

Smarter technology for a smarter planet.

IBM Tivoli® Endpoint Manager *built on BigFix technology*

Introduction to Tivoli Endpoint Manager 8.2

Michael Carr – mcarr@us.ibm.com

Tivoli Endpoint Manager Advisory Software Engineer



Tivoli Endpoint Manager, *Built on BigFix Technology*

IBM Tivoli® Endpoint Manager



Tivoli Endpoint Manager for
Security and Compliance



Tivoli Endpoint Manager for
Lifecycle Management



Tivoli Endpoint Manager for
Software Use Analysis



Tivoli Endpoint Manager for
Patch Management



Tivoli Endpoint Manager for
Power Management



Tivoli Endpoint Manager for
Core Protection



IBM Endpoint Manager for
Mobile Devices

Using Tivoli Endpoint Manager, organizations can:

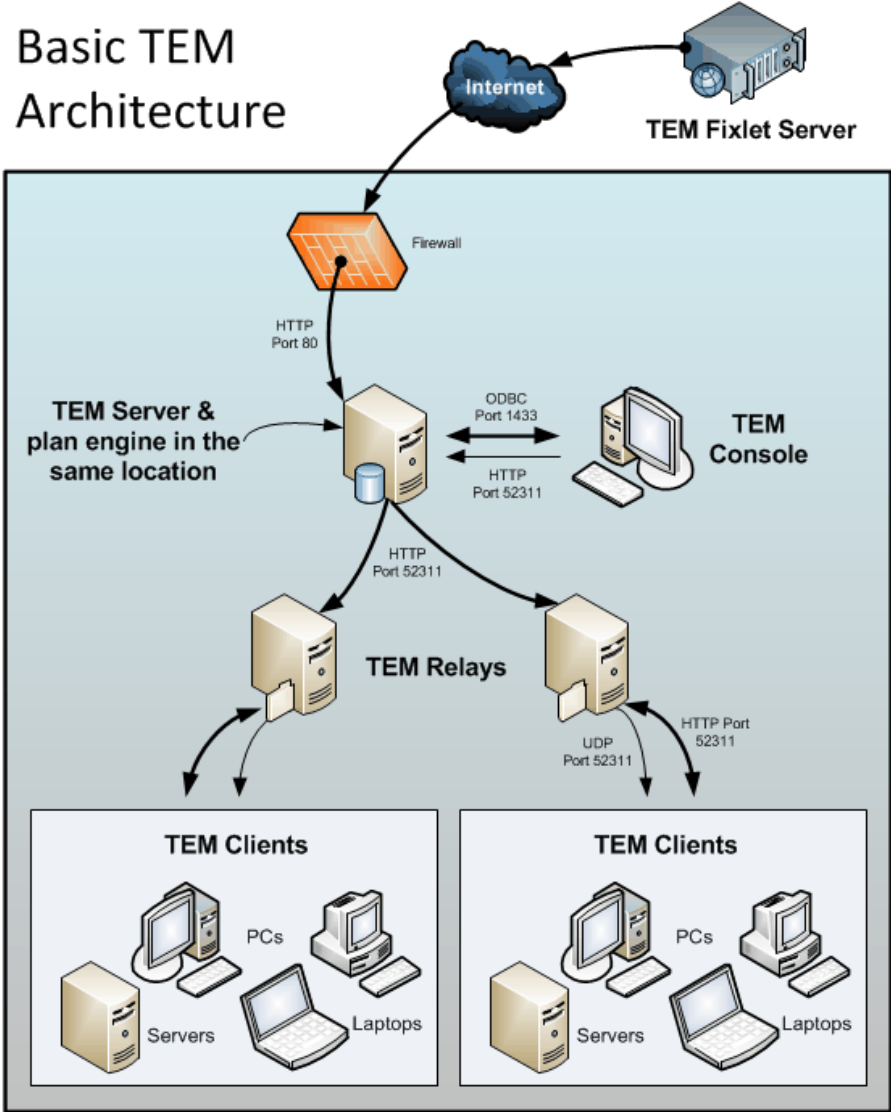
- See all endpoints: physical, virtual, fixed or mobile
- Fix issues anywhere in minutes, regardless of bandwidth or connectivity
- Deploy in days, over any network or geography
- Achieve continuous compliance – across platforms
- Simplify operations and enjoy rapid time to value





