Microsoft® | Services

Critical Situation Post Mortem Briefing

Users in Integrated Case Management system are experiencing widespread performance issues

114050711422886 / 114052311469931
June 13, 2014

Prepared For: BC Government

Prepared By
Ed Capko
Senior Technical Account Manager
Microsoft Canada Enterprise Services

Critical Situation Summary

Premier Support Case #	Technical Account Manager	Account Name	Microsoft Product
114050711422886	Ed Capko	BC Government	Windows Server / IIS
114052311469931	Ed Capko	BC Government	Windows Server / Networking

Incident Overview:

ICM has seen that access to the application is impacted intermittently. When the issue occurs all users see greatly increased response times that grow until the application is unusable.

Operational/Business Impact:

End users are disconnected and not able to log in and use the system until the system is recycled.

Current Status:

Full user load is working as expected. There are minor user disconnect incidents being worked on separately.

Troubleshooting Steps:

1. Reviewed available logs and analyzed for additional insight
2. Provided recommendations on additional enabling and running diagnostic tools to help identify root cause
3. Provided OS and IIS tuning recommendations as a parallel path
4. Provided all integrators analysis on findings
5. Under a separate case (114052311469931) provided t/shooting and guidance to help determine why pings to the IIS Server failed May 23rd
6. Provided why Performance Monitors show gaps during monitoring on the IIS servers and how to resolve
7. Validated that user performance issue indicators pointed to 3rd party owned components and Microsoft Premier services closed out

Root Cause Analysis:

Over the course of the troubleshooting performed many different factors were investigated including SiteMinder and Siebel performance, browser versioning differences, potential network issues as well as IIS performance. At this time none of the avenues has proved to be 100% conclusive and we are archiving the issue since the problem has not returned. If the issue does recur please let us know as soon as possible so we can reopen the Service Request and resume troubleshooting.

Recommendations:

1. Ensure that recommended Microsoft tuning is kept in place and diagnostic tools understood on how to enable as needed, to capture detailed statistics to speed up root cause analysis.
2. Develop detailed current state documentation of the end to end architecture and develop a “configuration management database” to identify core dependencies when changes are to be applied to prevent downtime.
3. Capture baseline performance metrics of all components to identify anomalies. Establish a capacity management process to review periodically.
4. Execute periodic disaster recovery tests.
5. Monitoring tool – end to end application checking at a granular level is not available. Look at Microsoft System Center Operations Manager which can do end to end application testing across different platforms (Oracle, etc).
6. Execute previously recommended Microsoft “health checks” on the core Microsoft products used and execute a remediation plan to address health/risk issues:
    a. Windows Server IIS Risk Assessment
    b. Windows Security Configuration Assessment or alternatively a Microsoft Security Risk Assessment (review against checklist of host configuration, security process and network environment)
7. IIS/OS service provider staff to be educated in how to effectively troubleshoot complex Windows / IIS through a Premier delivered Windows Advanced Troubleshooting workshop and IIS troubleshooting chalk talk.
8. Engage your Technical Account Manager sooner when issues occur to provide guidance on how to support root cause analysis more effectively in the future.
9. Prior to this incident, your TAM had started a “Proactive Service Maturity Review” with the ICM team (Cindy Beaton coordinator). This review is a high level look at your processes to identify current state, expected future goals based on process maturity. The interview has been completed and the next step is for your TAM to complete the assessment and report back with findings. Once this is done, this should be also reviewed as there are several overlaps with this incident, but may have other gaps that need to be addressed.

Incident Comments:

Through the course of the incident, in reviewing lessons learned outside of the technical work, the following information is share from an outsider perspective as food for thought.

1. As different parties became engaged at different points, it was not clear what the scope and when the incident would be determined to be resolved. Have a detailed written document to be shared as individuals were added, would be beneficial in the future.
2. As different parties were involved (outside of BC Govt) the Crisis Process and administrative tools used to administer the issue had several threads going in parallel, causing some re-work and confusion. Having a detailed written document on how the administration of the issue to share with all parties in advance would help.
3. It was very effective to have a regular rhythm for status updates and decisions on a daily basis
4. Working through the incident was effective through an openness and willingness by all the integrators to collaborate and share findings as they come to the surface.
5. Having all the integrators on-site expedited analysis and communications back to the core team.

