

IBM i

Compliance and security management on IBM i with IBM PowerSC

Thomas Barlen

Senior Managing Consultant – IBM Power System Security
IBM Technology Expert Labs

19th November 2024



What is Power**SC**

IBM Power**SC** manages
Security and Compliance of
IBM Power Systems and runs
on AIX, IBM i, or Linux.

Simplify
Compliance
Management

MFA is included in
since
Power**SC** 2.0

PowerSC Components **with** UI support

Security and Compliance Automation	AIX IBMi Linux	Security Compliance Automation provides pre-built profiles that are certified to comply with industry standards like the Payment Card Industry Data Security Standard(PCI) v3, Department of Defence Security Technical Implementation Guide for Unix (DOD STIG) , Control Objectives for Information and related Technology(COBIT), the Health Insurance Portability and Accountability Act Privacy and Security Rules(HIPAA), North American Electric Reliability Corporation compliance (NERC), General Data Protection Regulation (GDPR). It Simplifies management, by automating security and compliance configuration, auditing and monitoring. IBM i hardening profile available.
Real-Time Compliance	AIX	Simplifies management, by automating monitoring and providing immediate visibility to administrators sending alerts when a change to the system violates a rule that is identified in the configuration policy. The combination of both RTC as a component of PowerSC and AIX TE as OS feature complementing each other provide a powerful mechanisms for malware and intrusion prevention.
TNC and Patch Mngt.	AIX	Ensures patch level is installed based on patching policies and provides alerts if a security patch is issued that affects the systems.
Allow Listing	AIX Linux	The native Trusted Execution (TE) of AIX is also integrated into the PowerSC UI. You can configure TE policies, maintain entries in the Trusted Signature Database, and run a TSD scan. For Redhat Linux the fapolicyd daemon is used to provide allow listing features.
Object attribute and content changes	IBMi	IBM i audit journal is used to monitor object attribute and content changes. Events are reported to the PowerSC UI.
Group and cumulative PTF currency check	IBMi	PowerSC verifies if latest groups and cumulative PTF levels are installed. Installed and available levels are shown in the PowerSC UI.

PowerSC Components **with** UI support

Block Listing	IBMi Linux	You can configure a blocklist to find files on endpoints that match a list of user-provided virus hash values. The scanning can be performed manually or scheduled.
Alerts / EDR	AIX IBMi Linux	The PowerSC lets you prioritize security events. Different actions, such as sending an event, are available for the different event alert types.
Malware Detection	AIX IBMi Linux	PowerSC lets you integrate an existing ClamAV installation into the PowerSC UI.
Intrusion Detection	Linux AIX	The Linux Port Scan Attack Detector (psad) can report port scan attacks to the PowerSC UI. In AIX it is implemented in Intrusion Detection and Prevention (IDP).
Multi Factor Authentication	AIX IBMi Linux	Policy-based service that can require different authentication methods for users to be passed before gaining access to a system. Several different authentication methods available.

PowerSC provides a user-friendly, web-based UI to manage Security & Compliance

Security

- File Integrity Monitoring (FIM)
- Allow listing
- Endpoint Detection & Response

