

Patch Management Hands-on Exercise

Background Story

You have been hired as the lead IT Administrator at the Florida International University (FIU) to manage the computers at the School of Computing and Information Sciences (SCIS), the Machine Room (MR), the Green Library (GL), and the College of Engineering and Computing (CEC). As shown in Fig. 5.1, SCIS, MR, GL, and CEC are physically located in four buildings. SCIS maintains about 200 desktop workstations in its instructional lab, MR maintains about 5 servers, GL maintains about 50 open access guest desktops, and CEC maintains about 500 PCs and laptops. The exact number and configurations of computers are not well documented. Typically, the servers run Windows 2003 and the desktop workstations, PCs, and laptops all run Windows XP. Active Directory is implemented in one of the servers, named dc, and is assigned to all computers in SCIS and GL, but not to those in CEC. As the lead IT Administrator of the organization you are responsible for ensuring that all systems run efficiently with minimal disruption of computing services to the users.



You have decided to employ a Kaseya server to help you manage all computers at SCIS, MR, GL, and CEC. Your Kaseya server is now installed and is fully operational. In addition, you have successfully deployed agents on some of the machines under your management.

At this time, operating system patches are applied on an individual basis, one computer at a time, leading into a chaotic situation where 1) since all the computers are directly obtaining their updates from the internet, each patch is downloaded multiple times resulting in an artificially high network traffic, 2) unnecessary patches are being installed which in turn consumes large amounts of disk space, and 3) the potential for bugs and security risks are increased because it's unknown if all the computers are being patched on time, or if at all.

An organized and closely monitored method is needed to facilitate and monitor distribution and application of all necessary patches to the managed computers. Kaseya's Patch Management module will allow you to accomplish all these tasks and monitor patch activities.

193

Patch Management – Hands-On Exercises

Technical Information

Your dedicated virtual environment includes the computers and network devices depicted in Fig. 5.26 and further described below:

- NAT Router: 192.168.0.1 & 192.168.1.1 & 192.168.2.1 & 192.168.3.1
- SCIS: ws1.scis.fiu.edu 192.168.0.100
- MR: dc.scis.fiu.edu 192.168.0.10 & 192.168.1.10 & 192.168.3.10
- GL: guest1.gl.fiu.edu 192.168.1.100
- CEC: pc1.cec.fiu.edu 192.168.2.100 & laptop1: laptop1.cec.fiu.edu 192.168.2.200

Note: This virtual environment includes only a limited number of representative servers and workstations physically housed in the four buildings.



Exercise

It is now time to implement policies that will keep the computers updated and avoid potential security risks by having non-patched computers within the environment. Setting up Kaseya to scan all the computers, with agents, will allow the VSA to keep a detailed record as to which patches have been installed. This detailed information will lead into informed enforcement of patch policies that which patches to automatically install (for example all security patches) and which patches to apply only after obtaining user approval (for example all optional patches). You also would like to configure Kaseya to download the patches from one central server to save bandwidth and decrease redundant network traffic. To be prepared for future deployment of computers, it would be best to set the policies to the agent templates.

Part 1

To keep an accurate record of all the patches installed on each computer, it would be best to schedule a scan, through Kaseya's VSA, to all the computers. While this is not a heavy process, it would still be best to schedule the scan during a time when the computer is otherwise idle.

-Using Scan Machine, schedule a scan to run every day at 3:00am on all the agent templates.

1. Open the Patch Management module. Go to Manage Machines > Scan Machine.

Kaseva 🔹	laster IT Service Edition	KServer -	- Operational Role SD Admin 👻 Scope scope-JohnDoe 🗸
- Raseya			You have 4 unread messages johndoe Logo
口口。7 [~ 直]	Machine ID: * Q Apply Machine Grou	ıp: < All Groups > ▼ View	w: < No View > 🔻 🖉 Edit 😨 Reset
	Go to: < Select Page > ▼ < > Show 10	 8 machines 	
Patch Management	Schedule scans for missing patches and	updates. 📝 Remind me	when machines need a patch scan scheduled.
	Run Now		
1.3 Click on the	Scan Machine link.		Skip if machine offline
Scan Machine	Unselect All Machine.Group ID	Last Scan	Next Scan Recurrence
Patch Status	dc-1.mr.fiu-johndoe	3:40:00 am 5-Jul-10	Not Scheduled
Initial Update	guest.templates.fiu-johndoe		Not Scheduled
Pre/Post Procedure	guest1.gl.fiu-johndoe	3:28:05 am 5-Jul-10	Not Scheduled
Automatic Update	instructional.templates.fiu-jo		Not Scheduled
Machine History	Iaptop1.cec.fiu-johndoe	3:27:05 am 5-Jul-10	Not Scheduled
Manage Updates	pc1.cec.fiu-johndoe	3:25:06 am 5-Jul-10	Not Scheduled
Machine Update	server.templates.fiu-johndoe		Not Scheduled
	🔕 📼	2.07.00 5 1-1.40	Net Cohedulad



- 2. Select all the agent templates.
- 3. Click on the Schedule button.



- 4. Set the scan to run *Daily* at 3:00am with a Distribution window of 1 hour.
- 5. Click on Submit.

