values	Yes
		Network Configuration	TCP/IP Attributes	DDM PW Required (CHGDDMTCPA)	*USRID
		NetServer Information	NetServer Data	ROOT (/) is Shared	Yes
				ROOT (/) Permissions	*RW
		Operational Security	JOBD Authorities	*PUBLIC = *ALL	15
				*PUBLIC = *CHANGE	28
			OUTQ Authorities	*PUBLIC = *ALL	7
			Subsystem Authorities	*PUBLIC = *CHANGE	4
		System Values	Multiple Values	QALWOBJRST	*ALL
			Single Values	QINACTITV	240
		User Profiles	Default Passwords	Enabled	1
				Total	2
			Group Profiles	Group Profile(s) w/ Passwords	2
			Password Expiration	Never Expires (*NOMAX)	8
			Special Authorities	*ALLOBJ	28
				*JOBCTL	48
				*SAVSYS	32
				*SPLCTL	28
	2.Medium	Library Authorities	USER Libraries	Owners with a Password	375
				OTHR *ALLOBJ ADPT, *PUB=*CHG	18
		Network Attributes	RTVNETA Values	Network Job Action (JOBACN)	*FILE
		Operational Security	OUTQ Authorities	*PUBLIC = *CHANGE	1

Compliance Assessment and Reporting Tool

Cross System Analysis

Horizontal or vertical presentation of risk indicators across LPARs

				System Name BJSYSTEM	BSTGEN	BSTGENTOO	CTCDBV7R1	CTCI005C	CTCMOD
Category	Subcategory	Item Key	Item	Value	Value	Value	Value	Value	Value
Library Authorities	*IBM Libraries	LAIB0013	Owners with a Password	1			1		
		LAIB0160	*PUBLIC = *ALL						
		LAIB0171	*AUTL *PUB = *ALL						
		LAIB0172	*AUTL *PUB = *CHANGE						
		LAIB0180	*PUBLIC = *CHANGE	6	3	3	6	2	3
		LAIB0310	CRTAUT = *ALL						
		LAIB0450	System CMDs that have changed					2	
		LAIB0602	OTHR *ALLOBJ ADPT, *PUB=*ALL						
		LAIB0603	OTHR *ALLOBJ ADPT, *PUB=*CHG					1	
	USER Libraries	LAUS0013	Owners with a Password	133	143	129	133	100	323
		LAUS0220	*PUBLIC = *ALL					20	3
		LAUS0231	*AUTL *PUB = *ALL						
		LAUS0232	*AUTL *PUB = *CHANGE						
		LAUS0240	*PUBLIC = *CHANGE	122	106	93	122	851	294
		LAUS0370	CRTAUT = *ALL					4	
		LAUS0502	QSECOFR Adoption, Total PGMS	19	89	89	19	638	37
		LAUS0503	QSECOFR Adoption, *PUB=*ALL						
		LAUS0504	QSECOFR Adoption, *PUB=*CHG	4	9	9	4	544	15
		LAUS0601	OTHR *ALLOBJ ADPT, Total PGMS	1208	83	83	1208	58	305
		LAUS0602	OTHR *ALLOBJ ADPT, *PUB=*ALL	1			1	1	