Chronology of Device Services Issues Impacting MCFD/SDSI

Report to RMG 2014-001 ICM performance issues
Action Items: 0520-02/0523-10

Report Date: June 2, 2014
Report Version: 5

Executive Summary

- On May 15, 2014 a presentation (IE Settings and ICM May 15 2014.potx) was reviewed at the 3:00 pm RMG 2014-001 ICM performance issues meeting
- On May 16, 2014 an ICM IE sub-SWAT group was formed to review IE Settings and other workstation related concerns. In addition – ICM desired workstation setting are being reviewed.
- This report provides the current major findings of the ICM IE sub-SWAT – summary and details of Device Services issues impacting MCFD/SDSI including IBM remediation completed, in progress and planned. The potential impact to the ICM end user has been provided from Device Services understanding of the ICM application behaviour.

Executive Summary

- A number of additional desired workstation settings have just been defined by ICM as per the May 15 presentation, and are being managed by the ICM IE sub-SWAT (see summary – Slides #7-9)
- The ICM IE sub-SWAT is continuing its review of a number of workstation concerns that have been reported on a limited number of workstations
- Shared Services Service BC Service Desk - 7-7000 (Option1) agents have been using support scripts, which have been updated on a daily basis to include checks and corrections as they are identified within the ICM IE sub-SWAT

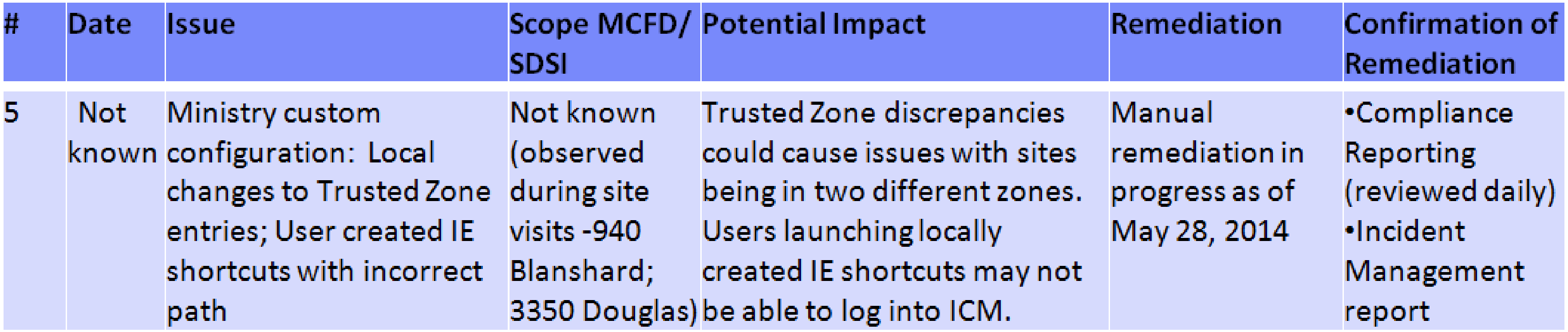
Issue Summary

#	Date	Issue	Scope MCFD/ SDSI	Potential Impact	Remediation	Confirmation of Remediation
1	Start of Workstation Refresh - December 2013	The removal of the Adobe Whitelist was not clearly identified within the CICR or Service Bulletin #519. Clients were indirectly advised. The impact was that a request for the Adobe Whitelist was received from MCFD but not requested by SDSI and as such the Adobe Whitelist was no installed on SDSI R3 workstations.	MCFD Win7 R3 = 0 SDSI Win7 R3 = 1601 (to May 26)	ICM end users may not be able to open or save PDF documents from or to some locations. Some users receive a pop-up to save PDF documents to the local device.	TBD - SCCM Electronic Software Distribution of Whitelist to SDSI R3 workstations.	Electronic Software Distribution reports, Compliance Report and manual QA checks to be performed on SDSI workstations to confirm successful roll-out
2	January 10, 2014	IE Settings script (Disable Tabbed Browsing/Disable Frame Merging) not included on MCFD Win7 R3 workstations	MCFD Win7 R3 = 1440 SDSI Win7 R3 = 0	ICM end users are unable to open multiple distinct ICM session on a single device. In the event multiple sessions are opened, data may be shared across those sessions.	May 21, 2014 – All newly imaged Win7 R3 have the settings applied May 22, 2014 - RFC #113394, Group Policy Object changes implemented (MCFD only)	•Quality Assurance review of imaging of Refresh Workstations •Compliance Reporting (reviewed daily)