Once	Run at 3:00:00 am Distribution window: 1 Hr
Hourly	Every: 1 day(e)
Daily	4.3 Select 3:00:00 AM.
4.1 Click on the L	
	Start/End
	Starting on: 06-Jul-10
	Ending after:
	No end date
	End after: 15 day(s)
	C Ending at:
- Europeine Options	
Execution Options	
Skip if offline (if P	ower up it offline is also checked, then skip script execution if power up failed)
Power up it offline	(Requires Wake-On-LAN or vPro and another managed system on the same LAN)
Exclude the follow	ing time range
5. Click on	the Submit button.
Submit	Cancel

Part 2

Policies are like templates in which you can approve/deny a group of patches, or an individual patch. Two policies can be created, one for all the XP machines and the other for the Windows 2003 Server machines. The policies should automatically apply all Security Updates by default on all machines and the optional updates should be set to Pending Approval. Once the patch policies are created and configured, they can be set within the designated agent templates.

Fig 5.28

Note: We are creating a W2K3 template since we only have Windows 2003 in our environment. Of course, if there are Windows 2008 servers or other servers in the environment, it would be better to name the policy for all the Windows servers as just "Servers", and for all workstations as just "Workstations".

- Create a patch policy, W2K3-PM-Policy-<**USERNAME**>, and set it to apply all future Security Updates by default. Everything else should be set to *Pending Approval*. Use a filter to deny patches that are optional and have not been superseded by other updates.

- 6. Open the Patch Management module. Go to Patch Policy > Create/Delete.
- 7. Type "W2K3-PM-Policy-<USERNAME>" under Enter name for a new patch policy.
- 8. Click on Create.

You have 5 unread messages Yo		aster IT Service Edition	KServer - Operational Role SD Admin V Scope scope
Image Machine Create Create button. patches. Initia 7. Type in W2K3-PM-Policy-johndoe in the textbox. Image Machine Enter name for a new patch policy. Enter name for a new patch policy. Image Machine Delete Delete checked patch policies. Rename a patch policy by clicking the Image icon. Select All	Казеуа 🔤		You have 5 unread messages johr
Patch Management Create Enter name for a new patch policy. Delete Delete Delete checked patch policies. Rename a patch policy by clicking the discon. Scan Machine	ᅟᅟᅟᅟᅟᅟ	Cre 8. Click on the Create button. patches. Initia 7.	Type in W2K3-PM-Policy-johndoe in the textbox.
Delete Delete G Manage Machines Delete checked patch policies. Scan Machine Select All	Patch Management	Create Enter name for a new patch policy.	
General Scan Machine Select All Select All	• • • • • • • • • • • • • • • • • • •	Delete Delete checked patch policies.	
- Scan Machine Select All	🖶 Manage Machines	Rename a patch policy by clicking the	e 🗐 icon.
	- Scan Machine	Select All	
Patch Status Unselect All Policy Name Member Count	Patch Status	Unselect All Policy Name	Member Count
Initial Update UV2K3-PM-Policy-JohnDoe 0 Show Members	- Initial Update	W2K3-PM-Policy-JohnDoe	0 Show Members
Pre/Post Procedure	- Pre/Post Procedure		
Automatic Update	- Automatic Update		
Machine History	Machine History		
a Manage Updates	🚊 Manage Updates		
Machine Update	Machine Update		
- Patch Update	- Patch Update		
Rolback	- Rollback		
Cancel Ug 6. Click on the Create/Delete link.	Cancel Up 6. Click on the Cre	ate/Delete link.	
Patch Policy	Patch Policy		
Create/Delete	- Create/Delete		
Membership	Membership		
Approval by Policy	Approval by Policy		

- 9. Go to Patch Policy > Approval by Policy.
- 10. Select "W2K3-PM-Policy-<USERNAME>" under the Policy dropdown list.
- 11. Click on the green checkmark for all the *Security Update* rows. The Green checkmark is under the column *Default Approval Status*.
- 12. Make sure the other rows' Default Approval Status is set to Pending Approval.
- 13. Click on *Total* at the bottom of the table. A new page will load up.

Sadjadi et al.



Fig 5.30



196



14. Click on Filter... A new window will open up.



- 15. Select Optional Updates from the Classification / Type dropdown.
- 16. Select Not Superseded from the Superseded dropdown.
- 17. Click on Apply.

ect Optional Updates from the ssification / Type dropdown.
ssification / Type dropdown.
•
•
ect Not Superseded from
Superseded dropdown.
•

197

Fig 5.34

- 18. Click on Select All.
- 19. Click on Deny.



- Create a patch policy, XP-PM-Policy-**USERNAME>**, and set it to all future Security Updates by default. Everything else should be set to *Pending Approval*.

- 20. Open the Patch Management module. Go to Patch Policy > Create/Delete.
- 21. Type "XP-PM-Policy-<USERNAME>" under Enter name for a new patch policy.
- 22. Click on Create.