Compliance Assessment and Reporting Tool

Cross System Analysis

PTF Inventory…

Category	Subcategory	Item Key	Item	System Name BJSYSTEM	BSTGEN	BSTGENTOO	BSTGEN2	CTCDBV7R1	CTCI005C	CTCMOD	CTCSEC	CTCSECI7	CTCTEST	CTCV71	FIVEC
System Information	Common PTF Groups	SIPTF002	Cumulative PTF Level	SF99710-INSTLLD-13298	SF99710-INSTLLD-13298	SF99710-INSTLLD-13298	SF99710-INSTLLD-13298	SF99540-INSTLLD-12094	SF99610-INSTLLD-14197	SF99710-INSTLLD-13298	SF99540-INSTLLD-12094	SF99720-INSTLLD-14101	SF99610-INSTLLD-13312	SF99710-INSTLLD-13037	SF996 INSTL
		SIPTF004	Group HIPER PTF Level	SF99709-INSTLLD-112	SF99709-INSTLLD-112	SF99709-INSTLLD-112	SF99709-INSTLLD-112	SF99539-INSTLLD-194	SF99609-INSTLLD-191	SF99709-INSTLLD-112	SF99539-INSTLLD-203	SF99719-INSTLLD-7	SF99609-INSTLLD-186	SF99709-INSTLLD-88	SF996 INSTL
		SIPTF006	Group Security PTF Level	SF99708-INSTLLD-32	SF99708-INSTLLD-32	SF99708-INSTLLD-32	SF99708-INSTLLD-32	SF99538-MISSING	SF99608-INSTLLD-49	SF99708-INSTLLD-32	SF99538-INSTLLD-32	SF99718-INSTLLD-5	SF99608-INSTLLD-46	SF99708-INSTLLD-26	SF996 INSTL
		SIPTF007	DB2 for IBM i PTF Level	SF99701-INSTLLD-28	SF99701-INSTLLD-28	SF99701-INSTLLD-28	SF99701-INSTLLD-28	SF99504-INSTLLD-33	SF99601-INSTLLD-33	SF99701-INSTLLD-28	SF99504-INSTLLD-33	SF99702-INSTLLD-1	SF99601-INSTLLD-32	SF99701-INSTLLD-31	SF996 INSTL
		SIPTF008	Technology Refresh PTF Level	SF99707-INSTLLD-7	SF99707-INSTLLD-7	SF99707-INSTLLD-7	SF99707-INSTLLD-7	**N/A**-MISSING	**N/A**-MISSING	SF99707-INSTLLD-7	**N/A**-MISSING	SF99717-MISSING	**N/A**-MISSING	SF99707-INSTLLD-6	**N/A MISSIN
		SIPTF012	TCP/IP PTF Level	SF99367-INSTLLD-8	SF99367-INSTLLD-8	SF99367-INSTLLD-8	SF99367-INSTLLD-8	SF99315-INSTLLD-22	SF99354-INSTLLD-16	SF99367-INSTLLD-8	SF99315-INSTLLD-22	SF99367-MISSING	SF99354-INSTLLD-16	SF99367-INSTLLD-7	SF993 INSTL
		SIPTF014	Performance PTF Level	SF99145-INSTLLD-7	SF99145-INSTLLD-7	SF99145-INSTLLD-7	SF99145-INSTLLD-7	SF99143-INSTLLD-7	SF99144-INSTLLD-10	SF99145-INSTLLD-7	SF99143-MISSING	SF99145-MISSING	SF99144-INSTLLD-8	SF99145-INSTLLD-4	SF991 INSTL
		SIPTF016	HTTP Server PTF Level	SF99368-INSTLLD-27	SF99368-INSTLLD-27	SF99368-INSTLLD-27	SF99368-INSTLLD-27	SF99114-INSTLLD-36	SF99115-INSTLLD-42	SF99368-INSTLLD-27	SF99114-MISSING	SF99713-INSTLLD-1	SF99115-INSTLLD-41	SF99368-INSTLLD-29	SF991 INSTL
		SIPTF018	JAVA PTF Level	SF99572-INSTLLD-18	SF99572-INSTLLD-18	SF99572-INSTLLD-18	SF99572-INSTLLD-18	SF99291-INSTLLD-33	SF99562-INSTLLD-30	SF99572-INSTLLD-18	SF99291-INSTLLD-34	SF99716-INSTLLD-2	SF99562-INSTLLD-29	SF99572-INSTLLD-18	SF995 INSTL
		SIPTF020	Hardware and Related PTF Level	SF99705-INSTLLD-10	SF99705-INSTLLD-10	SF99705-INSTLLD-10	SF99705-INSTLLD-10	**N/A**-MISSING	SF99605-INSTLLD-13	SF99705-INSTLLD-10	**N/A**-MISSING	SF99775-MISSING	SF99605-INSTLLD-12	SF99705-INSTLLD-4	SF996 INSTL
		SIPTF023	High Availability PTF Level	SF99706-INSTLLD-7	SF99706-INSTLLD-7	SF99706-INSTLLD-7	SF99706-INSTLLD-7	**N/A**-MISSING	SF99606-INSTLLD-4	SF99706-INSTLLD-7	**N/A**-MISSING	SF99776-MISSING	SF99606-INSTLLD-4	SF99706-INSTLLD-3	SF996 INSTL
		SIPTF026	Backup and Recovery PTF Level	SF99362-INSTLLD-35	SF99362-INSTLLD-35	SF99362-INSTLLD-35	SF99362-INSTLLD-35	SF99186-MISSING	SF99187-INSTLLD-54	SF99362-INSTLLD-35	SF99186-INSTLLD-57	SF99715-MISSING	SF99187-MISSING	SF99362-MISSING	SF991 INSTL
		SIPTF029	Print PTF Level	SF99366-INSTLLD-10	SF99366-INSTLLD-10	SF99366-INSTLLD-10	SF99366-INSTLLD-10	SF99347-MISSING	SF99356-INSTLLD-31	SF99366-INSTLLD-10	SF99347-MISSING	SF99766-INSTLLD-1	SF99356-MISSING	SF99366-INSTLLD-7	SF993 INSTL
		SIPTF032	Electronic Services PTF Level	SF99627-INSTLLD-11	SF99627-INSTLLD-11	SF99627-INSTLLD-11	SF99627-INSTLLD-11	SF99625-MISSING	SF99626-INSTLLD-11	SF99627-INSTLLD-11	SF99625-MISSING	SF99627-MISSING	SF99626-MISSING	SF99627-MISSING	SF996 INSTL
	Configuration at Runtime	SICAR001	System Name	MCV7R1	RCHBSTGE	RCHBSTGE	RCHBSTGE	MCV7R1	CTCI005C	CTCDBMOD	CTCSEC	CTCSECI7	CTCTEST	CTCV71	CTCI00
		SICAR002	System Type / Model	9406-MMA	9406-MMA	9406-MMA	9406-MMA	9406-MMA	9406-570	9406-MMA	9406-550	8202-E4B	9406-570	9406-MMA	9406-57
		SICAR003	System Serial Number	10-40F40	10-2D80D	10-2D80D	10-2D80D	10-40F40	10-3200C	10-40F40	10-B772D	10-5931R	10-3200C	10-40F40	10-320
		SICAR004	Processor Feature	5462	7054	7054	7054	5462	7476	5462	7154	8350	7476	5462	7476
		SICAR005	Operating System Level (VRM)	V7R1M0	V7R1M0	V7R1M0	V7R1M0	V7R1M0	V6R1M0	V7R1M0	V5R4M0	V7R2M0	V6R1M0	V7R1M0	V6R1

Compliance Assessment and Reporting Tool

Cross System Analysis

PTF Currency…

Parameters

ENTERPRISE_SYSTEM_NAME:
No Selection
BSTGEN
BSTGEN2
CTCI005C

PTF_GROUP_NAME:
No Selection
Backup Recovery Solutions
Current Cumulative PTF Media Documentation
DB2 for IBM i