Issue Summary

#	Date	Issue	Scope MCFD/ SDSI	Potential Impact	Remediation	Confirmation of Remediation
3	April 7, 2014	3,500 across the BC Government - Windows 7 workstations impacted by Microsoft update which installed Internet Explorer (IE) upgrades	MCFD/SDSI Win7 U3 = 36 Win7 R3 = 269 Total = 305	ICM not certified for IE9, 10, or 11. Using any version of IE other than IE8 may result in unexpected behavior.	April 8 – 11, 2014 - Remediation steps taken by IBM TES – Five (5) Request For Change (RFC) – deployed	Compliance Reporting (reviewed daily)
4	April 10, 2014	Remediation of Issue # 3 had unintended consequence of replacing the 32bit IE shortcuts with 64bit shortcuts in the Task Bar and Start menu. Note: Prior to current remediation - May 27 compliance reporting totals - IE shortcuts with 64bit shortcuts in the Task Bar (33) and in Start menu (32)	MCFD/SDSI Win 7 U3 = 36 Win 7 R3 = 269 Total = 305	The 32 bit Seibel active-x plug-in does not work with 64 bit IE. Users launching 64bit IE may be prompted to download/install (64 bit Seibel cab file). Users launching 64 bit IE cannot log into ICM.		•Compliance Reporting (reviewed daily) •Incident Management report

Issue Summary



#	Date	Issue	Scope MCFD/ SDSI	Potential Impact	Remediation	Confirmation of Remediation
5	Not known	Ministry custom configuration: Local changes to Trusted Zone entries; User created IE shortcuts with incorrect path	Not known (observed during site visits -940 Blanshard; 3350 Douglas)	Trusted Zone discrepancies could cause issues with sites being in two different zones. Users launching locally created IE shortcuts may not be able to log into ICM.	Manual remediation in progress as of May 28, 2014	•Compliance Reporting (reviewed daily) •Incident Management report

Note: See Slide #21 for details

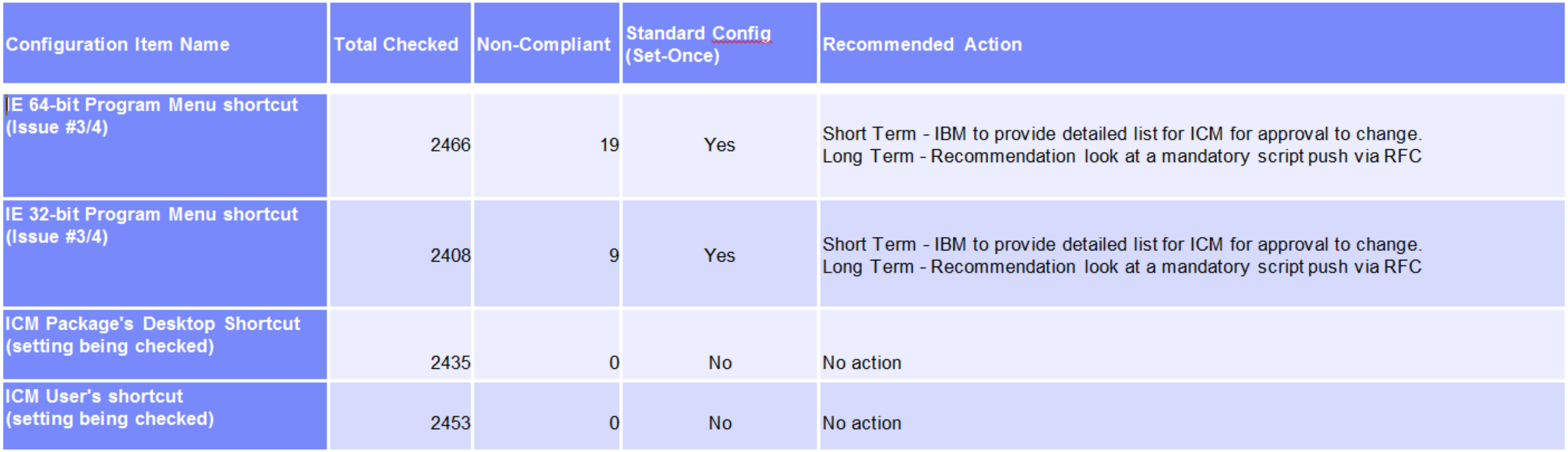
Remediation Plan (May 23 – 2:00 pm)

Configuration Item Name	Total Checked	Non-Compliant	Standard Config (Set-Once)	Recommended Action
Disable Tabbed Browsing (Issue #2)	3292	717	No	GPO released, ESD confirmed successful, 10 Test machines being QA'd
Disable FrameMerging (Issue #2)	3292	482	No	GPO released, ESD confirmed successful, 10 Test machines being QA'd
ProtectedMode (desired setting)	3292	2	Yes	Short Term - Correct virtually via registry settings. IBM to provide detailed list for ICM approval. Long Term - Recommendation set as GPO to enforce push via RFC
Local intranet (desired setting)	3292	43	Yes	Recommendation- set as GPO to enforce push via RFC.
Pop-up Blocker (desired setting)	3292	2	Yes	Short Term - Correct virtually via registry settings. IBM to provide detailed list for ICM approval. Long Term - Recommendation set as GPO enforce push via RFC
Clear Browsing History (setting being checked)	3293	2852	No	Recommendation - do not auto-update due to potential risk to Web Application performance and use. Recommendation remediation – managed on a call by call basis (Service Desk calls by client).