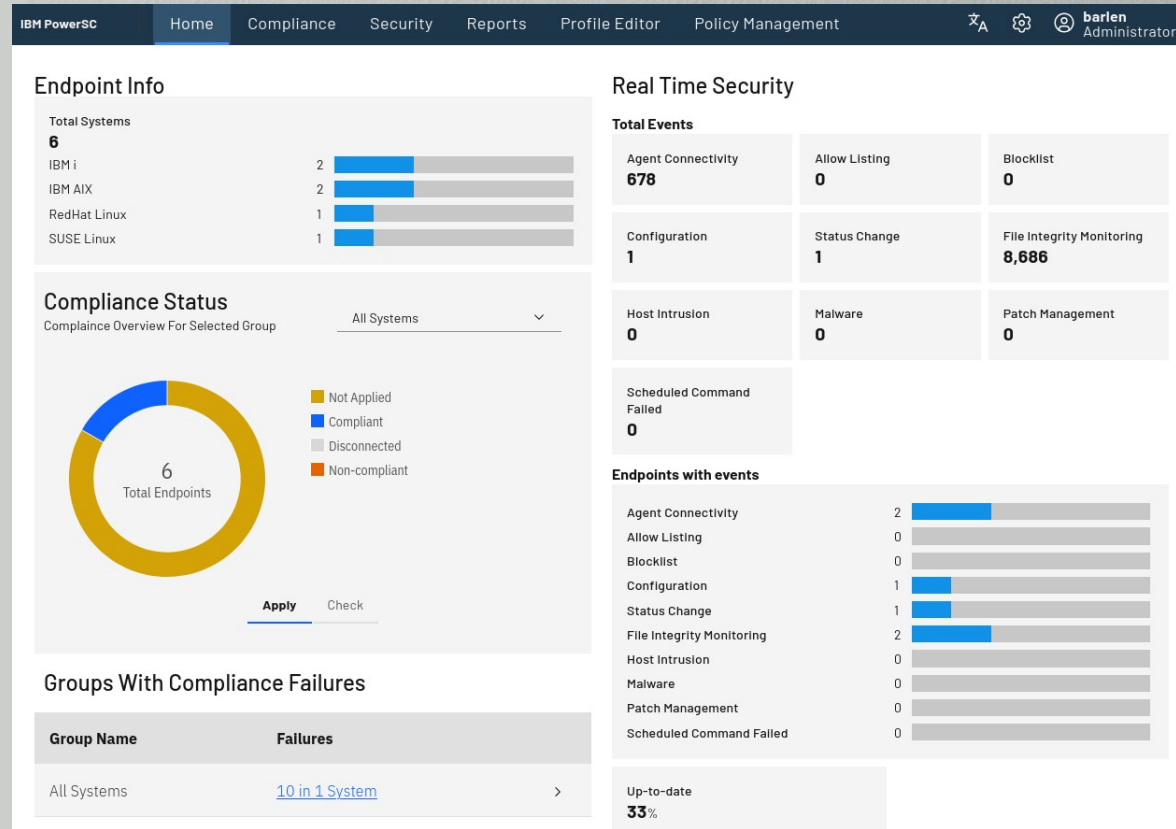
Compliance

- HIPAA, PCI, CIS, and more

Patch Management

- Trusted Network Connect (TNC)
- Detect & alert policy issues
- Policy enforcement

Multifactor Authentication



PowerSC Security Dashboard



- Real-time security dashboard
- Security overview status
- Endpoint description
- Event categories
- Drill down to event types

IBM PowerSC Home Compliance **Security Tab** Reports Profile Editor Policy Management barlen Administrator

>> All Systems 6 Systems Hide Summary Toggles Email Settings

Endpoints with events

Agent Connectivity	1	<div style="width: 25%;"></div>	Allow Listing	0	<div style="width: 0%;"></div>
Blocklist	0	<div style="width: 0%;"></div>	Configuration	1	<div style="width: 25%;"></div>
Status Change	1	<div style="width: 25%;"></div>	File Integrity Monitoring	0	<div style="width: 0%;"></div>
Host Intrusion	0	<div style="width: 0%;"></div>	Malware	0	<div style="width: 0%;"></div>
Patch Management	0	<div style="width: 0%;"></div>	Scheduled Command Failed	0	<div style="width: 0%;"></div>

Total Events

Agent Connectivity	Allow Listing	Blocklist	Configuration	Status Change	File Integrity Monitoring	Host Intrusion	Malware	Patch Management	Scheduled Command Failed
676	0	0	1	1	0	0	0	0	0

Search Refresh Interval Refresh Table Sync Endpoint Upload hash Hide all events

System Name	OS	FIM	Allow List	Patch	IDS	Alerts	Actions
ctcsect5.rchland.ibm.com	IBM i	✓	✗	✗	✗	▲0 ▲0 ▲0	⋮
tbaix.rchland.ibm.com	IBM AIX	✓	✓	—	✗	▲0 ▲0 ▲2	⋮
tbaix2.rchland.ibm.com	IBM AIX	✓	✓	✗	✓	▲0 ▲0 ▲0	⋮
tbibmi.rchland.ibm.com	IBM i	✓	✗	✗	✗	▲0 ▲0 ▲0	⋮

Security Overview

Endpoints

Monitor security from a single dashboard



PowerSC Compliance Dashboard

Compliance Tab



- Compliance dashboard
- Compliance overview status
- Automated enforcement
- Profile check and simulation
- Failure analysis
- Profile customization

IBM PowerSC Home Compliance Security Reports Profile Editor Policy Management barlen Administrator

Compliance Overview 6 Systems Hide Summary Email Settings

Total Rules Checked **2** Total Rule Checks Failed **1** Total Rules Applied **14** Total Rule Applies Failed **10**

Search Refresh Interval Refresh Table Sync Endpoint

<input type="checkbox"/>	System Name	OS	Last Applied Type	Apply Timestamp	Check Timestamp	Check Passed	Check Failed	Check Status
> <input type="checkbox"/>	ctcsect5.rchland.ibm.com	IBM i	IBMi_CIS_TestV1	11/13/2024, 9:13:57 AM	-	-	-	-
> <input type="checkbox"/>	tbaix.rchland.ibm.com	IBM AIX	N/A	-	-	-	-	-
<input type="checkbox"/>	tbaix2.rchland.ibm.com	IBM AIX	N/A	-	-	-	-	-
> <input type="checkbox"/>	tbibmi.rchland.ibm.com	IBM i	IBMi_CIS_TestV1	11/13/2024, 9:17:19 AM	11/13/2024, 9:18:08 AM	1	1	Failed
> <input type="checkbox"/>	tbrhel.rchland.ibm.com	RedHat Linux	BOSCH_LXS_V1	10/21/2024, 4:31:34 PM	-	-	-	-
> <input type="checkbox"/>	tbsles.rchland.ibm.com	SUSE Linux	N/A	-	-	-	-	-

Endpoints

7

Alerts sent for non-compliance



PowerSC Compliance Profiles

AIX Profiles

GDPR

PCI

CIS v1

CISv2_Level1

CISv2_Level2

HIPAA

NERC

DoD STIG

SAP Hardening



Compliance

Linux Profiles

GDPR

PCI

SAP Hardening (SLES and RHEL)

CIS v1

CIS v2 Level 1 and Level 2

DoD

HMC Hardening

IBM i Profiles **IBM i**

IBM i hardening

IBM i CIS Level 1 (7.4)

IBM i CIS Level 1 (7.5)

VIOS Profiles

CIS

PCI

PowerSC Compliance Profiles Editor

IBM PowerSC Home Compliance Security Reports Profile Editor Policy Management barlen Administrator