PTF_STATUS:
No Selection
Installed
Missing
Next IPL

RISK_LEVEL:
No Selection
Green
Red
Yellow

SYSTEM_VRM:
No Selection
V5R4M0
V6R1M0
V7R1M0

Run | Reset | Clear Output | Run in a new window

Enterprise System Name	Version	PTF Group ID	Risk Level	Current PTF Level	Available PTF Level	Days Since PTF Level Available	PTF Install Status	Descriptive of PTF Group Name	System Information Collected
BSTGEN	V7R1M0	SF99145	Red	7	9	155	Installed	Performance Tools	2015/09/12
		SF99362	Red	35	51	15	Installed	Backup Recovery Solutions	2015/09/12
		SF99366	Red	10	12	155	Installed	Print PTFs	2015/09/12
		SF99367	Green	8	9	39	Installed	TCP/IP PTF	2015/09/12
		SF99368	Red	31	36	13	Installed	IBM HTTP Server for i	2015/09/12
		SF99572	Green	22	22	68	Not Installed	Java	2015/09/12
		SF99627	Green	11	11	155	Installed	7.1 Electronic Services Group PTF	2015/09/12
		SF99701	Red	32	37	67	Installed	DB2 for IBM i	2015/09/12
		SF99705	Red	10	22	40	Installed	Hardware and Related PTFs	2015/09/12
		SF99706	Red	7	8	155	Installed	High Availability for IBM i	2015/09/12
		SF99707	Red	7	10	159	Installed	Technology Refresh	2015/09/12
		SF99708	Red	32	47	15	Installed	Group Security	2015/09/12
		SF99709	Red	112	152	0	Installed	Group Hiper	2015/09/12
		SF99710	Red	13298	15142	133	Installed	Current Cumulative PTF Media Documentation	2015/09/12
BSTGEN2	V7R1M0	SF99145	Red	7	9	155	Installed	Performance Tools	2015/11/08
		SF99362	Red	35	51	15	Installed	Backup Recovery Solutions	2015/11/08
		SF99366	Red	10	12	155	Installed	Print PTFs	2015/11/08
		SF99367	Green	8	9	39	Installed	TCP/IP PTF	2015/11/08
		SF99368	Red	31	36	13	Installed	IBM HTTP Server for i	2015/11/08
		SF99572	Green	22	22	68	Not Installed	Java	2015/11/08
		SF99627	Green	11	11	155	Installed	7.1 Electronic Services Group PTF	2015/11/08
		SF99701	Red	32	37	67	Installed	DB2 for IBM i	2015/11/08
		SF99705	Red	10	22	40	Installed	Hardware and Related PTFs	2015/11/08

