

InterConnect 2016

The Premier Cloud & Mobile Conference

Optimize your BigFix Deployment via Customization and Integration

Lee Wei



February 21 – 25
MGM Grand & Mandalay Bay
Las Vegas, Nevada

Topics / Goals

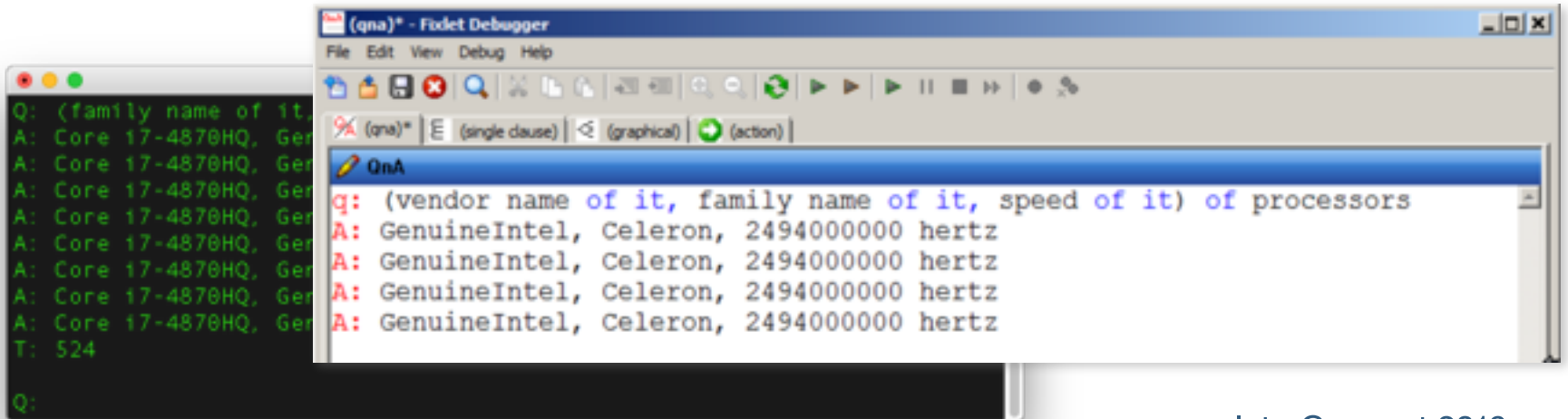
- Survey of what is available
- Walkthrough all the BigFix APIs
- Imagine the possibilities

Prerequisite

- Relevance
- Relevance
- Relevance

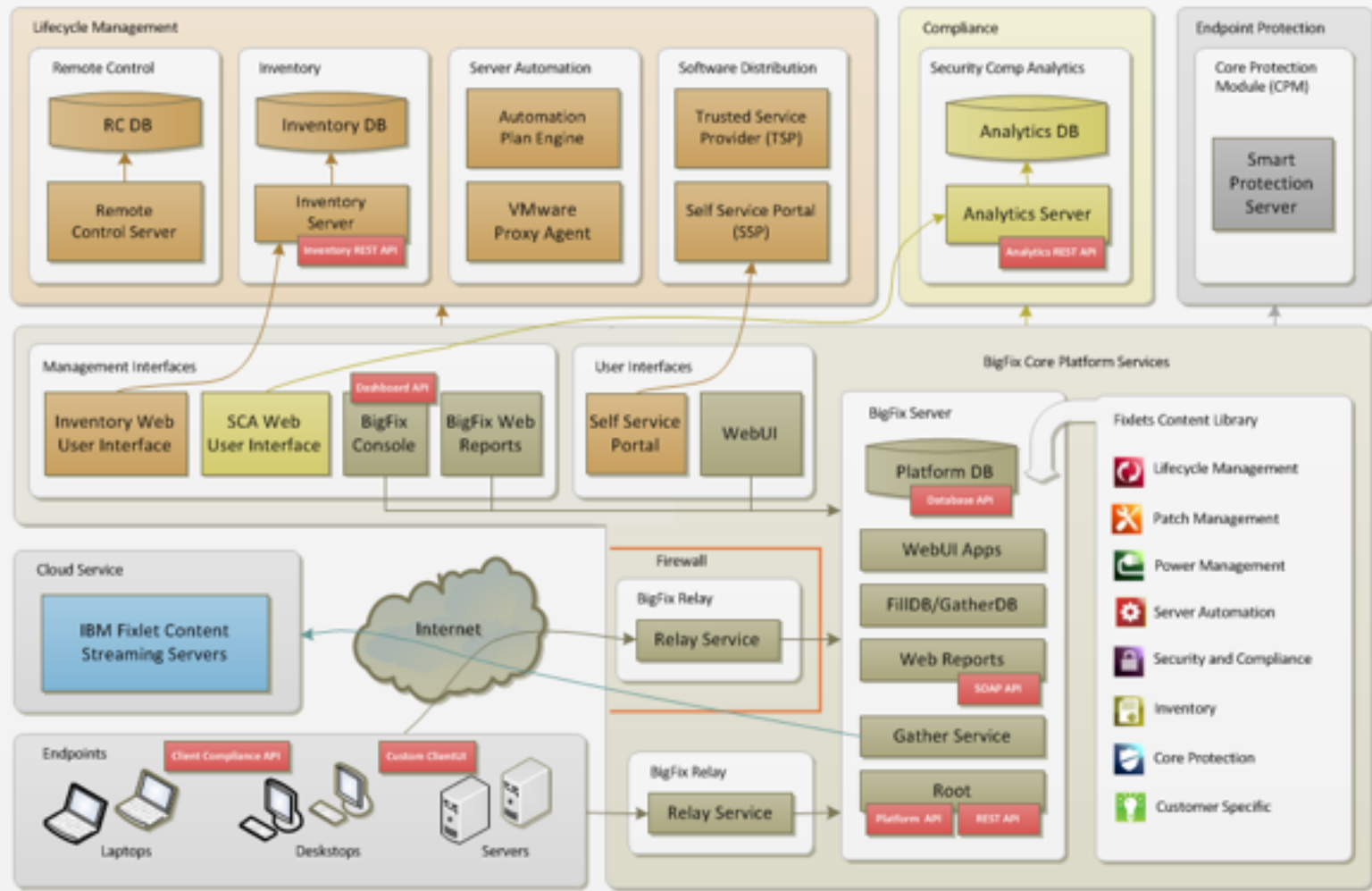
BigFix Relevance & ActionScript Language