Kaseva Ma	ster IT Serv	vice Edition		KServer - Oper	ational	Role SD Admin
• Ruscyu						You have 5 unrea
22. Click on the Creat Patch Management	e button. Pato Create	the policies to approve the policies to approve the policies to approve the policies to approve the policies to a policies to a policies to a policies to approve the policies	P-PM-Policy-jol	hndoe in th	ne textbo	X. y install approved
•	Delete	Delete checked patch po	licies.			
🖃 Manage Machines		Rename a patch policy b	y clicking the 🗐 ic	on.		
Scan Machine	Select All					
- Patch Status	Unselect All	Policy Name	Men	nber Count		
- Initial Update		VV2K3-PM-Policy-johndoe		0	Show	Aembers
- Pre/Post Procedure		XP-PM-Policy-johndoe		0	Show I	Members
- Automatic Update						
Machine History						
Manage Updates						
Machine Update						
Patch Update						
Rollback						
Cancel 20 Click on the Cre	ato/Doloto I	ink				
Patch Policy	01072/010101	inter a second s				
Create/Delete						
Membership						
Approval by Policy						

- 23. Go to Patch Policy > Approval by Policy.
- 24. Select "XP-PM-Policy-<USERNAME>" under the Policy dropdown list.

- 25. Click on the green checkmark for all the *Security Update* rows. The Green checkmark is under the column *Default Approval Status*.
- 26. Make sure the other rows' Default Approval Status is set to Pending Approval.

Kaseva Mas	ster IT Service Edition	KServer	- Operational	Role SD	Admin	 Scope scope-Joh 	
• Казсуа					Yo	u have 5	unread messages johndoe
Patch Management	Approve or de 24. Select XP-PM-Poli Initial Update and Policy XP-PM-Policy-Johndoe	cy-johndo	e in the dr Copy Appr	r <mark>opdown bo</mark> oval Statuses	x. to Policy	W2K3-P	M-Policy-johndoe 🔻
Manage Machines	Patch Approval Policy Status for XP-P	M-Policy-joh	ndoe	p	olicy View	/ Group	By: Classification -
Patch Status	Classification	Approved	25.	Click on the	Approv	ed butto	ons. Approval Status
Initial Update	Security Update - Critical (High Priority)	0	0	191	191	00	Approved
- Automatic Update	Security Update - Important (High Priority)	0	0	216	216	00	Approved
Machine History	Security Update - Moderate (High Priority)	0	0	<u>58</u>	<u>58</u>	0	Approved
Manage Updates	Security Update - Low (High Priority)	0	0	<u>19</u>	<u>19</u>	00	Approved
Machine Update	Security Update - Non-rated (High Priority)	0	0	2	<u>2</u>	0	Approved
Rollback	Critical Update (High Priority)	0	0	82	82	00	Pending Approval
Cancel Updates	Update Rollup (High Priority)	0	<u>6</u>	25	<u>31</u>	00	Pending Approval
Patch Policy	Service Pack (Optional - Software)	0	0	<u>34</u>	<u>34</u>	0	Pending Approval
Create/ 23. Click on the Appro-	ove by Policy link, - Software)	0	<u>3</u>	<u>71</u>	<u>74</u>	0	Pending Approval
Member	<u>i eature Fack (Optional - Software)</u>	0	0	<u>12</u>	<u>12</u>	0	Pending Approval
Approval by Policy	Tool (Optional - Software)	0	0	0	0	00	Pending Approval
Approval by Patch	Totals	0	<u>9</u>	26. Clic	k on the	Pendin	a Approval buttons
Configure	Click on the link Click on the icons u	s in this table nder Default i	to drill dowi Approval St	n t o me paron atus to chang	approvar o e the defai	ult status	5.

-Approve all Security Updates that have been released already for all patch policies.

- 27. Open the Patch Management module. Go to Patch Policy > Approve By Patch.
- 28. Click on Edit next to Patch View. A new window will open up.