Compliance Assessment and Reporting Tool

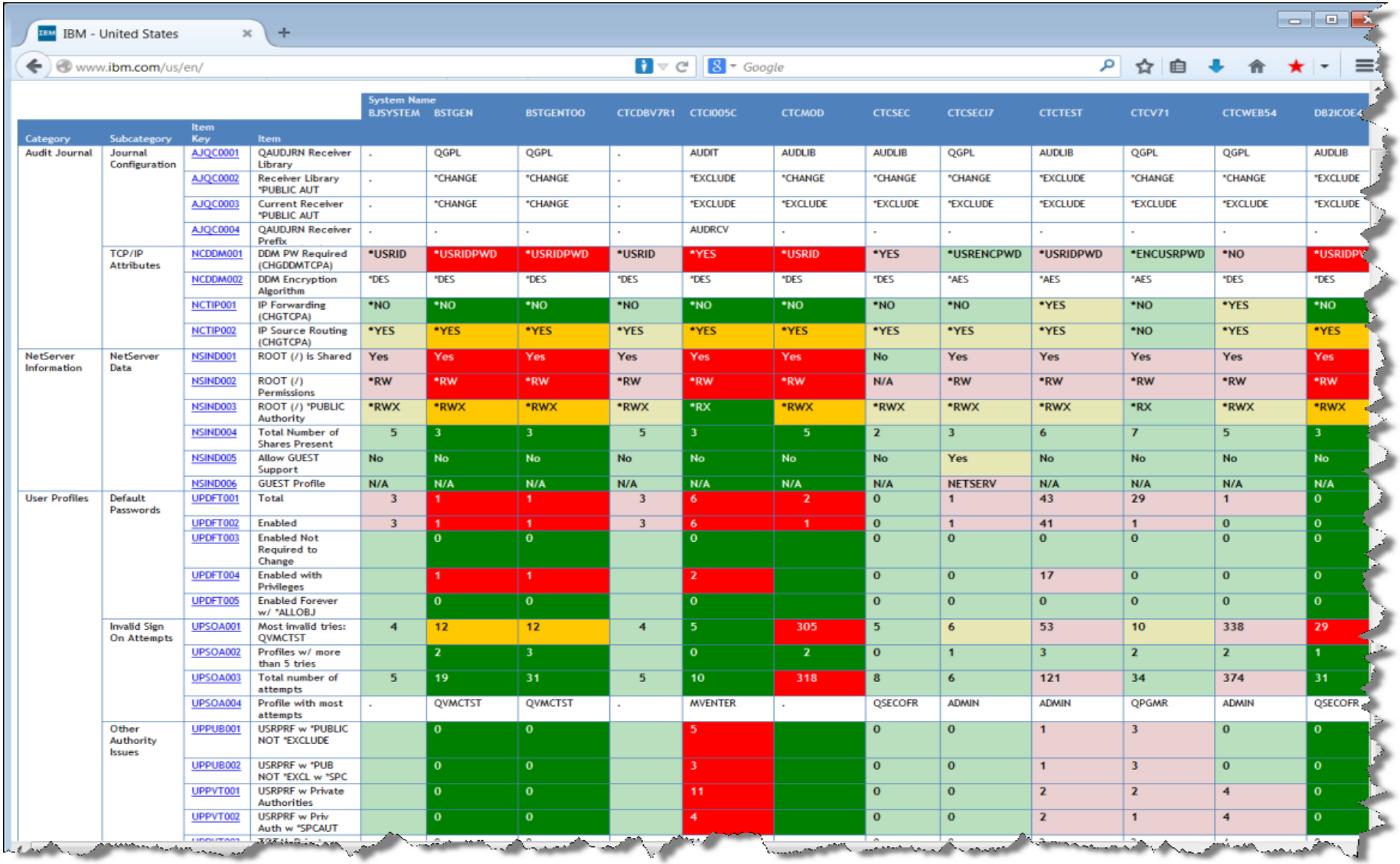
Cross System Analysis

Certificate Stores …

Category	Subcategory	Item Key	Item	System Name BJSYSTEM	BSTGEN	BSTGENTOO	BSTGEN2	CTCDBV7R1	CTCI005C
Certificate Stores	*PUBLIC Authority	CSPA0001	System Certificate Store Dir	*EXCLUDE	*EXCLUDE	*EXCLUDE	*USE	*EXCLUDE	*USE
		CSPA0002	Obj Sign/Sig Verify Cert Dir	*EXCLUDE	*EXCLUDE	*EXCLUDE	*USE	*EXCLUDE	*USE
		CSPA0003	Object Signing Certificate	*NOTFOUND	*NOTFOUND	*NOTFOUND	*NOTFOUND	*EXCLUDE	*NOTFOUND
		CSPA0004	Object Signing Certificate PW	*NOTFOUND	*NOTFOUND	*NOTFOUND	*NOTFOUND	*EXCLUDE	*NOTFOUND
		CSPA0005	Signature Verification Cert	*NOTFOUND	*NOTFOUND	*NOTFOUND	*NOTFOUND	*NOTFOUND	*NOTFOUND
		CSPA0006	Signature Verification Cert PW	*NOTFOUND	*NOTFOUND	*NOTFOUND	*NOTFOUND	*NOTFOUND	*NOTFOUND
		CSPA0007	System Certificate Store	*EXCLUDE	*EXCLUDE)	*EXCLUDE	*EXCLUDE	*EXCLUDE	*EXCLUDE
		CSPA0008	System Certificate Store PW	*EXCLUDE	*EXCLUDE)	*EXCLUDE	*EXCLUDE	*EXCLUDE	*EXCLUDE
	Certificate Analysis (V6)	CSSTA001	Certificates Present (*SYSTEM)	21	*NOTAVAIL	*NOTAVAIL	30	34	1
		CSSTA002	Certificates that are Expired	5	*NOTAVAIL	*NOTAVAIL	11	5	1
		CSSTA003	Expiration within 90 Days	0	*NOTAVAIL	*NOTAVAIL	0	1	2
		CSSTA004	Expiration within 60 Days	0	*NOTAVAIL	*NOTAVAIL	0	0	14
		CSSTA005	Expiration within 30 Days	0	*NOTAVAIL	*NOTAVAIL	0	0	7
		CSSTA006	Certificates NOT Trusted	0	*NOTAVAIL	*NOTAVAIL	0	0	0
		CSSTA007	Certificates with Private Key	2	*NOTAVAIL	*NOTAVAIL	6	14	11
		CSSTA008	Keys with size less than 2048	19	*NOTAVAIL	*NOTAVAIL	19	23	4
		CSSTA009	Keys stored in Hardware	0	*NOTAVAIL	*NOTAVAIL	0	0	0