- Foundational scripting language used for all
 - Fixlets, Tasks, Analyses, Baselines, Properties
 - Same language construct across all components
- High level non-procedural 4GL
- Cross platform for Windows, UNIX, Linux, and Mac OS X

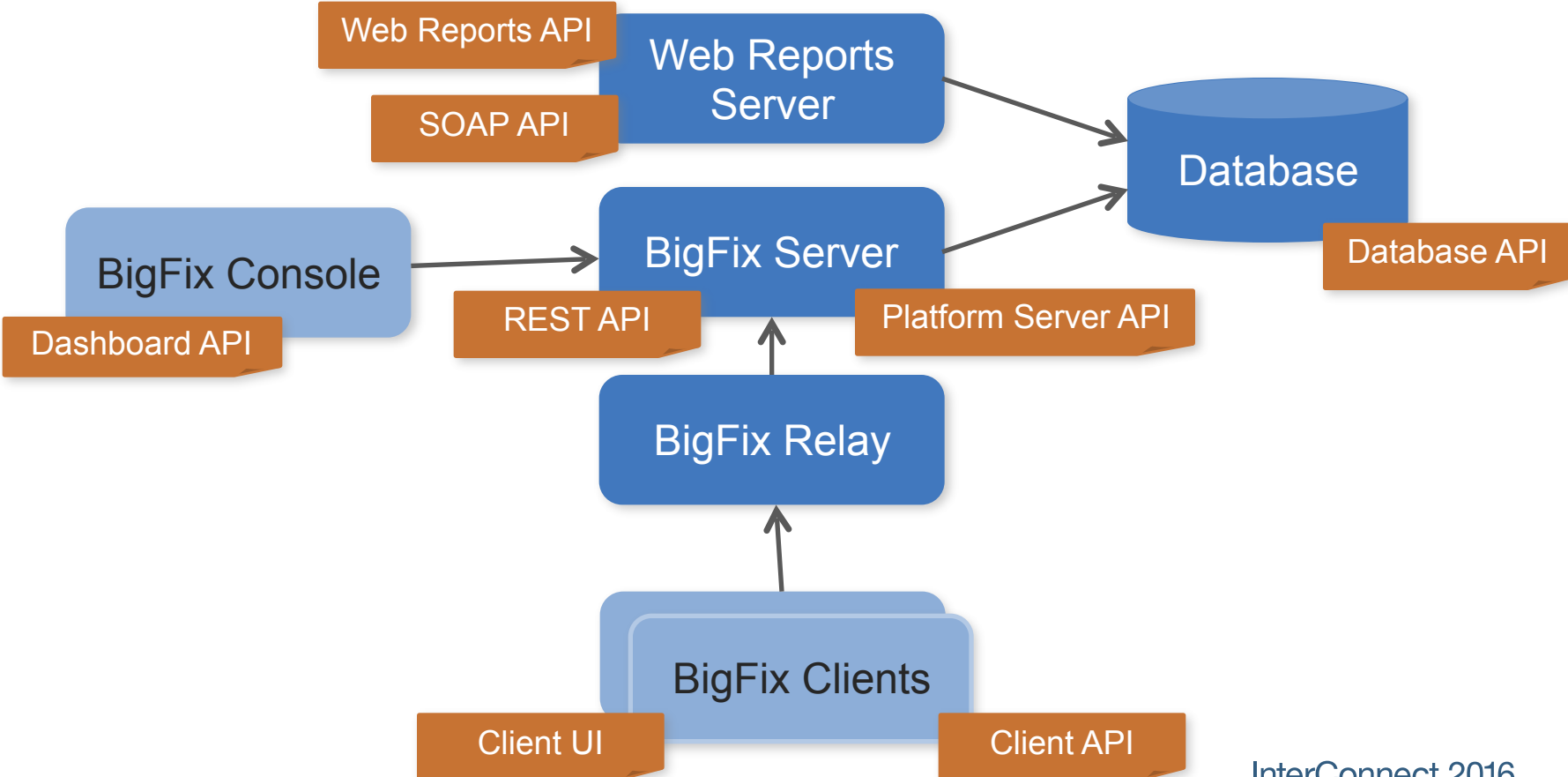


```
Q: (family name of it,
A: Core 17-4870HQ, Ger
A: Core 17-4870HQ, Ger
A: Core 17-4870HQ, Ger
A: Core 17-4870HQ, Ger
A: Core 17-4870HQ, Ger
A: Core 17-4870HQ, Ger
A: Core 17-4870HQ, Ger
A: Core 17-4870HQ, Ger
A: Core 17-4870HQ, Ger
T: 524
Q:

(qna)* - Fixlet Debugger
File Edit View Debug Help
(xna)* | E (single clause) | < (graphical) | (action)
QnA
q: (vendor name of it, family name of it, speed of it) of processors
A: GenuineIntel, Celeron, 2494000000 hertz
A: GenuineIntel, Celeron, 2494000000 hertz
A: GenuineIntel, Celeron, 2494000000 hertz
A: GenuineIntel, Celeron, 2494000000 hertz
```