춛 Kaseya 🛛 🗉	nterprise Edit	ion			28 0	Click on Ea	lit next to F	Patch View.	
mm, 7 km 🛍 🛛	KB Article:	Classifi	cation: All Sec	urity Updates (High Priority)	- Product: " Q.	Apply Patch Vie	w: johndoe Pa	tch View 👻 🥖	Edit
	Approve o	r deny patche	es by patch.						
Patch Management	Affects all p WARNING policies.	oatch policies r : Changing a	nanaged by a patch's appr	II administrators. Initial Update roval status from this page a	and Automatic Update only install utomatically changes the appro	approved patc oval status for	hes. r this patch i	n ALL patch	
Manage Machines	Patch Statu	ic Notes							
- Scan Machine	T atch Otatu	13 110163							
- Patch Status	Approve	Deny	/ 🗆	Show Details					
- Initial Update	Select All		Security				Approval		
- Pre/Post Procedure	Unselect All	KB Article	Bulletin	Product	Classification	Туре	Status	Published	Lang
- Automatic Update		KB2079403	MS10-051	Windows Server 2003	Security Update (Moderate)	High Priority	Mixed	10-Aug-10	Engli
Machine History		KB2079403	MS10-051	Windows XP	Security Update (Critical)	High Priority	Mixed	10-Aug-10	Engli
Manage Updates		KB2115168	MS10-052	Windows Server 2003	Security Update (Critical)	High Priority	Mixed	10-Aug-10	Engli
Machine Update	E3	KB2115168	MS10-052	Windows XP	Security Update (Critical)	High Priority	Mixed	10-Aug-10	Engli
Patch Update	E	KB2121546	MS10-069	Windows Server 2003	Security Update (Important)	High Priority	Mixed	14-Sep-10	Engli
Rollback	E	KB2124261	MS10-065	Windows Server 2003	Security Update (Important)	High Priority	Mixed	14-Sep-10	Engli
Patch Policy		KB2160329	MS10-048	Windows XP	Security Update (Important)	High Priority	Mixed	10-Aug-10	Engli
Create		100400461	MS10-053	Windows XP	Security Update (Critical)	High Priority	Mixed	10-Aug-10	Engli
Memb 27 Click on the Ar	prove by Pa	tch link. 👼	MS10.042	Windows Server 2003	Security Update (Low)	High Priority	Mixed	13_Jul_10	Engli
- Approval Policy	(m)	KB2220503	MS10.042	Windows XP	Security Update (Critical)	High Priority	Mixed	13. Jul 10	Engli
Approval by Patch		KB2251300	MS10.056	Office 2003	Security Update (Childal)	High Priority	Mixed	10 Aug 10	Larg
KB Override		KB2251399	MS10-000	Windows Sonior 2002	Security Update (Important)	High Priority	Mixed	14 Sop 10	Engli
Configure		KD2209922	MC40.057	Office 2002	Security Update (Important)	High Priority	Mixed	14-Sep-10	Engli
- Windows Auto Update		KD2204403	MC10-057	Office 2003	Security Update (Important)	High Priority	Mixed	10-Aug-10	Lang
- Reboot Action		KB2211941	MS10-056	Office 2007	Security Opdate (Important)	High Priority	Mixed	10-Aug-10	Lang
- File Source		KB2286198	MS10-046	Windows XP	Security Update (Critical)	High Priority	Mixed	2-Aug-10	Engli
-Patch Alert		KB2286198	MS10-046	Windows Server 2003	Security Update (Critical)	High Priority	Mixed	2-Aug-10	Engli
Office Source		KB2288613	<u>MS10-063</u>	Office 2003	Security Update (Important)	High Priority	Mixed	14-Sep-10	Lang
		KB2289187	<u>MS10-087</u>	Office 2003	Security Update (Important)	High Priority	Mixed	9-Nov-10	Lang
		KB2296011	MS10-081	Windows Server 2003	Security Update (Important)	High Priority	Mixed	12-Oct-10	Engli
		KB2345009	MS10-079	Office 2003	Security Update (Important)	High Priority	Mixed	12-Oct-10	Lang

29. Select All Security Updates (High Priority) from the Classification / Type dropdown.

- 30. Select Not Superseded from the Superseded dropdown.
- 31. Type "<USERNAME> Patch View" in the View Name textbox. Click on Save.

Select Patch View: johndoe Patch View 31.1 Type johndoe Patch View in the View Name to	The state of the s
View Name	johndoe Patch View
Make Public (others can view)	
KB Article	•
Security Bulletin 29 Select All Security Upd	ates (High Proiority)
Product from the Classification	7 Type dropdown.
Classification / Type	All Security Updates (High Priority)
Published (> "20070131" / Unspecified)	•
Language	* •
Approval Status	*
Title	*
Patch Status Note 30 Select Not Superse	ded from
Installation Warning the Superseded drop	Daown.
Superseded	Not Superseded -
	-

- 32. Click on Select All.
- 33. Click on Approve.

💽 казеуа	Enterprise Edi	tion							
ם מג ז ואי 🛍	KB Article:	Classific	ation: All Se	ecurity Updates (High Priority)	- Product:	Apply Patch Vie	ew: johndoe Pa	tch View 👻 🥒	Edit 🦻
	Approve of	or deny patche	s by patch.						
Patch Management	Affects all WARNING policies	patch policies m Changing a	anaged by a patch's app	all administrators. Initial Upda proval status from this page	e and Automatic Update only install automatically changes the appr	approved patc oval status fo	hes. r this patch i	n ALL patch	
Manage Machines	Patch 9 3	3 Click on t	he Appro	ove button.					
- Scan Machine	r aich g								
- Patch Status	Approve	Deny		Show Details					
 Initial Update Pre/Post Procedure 	Select All Unselect All	KB Article	Security Bulletin	Product	Classification	Туре	Approval Status	Published	Lang
- Automatic Update	32	Click on the	Select A	// link ows Server 2003	Security Update (Moderate)	High Priority	Mixed	10-Aug-10	Englis
Machine History	<u></u>	102013403	mo 10-001	www.ows XP	Security Update (Critical)	High Priority	Mixed	10-Aug-10	Englis
Manage Updates		KB2115168	MS10-052	Windows Server 2003	Security Update (Critical)	High Priority	Mixed	10-Aug-10	Englis
- Machine Opdate		KB2115168	MS10-052	Windows XP	Security Update (Critical)	High Priority	Mixed	10-Aug-10	Englis
Rollback		KB2121546	MS10-069	Windows Server 2003	Security Update (Important)	High Priority	Mixed	14-Sep-10	Englis
Cancel Updates		KB2124261	MS10-065	Windows Server 2003	Security Update (Important)	High Priority	Mixed	14-Sep-10	Englis
Patch Policy		KB2160329	MS10-048	Windows XP	Security Update (Important)	High Priority	Mixed	10-Aug-10	Englis
- Create/Delete		KB2183461	MS10-053	Windows XP	Security Update (Critical)	High Priority	Mixed	10-Aug-10	Englis
- Membership		KB2229593	MS10-042	Windows Server 2003	Security Update (Low)	High Priority	Mixed	13-Jul-10	Englis
Approval by Policy		KB2229593	MS10-042	Windows XP	Security Update (Critical)	High Priority	Mixed	13-Jul-10	Englis
Approval by Patch		KB2251399	MS10-056	Office 2003	Security Update (Important)	High Priority	Mixed	10-Aug-10	Langu
KB Override		KB2259922	MS10-067	Windows Server 2003	Security Update (Important)	High Priority	Mixed	14-Sep-10	Englis
Configure		KB2264403	MS10-057	Office 2003	Security Update (Important)	High Priority	Mixed	10-Aug-10	Langu
Pahoot Action		KB2277947	MS10-056	Office 2007	Security Update (Important)	High Priority	Mixed	10-Aug-10	Langu
- File Source		KB2286198	MS10-046	Windows XP	Security Update (Critical)	High Priority	Mixed	2-Aug-10	Englis
Patch Alert		KB2286198	MS10-046	Windows Server 2003	Security Update (Critical)	High Priority	Mixed	2-Aug-10	Englis
Office Source		KB2288613	MS10-063	Office 2003	Security Update (Important)	High Priority	Mixed	14-Sep-10	Langu
		KB2289187	MS10-087	Office 2003	Security Update (Important)	High Priority	Mixed	9-Nov-10	Langu
		KB2296011	MS10-081	Windows Server 2003	Security Update (Important)	High Priority	Mixed	12-Oct-10	Englis
		KB2345009	MS10-079	Office 2003	Security Update (Important)	High Priority	Mixed	12-Oct-10	Langu
		KB2347290	MS10-061	Windows Server 2003	Security Update (Important)	High Priority	Mixed	14-Sep-10	Englis
		1/0000007	11010.001			11.1.0		10.0.1.10	