Compliance Assessment and Reporting Tool

Monitoring Vulnerabilities



IBM - United States

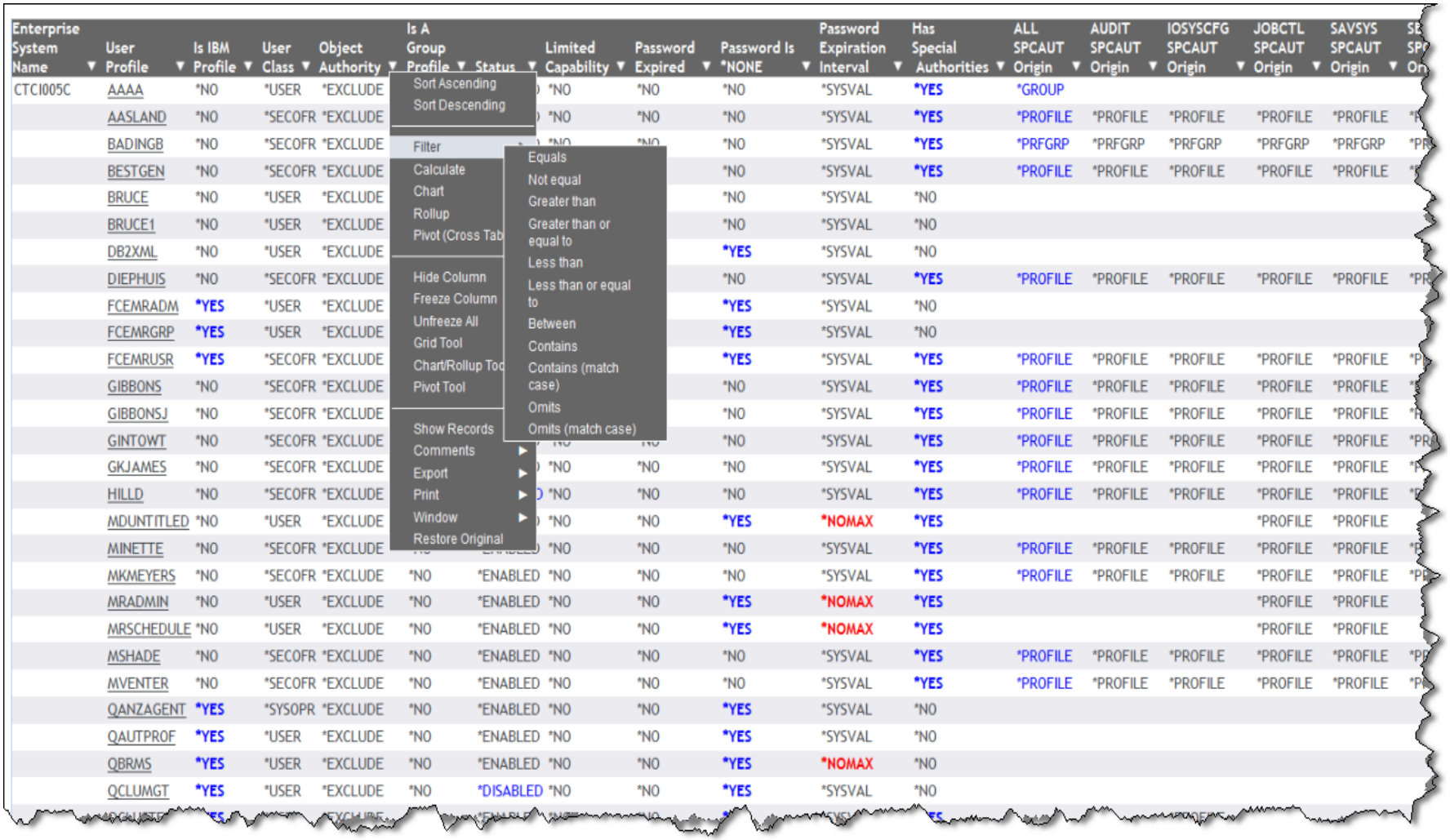
www.ibm.com/us/en/

				System Name											
				BJSYSTEM	BSTGEN	BSTGENTOO	CTCDBV7R1	CTCI005C	CTCMOD	CTCSEC	CTCSECI7	CTCTEST	CTCV71	CTCWEB54	DB2ICOE4
Category	Subcategory	Item Key	Item												
Audit Journal	Journal Configuration	AJQC0001	QAUDJRN Receiver Library	.	QGPL	QGPL	.	AUDIT	AUDLIB	AUDLIB	QGPL	AUDLIB	QGPL	QGPL	AUDLIB
		AJQC0002	Receiver Library *PUBLIC AUT	.	*CHANGE	*CHANGE	.	*EXCLUDE	*CHANGE	*CHANGE	*CHANGE	*EXCLUDE	*CHANGE	*CHANGE	*EXCLUDE
		AJQC0003	Current Receiver *PUBLIC AUT	.	*CHANGE	*CHANGE	.	*EXCLUDE	*EXCLUDE	*EXCLUDE	*EXCLUDE	*EXCLUDE	*EXCLUDE	*EXCLUDE	*EXCLUDE
		AJQC0004	QAUDJRN Receiver Prefix	.	.	.	.	AUDRCV	.	.	.	.	.	.	.
	TCP/IP Attributes	NCDDM001	DDM PW Required (CHGDDMTCPA)	*USRID	*USRIDPWD	*USRIDPWD	*USRID	*YES	*USRID	*YES	*USRENCPWD	*USRIDPWD	*ENCUSRPWD	*NO	*USRIDPW
		NCDDM002	DDM Encryption Algorithm	*DES	*DES	*DES	*DES	*DES	*DES	*DES	*AES	*AES	*AES	*DES	*DES
		NCTIP001	IP Forwarding (CHGTCPA)	*NO	*NO	*NO	*NO	*NO	*NO	*NO	*NO	*YES	*NO	*YES	*NO
		NCTIP002	IP Source Routing (CHGTCPA)	*YES	*YES	*YES	*YES	*YES	*YES	*YES	*YES	*YES	*NO	*YES	*YES
NetServer Information	NetServer Data	NSIND001	ROOT (/) is Shared	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
		NSIND002	ROOT (/) Permissions	*RW	*RW	*RW	*RW	*RW	*RW	N/A	*RW	*RW	*RW	*RW	*RW
		NSIND003	ROOT (/) *PUBLIC Authority	*RWX	*RWX	*RWX	*RWX	*RX	*RWX	*RWX	*RWX	*RWX	*RX	*RWX	*RWX
		NSIND004	Total Number of Shares Present	5	3	3	5	3	5	2	3	6	7	5	3
		NSIND005	Allow GUEST Support	No	No	No	No	No	No	No	Yes	No	No	No	No
		NSIND006	GUEST Profile	N/A	N/A	N/A	N/A	N/A	N/A	N/A	NETSERV	N/A	N/A	N/A	N/A
User Profiles	Default Passwords	UPDFT001	Total	3	1	1	3	6	2	0	1	43	29	1	0
		UPDFT002	Enabled	3	1	1	3	6	1	0	1	41	1	0	0
		UPDFT003	Enabled Not Required to Change		0	0		0		0	0	0	0	0	0
		UPDFT004	Enabled with Privileges		1	1		2		0	0	17	0	0	0
		UPDFT005	Enabled Forever w/ *ALLOBJ		0	0		0		0	0	0	0	0	0
	Invalid Sign On Attempts	UPSOA001	Most invalid tries: QVMCTST	4	12	12	4	5	305	5	6	53	10	338	29
		UPSOA002	Profiles w/ more than 5 tries		2	3		0	2	0	1	3	2	2	1
		UPSOA003	Total number of attempts	5	19	31	5	10	318	8	6	121	34	374	31
		UPSOA004	Profile with most attempts	.	QVMCTST	QVMCTST	.	MVENTER	.	QSECOFR	ADMIN	ADMIN	QPGMR	ADMIN	QSECOFR
	Other Authority Issues	UPPUB001	USRPRF w *PUBLIC NOT *EXCLUDE		0	0		5		0	0	1	3	0	0
		UPPUB002	USRPRF w *PUB NOT *EXCL w *SPC		0	0		3		0	0	1	3	0	0
		UPPVT001	USRPRF w Private Authorities		0	0		11		0	0	2	2	4	0
		UPPVT002	USRPRF w Priv Auth w *SPCAUT		0	0		4		0	0	2	1	4	0