BigFix APIs



InterConnect 2016

The Premier Cloud & Mobile Conference

Client Side APIs



February 21 – 25
MGM Grand & Mandalay Bay
Las Vegas, Nevada

BigFix Client APIs

API	Execute Against	Language / Interface	Read or Write	Popularity (10 – high, 1 – low)	Demo / Uploaded
Client API	BigFix Client	Client Relevance / MS COM	Read	2	Yes / Yes
Client UI	BigFix Client	HTML, Client Relevance / -	Read	2	Yes / No

Client API

- Microsoft COM based API
- Used to query BigFix Client for endpoint information
- Commonly used to interface with other endpoint agents (e.g. NAC), or custom end-user applications
- Allows BigFix partners and integrators to expose the results of an endpoint inspection conducted by the BigFix Client to their own logic embedded in 3rd-party clients executing on the client machine
- Potential use cases
 - Detect if security products (anti-virus, firewall) are installed or running
 - Detect that wireless networks are disabled
 - Patch status on the endpoint

Client API – Example Client API Tester

Big/ix Client API Tester (Version 9.2)

File Help

```
values of headers "Subject" of
relevant fixlets
  whose (value of header "X-Fixlet-Source-Severity" of it = "Critical")
of site whose (name of it = "Enterprise Security")|
```

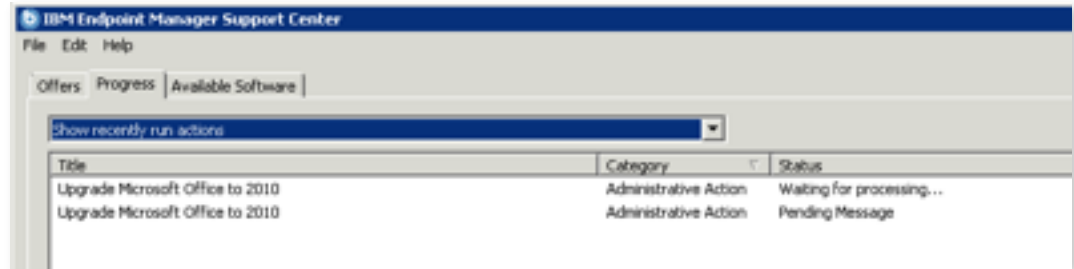
MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Server 2008 R2 SP1 - KB3078601
MS15-081: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - Office 2010 SP2 - KB2553313
MS15-109: Security Update for Windows Shell to Address Remote Code Execution - Windows Server 2008 R2 SP1 - KB3080446 (x64)
MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Office 2007 SP3 - KB3085616
MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows Server 2008 R2 SP1 - KB3109094
MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows Server 2008 R2 SP1 / Windows 7
MS15-130: Security Update for Microsoft Uniscribe to Address Remote Code Execution - Windows Server 2008 R2 SP1 - KB3108670 (x64)
MS16-004: Security Update for Microsoft Office to Address Remote Code Execution - Office 2010 SP2 - KB3114553
MS16-005: Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution - Windows Server 2008 R2 SP1 - KB3124000
MS16-006: Security Update for Silverlight to Address Remote Code Execution - Silverlight 5 Developer Runtime - KB3126036 (x64)

Items: 10 Evaluation time: 00:00:03.011

Devote CPU while processing Sort Results Continuously Evaluation Evaluate

ClientUI Customization

- The Client Dashboard provides a standard UI for user interactions
 - Offers
 - Progress of actions
 - Available Software
- 2 additional tabs can be customized
 - Dashboard
 - Technician Mode (Ctrl-Alt-Shift-T)



ClientUI Customization - Dashboard

The screenshot displays the IBM BigFix Support Center interface. At the top, there is a navigation bar with 'Offers', 'Progress', and 'Dashboard' tabs. The main content area is titled 'Computer Health Monitoring' and includes a sub-header 'Powered by BigFix' and a timestamp 'Page last updated: Sat, 06 Feb 2016 20:20:14 -0600 Refresh'.

The first section is 'Computer Information', which contains a table with the following data:

Computer Name	TNTIN
Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
CPU	Intel(R) Core(TM) i7-4870HQ CPU @ 2.50GHz
Memory	8192 MB
Hard Disks	C: 85791 MB (7 percent free)
IP Address	192.168.1.74

The second section is 'Microsoft Security Hotfixes Missing (148 items)'. It includes a paragraph explaining that Microsoft provides security updates on the second Tuesday of each month. Below this is a table listing missing hotfixes:

ID	Severity	Release Date	Security Hotfix
KB2520155	Unspecified	11 Mar 2011	2520155: DNS Host record of a computer is deleted after you change the DNS server assignment - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
KB2617858	Unspecified	21 Sep 2011	2617858: Unexpectedly slow startup or logon process in Windows Server 2008 R2 or in Windows 7 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
KB3099862	Critical	08 Dec 2015	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB3099862 (x64)
KB3126036	Critical	12 Jan 2016	MS16-006: Security Update for Silverlight to Address Remote Code Execution - Silverlight 5 Developer Runtime - KB3126036 (x64)

ClientUI Customization – Technician Mode

The screenshot displays the BigFix ClientUI in Technician Mode. The window title is "BigFix Support Center" and the menu bar includes "File", "Edit", and "Help". The navigation tabs are "Offers", "Progress", "Dashboard", and "Technician". The main content area is titled "Detailed Computer Information" and includes a sub-header "Technician Mode - Powered by BigFix" and a refresh link. Below this is a "Computer Information" section with a table of system details.