-Set the *Policy Membership* of W2K3-PM-Policy-<*USERNAME*> to the Server machine template then set the *Policy Membership* of XP-PM-Policy-<*USERNAME*> to the Instructional and Guest templates.

- 34. Open the Patch Management module. Go to *Patch Policy > Membership*.
- 35. Select "W2K3-PM-Policy-<USERNAME>" in the list box.

Fig 5.39

- 36. Select the checkbox next to "server.templates.fiu -< USERNAME>".
- 37. Click on Add.



38. Repeat steps 34-37 for the Instructional and Guest templates.



Note: This is only one way of setting up Patch Management. The number of different configurations are endless and you should set it up to best fit your needs. There is no "right way" of setting up Patch Management, only efficient or inefficient ones.

Part 3

Downloading all the patches to a file server and distributing it to all the machines on network will allow you to save bandwidth. Configure all the templates to pull from the file server using the UNC path "\\dc\ PatchTemp" from the DC, then set the temporary directory to "C:\PatchTemp" on the dc server. The UNC path is used to point to the local address, on the DC, where the patch files are stored. If the computer cannot access DC, it should then download from the internet.

-Using File Source set up all the machines so that they download their updates from the DC. If the DC is unreachable, the machine should then download it from the Internet. The UNC path should be "\\dc\ PatchTemp" while the local directory should be "C:\PatchTemp".

- 39. Open the Patch Management module. Go to Configure > File Source.
- 40. Select all the agent templates.
- 41. Select Pulled from file server using UNC path.
- 42. Type "\\dc\PatchTemp" next to Pulled from file server using UNC path.
- 43. Select "fiu-<USERNAME>.mr" next to Machine Group Filter.

- 44. Select "dc.mr.fiu-<USERNAME>" next to File share located on.
- 45. Type in "C:\PatchTemp" next to in local directory.
- 46. Select the Download from Internet if machine is unable to connect to the file server checkbox..Click on Apply.