Remediation Plan (May 23 – 2:00 pm)

Configuration Item Name	Total Checked	Non-Compliant	Standard Config (Set-Once)	Recommended Action
AllowWindowsReuse (desired setting)	3292	3224	No	GPO released, ESD confirmed successful, 10 Test machines being QA'd
Adobe white list installed (Issue #1)	3033	909	No	MCFD has Set-Once in place, SDSI does not. This is not a mandatory package, but will investigate action to deploy to SDSI
ICM trusted site (desired setting)	2946	2946	No	No action to be taken, based on sub-SWAT discussion, Scripting modification needed for compliance reporting which was reversed logic. Pending additional results.
IE version (Issue #3/4)	3005	26	Yes	Recommendation that we roll-back to IE8 as per Executive instruction manually. IBM to provide detailed list for ICM for approval.
Default Browser (Issue #3/4)	2946	28	Yes	Short Term - IBM to provide detailed list for ICM for approval to change. Long Term - Recommendation look at a mandatory script push via RFC
Compatibility View Settings - Updated (desired setting)	2995	3	Yes	Short Term - Correct virtually via registry settings. IBM to provide detailed list for ICM approval. Long Term - Recommendation set as enforced GPO push via RFC
IE Taskbar shortcut (Issue #3/4)	2261	18	Yes	Short Term - IBM to provide detailed list for ICM for approval to change. Long Term - Recommendation look at a mandatory script push via RFC

Remediation Plan (May 23 – 2:00 pm)



Configuration Item Name	Total Checked	Non-Compliant	Standard Config (Set-Once)	Recommended Action
IE 64-bit Program Menu shortcut (Issue #3/4)	2466	19	Yes	Short Term - IBM to provide detailed list for ICM for approval to change. Long Term - Recommendation look at a mandatory script push via RFC
IE 32-bit Program Menu shortcut (Issue #3/4)	2408	9	Yes	Short Term - IBM to provide detailed list for ICM for approval to change. Long Term - Recommendation look at a mandatory script push via RFC
ICM Package's Desktop Shortcut (setting being checked)	2435	0	No	No action
ICM User's shortcut (setting being checked)	2453	0	No	No action

Issue Details

Details: Issue #1 - Adobe Whitelist

Background

- Adobe Whitelist was not listed as a mandatory application for Windows 7 R3 workstations. Clients were **indirectly** advised (via the Win 7 refresh Core Image Configuration Report (CICR) – apendex1 initial Load of packages and SB519 regarding "The removal of non-essential software from pre-installed core software") and provided with a list of options available to refresh end users for installing "zero-cost" software products. The removal of the Adobe Whitelist was not clearly identified within the CICR, P&D tool (the main tool for identifying workstation software for ministries) or SB519 (the SB focused on the most commonly used apps that were removed from core).
- MCFD submitted a project request to have Whitelist added to their Windows 7 R3 workstations.

Issue

- The removal of the Adobe Whitelist was not clearly identified within the CICR or SB519 (the SB focused on the most commonly used apps that were removed from core). Client were indirectly advised. The impact was that a specific request for the Adobe Whitelist was not submitted by SDSI.

Remediation

- As of May 23 SDSI refresh workstations deployed from the warehouse will have Adobe Whitelist included.
- Pending decision by SDSI - SCCM Electronic Software Distribution of Adobe Whitelist to SDSI R3 workstations (in production).

Evidence of Remediation

- Electronic Software Distribution reports are run 3 days from SCCM PS3 deployment.