Source profiles i.e. built-in profiles

Custom profile

IBMi_CIS.xml

Name:IBMi_CISTom.xml Type:IBMi_CISTom

Save & Copy Save Cancel / Close

<input type="checkbox"/>	Rule Name	Type	
<input type="checkbox"/>	IBMiCIS31	IBMiCIS	
<input type="checkbox"/>	IBMiCIS32	IBMiCIS	
<input type="checkbox"/>	IBMiCIS33	IBMiCIS	
<input type="checkbox"/>	IBMiCIS35	IBMiCIS	
<input type="checkbox"/>	IBMiCIS36	IBMiCIS	
<input type="checkbox"/>	IBMiCIS37	IBMiCIS	
<input type="checkbox"/>	IBMiCIS311	IBMiCIS	

<input type="checkbox"/>	Rule Name	Type	
<input type="checkbox"/>	IBMiCIS_QPWDEXPITV	IBMiCIS	
<input type="checkbox"/>	IBMiCIS_QPWDEXPWRN	IBMiCIS	
<input type="checkbox"/>	IBMiCIS_QAUDCTL	IBMiCIS	
<input type="checkbox"/>	IBMiCIS_QAUDENDACN	IBMiCIS	
<input type="checkbox"/>	IBMiCIS_QAUDFRCLVL	IBMiCIS	
<input type="checkbox"/>	IBMiCIS_QAUDLVL	IBMiCIS	
<input type="checkbox"/>	IBMiCIS_QAUDLVL2	IBMiCIS	

9

Custom compliance profiles can be created and tailored to your needs



PowerSC Compliance Profiles Editor (cont'd)

Edit rule arguments

Warning: You should only change these if you are familiar with the script. Bad values here will prevent the rule from working properly! See the script for details about how these arguments are used.

Name:

Description:

Script:

Prereq List:

Arguments:

Buttons: Cancel, Confirm

Background interface: Custom profile, Name: IBMi_CISTom.xml, Type: IBMi_CISTom

Rule Name	Type	Icon
<input type="checkbox"/> IBMiCIS_QPWDEXPITV	IBMiCIS	🔧
<input type="checkbox"/> IBMiCIS_QPWDEXPWRN	IBMiCIS	🔧
<input type="checkbox"/> IBMiCIS_QAUDCTL	IBMiCIS	🔧
<input type="checkbox"/> IBMiCIS_QAUDENDACN	IBMiCIS	🔧
<input type="checkbox"/> IBMiCIS_QAUDFRCLVL	IBMiCIS	🔧
<input type="checkbox"/> IBMiCIS_QAUDLVL	IBMiCIS	🔧
<input type="checkbox"/> IBMiCIS_QAUDLVL2	IBMiCIS	🔧

Rule settings can be changed

PowerSC Compliance Profile Simulation

The screenshot displays the IBM PowerSC Compliance Profile Simulation interface. The top navigation bar includes 'Home', 'Compliance', 'Security', 'Reports', 'Profile Editor', and 'Policy Management'. The user is logged in as 'barlen Administrator'. The main area shows 'All Systems' with '6 Systems' selected. Summary statistics indicate: Total Rules Checked: 2, Total Rule Checks Failed: 1, Total Rules Applied: 14, and Total Rule Applies Failed: 10. A toolbar contains 'Apply', 'Simulate', 'Undo', 'Check', 'Schedule', and 'Cancel' buttons. A table lists systems with columns for System Name, OS, Last Applied Type, Apply Timestamp, Check Timestamp, Check Passed, and Check Failed. A modal dialog titled 'Select Profile to Simulate on 1 endpoint' is open, showing 'Built-in Profiles' (IBMI_best_practices.xml, IBMI_CIS.xml, IBMI_CIS75.xml) and 'Custom Profiles' (IBMI_CIS_TestV1.xml, IBMI_CISTom.xml). The 'IBMI_CIS_TestV1.xml' profile is selected. A blue callout box points to the 'Simulate' button with the text 'Select profile to simulate'. The dialog has 'Cancel' and 'Yes' buttons at the bottom.

System Name	OS	Last Applied Type	Apply Timestamp	Check Timestamp	Check Passed	Check Failed
ctcsect5.rchland.ibm.com	IBMI IBM i	IBMI_CIS_TestV1	11/13/2024, 9:13:57 AM	-	-	-
tbaix.rchland.ibm.com	AIX IE				-	-
tbaix2.rchland.ibm.com	AIX IE				-	-
tbibmi.rchland.ibm.com	IBMI IE			11/13/2024, 11:18:08 AM	1	1
tbrhel.rchland.ibm.com	RHEL S				-	-
tbsles.rchland.ibm.com	SLES S				-	-

Rule settings can be changed

PowerSC Compliance Profile Apply via Policies

Create a Policy

Policy Name [?]
IBMI_V1

Select Group [?]
IBMI

Select the profile to apply to this group. [?]
IBMI_CIS_TestV1.xml

Compliance Operations
 Check Simulate

Auto Schedule
 ON

Schedule Type
 Daily Weekly Monthly

Hour: 1 Minute: 0

Send me an email report?
 No

Cancel Create Policy

Create policy for group of systems

<input type="checkbox"/>	System Name	OS	Last Applied Type	Apply Timestamp
> <input type="checkbox"/>	ctcsect5.rchland.ibm.com	IBMI IBM i	IBMi_CIS_TestV1	11/13/2024, 11:55:22 AM
> <input type="checkbox"/>	tbaix.rchland.ibm.com	AIX IBM AIX	N/A	-
<input type="checkbox"/>	tbaix2.rchland.ibm.com	AIX IBM AIX	N/A	-
> <input type="checkbox"/>	tbibmi.rchland.ibm.com	IBMI IBM i	IBMi_CIS_TestV1	11/13/2024, 11:58:40 AM