				and Course and InterDec	
Kaseva 🛛 🕅	laster IT Service Edition	KServer - Operational	Role SD Admin	 Scope scope-JohnDoe 	~
• • • • • • •			You have	5 unread messages johndoe Lo	qoff
mm 7 km 💼 🕷	Machine ID: * Q. Apply Machine Group: < All Groups >	▼ View: < No View >	👻 🥟 Edit	👿 Reset	
	Go to 46. Click on the Apply button. 8 machines				
Patch Management	Apply Specify location to fetch patches and updates	The destination working	directory is set	here.	
▼	Copy packages to the working directory on local drive with	most free space.			
🖃 Manage Machines 🖉	Delete package after install (from working directory)				
Scan Machine	41 Select the Pulled from file server using UNC	path radio button.	2 Type \\dc\	Patch Temp in the textbo	DX.
- Patch Status	Pulled from system server Clear Cache	, (<u> </u>	_	
- Initial Update	Pulled from file server using UNC path \\dc\patchtemp				
Pre/Post Procedure	File share located on: dc-1.mr.flu-johndoe 🔹	Hachine Group Fil	lter fiu-johndoe	. Rr 🔻	
- Automatic Update	Ctory C:\patchtemp) (12 Soloct fill inhadoo	
Machine History	44 Select dc.mr.fiu-johndoe. h files from (1) the Interr			45 Select IIu-Johnuoe.	
🖃 Manage Updates	Download from Internet if machine is unable to connect	to the 45 Type in C.	PatchTemr		
Machine Update	bownload norm internet in machine is drable to connect	netw novt to in loc	al directory	'	
Patch Update	46.1 Select the Download from	next to in loc	ar unectory.		
Rollback	Se Internet if machine is checkbox.				
Cancel Updates	Uns ch source				
Patch Policy	40.1 Select the template checkboxes ar Cache	From \\dc\patchtemp\ (or	n dc-1.mr.fiu-jo	hndoe at C:\patchtemp\ via	~
- Create/Delete	met) - To te	mp directory on drive with	most free spa	ce - Delete after install	
Membership	Clear Cache	From \\dc\patchtemp\ (or	n dc-1.mr.fiu-jo	hndoe at C:\patchtemp\ via	
Approval by Policy	Internet) - 10 te	From \\dc\patchtemp\ (or	nust tree spat	be - Delete alter Install	
Approval by Patch	U 40.2 Select the template checkboxes. Par cacle	mp directory on drive with	most free sna	re - Delete after install	Ξ
KB Override	Clear Cache	From \\dc\patchtemp\ (or	n dc-1.mr.fiu-jo	hndoe at C:\patchtemp\ via	
Configure	Internet) - To te	mp directory on drive with	most free spa	ce - Delete after install	
39 Select the File Sou	rce link. I aptop1.cec.fiu-johndoe Clear Cache Internet) - To te	From \\dc\patchtemp\ (or mp directory on drive with	n dc-1.mr.fiu-jo. most free spa	hndoe at C:\patchtemp\ via ce - Delete after install	
File Source	40.3 Select the template checkboxes ^{in Cache}	From \\dc\patchtemp\ (or	n dc-1.mr.fiu-jo	hndoe at C:\patchtemp\ via	
Patch Alert	et) - To te	mp directory on drive with	most free spa	ce - Delete after install	
Office Source	Clear Cache	From \\dc\patchtemp\ (or	n dc-1.mr.fiu-jo	hndoe at C:\patchtemp\ via	Ψ.

Part 4

Certain updates require the Windows OS to restart to finish installation. It would be best to set up the XP machines so that they restart only when a user is not online. As for the server machines, set up an email notification so that you can plan the restart and notify in advance the users of the server maintenance.

-Use Reboot Action to set the Guest and Instructor templates to Skip reboot if user logged in immediately after applying new patches and updates. Then, set the Server template to notify you immediately, via email, when a reboot is required after applying new patches and updates.

- 47. Open the Patch Management module. Go to *Configure > Reboot Action*.
- 48. Select the Guest and Instructor templates.
- 49. Click on Skip reboot if user logged in.
- 50. Click on Apply.

Fig 5.42



51. Repeat steps 47-50 for the Server template. Set the Server template to send the reboot notification to your personal email.



Note: Setting to *skip* reboot means it may take longer for the patch to take effect, thus increasing the risk of vulnerability. Therefore, it is best if all the instructional computers would be set to reboot at night automatically after an install, since these are not real user machines and we do not worry about losing open files. However if the target machines were end user machines, the best policy would be to set the workstations to "ask" and reboot if not logged in.

Part 5

Now that we have setup the patch policies to our liking, we need to setup Kaseya to apply the patches automatically to the machines.

52. Open Patch Management module. Go to Manage Machines > Automatic Update.

Enterprise Edition - Windows Internet E	ixplorer	
Http://kaseya2.cis.fiu.ec	du/vsaPres/Web20/core/KHome.aspx?firstIn=True&ReferringWeb\	VindowId=b0 • • • X Bing
👷 Favorites 🔀 Enterprise Edition		🛅 👻 🔂 👻 🖃 🖶 💌 Page 👻 Safety 👻 Tools 👻 🔞 👻
Kaseva En	terprise Edition	KServer - Operational Role SD Admin 👻 Scope scope-JohnDoe 👻
- Ruscyu -		johndoe <u>Logoff</u>
mm, 7 🗠 🗎 🛛	Machine ID: Q Apply Machine Group: fiu-johndoe	▼ View: < No View > ▼
	Go to: < Select Page > ▼ < > Show 10 ▼ 8 machines	
🞲 Patch Management	Apply Specify how to report after applying new pat	ches and undates
	Debest immediately after undate	
	Reboot infinediately alter update. Paboot every day at 12 am x :00 x after in	astall
Saan Machines	Repool every day at 12 and 500 v alter	Istall.
Datch Statue	Warn user that machine will reboot in 10 minutes (without asking permission).
Initial lindate 52 Click on Au	tomatic LIndate	
Pre/Post Procedure	in ask to reboot every 10 minutes un	til the reboot occurs. Reboot if user not logged in.
- Automatic Undate	If user logged in ask permission. Reboot if no respons	e in 10 minutes. Reboot if user not logged in.
Machine History	If user logged in ask permission. Do nothing if no resp	onse in 10 minutes. Reboot if user not logged in.
Manage Updates	Do not reboot after update. When reboot required.	send email to johndoe@flu.edu
Machine Update	Run select agent procedure before machine is reboote	ed Run select agent procedure after machine is rebooted
- Patch Update		
Rollback	Select All	
- Cancel Updates	Unselect All Machine.Group ID	Reboot action
Patch Policy	U dc.mr.fiu-johndoe	Do not reboot. Send email to johndoe@fiu.edu after update
- Create/Delete	guest.templates.fiu-johndoe	Skip reboot if user logged in
- Membership	🔘 🔲 guest1.gl.fiu-johndoe	Skip reboot if user logged in
- Approval by Policy	Instructional.templates.fiu-johndoe	Skip reboot if user logged in
Approval by Patch	Iaptop1.cec.fiu-johndoe	Skip reboot if user logged in
- KB Override	🔘 🔟 pc1.cec.fiu-johndoe	Skip reboot if user logged in
☐ Configure	Image:	Do not reboot. Send email to johndoe@fiu.edu after update
- windows Auto Update	🔘 🗉 💷 ws1.scis.fiu-johndoe	Skip reboot if user logged in
Rebool Action		
- Datab Alart		
Office Source		
Downloading picture http://kaseya2.cis.fiu.	.edu/inc/ext-3.2.0/resources/images/default/	😜 Internet Protected Mode: Off 🛛 🖓 👻 🔍 105% 👻
Enterprise Edition	Cp Adobe Captivate	🐨 🖪 🏷 😳 🖬 🕪 🎠 📲 4:30 PM 3/28/2011