Details: Issue #2 - IE Settings script not included on MCFD Win7 R3 workstations

Background

- **Note**: The IE settings are applied to Windows Vista and Windows 7 Upgrade 3 (U3) workstations via Group Policy.
- **September 23, 2013** – Per **iStore** #533990, **PSP** #130276, was submitted by Social Development and Social Innovation (SDSI), the client requested:
  - "The Ministry of Social Development and Social Innovation (SDSI) requests to create an SCCM published script to add the following settings to Internet Explorer for all future Refresh 3 Windows 7 workstations for SDSI and the Ministry of Children and Family Development (MCFD):"
  - Disable Tabbed Browsing
  - Disable FrameMerging
- **October 18, 2013** - The above project request was implemented by:
  - Updating the [CFD] and [SDSI] sections of the XML file used by the P&D tool. Newly created Active Directory workstation objects for CFD and SDSI would have the settings applied when imaged at the warehouse or reimaged in the field.

Details: Issue #2 - IE Settings script not included on MCFD Win7 R3 workstations

Background (continued)

- **December 2, 2013** - Per **iStore** #130261, **PSP** #130261, submitted by the Ministry of Children and Family Development (MCFD), the client requested:
  - “The Ministry of Children and Family Development (MCF) requests assistance to create an SCCM published script to set the Internet Explorer homepage for Windows 7 R3. Currently, with refresh the IE default homepage will be https://gww.gov.bc.ca/. However MCF would like it to be http://icw.mcf.gov.bc.ca/. The script package will be added to MCF mandatory Set-once. This setting will run only once when the user logs in for the first time when user profile is created. It will not re-run if user manually changes the settings
  - There will be two script packages for MCF Windows 7 R3 that relate to Internet Explorer:
  - 1) “IBM_InternetExplorerConfig_1.0_SDSI_S0” - to disable IE 8 tabbed browsing and frame merge (via PSP130276)
  - 2) Script package created by this project to set IE home page default for MCF.”
- **January 10, 2014** - The above project request was implemented by:
  - Updating the [CFD] section of the XML file used by the P&D tool. This would apply the home page setting to workstations imaged at the warehouse or any devices reimaged in the field

Details: Issue #2 - IE Settings script not included on MCFD Win7 R3 workstations

Issue

- **May 21, 2014** – As part of the ICM IE sub-SWAT looking at Internet Explorer settings IBM identified a discrepancy between the number of workstations in the Active Directory group "WS_RDM_S_IBM_InternetExplorerConfig_1.0_SDSI_U3" versus the number of combined MCFD and SDSI workstations.
- **Root Cause**: When PSP #130261 was implemented the implementer **replaced** "WS_RDM_S_IBM_InternetExplorerConfig_1.0_**SDSI**_U3" in the [CFD] section of the XML file with "WS_RDM_P_IBM_InternetExplorerConfig_1.0_**CFD**_U3" when they should have done an **add**.
- The resulting impact of this change was that all workstations objects (~1440) created in Active Directory for MCFD from that point forward were not added to the AD group "WS_RDM_S_IBM_InternetExplorerConfig_1.0_SDSI_U3", which is the group required to have the Disable TabBrowsing and Disable FrameMerge settings applied.
- Note - the custom ICM shortcuts deployed by the Ministries include command line switch that disable frame merge – the significance of this is that although the disable tabbed browsing frame merge script failed as of January 10, 2014, it if users launch ICM via the custom ICM shortcuts – then disable frame merge would be in effect. See Slide 16 notes.

Details: Issue #2 - IE Settings script not included on MCFD Win7 R3 workstations

Remediation

- Two steps were required to fully remediate:
- **May 21, 2014** – The XML file was updated to add the “IBM_InternetExplorerConfig_1.0_**SDSI**_R3” line back to the [CFD] section. All newly created AD workstation objects will have the settings applied.
- **May 22, 2014** - Per **ITIMS RFC** #113394, Group Policy Object changes were implemented to disable Tabbed Browsing and FrameMerge on all CFD Windows 7 workstations in the field.

Evidence of Remediation

- Compliance numbers as of 05/22/2014 04:28 PM (MCFD/SDSI)

Configuration Item Name	Compliance %	Compliant	Non-Compliant	Failed	Not-Detected
Disable Tabbed Browsing	55%	1766	1451	1	1
Disable FrameMerging	66%	2121	1096	1	1

- Compliance numbers as of 05/23/2014 12:45 PM (MCFD/SDSI)

Configuration Item Name	Compliance %	Compliant	Non-Compliant	Failed	Not-Detected
Disable Tabbed Browsing	77.8%	2575	717	15	1
Disable FrameMerging	84.9%	2810	482	15	1

Details: Issue #3/4: Un-intended installed Internet Explorer (IE) upgrades

Background

- Beginning on April 7, 2014, approximately 3,500 Windows 7 workstations across the BC Government by-passed the SSBC internal Enterprise Windows Server Update Services (WSUS) server when synchronization with System Center Configuration Manager (SCCM) 2012 had failed the previous day. This resulted in a direct connection to Microsoft auto update which installed Internet Explorer (IE) upgrades.