Computer System	
Computer Name:	TINTIN
System Model:	VMware, Inc. VMware Virtual Platform
Service Tag:	VMware-56 4d 19 8c 04 2e 60 2e eb 4b 8 31 56 80 02 8b
Serial Number:	None
Motherboard:	Intel Corporation 440BX Desktop Reference Platform
Display Adapter:	VMware SVGA 3D
Display Monitor:	
Operating System	
Name:	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1 (Build 7601)
Version:	6.1.7601
Product ID:	55041-567-4893297-84616
Registered User:	Windows User
Installation Date:	2012-12-27
Uptime:	0 days
Last Boot Up Time:	2016-02-06
Language:	English (United States)

CPU

InterConnect 2016

The Premier Cloud & Mobile Conference

Server Side APIs



February 21 – 25
MGM Grand & Mandalay Bay
Las Vegas, Nevada

BigFix Server APIs

API	Execute Against	Language / Interface	Read or Write	Popularity (10 – high, 1 – low)	Demo / Uploaded
REST API (Platform)	BigFix Server	Any Language / HTTPS	Read / Write	10	Yes / No
REST API (Inventory)	Inventory Server	Any Language / HTTPS	Read / Write	3	No / No
REST API (SCA)	Security Compliance Analytics Server	Any Language / HTTPS	Read / Write	3	No / No
Platform Server API	BigFix Server	Any Language / MS COM	Write	4	Yes / Yes
Database API	BigFix Database	SQL / (ODBC, ADO, JDBC)	Read	3	Yes / Yes
SOAP API	Web Reports	Session Relevance / SOAP	Read	5	Yes / Yes
Dashboard API	BigFix Console	Session Relevance / -	Read / Write	2	Yes / No

Database API

- The Database API is a published schema describing Views to the underlying tables
- All information collected from managed endpoints available from the database
- Any programming language that has an ODBC interface can be used to access the database
- Used only for reads, no writes
- Some fields are stored as binary data to be extracted with function
 - `Fn_Extractfield()`
- [Online documentation](#)

Database API – Example to extract comp properties

The screenshot displays the SQL Server Enterprise interface. On the left, the Object Explorer shows the database structure, with the 'Columns' folder expanded under 'dbo.BES_COLUMN_HEADINGS'. The main window shows a query window with the following SQL code:

```
select
    A.ComputerID,
    A.Value,
    B.Name,
    B.Value
from BES_COLUMN_HEADINGS A,
BES_COLUMN_HEADINGS B
where
    A.ComputerID = B.ComputerID and
    A.Name = 'Computer Name' and
    A.Value like 'TINTIN%'
```

The Results pane shows the output of the query, which is a table with 5 columns: ComputerID, Value, Name, and Value. The data is as follows:

	ComputerID	Value	Name	Value
1	11577043	TINTIN	Computer Name	TINTIN
2	11577043	TINTIN	OS	Win2008R2 6.1.7601
3	11577043	TINTIN	CPU	2500 MHz Celeron
4	11577043	TINTIN	Last Report Time	Sat, 20 Feb 2016 03:56:39 +0000
5	11577043	TINTIN	Locked	No
6	11577043	TINTIN	Lock Expiration	
7	11577043	TINTIN	BES Relay Selection Method	Manual
8	11577043	TINTIN	Relay	BES Root Server
9	11577043	TINTIN	Distance to BES Relay	0
10	11577043	TINTIN	BES Relay Service Installed	BES Root Server
11	11577043	TINTIN	Relay Name of Client	tintin
12	11577043	TINTIN	DNS Name	tintin
13	11577043	TINTIN	Active Directory Path	<none>
14	11577043	TINTIN	Client Administrators	__op_10 __op_2
15	11577043	TINTIN	Client Settings	ITSIT_Deny=0 ITSIT_Scanner_Debug=0 ITSIT_Scanner...
16	11577043	TINTIN	IP Address	169.254.194.249

The status bar at the bottom indicates that the query was executed successfully, returning 37 rows in 00:00:00. The current user is tintin (10.50 SP1) and the server is TINTIN\jeewei (72).

Database API – Example to extract Fixlet info

The screenshot displays the SQL Server Enterprise interface. On the left, the Object Explorer shows the database structure for 'dbo.BES_OBJECT_DEFS', with the 'Columns' folder expanded to show fields like 'Name', 'Source Severity', 'Source Release Date', 'Category', and 'Download Size'. The main window shows a SQL query that uses the 'dbo.fn_ExtractField' function to extract these fields from the 'BES_OBJECT_DEFS' table, filtering for records where 'IsFixlet = 1' and the 'Name' starts with 'MS16-004'.

```
select
    Name,
    dbo.fn_ExtractField('Source Severity', 0, Fields) as "Source Severity",
    dbo.fn_ExtractField('Source Release Date', 0, Fields) as "Source Release Date",
    dbo.fn_ExtractField('Category', 0, Fields) as "Category",
    dbo.fn_ExtractField('Download Size', 0, Fields) as "Download Size"
from BES_OBJECT_DEFS
where
    IsFixlet = 1 and
    Sitename like '%Enterprise Security%' and
    Name like 'MS16-004'
```

The query results are displayed in a table with the following columns: Name, Source Severity, Source Release Date, Category, and Download Size. The table contains 16 rows of data, all representing cumulative security updates for Internet Explorer (MS16-001).