Compliance Assessment and Reporting Tool

Profile Analysis

Horizontal or vertical presentation of user profiles across LPARs



Enterprise System Name	User Profile	Is IBM Profile	User Class	Object Authority	Is A Group Profile	Status	Limited Capability	Password Expired	Password Is *NONE	Password Expiration Interval	Has Special Authorities	ALL SPCAUT Origin	AUDIT SPCAUT Origin	IOSYSCFG SPCAUT Origin	JOBCTL SPCAUT Origin	SAVSYS SPCAUT Origin
CTCI005C	AAAA	*NO	*USER	*EXCLUDE			*NO	*NO	*NO	*SYSVAL	*YES	*GROUP				
	AASLAND	*NO	*SECOFR	*EXCLUDE			*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	BADINGB	*NO	*SECOFR	*EXCLUDE					*NO	*SYSVAL	*YES	*PRFGRP	*PRFGRP	*PRFGRP	*PRFGRP	*PRFGRP
	BESTGEN	*NO	*SECOFR	*EXCLUDE					*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	BRUCE	*NO	*USER	*EXCLUDE					*NO	*SYSVAL	*NO					
	BRUCE1	*NO	*USER	*EXCLUDE					*NO	*SYSVAL	*NO					
	DB2XML	*NO	*USER	*EXCLUDE					*YES	*SYSVAL	*NO					
	DIEPHUIS	*NO	*SECOFR	*EXCLUDE					*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	FCEMRADM	*YES	*USER	*EXCLUDE					*YES	*SYSVAL	*NO					
	FCEMRGRP	*YES	*USER	*EXCLUDE					*YES	*SYSVAL	*NO					
	FCEMRUSR	*YES	*SECOFR	*EXCLUDE					*YES	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	GIBBONS	*NO	*SECOFR	*EXCLUDE					*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	GIBBONSJ	*NO	*SECOFR	*EXCLUDE					*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	GINTOWT	*NO	*SECOFR	*EXCLUDE					*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	GKJAMES	*NO	*SECOFR	*EXCLUDE			*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	HILLD	*NO	*SECOFR	*EXCLUDE			*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	MDUNTITLED	*NO	*USER	*EXCLUDE			*NO	*NO	*YES	*NOMAX	*YES				*PROFILE	*PROFILE
	MINETTE	*NO	*SECOFR	*EXCLUDE			*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	MKMEYERS	*NO	*SECOFR	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	MRADMIN	*NO	*USER	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*YES	*NOMAX	*YES				*PROFILE	*PROFILE
	MRSCHEDULE	*NO	*USER	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*YES	*NOMAX	*YES				*PROFILE	*PROFILE
	MSHADE	*NO	*SECOFR	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	MVENTER	*NO	*SECOFR	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE
	QANZAGENT	*YES	*SYSOPR	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*YES	*SYSVAL	*NO					
	QAUTPROF	*YES	*USER	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*YES	*SYSVAL	*NO					
	QBRMS	*YES	*USER	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*YES	*NOMAX	*NO					
	QCLUMGT	*YES	*USER	*EXCLUDE	*NO	*DISABLED	*NO	*NO	*YES	*SYSVAL	*NO					

Compliance Assessment and Reporting Tool

Profile Analysis

Aggregation of user profiles across LPARs

User Profile	Total Systems With Profile	Systems With Enabled Profiles	Systems With All Object Special Authority	Systems With Audit Special Authority	Systems With I/O System Special Authority	Systems With Job Control Special Authority	Systems With Save System Special Authority	Systems With Security Administrator Special Authority	Systems With Spool Control Special Authority	Profile Description
AAAA	1	1	0	0	0	0	0	0	0	
AASLAND	3	3	3	3	3	3	3	3	3	Christian Aasland 612-397-2947, XLU
ABONIFAC	1	1	1	1	1	1	1	1	1	Antonio Bonifacio
ADMGROUP	1	1	0	0	0	0	0	0	0	Used in Security lab
ADMIN	2	0	2	2	2	2	2	2	2	CBC Administrator for Management Centra
ADMOWN	1	0	1	1	1	1	1	1	1	Security Fundamentals Owner
ADM01	1	1	0	0	0	0	0	1	0	System Admin and Control class
ADM02	1	1	0	0	0	0	0	1	0	System Admin and Control class
ADM03	1	1	0	0	0	0	0	1	0	System Admin and Control class
ADM04	1	1	0	0	0	0	0	1	0	System Admin and Control class
ADM05	1	1	0	0	0	0	0	1	0	System Admin and Control class
ADM06	1	1	0	0	0	0	0	1	0	System Admin and Control class
ADM07	1	1	0	0	0	0	0	1	0	System Admin and Control class
ADM08	1	1	0	0	0	0	0	1	0	System Admin and Control class
ADM09	1	1	0	0	0	0	0	1	0	System Admin and Control class
ADM10	1	1	0	0	0	0	0	1	0	System Admin and Control class
ADPOWN	1	1	1	1	1	1	1	1	1	
AJFISHER	2	1	2	2	2	2	2	2	2	Arv Fisher - Java dev't
AKENNEDY	1	1	1	1	1	1	1	1	1	Alan Kennedy
ALLOBJ	2	2	2	1	1	1	1	1	1	
AMRA	1	1	1	1	1	1	1	1	1	Nadir Amra
APPGROUP1	1	1	0	0	0	0	0	0	0	
APPGRP	1	1	0	0	0	0	0	0	0	
APPGRP1	1	1	0	0	0	0	0	0	0	
APPGRP2	1	1	0	0	0	0	0	0	0	
APPLIBOWN	1	1	0	0	0	0	0	0	0	
APPOWN	1	0	0	0	0	0	0	0	0	
APPOWN1	1	0	0	0	0	0	0	0	0	
APPSECOFR	1	1	1	0	0	0	0	0	0	