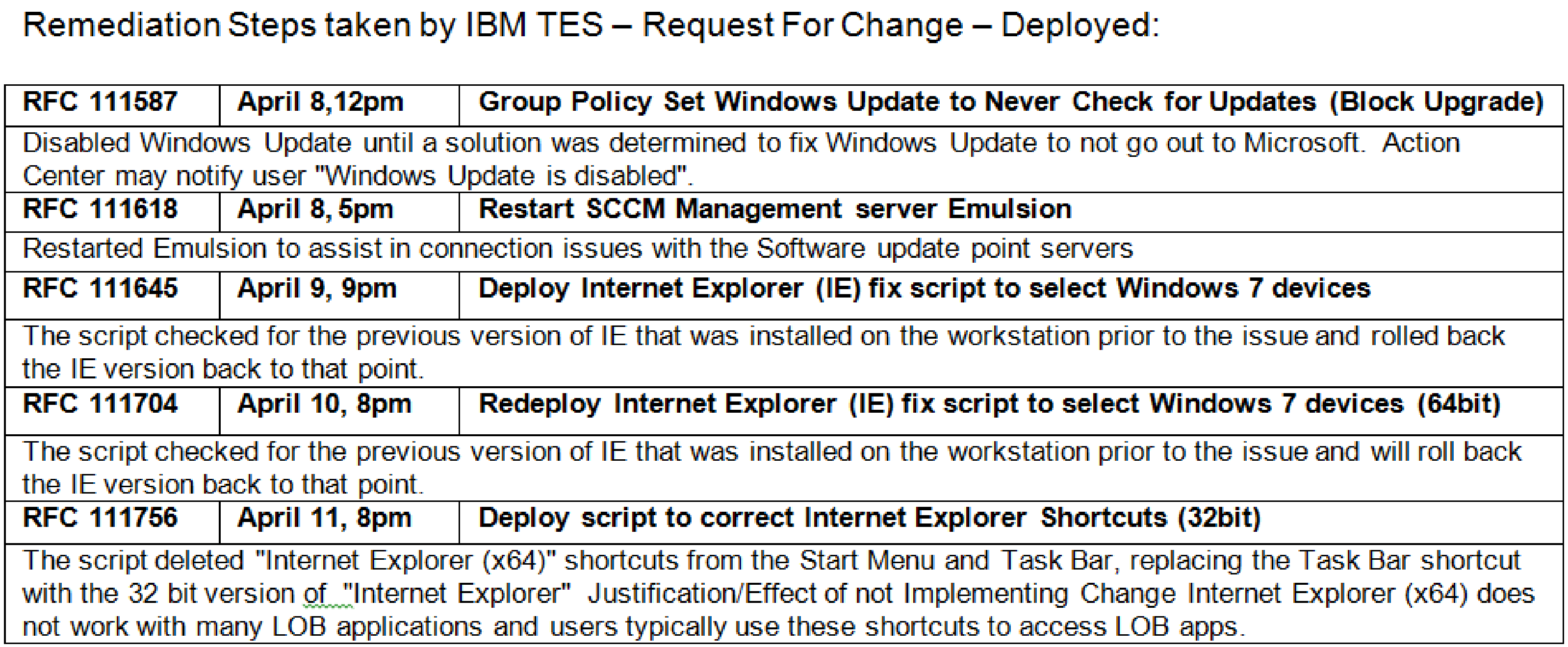
Issue

- This IE upgrade prevented some LOB applications from functioning due to their dependence on specific older versions of IE.
- The script to correct "un-intended" IE update did not work for all machines and some had to be rolled back manually
- Scope of impact to MCFD/SDSI:

Operating System	Number of workstations Impacted with IE Issues April 8th-11TH MCFD / SDSI
Vista	0
Windows 7 (U3)	36
Windows 7 (R3)	269
Total	305

Details: Issue #3/4: Un-intended installed Internet Explorer (IE) upgrades

Remediation



Remediation Steps taken by IBM TES – Request For Change – Deployed:

<table>
<tr><td><b>RFC 111587</b></td><td><b>April 8,12pm</b></td><td><b>Group Policy Set Windows Update to Never Check for Updates (Block Upgrade)</b></td></tr>
<tr><td colspan="3">Disabled Windows Update until a solution was determined to fix Windows Update to not go out to Microsoft. Action Center may notify user "Windows Update is disabled".</td></tr>
<tr><td><b>RFC 111618</b></td><td><b>April 8, 5pm</b></td><td><b>Restart SCCM Management server Emulsion</b></td></tr>
<tr><td colspan="3">Restarted Emulsion to assist in connection issues with the Software update point servers</td></tr>
<tr><td><b>RFC 111645</b></td><td><b>April 9, 9pm</b></td><td><b>Deploy Internet Explorer (IE) fix script to select Windows 7 devices</b></td></tr>
<tr><td colspan="3">The script checked for the previous version of IE that was installed on the workstation prior to the issue and rolled back the IE version back to that point.</td></tr>
<tr><td><b>RFC 111704</b></td><td><b>April 10, 8pm</b></td><td><b>Redeploy Internet Explorer (IE) fix script to select Windows 7 devices (64bit)</b></td></tr>
<tr><td colspan="3">The script checked for the previous version of IE that was installed on the workstation prior to the issue and will roll back the IE version back to that point.</td></tr>
<tr><td><b>RFC 111756</b></td><td><b>April 11, 8pm</b></td><td><b>Deploy script to correct Internet Explorer Shortcuts (32bit)</b></td></tr>
<tr><td colspan="3">The script deleted "Internet Explorer (x64)" shortcuts from the Start Menu and Task Bar, replacing the Task Bar shortcut with the 32 bit version of "Internet Explorer" Justification/Effect of not Implementing Change Internet Explorer (x64) does not work with many LOB applications and users typically use these shortcuts to access LOB apps.</td></tr>
</table>

Details: Issue #3/4: Un-intended installed Internet Explorer (IE) upgrades

Evidence of Remediation

Operating System	Number of workstations Impacted with IE Issues April 8-11 MCFD/SDSI	Number of workstations confirmed to have received remediation scripts May 21 MCFD/SDSI
Vista	0	0
Windows 7 (U3)	36	15
Windows 7 (R3)	269	299
Total	305	314

- Some totals show no progress or negative progress. The totals reflect what TES's script was able to return for workstations when found on the network. If not found, no data was returned
- Some workstations may have gone through refresh so they no longer exist

Notes

- For refreshed workstations upon first use, end users were presented with “out of the box” default pop-up (set-up) prompts. Several of these prompts empowered an end user (both Standard and Locked) to enable “Windows Auto Update”. Normally the SSBC internal enterprise WSUS server prevents direct updates from Microsoft.

The importance of the above event, is that when the SSBC internal enterprise WSUS crashed, workstations configured with windows Auto update went directly to Microsoft to obtain updates. (the text in italics below was copied from Microsoft web)
Users of Windows 7, Windows Server 2008 R2, Windows Vista and Windows Server 2008 will receive Internet Explorer 9, (same for 10 and 11) *as an important update, if they have Automatic Updates enabled, or if they perform a manual scan for updates on Windows Update.*
To prevent IE updates on Government workstations, steps were taken / applied to the SSBC enterprise WSUS, to ensure Windows Internet Explorer updates are “not automatically approved” for installation and so would not be installed via the SSBC internal enterprise WSUS.
Internet Explorer 9, (same for 10 and 11) *will not install automatically – the Automatic Updates delivery process includes a welcome screen that offers users (Standard and Locked) choices of Install, Don’t Install, and Ask Me Later prior to installation. (Windows Auto updates are installed with privileged credentials via Local System Account).*

Other issue reviewed – Intranet site to Zone script issue?

Background

- **September 2013** - The package IBM_InternetExplorerConfig_1.0_Gen_P0 was published and targeted via SCCM 2012 to all devices in the Active Directory group: WS_RDM_P_IBM_InternetExplorerConfig_1.0_Gen_U3
- The script applies the following settings:
  - Adds *.gov.bc.ca to the intranet zone 1
    Adds *.idir.bcgov to the intranet zone 1
    Sets the home page to https://gww.gov.bc.ca
- This script is a mandatory package for all the R3 workstations.

Issue

- The client reported concern that the Local Intranet zones may have had the above settings overwritten due the IE error in April.

Remediation

- None Required. Compliance reports support that the settings are still present in the Local Intranet zone.

Evidence of Remediation

- Compliance report provided to the client.