TEM Architecture

Basic TEM Architecture





Console Overview - Computers

Tivoli Endpoint Manager Console

File Edit View Go Tools Help Debug

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

All Content << Computers Search Computers

Computer N...	OS	CPU	Last Report Time	Average Eval Loop	Locked	BES Relay Selec...
WR1	Win2003 5.2.3790	2700 MHz Xeon	12/21/2012 9:57:19 PM	1	No	Manual
WINXP	WinXP 5.1.2600	2700 MHz Xeon	1/11/2013 10:55:10 PM	5	No	Manual
WIN2K3X64	Win2003 5.2.3790	2700 MHz Xeon	1/11/2013 10:53:58 PM	2	No	Manual
WIN2K1	Win2000 5.0.2195	2700 MHz Xeon	1/11/2013 10:55:07 PM	6	No	Manual
sles1164	Linux SuSE Enterprise Server 11 (2.6.27.48-0.12-default)	2700 MHz Xeon	1/11/2013 10:50:59 PM	0	No	Manual
rhel5564	Linux Red Hat Enterprise Server 5.5 (2.6.18-194.17.4.el5)	2700 MHz Xeon	1/11/2013 10:52:52 PM	0	No	Manual
PC-201	Win2000 5.0.2195	2700 MHz Xeon	1/11/2013 10:55:32 PM	4	No	Manual
BES	Win2003 5.2.3790	2700 MHz Xeon	1/11/2013 10:58:36 PM	3	No	Manual

Computer: WR1

Edit Settings Remove From Database Send Refresh

Summary Relevant Fixlets and Tasks (271) Relevant Baselines (0) Baseline Component Applicability Action History (0) User Management Rights (2) Role Management Rights (1)

[\[collapse all\]](#) / [\[expand all\]](#)

Computer Properties

Core Properties

- Active Directory Path TMC / Computers / WR1
- OS Win2003 5.2.3790
- CPU 2700 MHz Xeon
- DNS Name wr1.TMC.com
- IP Address 10.1.3.16
- IPv6 Address <none>
- Last Reported 12/21/2012 9:57:19 PM
- Locked No

8 items in list, 1 selected. Connected to 'BES.TMC.com' as user 'operator'



Console Overview – Sites

The screenshot displays the Tivoli Endpoint Manager Console interface. On the left, a tree view shows the 'Sites' hierarchy, with 'Patches for Windows (English)' selected. The main pane shows the configuration for this site, including a 'Details' section with fields for Type, Current Version, Gather URL, and Publisher. Below this is a 'Subscription' section with a text area for 'External Subscription Constraints' containing a relevance rule. The bottom status bar indicates the user is connected to 'BES.TMC.com' as 'operator'.

External Site: Patches for Windows (English)

Save Changes | Discard Changes | Gather | Add Files... | Remove

Details | Computer Subscriptions | Operator Permissions | Role Permissions

Details

Type	External Content Site
Current Version	1,705
Gather URL	http://sync.bigfix.com/cgi-bin/bfgather/bessecurity
Publisher	BigFix, Inc.

Subscription

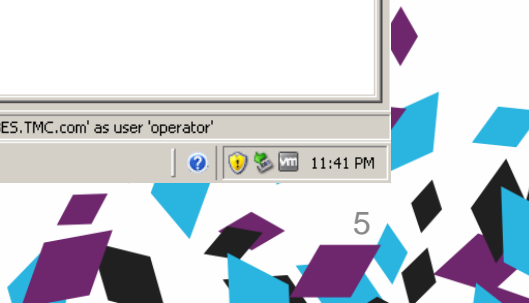
All clients that satisfy the externally defined criteria are subscribed to this site.