All members of specified group automatically get profile applied



PowerSC Compliance Violation Example

The screenshot shows the IBM PowerSC interface. The top navigation bar includes Home, Compliance, Security, Reports, Profile Editor, and Policy Management. The user is logged in as 'barlen Administrator'. The main content area displays 'IBMi 2 Systems' with summary statistics: Total Rules Checked (2), Total Rule Checks Failed (1), Total Rules Applied (4), and Total Rule Applies Failed (0). A table lists the systems, with the second system, 'tbibmi.rchland.ibm.com', highlighted. Below the table, a detailed view for 'Checked IBMi_CIS_TestV1' is shown, including a 'Failed Rules' section with a specific violation message: '11/13/2024, 12:15:54 PM IBMiCIS_QPWDEXPWR: Compliance check for system value QPWDEXPWRN failed. System value should have value 7 but has value 8.' The 'Passed Rules' section shows '11/13/2024, 12:15:54 PM IBMiCIS_QAUDCT:'. The 'Console Output' section displays the command execution results: 'Compliance check for system value QAUDCTL passed. System value has value *NOQTEMP *OBJAUD *AUDLVL. Processedrules=2 Passedrules=1 Failedrules=1 Level=IBMi_CIS_TestV1 Input file=/etc/security/pscxpert/core/appliedrules.xml'.

System Name	OS	Last Applied Type	Apply Timestamp	Check Timestamp	Check Passed	Check Failed	Check Status
ctcsect5.rchland.ibm.com	IBMi	IBMi_CIS_TestV1	11/13/2024, 11:55:22 AM	-	-	-	-
tbibmi.rchland.ibm.com	IBMi	IBMi_CIS_TestV1	11/13/2024, 11:58:40 AM	11/13/2024, 12:15:54 PM	1	1	Failed

Checked IBMi_CIS_TestV1

Failed Rules:

- 11/13/2024, 12:15:54 PM IBMiCIS_QPWDEXPWR: Compliance check for system value QPWDEXPWRN failed. System value should have value 7 but has value 8.

Passed Rules:

- 11/13/2024, 12:15:54 PM IBMiCIS_QAUDCT:

Console Output

```
Compliance check for system value QAUDCTL passed. System value has value *NOQTEMP *OBJAUD *AUDLVL.
Processedrules=2 Passedrules=1 Failedrules=1 Level=IBMi_CIS_TestV1
Input file=/etc/security/pscxpert/core/appliedrules.xml
```

Easy to drill down on compliance violation details



PowerSC Patch Management



IBM PowerSC Home Compliance Security Reports Profile Editor Policy Management barlen Administrator

>> All Systems 6 Systems Hide Summary Toggles Email Settings

Endpoints with events

Agent Connectivity	1	<div style="width: 25%;"></div>	Allow Listing	0	<div style="width: 0%;"></div>
Blocklist	0	<div style="width: 0%;"></div>	Configuration	1	<div style="width: 25%;"></div>
Status Change	1	<div style="width: 25%;"></div>	File Integrity Monitoring	0	<div style="width: 0%;"></div>
Host Intrusion	0	<div style="width: 0%;"></div>	Malware	0	<div style="width: 0%;"></div>
Patch Management	0	<div style="width: 0%;"></div>	Scheduled Command Failed	0	<div style="width: 0%;"></div>

Total Events

Agent Connectivity	Allow Listing	Blocklist	Configuration	Status Change	File Integrity Monitoring	Host Intrusion	Malware	Patch Management	Scheduled Command Failed
676	0	0	1	1	0	0	0	0	0

Search Refresh Interval Refresh Table Sync Endpoint Upload hash Hide all events

System Name	OS	FIM	Allow List	Patch	IDS	Alerts	Actions
ctcsect5.rchland.ibm.com	IBM i	✓	✗	✗	✗	▲0 ▲0 ▲0	⋮
tbaix.rchland.ibm.com	IBM AIX	✓	✓	–	✗	▲0 ▲0 ▲2	⋮
tbaix2.rchland.ibm.com	IBM AIX	✓	✓	✗	✓	▲0 ▲0 ▲0	⋮
tbibmi.rchland.ibm.com	IBM i	✓	✗	✗	✗	▲0 ▲0 ▲0	⋮

Compliance View

Patch Management Status

Endpoints

The patch management feature detects virtual machines that do not meet patch management policies.

The dashboard shows VM's with missing security patches.

Compliance status overview

PowerSC Patch Management (cont'd)



IBM PowerSC Home Compliance Security Reports Profile Editor Policy Management barlen Administrator