Compliance Assessment and Reporting Tool

Profile Analysis

Drill down into user profiles as configured across LPARs

User Profile Details for Selected Systems

User Profile: QSECOFR

Region	Data Center	System Name	User Profile	Is IBM Profile	User Class	Object Authority	Is A Group Profile	Status	Limited Capability	Password Expired	Password Is *NONE	Password Expiration Interval	Has Special Authorities	ALL SPCAUT Origin	AUDIT SPCAUT Origin	IOSYSCFG SPCAUT Origin	JOBCTL SPCAUT Origin	SAVSYS SPCAUT Origin	SECADM SPCAUT Origin	SE... Si... C...
Latin America-North	Mexico	BSTGEN2	QSECOFR	*YES	*SECOFR	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PR...
	ROBS	CTCMOD	QSECOFR	*YES	*SECOFR	*EXCLUDE	*NO	*DISABLED	*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PR...
Latin America-South	Argentina	BSTGEN	QSECOFR	*YES	*SECOFR	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PR...
		BSTGENTOO	QSECOFR	*YES	*SECOFR	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*P...
		CTCDBV7R1	QSECOFR																	
		CTCSEC	QSECOFR	*YES	*SECOFR	*EXCLUDE	*NO	*DISABLED	*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*P...
		CTCSECI7	QSECOFR	*YES	*SECOFR	*EXCLUDE	*YES	*ENABLED	*NO	*NO	*NO	*NOMAX	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*P...
		FIVECTESTSYS	QSECOFR	*YES	*SECOFR	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*P...
North America	Rochester	CTCTEST	QSECOFR	*YES	*SECOFR	*EXCLUDE	*YES	*ENABLED	*NO	*NO	*NO	*NOMAX	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PR...
		CTCV71	QSECOFR	*YES	*SECOFR	*EXCLUDE	*YES	*DISABLED	*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*P...
	ROBS2	BJSYSTEM	QSECOFR																	
	ROB3	CTCJ05C	QSECOFR	*YES	*SECOFR	*EXCLUDE	*NO	*ENABLED	*NO	*NO	*NO	*SYSVAL	*YES	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PROFILE	*PR...

Compliance Assessment and Reporting Tool

Event Monitoring

Early Detection of Administrative Mistakes or Malicious Activity

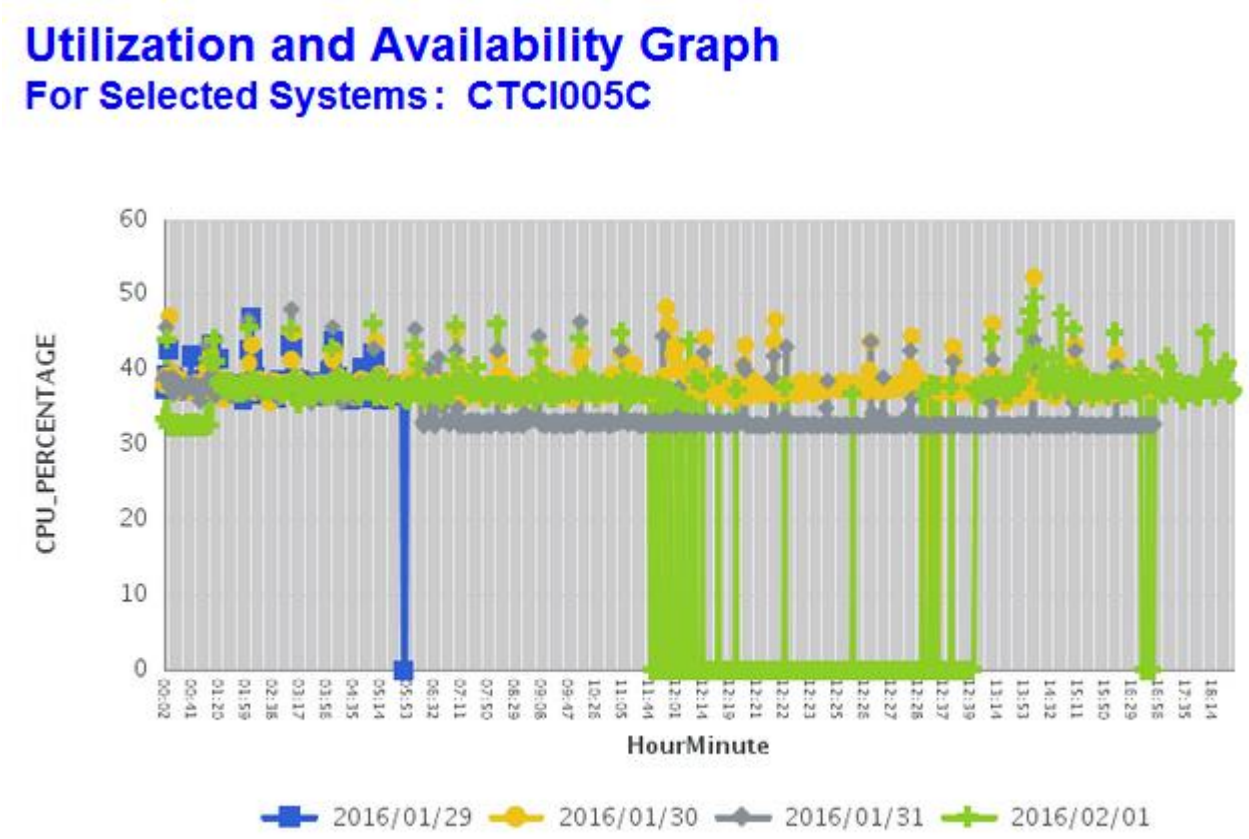
Security Event Details
For Selected Systems: CTCI005C