External Subscription Constraints

Site Level Relevance

```
(if( name of operating system starts with "Win" ) then platform id of operating system != 3 else false) AND (if exists property "in proxy agent context" then ( not in proxy agent context ) else true )
```

Connected to 'BES.TMC.com' as user 'operator'





Console Overview – Fixlets & Tasks

The screenshot displays the Tivoli Endpoint Manager Console interface. On the left, a tree view shows the navigation structure, including 'All Content', 'Sites (24)', 'External Sites (21)', and 'Fixlets and Tasks (240)'. The main area shows a table of Fixlets and Tasks. The selected item is MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4 - Windows XP SP3 / Windows Server 2003 SP2 / Windows Vista SP2 ...

ID	Name	Source Severity	Site	Applicable Com...	Open Action C
1300405	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET...	Important	Patches for Win...	1 / 6	0
1207725	MS12-077: Cumulative Security Update for Internet Explorer - IE 8 - Windows XP SP3	<Unspecified>	Patches for Win...	1 / 6	0
1207409	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - ...	Important	Patches for Win...	1 / 6	0
1300407	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET...	Important	Patches for Win...	1 / 6	0
1203423	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framew...	Critical	Patches for Win...	1 / 6	0

Fixlet: MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4 - Windows XP SP3 / Windows Server 2003 SP2 / Windows Vista SP2 ...

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (1) | Action History (0)

Description

Microsoft has released a security update that resolves four privately reported vulnerabilities in the .NET Framework. The most severe of these vulnerabilities could allow elevation of privilege if a user views a specially crafted webpage using a web browser that can run XAML Browser Applications (XBAPs). The vulnerabilities could also be used by Windows .NET applications to bypass Code Access Security (CAS) restrictions. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the logged-on user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

After downloading and installing this update, affected computers will no longer be susceptible to these vulnerabilities.

Note: Affected computers may report back as 'Pending Restart' once the update has run successfully, but will not report back their final status until the computer has been restarted.

Note: Microsoft has announced that this update may be included in a future service pack or update rollup.

Note: This security update is also referenced under KB2742595.

File Size: 11.1 MB

Actions

Click [here](#) to initiate the deployment process.

240 items in list, 1 selected. Connected to 'BES.TMC.com' as user 'operator' 11:43 PM



Console Overview - Actions

Take Action

Name: Create in domain:

Preset: Show only personal presets

Target

Target:

Specific computers selected in the list below

All computers with the property values selected in the tree below

The computers specified in the list of names below (one per line)

By Retrieved Properties

- By Computer Name
- By OS
- By CPU
- By Last Report Time
- By Average Eval Loop
- By Locked
- By BES Relay Selection Method
- By Relay
- By User Name
- By RAM
- By Free Space on System Drive
- By Total Size of System Drive
- By Subnet Address
- By BES Relay Service Installed
- By Agent Version
- By site
- By Group

This action will be targeted at all computers with the retrieved property values selected on the left. There are currently 8 computers with the selected property values.

Any computers that change to match the selected property values while the action is open will be targeted as well.

This action will end 1/13/2013 11:44:04 PM, client local time. See the Execution tab for more details.



Properties

Manage Properties

- All Properties (819)
 - By Category
 - By Site
 - BES Asset Discovery (19)
 - BES Inventory and License (208)
 - BES Support (55)
 - BigFix Labs (6)
 - Client Manager for Endpoint Protection (143)
 - GTS SCM Windows (179)
 - GTS Support (4)
 - Master Action Site (5)
 - Patches for ESXi (7)
 - Patches for Windows (English) (1)
 - Patching Support (10)
 - Power Management (63)
 - Predefined (6)
 - Reserved (23)
 - SANS Top Vulnerabilities to Windows Systems (6)
 - Software Distribution (3)
 - Tivoli Endpoint Manager for Software Usage Analysis (1)
 - Virtual Endpoint Manager (28)
 - By Analysis