Endpoint up to date status details

11/13/2024, 8:20:04 AM

PTF_GROUP_TITLE	PTF_GROUP_CURRENCY	PTF_GROUP_LEVEL_INSTALLED	PTF_GROUP_LEVEL_AVAILABLE
SF99652 - 740 Content Manager OnDemand for i - 5770-RD1 7.4	INSTALLED LEVEL IS CURRENT	19	19
SF99654 - 740 Db2 Web Query for i V2.3.0	INSTALLED LEVEL IS CURRENT	9	9
SF99659 - 740 IBM MQ for IBM i - v9.0/v9.1/v9.2/v9.3/v9.4	UPDATE AVAILABLE	10	40
SF99661 - 740 WebSphere App Server V8.5	INSTALLED LEVEL IS CURRENT	10	10
SF99662 - 740 IBM HTTP Server for i	UPDATE AVAILABLE	37	38
SF99663 - 740 Performance Tools	INSTALLED LEVEL IS CURRENT	14	14
SF99664 - 740 Backup Recovery Solutions	UPDATE AVAILABLE	43	44
SF99665 - 740 Java	UPDATE AVAILABLE	24	25
SF99666 - 740 High Availability for IBM i	UPDATE AVAILABLE	18	19
SF99667 - 740 740 TCP/IP PTF	UPDATE AVAILABLE	12	13
SF99668 - 740 IBM Db2 Mirror for i	INSTALLED LEVEL IS CURRENT	24	24
SF99672 - 740 Db2 Web Query for i V2.4.0	INSTALLED LEVEL IS CURRENT	4	4
SF99675 - 740 Hardware and Related PTFs	INSTALLED LEVEL IS CURRENT	2	2
SF99704 - 740 Db2 for IBM i	INSTALLED LEVEL IS CURRENT	28	28
SF99736 - 740 Technology Refresh plus Recommended Groups	INSTALLED LEVEL IS CURRENT	1	1
SF99737 - 740 Technology Refresh	INSTALLED LEVEL IS CURRENT	10	10
SF99738 - 740 Group Security	UPDATE AVAILABLE	68	71
SF99739 - 740 Group Hiper	UPDATE AVAILABLE	135	139
SF99740 - 740 Cumulative PTF Package	INSTALLED LEVEL IS CURRENT	24158	24158
SF99741 - 740 All PTF Groups except Cumulative PTF Package & MQ	INSTALLED LEVEL IS CURRENT	9	9

ctcsect5.rchland.ibm.com	IBM i	✓	✗	✗	✗	▲0 ▲0 ▲0	:
> tbaix.rchland.ibm.com	AIX IBM AIX	✓	✓	-	✗	▲0 ▲0 ▲2	:
tbaix2.rchland.ibm.com	AIX IBM AIX	✓	✓	✗	✓	▲0 ▲0 ▲0	:
tbibmi.rchland.ibm.com	IBM i	✓	✗	✗	✗	▲0 ▲0 ▲0	:

IBM i patch status shows current and available cumulative and group PTF levels

Requires online access (direct or via proxy)

Compliance status overview

PowerSC Reporting

Reports provide on-demand or daily information about compliance state and file integrity monitor events

The screenshot displays the IBM PowerSC Reports interface. The main header includes navigation tabs: Home, Compliance, Security, Reports, Profile Editor, and Policy Management. The user is logged in as 'barlen Administrator'. The left sidebar lists various report types, with 'Combined Compliance and FIM for IBMi' selected. The main content area shows a report titled 'Combined Compliance and FIM for IBMi group' dated 11/13/2024, 9:25:40 AM. A modal window is open for scheduling the report, with the following details:

- Report Title: Schedule Combined Compliance and FIM report email for barlen
- Send me an email report? Yes
- Schedule Type: Daily Weekly Monthly
- Hour: 19 Minute: 0
- Addresses (comma separated):
- Subject: PowerSC Timeline Server Report for IBMi group
- Buttons: Cancel, Save

The main content area also features a table titled 'Endpoints with events' and a summary table:

Endpoints with events	
Agent Connectivity	0
Blocklist	0
Status Change	0
Host Intrusion	0
Patch Management	0
Allow Listing	0
Configuration	0
File Integrity Monitoring	0
Malware	0
Scheduled Command Failed	0

Last Applied Type	#Failed Rules	#Passed Rules
IBMi_CIS_TestV1	0	2
IBMi_CIS_TestV1	1	1

Reports can be scheduled

Centralized GUI - Big Picture

- **UI Server**

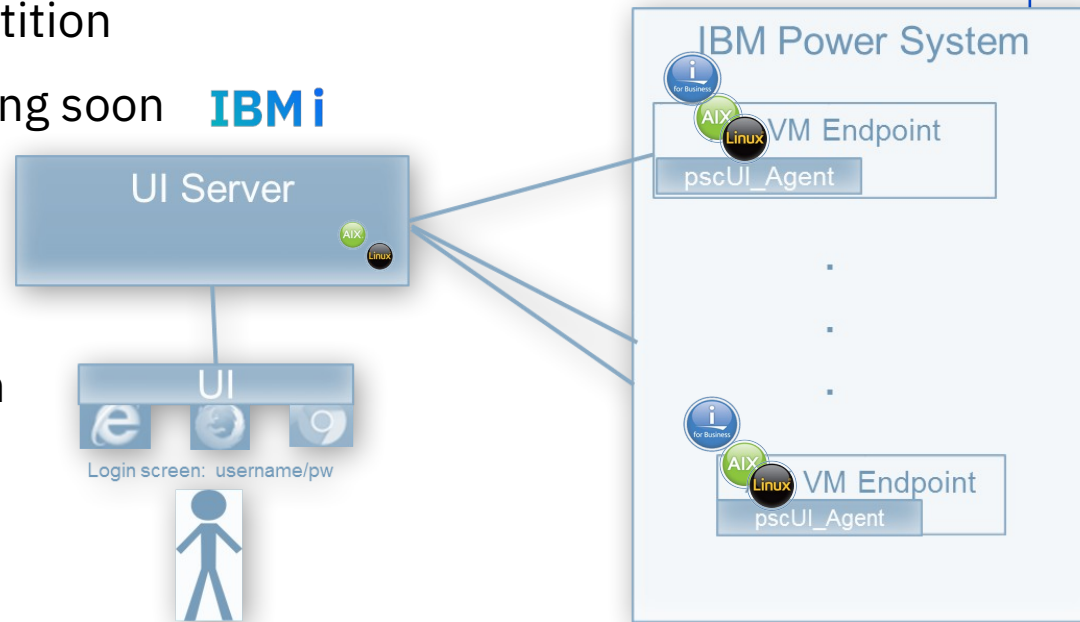
- AIX LPAR / Linux on Power / Linux on x86 / as a dedicated appliance server partition
- IBM i as server coming soon **IBM i**