	Name	Source Severity	Source Release Date	Category	Download Size
1	MS16-001: Cumulative Security Update for Intern...	Critical	12 Jan 2016	Security Update	54415320
2	MS16-001: Cumulative Security Update for Intern...	Moderate	12 Jan 2016	Security Update	44805580
3	MS16-001: Cumulative Security Update for Intern...	Critical	12 Jan 2016	Security Update	40428857
4	MS16-001: Cumulative Security Update for Intern...	Moderate	12 Jan 2016	Security Update	54415320
5	MS16-001: Cumulative Security Update for Intern...	Critical	12 Jan 2016	Security Update	12800380
6	MS16-001: Cumulative Security Update for Intern...	Critical	12 Jan 2016	Security Update	30966705
7	MS16-001: Cumulative Security Update for Intern...	Moderate	12 Jan 2016	Security Update	15181547
8	MS16-001: Cumulative Security Update for Intern...	Moderate	12 Jan 2016	Security Update	40428857
9	MS16-001: Cumulative Security Update for Intern...	Moderate	12 Jan 2016	Security Update	30966705
10	MS16-001: Cumulative Security Update for Intern...	Critical	12 Jan 2016	Security Update	29426701
11	MS16-001: Cumulative Security Update for Intern...	Moderate	12 Jan 2016	Security Update	16151363
12	MS16-001: Cumulative Security Update for Intern...	Moderate	12 Jan 2016	Security Update	22085513
13	MS16-001: Cumulative Security Update for Intern...	Moderate	12 Jan 2016	Security Update	11288537
14	MS16-001: Cumulative Security Update for Intern...	Critical	12 Jan 2016	Security Update	16151363
15	MS16-001: Cumulative Security Update for Intern...	Critical	12 Jan 2016	Security Update	23810260
16	MS16-001: Cumulative Security Update for Intern...	Critical	12 Jan 2016	Security Update	55896184

At the bottom of the window, a status bar indicates that the query was executed successfully, returning 190 rows.

SOAP API

- XML based SOAP API for querying objects in the BES Web Reports
- Results returned as XML documents
- Used only for reading

SOAP API – Example Session Relevance Tester

The screenshot displays a web browser window titled "Filelets - Critical MS patches last 30 days.tsr - BigFix Session Relevance Tester". The browser's address bar shows the URL "http://localhost:8080/". The page content is divided into two main sections: a code editor and a results list.

Code Editor: The code editor contains the following XQL query:

```
1// All Microsoft critical patches released within the last 90 days
2
3names of bes fixlets whose (
4  name of site of it = "Enterprise Security" and
5  source severity of it = "Critical" and
6  (current date - source release date of it) < 90*day
7  and name of it as lowercase does not contain "oorrupt")
```

Results: The results section displays a list of 16 items, each representing a Microsoft patch. The items are as follows:

- MS16-001, MS16-002, MS16-005, MS16-007, MS16-008, 3118753: Cumulative Update for Windows 10 - Windows 10 - KB3124266
- MS16-001, MS16-002, MS16-005, MS16-007, MS16-008, 3118753: Cumulative Update for Windows 10 - Windows 10 - KB3124266 (x64)
- MS16-001, MS16-002, MS16-005, MS16-007, MS16-008, 3118753: Cumulative Update for Windows 10 - Windows 10 Version 1511 - KB3124263
- MS16-001, MS16-002, MS16-005, MS16-007, MS16-008, 3118753: Cumulative Update for Windows 10 - Windows 10 Version 1511 - KB3124263 (x64)
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 10 - KB3124275
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 10 - KB3124275 (x64)
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 11 - KB3124275
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 11 - KB3124275 (x64)
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 8 - KB3124275
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 8 - KB3124275 (x64)
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 9 - KB3124275
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 9 - KB3124275 (x64)
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 8 Gold - IE 10 - KB3124275
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 8 Gold - IE 10 - KB3124275 (x64)
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 8.1 Gold - IE 11 - KB3124275
- MS16-001: Cumulative Security Update for Internet Explorer - Windows 8.1 Gold - IE 11 - KB3124275 (x64)
- MS16-001: Cumulative Security Update for Internet Explorer - Windows Vista SP2 - IE 7 - KB3124275

At the bottom of the browser window, the status bar shows "Results: 46 items returned" and "Evaluation time: 00:00:00.561 | Connected to trln:52312 as leavel - Web Reports Version: 3.2.6.34".