Enterprise System Name	Item	Category	Value Retrieved	Remote Job	Remote User	Remote System Run Timestamp
CTCI005C	Private Authority on Profile G	Events	U:BARLEN PA:*CHANGE TO:TESTPWD	QPADEV000L/BADINGB/335590	BADINGB	2016/01/30 09:30:52.188720
			U:BBBB PA:*ALL TO:SHARONSU	QPADEV000L/BADINGB/335590	BADINGB	2016/01/30 09:34:28.04352
			U:BBTEMP PA:*USE TO:BBBB	QPADEV000L/BADINGB/335590	BADINGB	2016/01/30 09:38:03.40723
			U:DARLINE PA:*USE TO:BBTEMP	QPADEV000L/BADINGB/335590	BADINGB	2016/01/30 09:38:19.822176
			U:DB2XML PA:*USE TO:TAFTEMP2	QPADEV000L/BADINGB/335590	BADINGB	2016/01/30 17:57:32.542944
			U:DIEPHUIS PA:*USE TO:DARLINE	QPADEV000L/BADINGB/335590	BADINGB	2016/01/30 09:41:19.852336
			U:QSYSOPR PA:*USE TO:TAFTEMP2	QPADEV000L/BADINGB/335590	BADINGB	2016/01/30 18:22:42.935280
			U:T PA:*USE TO:DIEPHUIS	QPADEV000L/BADINGB/335590	BADINGB	2016/01/30 11:16:53.851184
			U:TAFBAK PA:*CHANGE TO:T	QPADEV000L/BADINGB/335590	BADINGB	2016/01/30 11:17:07.740688
			U:TAFTEMP2 PA:*ALL TO:TAFBAK	QPADEV000L/BADINGB/335590	BADINGB	2016/01/30 11:17:23.239072
			U:TESTPWD PA:*USE TO:BRUCEB	QPADEV000L/BADINGB/335590	BADINGB	2016/01/29 19:29:33.356912
	Program set to ADOPT *OWNER...	Alerts	P:QWKEVTCKB L:QZRDQWKSEC O:QSECOFR	336801/TAFORD/QPADEV000H	TAFORD	2016/01/30 21:10:05.939168
			P:QWKEVTCKQ L:QZRDQWKSEC O:QSECOFR	336801/TAFORD/QPADEV000H	TAFORD	2016/01/30 22:01:33.864464
						2016/01/30 22:11:00.777824
						2016/01/30 22:50:37.121072
						2016/01/30 23:03:49.897456
						2016/01/30 23:24:53.458176
						2016/01/30 23:25:39.988240
						2016/01/30 23:33:55.343776
						2016/01/30 23:39:54.298256
						2016/01/30 23:53:30.011648
			P:QWKSECRST L:QZRDQWKSEC O:QSECOFR	QRWTSRVR/QUSER/335854	QWKUSER	2016/01/30 13:59:38.972640
						2016/01/30 13:59:39.852048
				QRWTSRVR/QUSER/335905	QWKUSER	2016/01/30 14:03:11.202352
						2016/01/30 14:03:12.114992
				QRWTSRVR/QUSER/335941	QWKUSER	2016/01/30 16:03:15.692224
						2016/01/30 16:03:17.556848
				QRWTSRVR/QUSER/335943	QWKUSER	2016/01/30 15:03:14.974384
						2016/01/30 15:03:16.096832
				337233/QUSER/QRWTSRVR	QWKUSER	2016/01/31 13:59:34.544800
						2016/01/31 13:59:35.167440

Compliance Assessment and Reporting Tool

Performance and Availability Analysis

Understand Risk of Outage due to Performance or Availability constraints



PowerSC Tools for IBM i
Proven Security Solutions

- ✓ ***Simplifies management*** *and measurement of security & compliance*
- ✓ ***Reduces cost*** *of security & compliance*
- ✓ ***Improves detection*** *and reporting of security exposures*
- ✓ ***Improves*** *the* ***audit capability*** *to satisfy reporting requirements*

IBM Lab Services offerings for IBM i security:

- ✓ *IBM i Security Assessment*
- ✓ *IBM i Single Sign On Implementation*
- ✓ *IBM i Security Remediation*
- ✓ *Password Validation, Synchronization, 2FA*
- ✓ *IBM i Encryption*

PowerSC Tools for IBM i	Benefits
Compliance Assessment and Reporting. Includes Security Event Monitoring	Demonstrate adherence to pre-defined and customer defined security polices, system component inventory. Centralize security management and reporting via Db2 Web Query
Security Diagnostics	Reduces operator time involved in remediating exposures
Privileged Elevation Tool	Ensures compliance with guidelines on privileged users
Access Control Monitor	Prevents user application failures due to inconsistent controls
Network Interface Firewall	Reduces threat of unauthorized security breach and data loss
Certificate Expiration Manager	Prevents system outages due to expired certificates
Password Validation / Synchronization / TOTP Two Factor Authentication (2FA)	Ensures user passwords are not trivial and are in synchronization across all LPARs. Insure service accounts adhere to policy - including SVRAUTE. Enhance applications with 2FA service program.
Single Sign On (SSO) Suite	Reduces for password resets and simplifies user experience

PowerSC Tools for IBM i are service offerings from IBM Systems Lab Services

For more information on PowerSC Tools for IBM i offerings and services, contact: Terry Ford taford@us.ibm.com Practice Leader, IBM Systems Lab Services Security

IBM Systems Lab Services and Training

Our Mission and Profile

- Support the IBM Systems Agenda and accelerate the adoption of new products and solutions
- Maximize performance of our clients' existing IBM systems
- Deliver technical training, conferences, and other services tailored to meet client needs
- Team with IBM Service Providers to optimize the deployment of IBM solutions (GTS, GBS, SWG Lab Services and our IBM Business Partners)

Our Competitive Advantage

- Leverage relationships with the IBM development labs to build deep technical skills and exploit the expertise of our developers
- Combined expertise of Lab Services and the Training for Systems team
- Skills can be deployed worldwide to assure client requests can be met

Successful Worldwide History

- 18 years in Americas
- 10 years in Europe/Middle East/Africa
- 6 years in Asia Pacific

www.ibm.com/systems/services/labservices
ibmsls@us.ibm.com

Mainframe Systems

Power Systems

System Storage

IT Infrastructure Optimization

Data Center Services

Training Services

IBM Systems Lab Services and Training

Leverage the skills and expertise of IBM's technical consultants to implement projects that achieve faster business value

- ✓ Ensure a smooth upgrade
- ✓ Improve your availability
- ✓ Design for efficient virtualization
- ✓ Reduce management complexity
- ✓ Assess your system security
- ✓ Optimize database performance
- ✓ Modernize applications for iPad
- ✓ Deliver training classes & conferences

How to contact us

- email us at ibmsls@us.ibm.com
- Follow us at @IBMSLST
- Learn more ibm.com/systems/services/labservices

IBM ESA Electronic Service Agent

AIX for Business Linux

POWER7+ BUILT ON Power

PowerVM PowerHA PowerSC IBM Systems Director

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 Security

Intelligence. Integration. Expertise.