- **UI Endpoint Agent**

- Monitoring
- Command Execution

- **Browser**

- User interaction



Central UI server provides Web-based user interface and interacts with agents

Centralized GUI - Secure Communication & Validation

- **SSL Certificates & agent-server Handshake**
 - Communication between UI components such as agent-to-server or browser-to-server uses industry-standard technology (such as SSL Certificates) as well as additional application-specific technology (such as agent-server handshakes)
- **Discovery of endpoints by the server**
- **Logging into UI Server from Browser - LDAP or Local Accounts**
 - UI access supports LDAP or local accounts and allows management of access and endpoint-control authority using AIX group membership
- **Heartbeat from agent to server**
 - A heartbeat agreement between the endpoint agents and the server helps to insure that the UI is fully up-to-date and functioning

Secure communications between server and agents

Group memberships can be used to determine who can log in to the Web interface and manage systems

PowerSC REST API Support

Integrate PowerSC into existing management applications

Period or event driven
PowerSC actions triggered
by external applications

- **REST APIs can be used to**
 - Manage agent group definitions and memberships
 - Retrieve all UI server kept attributes, such as compliance state, number of failed rules, applied compliance profiles, etc.
 - Getting a list of existing compliance profiles
 - Submit commands to manage file lists (Trusted Execution or fapolicyd), apply profiles, check for compliance, define RTC and auditd policies, etc,
 - Check patch compliance state and initiate patch update process
- **Swagger examples are provided on IBM Docs Web page**

PowerSC Multi Factor Authentication

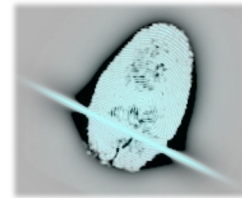
Authentication Factors

- Something you know
 - A password / PIN Code
- Something you have
 - ID badge or a cryptographic
- Something you are
 - Fingerprint or other biometric data

Login

User Name

Password



At least two authentication factors are used to confirm **separate pieces** of evidences in order to grant access to a system.

PowerSC MFA - Factors

- RSA SecurID (via fob)
- PIN-protected certificates on PIV/CAC smart cards
- TOTP (IBM Verify / Google Authenticator, etc.)
- Yubikey (via USB on laptop e.g.)
- Radius Protocol (Generic, Gemalto Safenet, RSA)
- Password / LDAP



PowerSC MFA Policy Based Solution

Factor

- An authentication technology – sourced from something you know (password), something you have (PIV/CAC smart card), or something you are (fingerprint, facial recognition).

Policy

- Rules that govern which factor credentials must be supplied for an authentication and define the lifetime of the generated Cache Token Credentials and their re-usability.

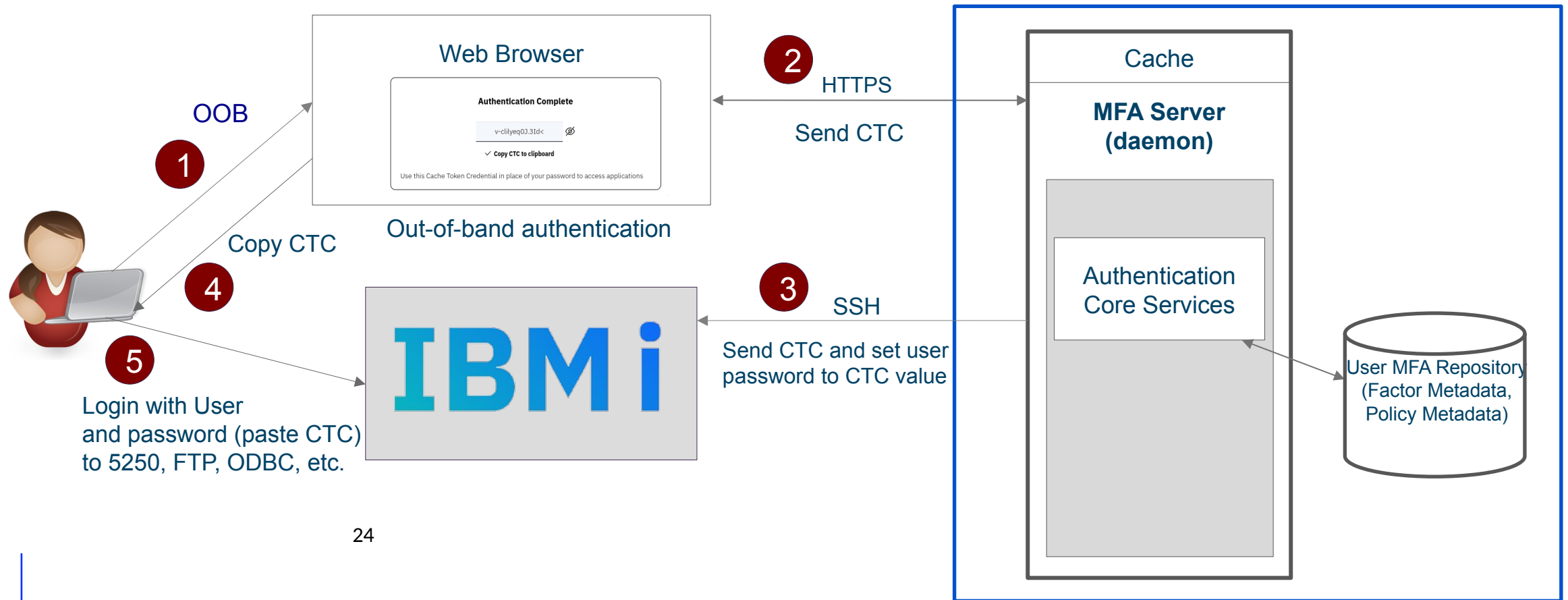
Cache Token Credential (CTC)

- A 16-character credential returned after a successful authentication.