Platform Server API

- Microsoft COM based API
- Full programmer's interface into creating Fixlets/Tasks/Properties/Actions/Analysis in BigFix
- Callable from languages such as Java, VBScript, JavaScript, Perl, C, C++, .NET, and etc.
- Often used to replicate functionality of the BigFix Console

Platform Server API – Example Bricks

The screenshot displays the Bricks (v1.1) management console interface. The main window is titled "Bricks (v1.1) - TINTIN : Win2008R2 6.1.7601". The interface is divided into several panes:

- Search Computer:** A search bar and a table of computers. The table has columns for Computer, Operating System, and Last Report Time. The selected computer is TINTIN, Win2008R2 6.1., with a last report time of 2016/02/21 22:49.
- Computer Details:** A navigation pane showing "Applicable Tasks (115)" categorized by site. The selected task is "BES Client Setting: CPU Usage".
- Task Configuration:** A table of tasks with columns for ID, Task Name, Source Severity, Site Name, and Source. The selected task is ID 168, "BES Client Setting: CPU Usage", with a source severity of <Unspecified> and source of BES Support.
- Description:** A text box explaining the task: "The BES Client is designed to use only a small fraction of the computer's CPU (< 1-2%) on average. Use the options below to configure the BES Client to use more CPU (and work faster) or use less CPU (and work slower)." It includes a note about default settings and an important note about locked clients.
- Actions:** Two action items: "Click [here](#) to set the BES Client to use very low CPU usage (< .5%). (Not Recommended)" and "Click [here](#) to set the BES Client to use default CPU usage (< 1-2%)."
- At a Glance:** A sidebar with three gauges: "3 mins ago Last Report Time", "16.71% Free Space System Disk", and "91.11% OS Patch Compliance".

At the bottom, a message pane shows: "Messages (Connected to IEM Server Tintin - version 9.2.6.94) Retrieving all the actions and links for this task..."

REST API

- Perform the majority of tasks present in the console via a standardized and operating system independent method
- Communicates over HTTPS
- Results in either XML or JSON
- The only API that allows performing
 - Visibility / read functions, e.g. get info
 - Control / write functions, e.g. take actions

REST API – Example Excel Connector

The screenshot shows the Microsoft Excel interface with the BES BigFix Connector ribbon. The main spreadsheet displays a table with the following data:

Computer Name	CPU
CSDMQ	3.60 GHz Intel Core i5-35
Fern's MacBook Pro	3.60 GHz Intel Core i5-35
leiva	AMD Phenom II X2 3.1 GHz
WIN-DP9775HMT13	3.90 GHz Intel Core i7-43
2003-SE-SERVER	3.60 GHz Intel Core i5-34
MINILAT	3.20 GHz Intel Core i7-55
SIADELL	AMD Phenom II X2 3.1 GHz
FernMac	3.90 GHz Intel Core i7-43
lorbes	3.60 GHz Intel Core i5-35
PDNING	3700 MHz Core i7-3740Q
Aberlard-364406	AMD Phenom II X2 3.1 GHz
Aberlard-889316	3.60 GHz Intel Core i5-35
Ambrose-701776	3.90 GHz Intel Core i7-43
Anslem-070597	AMD Phenom II X2 3.1 GHz
Anslem-489420	AMD Phenom II X2 3.1 GHz
Antiochus-035464	3.20 GHz Intel Core i7-56
Antiochus-786743	3.20 GHz Intel Core i7-56
Aristotle-364943	3.60 GHz Intel Core i5-34
Aristotle-581731	3.60 GHz Intel Core i5-34
Aristotle-609164	3.20 GHz Intel Core i7-55
Augustine-433055	3.60 GHz Intel Core i5-35
Augustine-600400	AMD Phenom II X2 3.1 GHz
Augustine-948180	3.90 GHz Intel Core i7-43
Aurelius-142246	3.20 GHz Intel Core i7-56

The dialog box 'Attributes Available for BES Computers' shows a list of attributes with checkboxes. The 'Selected' list includes: Computer Name, CPU, OS, Last Report Time, IP Address, Distance to BES Relay, Client Administrators, Client Settings, Computer Name, Computer Type, Current User, Device Type, Distance to BES Relay, DNS Name, Free Space on System Drive, ID, and Total Size of System Drive. The 'Group Analysis Properties' section is checked, and the 'Concatenate Multi-Value Results' checkbox is also checked.

Dashboard API

- Provides an interface to author own dashboard, create customize views
- Manifests as:
 - Custom report in Web Reports
 - Dashboard in the Console
 - Wizard in the Console
- Uses XML to hook into Console and Web Reports
- Typical technologies used:
 - Data extraction: Session Relevance
 - Logic processing: JavaScript
 - Presentation formatting: HTML