Name	Activated	Site	Analysis	Period	Category
Actionsite Size	Globally	BES Support	BES Health Checks Analysis	15 minutes	BES He
Actionsite Version	Globally	BES Support	BES Health Checks Analysis	Every Report	BES He
AntiPest 2 Extension Version	Globally	BES Support	BES Client Logging Service V...	1 day	
AntiVirus Extension Version	Globally	BES Support	BES Client Logging Service V...	1 day	
BES API Version	Globally	BES Support	BES Component Versions	Every Report	
BES Client Download Throttling	Globally	BES Support	Bandwidth Throttling Status	Every Report	
BES Client Dynamic Download Throttli...	Globally	BES Support	Bandwidth Throttling Status	Every Report	
BES Client Helper Status	Globally	BES Support	BES Client Helper Service	Every Report	BES Cli
BES Client Logging Service Version	Globally	BES Support	BES Client Logging Service V...	1 day	
BES Client Version	Globally	BES Support	BES Component Versions	Every Report	
BES Client's Parent Relay	Globally	BES Support	BES Relay Status	Every Report	
BES Console Version	Globally	BES Support	BES Component Versions	Every Report	
BES Relay Cache Size	Globally	BES Support	BES Relay Cache Information	1 day	
BES Relay Download Throttling	Globally	BES Support	Bandwidth Throttling Status	Every Report	
BES Relay Drive Info	Globally	BES Support	BES Relay Cache Information	1 day	
BES Relay Dynamic Download Throttli...	Globally	BES Support	Bandwidth Throttling Status	Every Report	
BES Relay Free Disk Space	Globally	BES Support	BES Health Checks Analysis	Every Report	BES He
BES Relay Installed Status	Globally	BES Support	BES Relay Status	Every Report	
BES Relay Total Outbound Dynamic T...	Globally	BES Support	Bandwidth Throttling Status	Every Report	
BES Relay Total Outbound Throttling	Globally	BES Support	Bandwidth Throttling Status	Every Report	
BES Relay Used Action Cache	Globally	BES Support	BES Relay Cache Information	1 day	
BES Relay Used Download Cache	Globally	BES Support	BES Relay Cache Information	1 day	
BES Relay Version	Globally	BES Support	BES Component Versions	Every Report	
BES Relay's Parent Relay	Globally	BES Support	BES Relay Status	Every Report	
BES Server Total Outbound Dynamic ...	Globally	BES Support	Bandwidth Throttling Status	Every Report	
BES Server Total Outbound Throttling	Globally	BES Support	Bandwidth Throttling Status	Every Report	
BES Server Version	Globally	BES Support	BES Component Versions	Every Report	
RFS Web Reports Version	Globally	RFS Support	RFS Component Versions	Every Report	

Name: BES Health Checks::Actionsite Size

Relevance: `if (exists main gather service) then ((sum of sizes of files of client folder of site "actionsite") / 1024) as string & " KB") else "N/A"`

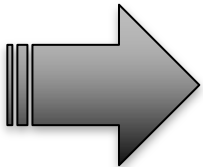
Evaluate: 15 minutes

Buttons: Add New, Delete, Make Custom Copy, Export...



Legacy Solutions

TEM Smart Agent



Traditional compliance



Continuous compliance



Tivoli Endpoint Manager 8.2 IBM Tivoli® Endpoint Manager

Supported Platforms



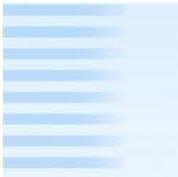
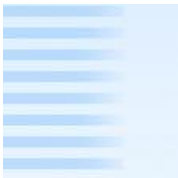
Supported Agents

AIX	Mobile Devices *
CentOS	Android
ESX Server	iOS
HP-UX	Windows Mobile
Mac OSX	Symbian
Oracle Enterprise Linux	
Red Hat Linux	
Solaris	
SUSE	
Windows	
zLinux	





TEM AVP Team



Mike Bell	DHS CBP, DHS ICE, EPA, FBI
Michael Carr	Citi, IBM GTS, Sears, Wal-mart
Aram Eblighatian	Bank of America, Deutsche Bank, Federal Reserve, Morgan Stanley, Wal-mart
Michael Paishon	Dept of Justice
Dan Reamy	Veterans Affairs
John Riddle	Bank of America
Jack Ruben	Dept of Transportation
Bianca Sancio	FBI
Joe Saylor	IBM CIO, Intel, Kaiser Permanente