53. Select all the template agents in the list.



Fig 5.44

Fig 5.43

54. Click on Schedule



- 55. Click on Daily
- 56. Set the run time to 5:00 AM with a distribution window of 1 hour.
- 57. Click on Submit

nup://kaseyaz.cis	Sinceour Common Controls/ Schedulerage.spx:CalibackeschedulerSobmicCalibackesdminitd=SobSHoszeapartitionid=LevendpL=PATCH_A0TOUPDATEdct
Recurrence	Daily Schedule Options
Once	Run at: 12:00:00 am V V Distribution window: 1 Hr V
Daily	Every: 1 day(s)
Weekly	
Monthly	
	Real Prod
	Starticno
	Starting on. 20-mar-11
	Ending after:
	Fod after 15 dov/o
	uay(s)
	C Ending at:
Execution Option	S
Skip if offline	(if 'Power up if offline' is also checked, then skip script execution if power up failed)
🔲 Power up if o	ffline (Requires Wake-On-LAN or vPro and another managed system on the same LAN)
57 Click	on Submit
Submit	Cancel
Done	Set internet Protected Mode: Off

Fig 5.46

Part 6

Now that all three agents templates contain all the patch management settings, it is time to push the settings captured in the templates to all the currently deployed agents with the similar roles.

-Copy the settings from the templates to the specified computers on the network. Server template will be used for the MR building. Instructional template will be used for the SCIS and CEC buildings. Guest template will be used for the GL building.

- 58. Open the Agent module. Go to Configure Agents > Copy Settings.
- 59. Click on select machine ID link and a new window will open up.



- 60. Select "fiu-<USERNAME>.templates" from the Group ID dropdown list.
- 61. Click on "Server" from the list of templates shown.

Fig 5.47

Fig 5.48

Pavortes Anter II Service La	🔗 Machine ID Selector - Windows Internet Explorer	* Page * Safety * Tools * 🔐 *
🔄 Kaseya 🛛 🗠	Intrp://www.witcis.fla.edu/Toolitow/machinePickec.asp?copyParamoutoue Machine D Group D	dmin v Scope scope-Jahr/Doe v
따 다 ? 🗠 📋 🛚	fu-johndoetem • Update	Post. Water
Agent	guest temptates /u-phndce v >>	
g Machine Status A Agent Status	instructional to instructional to instructional to instructional to instructional to instructional to instructional	indoe at 9.05.49 pm 7-Jul-10
- Agent Logs - Log History		indoe at 9.09.30 pm 7-Jul-10
- Event Log Settings		Evidendoe at 9.04/35 pm 7-34/10
a instal Aports		flu-johndoe at 9.04:35 pm 7-Jul-10
Depicy Agents		
Create	¥	flu-johndoe at 9.04:35 pm 7-Jul-10
Terrer .		
Charge Group		
LAN Decevery		
- LAN Wetch		
Instal Agents		
- View LAN		
View AD Computers		
- View AD Users		
Vew vPro		

62. Click the Select All under the Do Not Copy column and then select replace for Patch Settings, Patch File Source and Patch Policy Memberships, Agent Procedure Schedules and click on *Done*.



Fig 5.49



Note: When you have a schedule in Agent Procedures activity on an agent template, you need to make sure *Agent Procedure Schedules* is selected in copy settings.

- 63. Select all the computers in the MR building and click on the Copy button.
- 64. Repeat steps 52-57 for the Instructional and Guest templates.

Part 7

Windows Automatic Update can interfere with the functionality of Kaseya's Patch Management and must be disabled. While Kaseya allows you to disable Windows Automatic Update from within the Patch Management module this option cannot be implemented in a template and must be implemented by selecting agent(s) that check in.

207

-Disable Windows Automatic Update for all computers.

- 65. Open the Patch Management module. Go to Configure > Windows Auto Update.
- 66. Select all the computers.
- 67. Select Disable Disable Windows automatic Update to let patch management control system patching.
- 68. Click on Apply.

Fig 5.50



Note: If the checkboxes are missing, please wait 5-10 minutes and refresh the page as the Patch Scan is not completed yet. Checkboxes will not display for any machine that either has an operating system that does not support Windows Automatic Updates, or for which an initial Scan Machine has not been completed.