Dashboard API

IBM BigFix Console

File Edit View Go Tools Help Debug

Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console

All Content

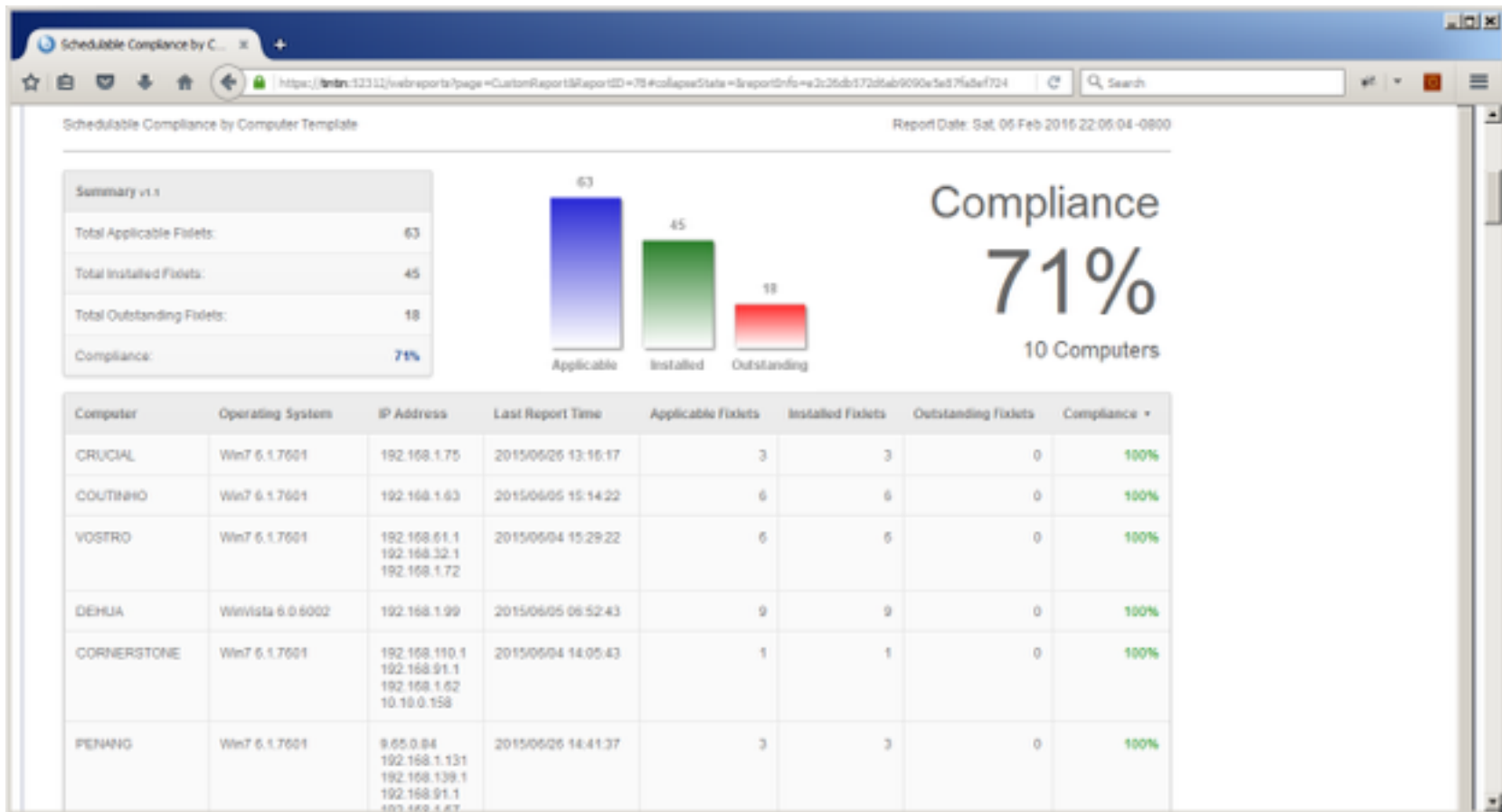
National Vulnerability Database CVE Dashboard