Notes

- Copy of IE Settings and ICM May 15 2014 presentation:

IE Settings and
ICM May 15 2014

- Refresh (R3) totals as of May 26, 2014 (actuals/planned)

	Actual Dec 2 to May 26	June	July	Aug	Sep	Oct	Nov	Totals
MCFD	2668	533	200	485	205	269	75	4435
SDSI	1601	266	264	309	57	227	0	2724
	4269	799	464	794	262	496	75	7159

- May 7 2014 – Keith Parkin inquired as to the default compatibility View settings on Workstations, It was confirmed the out of the box default is “compatibility view enabled” for the intranet zone.
  -

Outlook Item

Notes

- Other observations to date:
  - Analysis by the IBM onsite technician (at 940 Blanshard – May 20; 3350 Douglas – May 22) has identified:

    1. **IE default version appears consistent–** All machines were running IE 8 32 bit as the default browser. Also, the task bar icon and the Start Menu item for all machines was set to IE 8 32 bit as expected.
    2. **Trusted Site discrepancies** – It appears that local changes have been made to include ICM in the Trusted Zone. This is not required and could cause issues with sites being in 2 different zones.
    3. **IE Shortcuts -** Some users have local shortcuts set up by User/LOB/Stored on H:Drive and/or possibly imported during Workstation Refresh event, which utilize a Vista 32 bit IE path (IE folder location on the c: drive) of which the same path on win7 is for the 64 bit IE executable, causing ICM launch issues.

  - ICM/IBM/HPAS have been trouble shooting IE performance deploying 'Fiddler' (http://www.telerik.com/fiddler) debug/web analytics tool to gather statistics on performance. Microsoft (Snr Tech Acct Mgr) have subsequently commented as of present from Fiddler statistics (analysis is continuing of traces captured):
    - No significant differences between each run with data load and response times
    - Conclusion based on testing – performance issue on web servers not impacted by client IE settings.

Notes

- **Version 2 – May 27**
  - Based on feedback provided:
    - **Keith Parkin**
    - One correction on slide 7. The ICM Win 7 icons only force no frame merging, tabbed browsing would still work.
    - "C:\Program Files (x86)\Internet Explorer\iexplore.exe" -nomerge https://icm.gov.bc.ca/epublicsector_prd
    - Also the implementation of this command line option has been superseded and may stop working at any point if it hasn't already.
    - http://msdn.microsoft.com/en-us/library/ie/hh826025(v=vs.85).aspx

    - **David Blacoe**
    - Agreed to wording for Background – Slide 4
- **Version 3 – May 27**
  - Based on feedback from client:
    - Executive Summary – Slide 2 – added statement to third bullet; added new bullet:
    - The potential impact to the ICM end user has been provided from Device Services understanding of the ICM application behaviour
    - Shared Services Service BC Service Desk - 7-7000 (Option1) agents have been using the scripts, which have been updated on a daily basis to include checks and corrections as they are identified within the ICM IE sub-SWAT
    - Issue Summary – Slide 3 – added column "Potential Impact"
    - Issue Details – Slide 4 – added section page "Issue Details"

Notes

- **Version 4 – May 29**
  - Based on feedback provided:
    - **Cindy Beaton**
    - Executive Summary – content presented on two slides; Issue Summary presented on two slides; Remediation Plan moved from Notes section to after the Issue Summary and presented on three slides
    - **David Blacoe**
    - Issue Summary and Issue Details updated to reflect:
    - Issue #1: should read: “the removal of the Adobe White list was not clearly identified within the CICR or SB519 (the SB focused on the most commonly used apps that were removed from core). Client were indirectly advised. “ The impact is a specific request for the whitelist was not submitted.
      Issue #3: there should be a statement about the SSBC server that was down because this triggered the MS updates. Page 10 states it better when it says “workstations by-passed SSBC internal WSUS. The wording for Issue #3 should be: “ 3,500 workstations bypassed SSBC internal WSUS causing MS updates which installed IE upgrades.
      Issue #1 Details: The Issue needs to realign with the issue statement on Issue Sumary, as noted above
    - **Sharlene Boschma**
    - Issue #3/4 Details updated to reflect:
    - Should be a statement that the script they ran to correct “un-intended” IE update did not work for all machines and some had to be rolled back manually—in my case twice—to get corrected.
    - **Sue Goldsmith**
    - Issue Summary (Slide 4/5/6) – additional details added; Issue #5 added
    - Remediation Plan – additional details added
    - Slide 17 – addition of this text in Notes section: “Normally the SSBC internal enterprise WSUS server prevents direct updates from Microsoft.”

Notes

- **Version 5 – June 2**
  - Based on feedback provided:
  - **Cindy Beaton**
  - Executive Summary – Slide 3 – new text provided for first bullet on this slide:
    - A number of additional desired workstation settings have just been defined by ICM as per the May 15 presentation, and are being managed by the ICM IE sub-SWAT (see summary – Slides #7-9)