Part 8

Microsoft has just released a new KB article and it entails a new version of Internet Explorer; however, management has asked you not to install it and to prevent future installations of it via Windows Updates. KB Override is the best choice to accomplish this task since it will override all current patch policies and future patches. Using KB Override prevent Internet Explorer from being installed using the KB article (KB944036).

-Prevent Internet Explorer from installing by using KB Override.

69. Open the Patch Management module. Go to Patch Policy > KB Override.

- 70. Type in "944036" in the KB Article textbox.
- 71. Click Deny.





Note: If this patch has already been denied, it means that another administrator who shares this Kaseya server with you have already performed this task. If this is the case, you can first remove it, by clicking on the X icon, and add this setting by going through the above steps. This way, you will make sure that your work is reflected in the system logs for future reference.

Part 9

Management still needs the patch management report by the end of the work day. The patch management report should contain a brief overview of the patches. To accomplish this, you will rely on the Info Center module to generate a patch management report.

- 72. Open the Info Center module. Go to Reporting > Reports.
- 73. Click on your Private folder, "myReports-<**USERNAME**>", choose *New Report* and a new window will open up.



Fig 5.52

Enterprise Edition - Windows Internet Exercise Content of the second	xplorer u/vsaPres/Web20/core/KHome.aspx?firstln=True&ReferringWeb1	Vindowid=b0 • 47 × 5 Bing P •
🔆 Favorites 🔀 Enterprise Edition		👌 🔻 🗋 👻 🚍 🖶 👻 Page 🕶 Safety 👻 Tools 👻 🔞 👻
Kaseya Ent	erprise Edition	KServer - Operational Role SD Admin 🗸 Scope scope-JohnDoe 🗸 johndoe Loooff
Control Center C	Private 73 Click on myReports-Johndoe Image: myReports - shape Image: myReports - shape <t< td=""><td>Invate Folders You can create objects for your own use—such as reports, procedures, or montor sets—a a lober with your user name undername a Private cabled. This means only you, the creater of the objects and that does, can it with bose objects, oot them, or not before sharing the object with other users. To share a private object—such as a report, procedure, or monitor set—with other users, you have to drag and drop t into a tober undername the Shared cabled.</td></t<>	Invate Folders You can create objects for your own use—such as reports, procedures, or montor sets—a a lober with your user name undername a Private cabled. This means only you, the creater of the objects and that does, can it with bose objects, oot them, or not before sharing the object with other users. To share a private object—such as a report, procedure, or monitor set—with other users, you have to drag and drop t into a tober undername the Shared cabled.
Downloading picture http://kaseya2.cis.fiu.e	edu/vsaPres/App_Themes/0/Images/SIZE16/	😜 Internet Protected Mode: Off 🛛 🖓 👻 🔍 105% 👻
Enterprise Edition	Cp Adobe Captivate	ा 🚺 🦏 😋 🖬 🕪 隆सा 3/28/2011

- 74. Choose *Patch* in the left column.
- 75. Choose Patch Management report template.

I Ne	ew Report		75 Click on Patch Ma	nagement	? 🗆 🗙	Scope scope-JohnDoe
pp ox ining hed oort oar oar oar oar oar sho b	Audit Executive Tresheets 174 Click on Patch Path Software Software Treketing Backup Security Desktop Policy Anti-Malware	Patch Ma	A Click on Patch Ma	nagement		as reports, procedures, or monitor ha Private cabinet. This means only view thase objects, edit hem, run iders to prototype and lest an object bedure, or monitor sel—with other underneath the Shared cabinet.
				Next Car		

- 77. Leave all the default options and choose Save.
- 78. Select the newly created report under your folder then choose Run Now.

Fig 5.54



- 79. Choose "FIU-<USERNAME>" next to Organization in the new window.
- 80. Click on Submit.
- 81. Once the scheduled report is done, the report will open automatically.

C Enterprise Editi	on - Windows Interne	t Explorer	Hanna and Startin Tara Subatan			0:	
Favorites	Run Now Patch Ma	nagement - Windows Intern	et Explorer				
	http://kaseya2.cis.	fiu.edu/vsaPres/Web20/actio	ons/ClassWindowInteractionDia	ilog.aspx			
K	 Patch Mana 	agement					indoe Logoff
	Data Filters	79.	Click on fiu-johndoe				fresh
🐴 Info Cer	Organization:	fiu-johr	ndoe			~	
	Machine Group:	AI				~	
Desktop	Machine ID:	×				Q	
Inbox Reporting	Select View:	No V	'iew Selected			~	
Schedule							
Reports Report Se							
Customize							
 Dashboard View Das 							
- Layout Da							
- Dashboan - Settings							
						80 Click on S	ubmit
						Submit Can	cel
Done	lone		•	Internet Protected	Mode: Off	🖓 🔻 🔍 105%	• a 105% •
👩 🙆	Enterprise Edition	Run Now Patch	Cp Adobe Captivate		-	o 🚺 🍾 💿 🛄 🌗	5:11 PM 3/28/2011

Note: Use the report to check and see if the audit ran successfully. The report can be printed out for record keeping; however, this is not necessary for this exercise.



Patch Management – Hands-On Exercises

		-7
		4
	-/*	
ł	NLat	

Note: If your report comes out incomplete, wait 15-20 minutes before running it again. This is due to the patch scan not being completed in time.