Search 1293 items

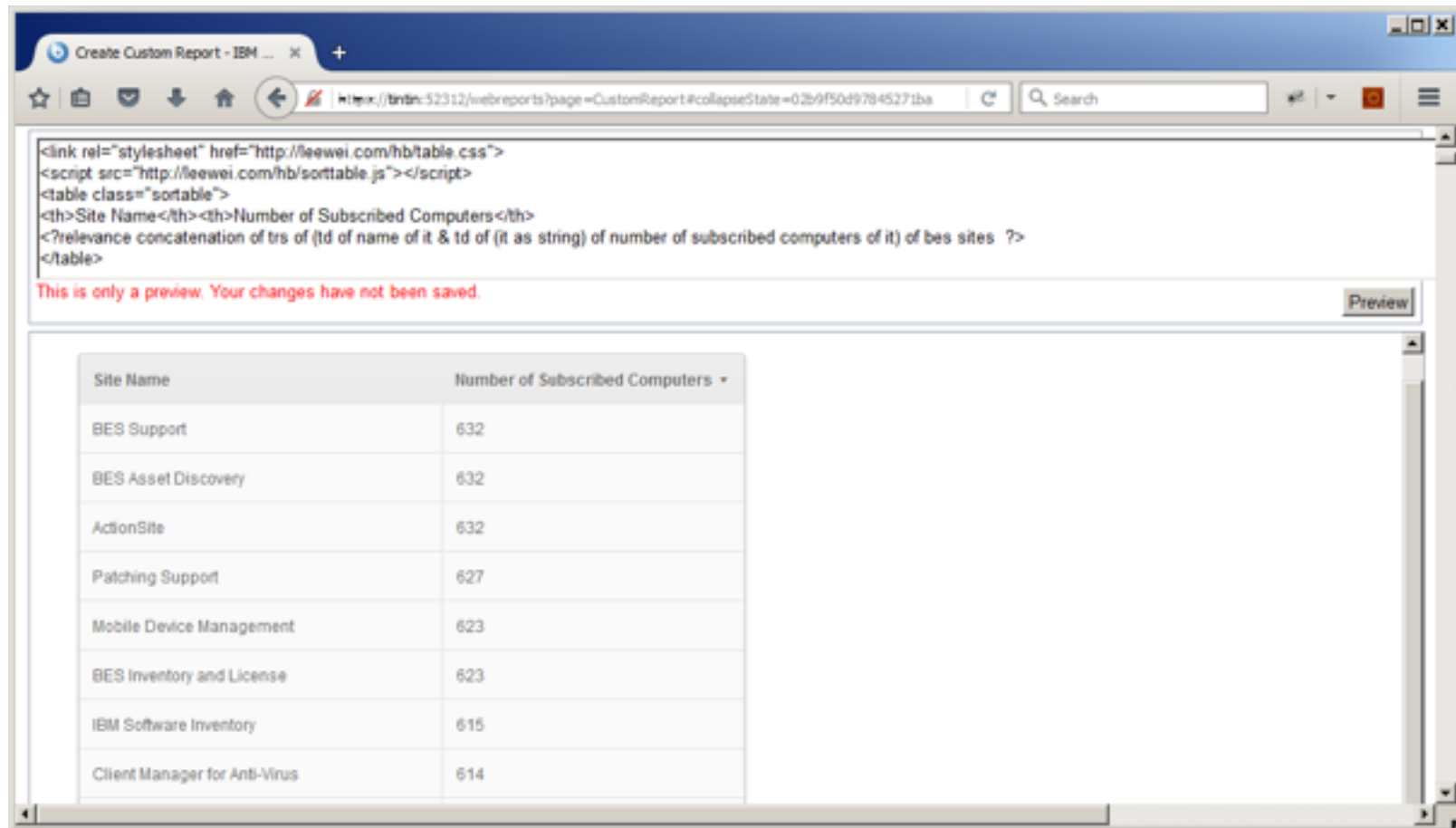
CVE ID	Published Date	CVSS Score	Related Fixlets	Applicable Computers	Summary
CVE-2015-0001	2015-01-13	1.9	13	21	The Windows Error Reporting (WER) component in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to bypass the Protected Process Light protection mechanism and read the contents of arbitrary process-memory locations by leveraging administrative privileges, aka "Windows Error Reporting Security Feature Bypass Vulnerability."
CVE-2015-0002	2015-01-13	7.2	2	43	The AfxVerifyAdminContext function in aocache.sys in the Application Compatibility component in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not verify that an impersonation token is associated with an administrative account, which allows local users to gain privileges by running AppCompatCache.exe with a crafted DLL file, aka MSRC ID 20544 or "Microsoft Application Compatibility Infrastructure Elevation of Privilege Vulnerability."
CVE-2015-0003	2015-02-10	6.9	82	32	win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges or cause a denial of service (NULL pointer dereference) via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."
CVE-2015-0004	2015-01-13	7.2	35	142	The User Profile Service (aka ProfSvc) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges by conducting a junction attack to load another user's UserClass.dat registry hive, aka MSRC ID 20674 or "Microsoft User Profile Service Elevation of Privilege Vulnerability."
CVE-2015-0005	2015-03-11	4.3	19	0	The NETLOGON service in Microsoft Windows Server 2003 SP2, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 Gold and R2, when a Domain Controller is configured, allows remote attackers to spoof the computer name of a secure channel's endpoint, and obtain sensitive session information, by running a crafted application and leveraging the ability to sniff network traffic, aka "NETLOGON Spoofing Vulnerability."
CVE-2015-0006	2015-01-13	6.1	27	131	The Network Location Awareness (NLA) service in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not perform mutual authentication to determine a domain connection, which allows remote attackers to trigger an unintended permissive configuration by spoofing DNS and LDAP responses on a local network, aka "NLA Security Feature Bypass Vulnerability."
CVE-2015-0008	2015-02-10	8.3	27	140	The UNC implementation in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not include authentication from the server to the client, which allows remote attackers to execute arbitrary code by making crafted data available on a UNC share, as demonstrated by Group Policy data from a spoofed domain controller, aka "Group Policy Remote Code Execution Vulnerability."

Connected to 'win7' as user 'Server'

Web Reports



Web Reports



The screenshot shows a web browser window titled "Create Custom Report - IBM ...". The address bar contains the URL: `http://tntn:52312/webreports?page=CustomReport#collapseState=02b9f50d97945271ba`. The main content area displays the following HTML code:

```
<link rel="stylesheet" href="http://feewei.com/hb/table.css">
<script src="http://feewei.com/hb/sortable.js"></script>
<table class="sortable">
<th>Site Name</th><th>Number of Subscribed Computers</th>
<?relevance concatenation of trs of (td of name of it & td of (it as string) of number of subscribed computers of it) of bes sites ?>
</table>
```

Below the code, a red warning message states: "This is only a preview. Your changes have not been saved." A "Preview" button is located to the right of this message.

The preview shows a table with the following data:

Site Name	Number of Subscribed Computers
BES Support	632
BES Asset Discovery	632
ActionSite	632
Patching Support	627
Mobile Device Management	623
BES Inventory and License	623
IBM Software Inventory	615
Client Manager for Anti-Virus	614

Where to get Presentation and Demos

- This deck and all associated demos and apps are available here

<http://leewei.com/interconnect2016>

Notices and Disclaimers

Copyright © 2016 by International Business Machines Corporation (IBM). 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 according to the terms and conditions of the agreements under which they are provided.

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 is in compliance with any law

Notices and Disclaimers Con't.

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 in connection with 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 PARTICULAR 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, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services®, Global Technology Services®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli®, Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, 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.

Thank You

InterConnect 2016
The Premier Cloud & Mobile Conference

Your Feedback is Important!

Access the InterConnect 2016 Conference Attendee Portal to complete your session surveys from your smartphone, laptop or conference kiosk.



February 21 – 25
MGM Grand & Mandalay Bay
Las Vegas, Nevada