PowerSC MFA – Out of Band Usage with IBM i

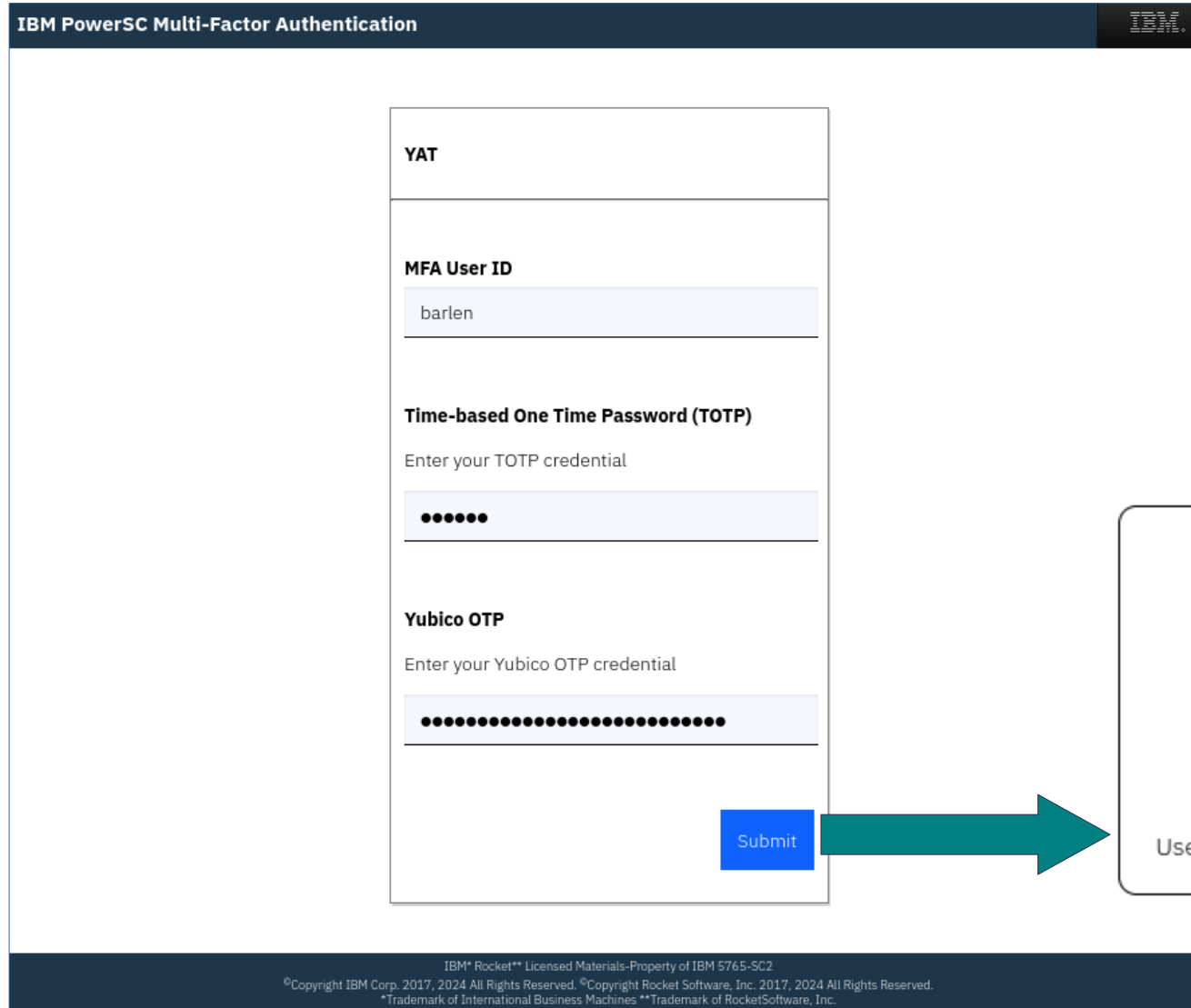
PowerSC MFA CTC broadcasting service is used to set IBM i user profile passwords to CTC value

- CTC length and type might need adjustment depending on IBM i password level



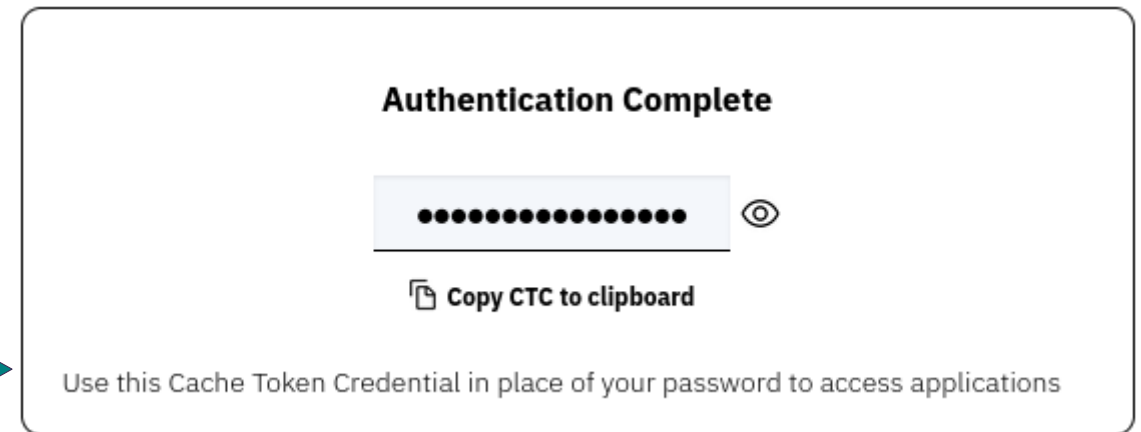
PowerSC MFA Out of Band Authentication

User enters login URL (generic or policy-specific)



The screenshot shows the IBM PowerSC Multi-Factor Authentication login interface. At the top, there is a dark blue header with the text "IBM PowerSC Multi-Factor Authentication" on the left and the IBM logo on the right. The main content area is white and contains several sections: "YAT" (likely a placeholder for a YubiKey), "MFA User ID" with a text input field containing "barlen", "Time-based One Time Password (TOTP)" with a prompt "Enter your TOTP credential" and a masked input field with six dots, and "Yubico OTP" with a prompt "Enter your Yubico OTP credential" and a masked input field with sixteen dots. A blue "Submit" button is located at the bottom right of the form. A large green arrow points from the "Submit" button to the right, towards the "Authentication Complete" screen.

- *User is prompted for factors defined in policy*
- *After successful authentication, CTC can be displayed or just copied*
- *Paste the CTC to IBM i login prompt as password*



The "Authentication Complete" screen is shown in a rounded rectangular box. It features the title "Authentication Complete" at the top. Below the title is a masked input field with sixteen dots and a toggle icon (an eye) to its right. Underneath the input field is a button with a clipboard icon and the text "Copy CTC to clipboard". At the bottom of the box, there is a line of text: "Use this Cache Token Credential in place of your password to access applications".

Thanks for your attention

Questions ?

Thomas Barlen

barlen@de.ibm.com

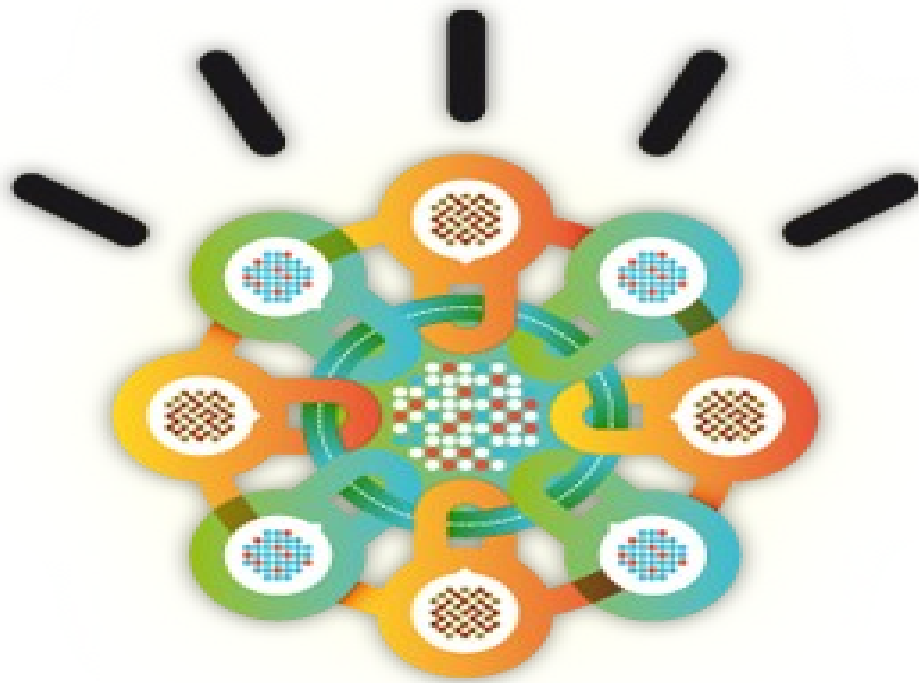
Senior Managing Consultant

IBM Power System Security

IBM Technology Expert Labs



IBM Technology Expert Labs Can Help!



- IBM Technology Expert Labs can offer consulting and security services:
 - ◆ IBM i, AIX, and Linux Security Assessment
 - ◆ IBM i Network Encryption (TLS)
 - ◆ IBM i Single Sign On Setup
 - ◆ IBM i Cryptography
 - ◆ AIX RBAC and Trusted Execution Services
 - ◆ IBM PowerSC Implementation Services
 - ◆ AIX and Linux LDAP Integration Services
- IBM Technology Expert also has several security tools:
 - ◆ IBM i Privilege Elevation (Firecall)
 - ◆ IBM i Password Validation and Password Sync
 - ◆ IBM i Advanced Authentication (2FA – RFC 6238)
 - ◆ IBM i Compliance and Reporting Tool with Event Monitoring
 - ◆ IBM i Certificate Expiration Manager
 - ◆ IBM i Syslog Reporting Manager
 - ◆ IBM i Software Firewall (Exit Point Tool)
 - ◆ And many more security related tools
- Visit ibm.biz/IBMiSecurity
- to learn more about all of these offerings!

Notices and disclaimers

© 2024 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those
- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.
- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
- It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

— IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml