

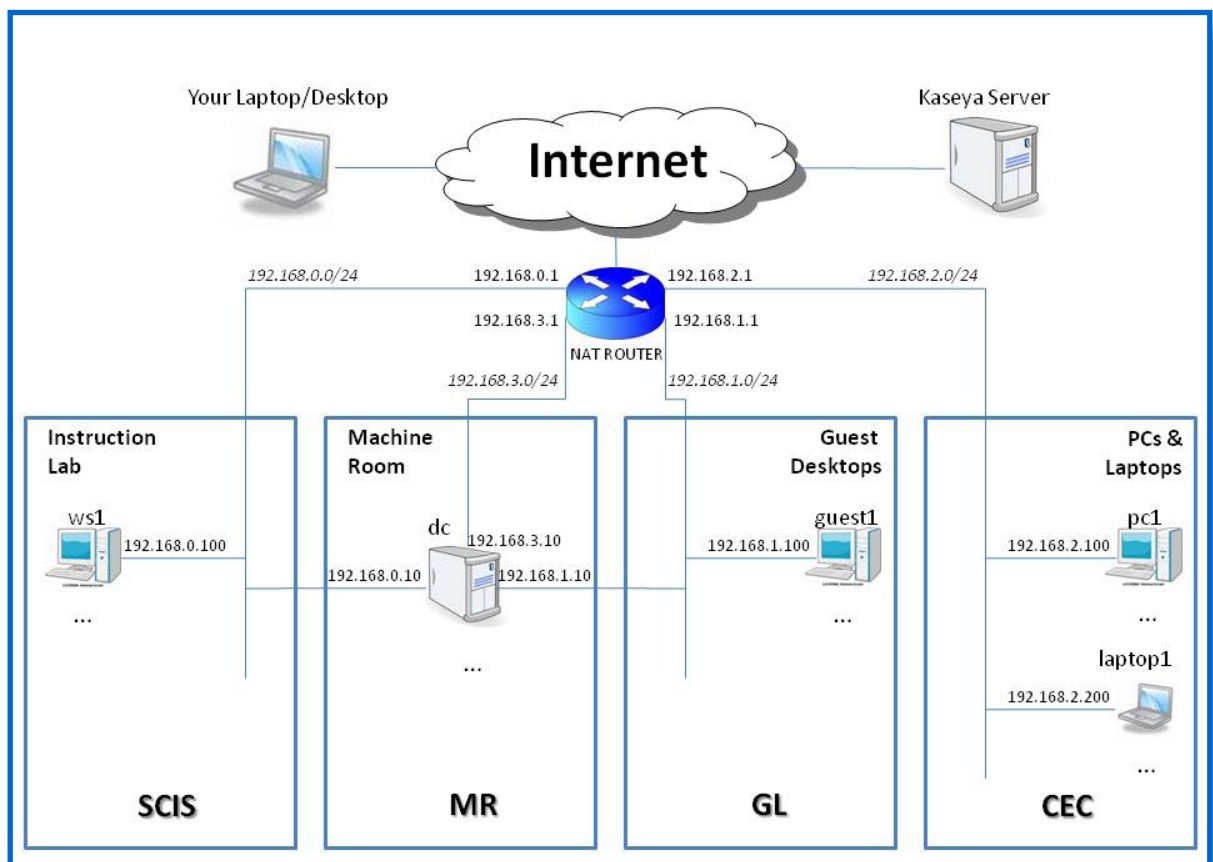


Audit Hands-on Exercise

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. 3.1, 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.

Fig. 3.23:
A logical
diagram of FIU's
network.



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. Now it is time to perform an inventory to discover what computing resources SCIS, MR, GL, and CEC buildings contain. However, as going to each workstation and server is a tedious task, you decide to use the Audit module in Kaseya to automatically perform this task. You also realize that it would be beneficial to be more proactive and prepare the settings for computers that may be discovered or added to your environment in the future. To do this, you can take advantage of agent templates that allow you to save and deploy useful agent settings for future computers with similar roles in your environment.

Technical Information

Your dedicated virtual environment includes the computers and network devices depicted in Fig. 3.1 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

Management needs an immediate report of a current inventory of all the computers, their hardware, and software licenses associated with those computers. They also need a weekly report of the inventory on an ongoing basis. You must find a way to schedule an audit for weekly execution. You have also received notification to prepare for about 100 computers being added to the environment under your management in the next few months. These computers should be audited the same way as for the existing managed machines.

Part 1

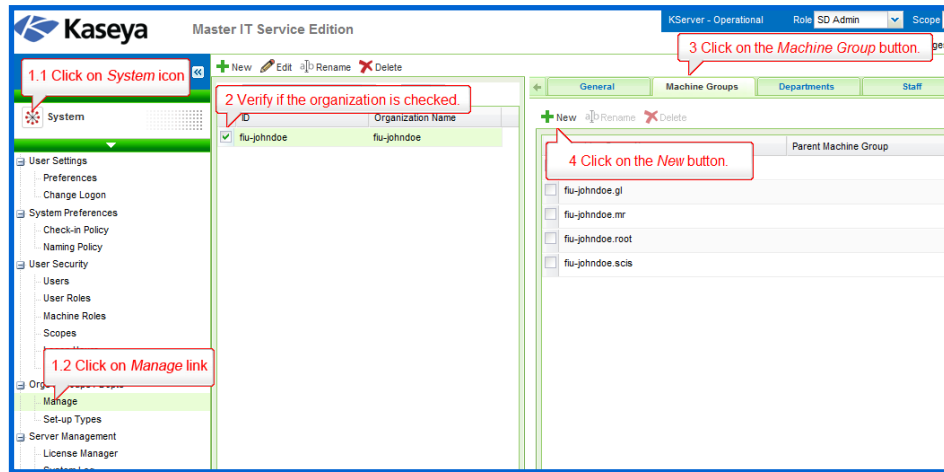
Since in the next few months a large number of computers will be added to your environment, it will be best to have some customized agent templates that incorporate the required agent settings for machines with similar roles in your environment. This way, once the new machines arrive, you can use the appropriate agent template to copy corresponding audit settings onto those machines. After some study and interaction with the users of the computers under your management, you realize that even though there are many computers in your organization, they all have one of three possible roles: instructional lab computers, guest computers, and servers. You are able to configure different settings, from different Kaseya modules, for all the current and future agents for computers with similar roles. To keep things organized, it will be best to create a group for the templates.

-Create a machine group under the “FIU-**<USERNAME>**” organization for templates, called “Templates”.

1. Open the System module. Go to *Orgs / Groups / Depts / Staff > Manage*.
2. Verify if the Organization “FIU-**<USERNAME>**” is checked.

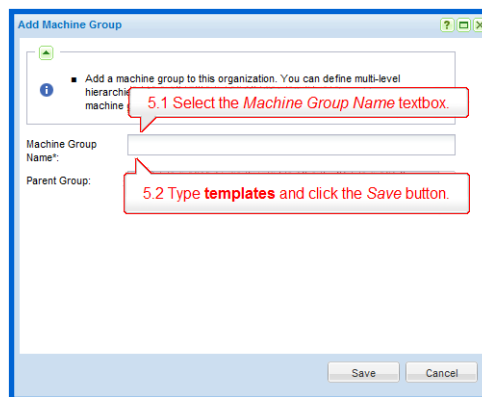
Fig. 3.24

3. Click on *Machine Group* on the right hand side of the module.
4. Click on *New*.



5. Create a group by typing its name “*Templates*” under *Machine Group Name*. Click *Save*.

Fig. 3.25



-Create three agent templates named “*Server*”, “*Instructional*”, and “*Guest*” to help you with the pre-configuration of some settings for the server and workstation machines.

6. Open the Agent module. Go to *Install Agents > Create*.
7. Type in “*Server*” in the textbox under *New Machine ID*.
8. Select “*Templates*” under the *Group ID* textbox.
9. Click on *Create*.

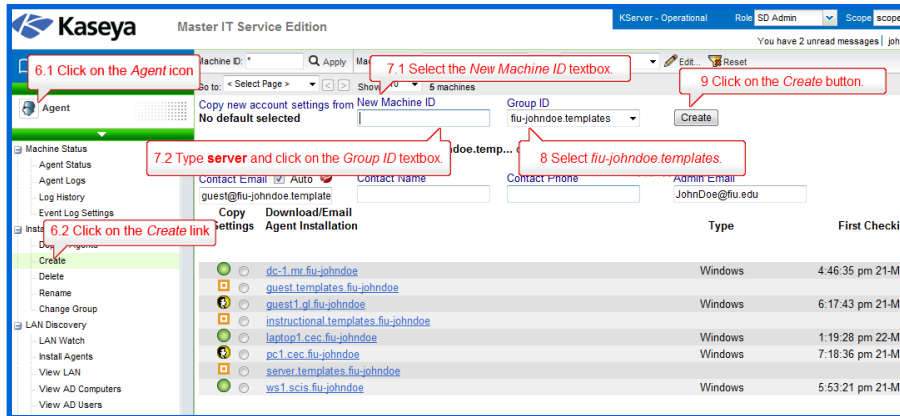


Fig. 3.26

10. Repeat steps 6-9 for the “InstructionalTemplate” and “GuestTemplate”.

Note: An agent template will have an orange square icon to emphasize the fact that the agent template will never be installed on a computer. Its sole purpose is to provide additional customized settings for agents with similar roles so that such setting can be added to the settings of already deployed agents or be used as part of an agent package.



Notes

Part 2

Generally speaking, Baseline Audit and System Info should be executed only once. The Baseline Audit captures the configuration of the system in a known working state and the System Info captures the system's information that will rarely change (*i.e.*, processor, disk drive, memory information, etc.). The Latest Audit captures the most up-to-date configuration of the system and you will configure it to audit changes made to the machine on a daily bases.

- Schedule a *Baseline Audit* to be executed immediately on all the templates.

11. Open the Audit module, then go to *Collect Data > Run Audit*.

12. Select all the templates, click on *Run Audit Now* and then select *Baseline Audit* then *Run Now*.

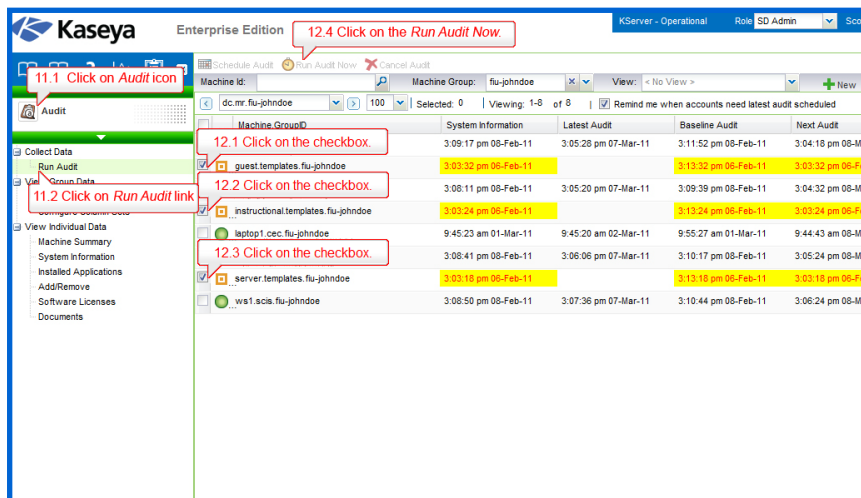
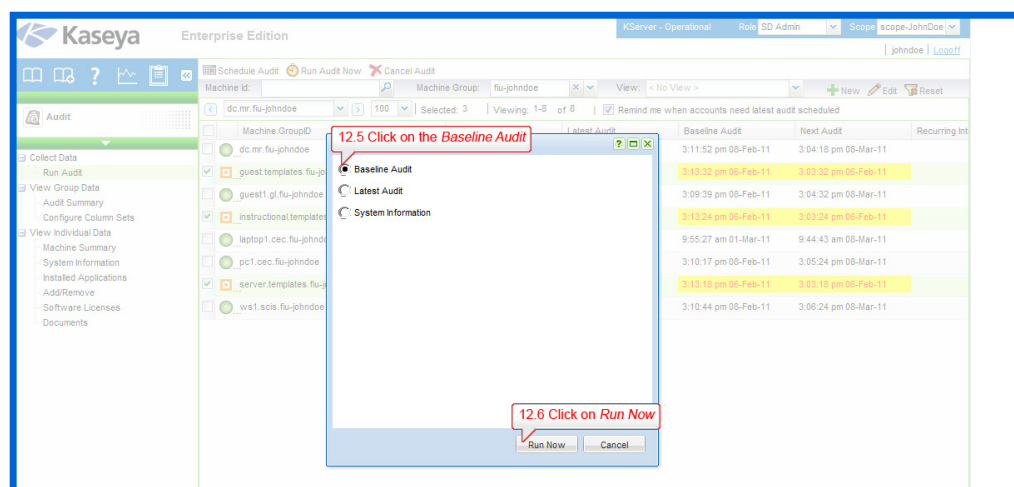


Fig. 3.27

Fig. 3.28

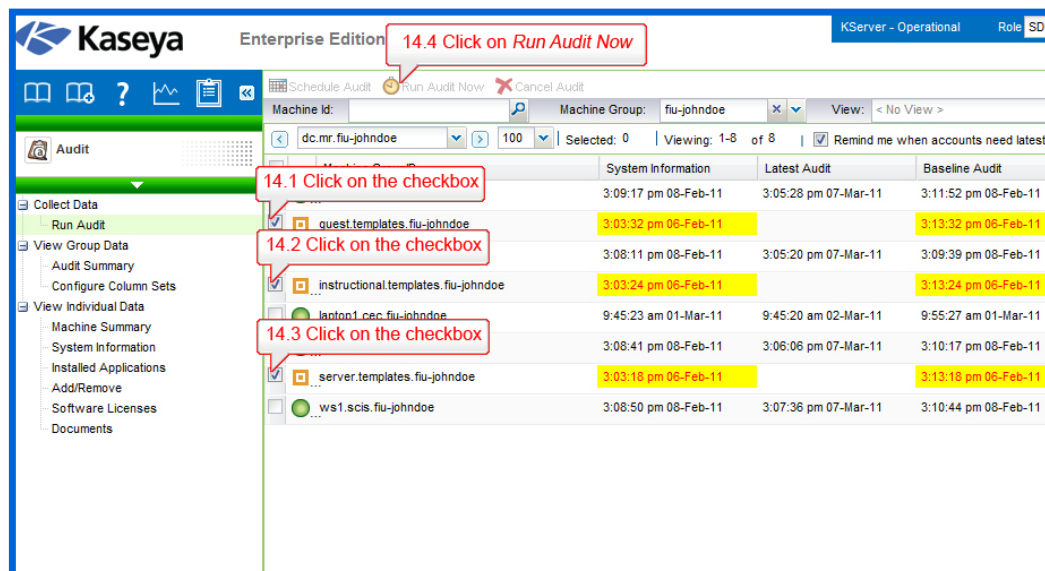


- Schedule a *System Info* to be executed immediately on all the templates.

13. Open the Audit module, the go to *Collect Data > Run Audit*.

14. Select all the templates, click on *Run Audit Now* and then select *System Information* then *Run Now*.

Fig. 3.29



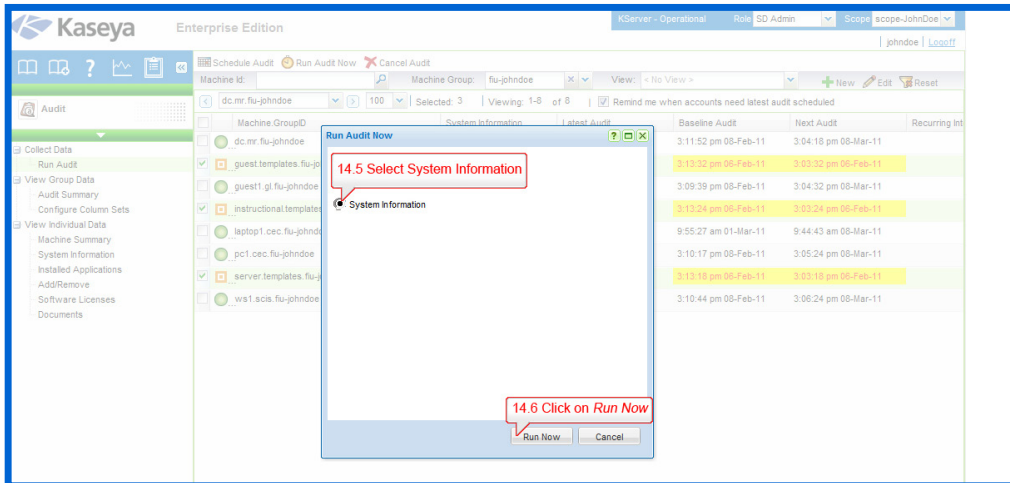


Fig. 3.30

-Schedule a *Latest Audit* to be executed at midnight on a daily basis on all the templates with a distribution window of 2 hours.

15. Open the Audit module, then go to *Collect Data > Run Audit*.
16. Select all the templates, click on *Schedule Audit* and then select *Latest Audit*.
17. In the *Recurrence* box, select *Daily*.

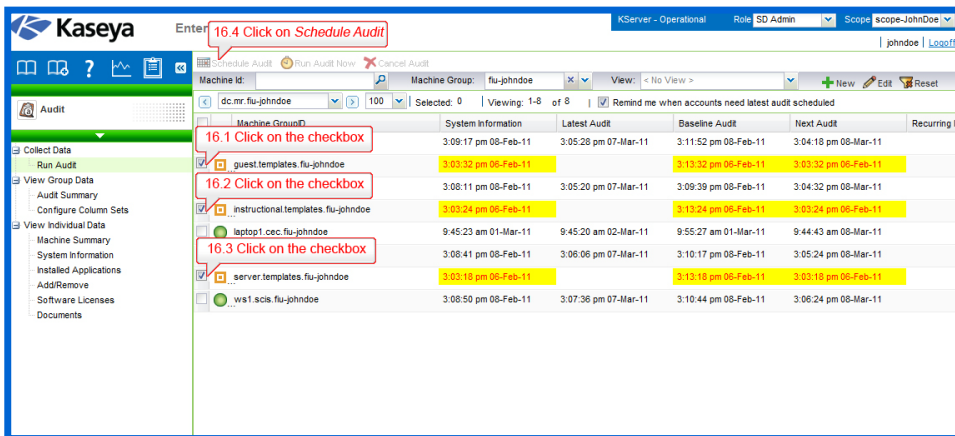


Fig. 3.31

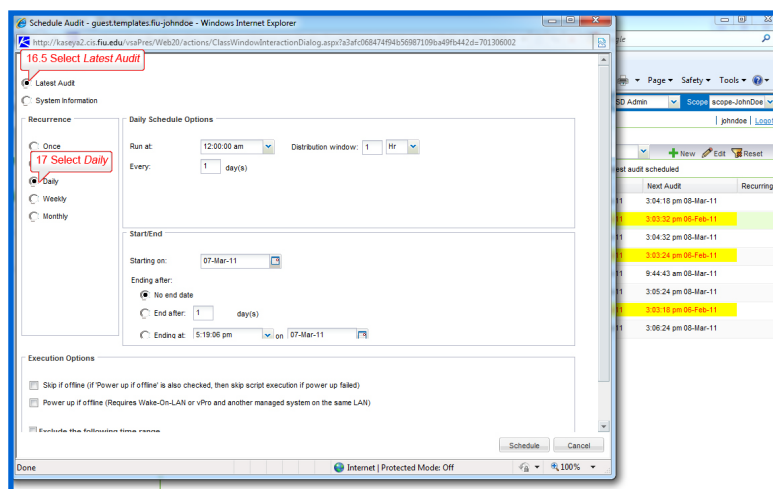
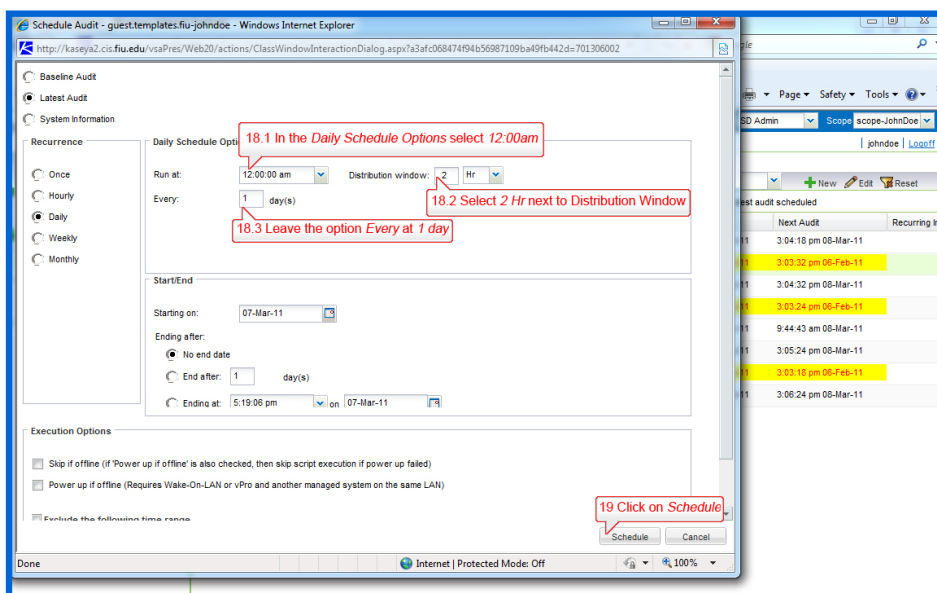


Fig. 3.32

18. In the *Daily Schedule Options* box, select 12:00am next to *Run at*, select two hours next to *Distribution Window*, and leave the option *Every* at 1 day.
19. Click on *Schedule* after everything is done.

Fig. 3.33



Part 3

Now that all three agent templates contain all the audit settings, it is now 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.

20. Open the Agent module, then go to *Configure Agents > Copy Settings*.
21. Click on *select machine ID* link and a new window will open up.

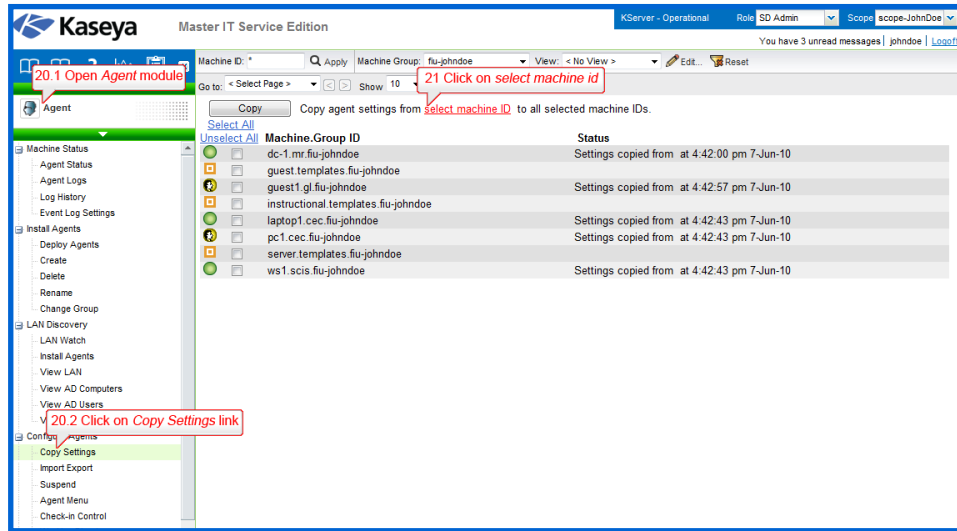


Fig. 3.34

22. Select "Templates" from the *Group ID* dropdown list.
23. Click on "Server" from the list of templates shown.

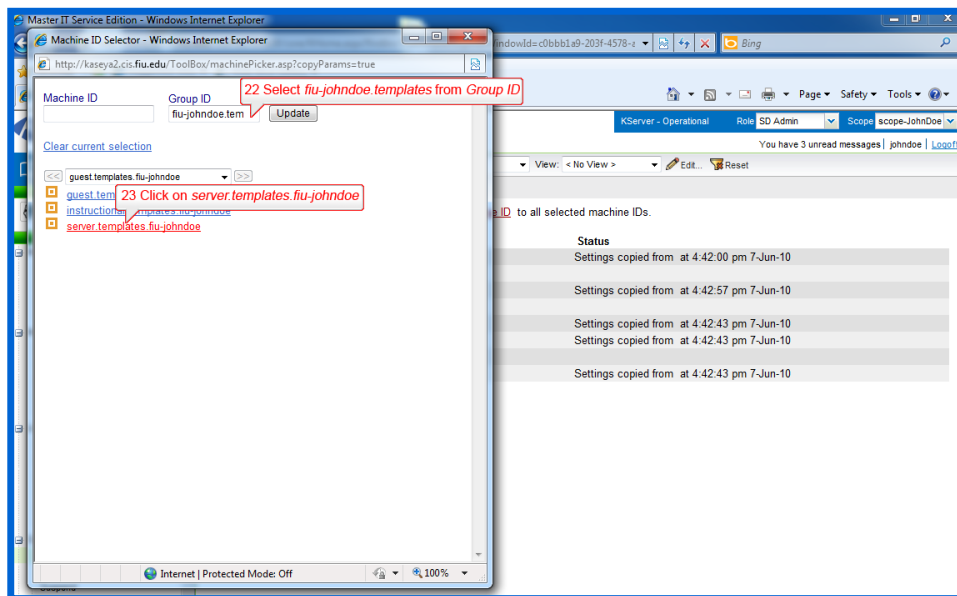
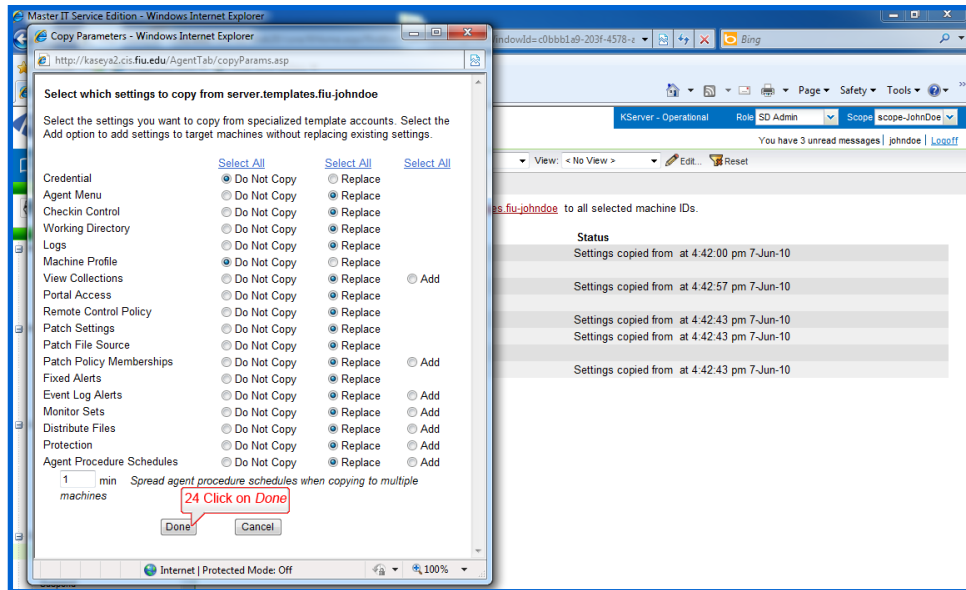


Fig. 3.35

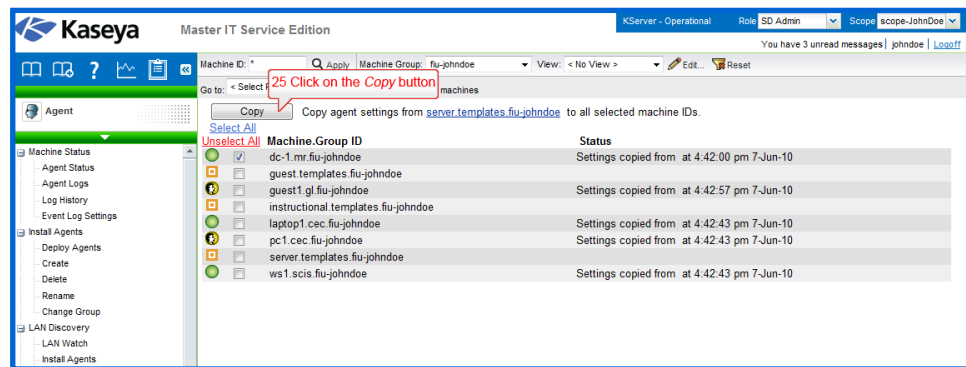
24. Leave everything as its default selection in the next page and click on *Done*.

Fig. 3.36



25. Select all the computers in the MR building and click on the *Copy* button.

Fig. 3.37



26. Repeat steps 20-25 for the “Instructional” and “Guest”.



Notes

Note: Depending on the network traffic and system resources, Baseline Audit and System Info should execute and send the results to the Kaseya VSA almost immediately. If not, please wait until the results are sent back to the Kaseya VSA.

Part 4

Now that the auditing has been completed and scheduled, you can view the audit information of the computers that Kaseya manages.

27. View all the tabs under the two groups, *View Group Data* and *View Individual Data*. Note what type of information can be obtained through audit and what it can be used for future applications.

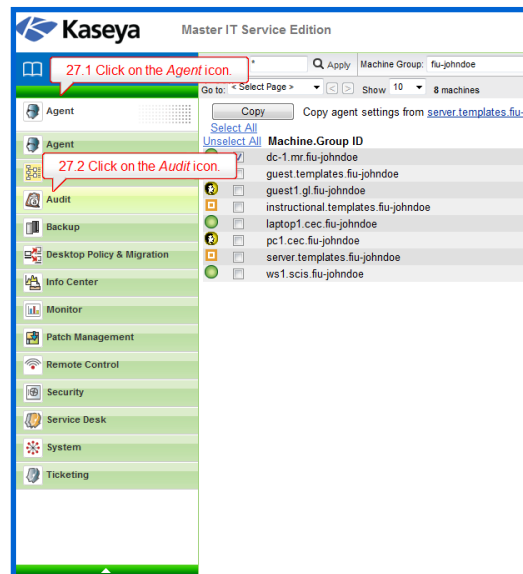


Fig. 3.38

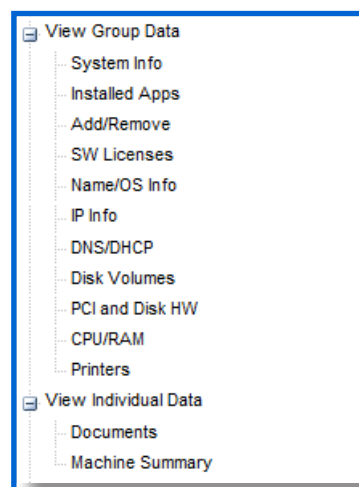


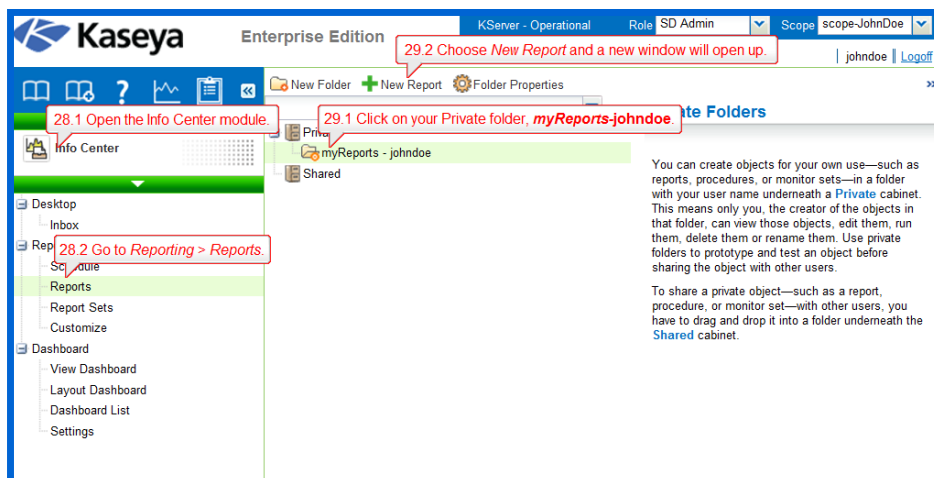
Fig. 3.39

Part 5

Management still needs the audit report by the end of the work day. The audit report should contain a list of all the computers within each building. To accomplish this, you will rely on the Info Center module to generate an audit report.

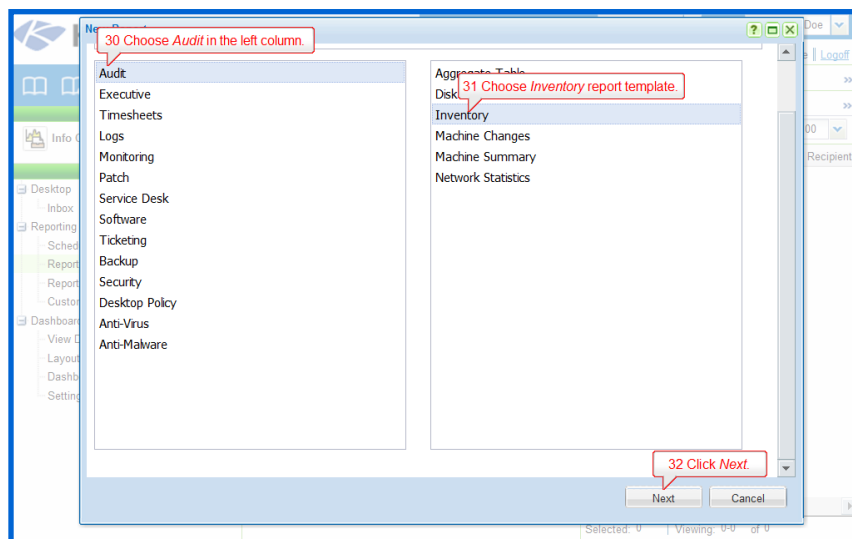
28. Open the Info Center module. Go to *Reporting > Reports*.
29. Click on your Private folder, “myReports-<USERNAME>”, choose *New Report* and a new window will open up.

Fig. 3.40



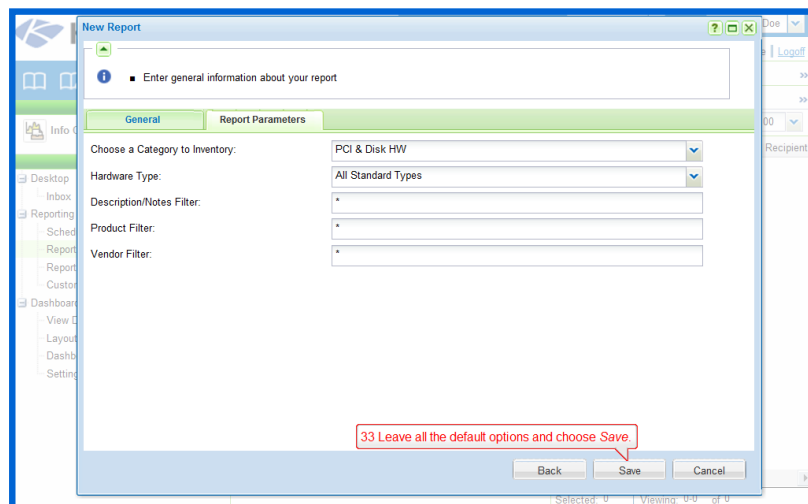
30. Choose *Audit* in the left column.
31. Choose *Inventory* report template.
32. Click *Next*.

Fig. 3.41



33. Leave all the default options and choose *Save*.

Fig. 3.42



34. Select the newly created report under your folder then choose *Run Report*.

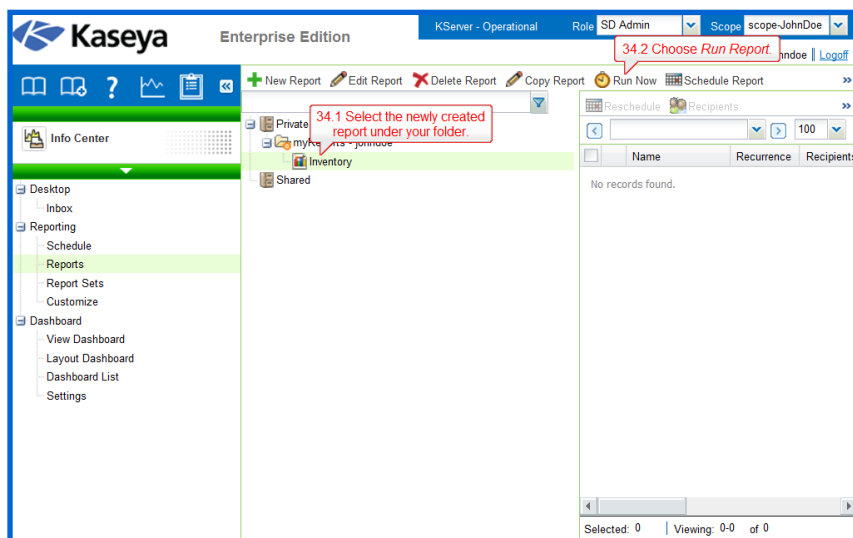


Fig. 3.43

35. Choose “FIU-<USERNAME>” next to *Organization* in the new window.

36. Click on *Submit*.

37. Once the scheduled report is done, the report will open automatically.

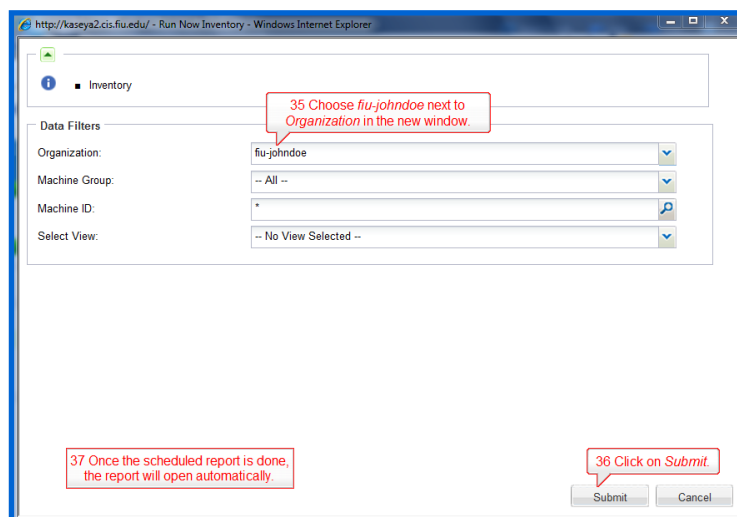


Fig. 3.44

Fig. 3.45

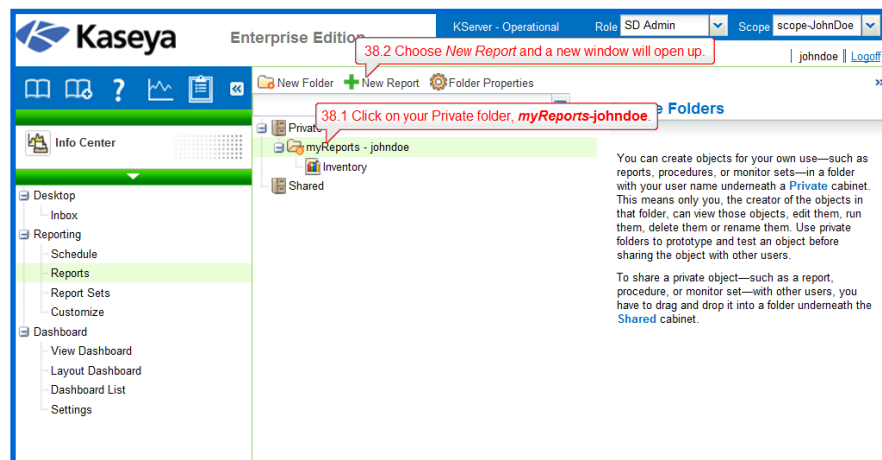
My Organization
Inventory
Report Date: 4:52:35 PM 11-Mar-11
Effective Date: 11-Mar-11

PCI & Disk HW" & " Inventory Report
Inventory information from latest audit for 'all machines' in 'all groups' in the organization 'fiu-johndoe'
Hardware Type: 'All Standard Types'
Vendor Filter: ""
Notes: ""
Product Filter: ""

Quantity	H/W Type	Vendor	Machine, Group ID	Product Notes
5	PCI Network	Advanced Micro Devices		Am79C970/1/2/3/5/6 PCnet LANCE PCI Ethernet Controller
			dc.mr.fiu-johndoe	
			guest1.gl.fiu-johndoe	
			laptop1.cec.fiu-johndoe	
			pc1.cec.fiu-johndoe	
			ws1.scis.fiu-johndoe	
5	PCI Graphics	VMware Inc.		9500MGS NVIDIA
			dc.mr.fiu-johndoe	
			guest1.gl.fiu-johndoe	
			laptop1.cec.fiu-johndoe	
			pc1.cec.fiu-johndoe	

38. Click on your Private folder, “myReports-<USERNAME>”, choose *New Report* and a new window will open up.

Fig. 3.46



39. Choose *Software* in the left column.
40. Choose *Software Applications Installed* report template.
41. Click *Next*.

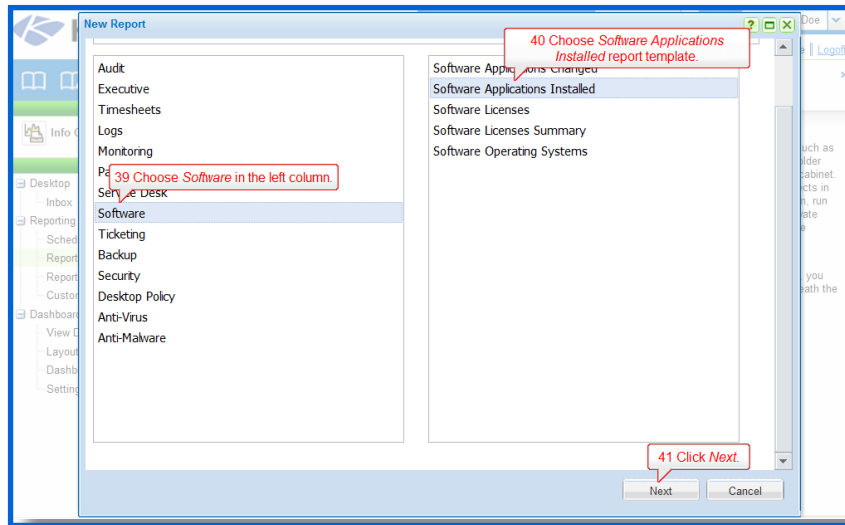


Fig. 3.47

42. Leave all the default options and choose Save.

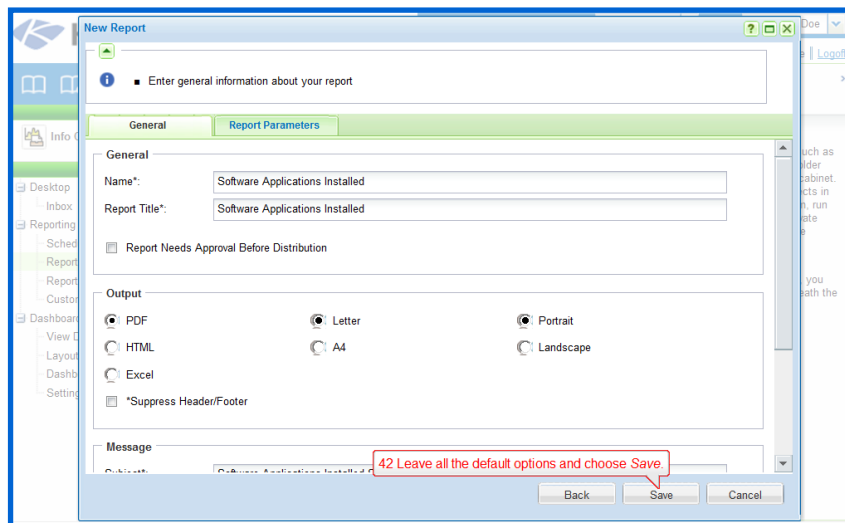


Fig. 3.48

43. Select the newly created report under your folder then choose *Run Report*.

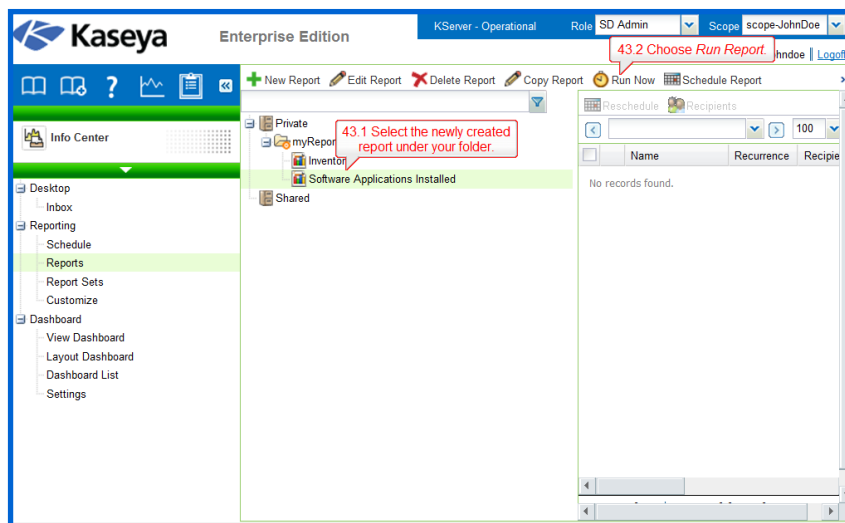


Fig. 3.49

44. Choose "FIU-**USERNAME**" next to *Organization* in the new window.

45. Click on *Submit*.

Fig. 3.50

44 Choose *fiu-johndoe* next to *Organization* in the new window.

45 Click on *Submit*.

46 Once the scheduled report is done, the report will open automatically.

46. Once the scheduled report is done, the report will open automatically.

Fig. 3.51

My Organization
Software Applications Installed
Report Date: 5:47:00 PM 11-Mar-11
Effective Date: 11-Mar-11

Software All Applications
Software All Applications information from latest audit for 'all machines' in 'all groups' in the organization 'fiu-johndoe' Report

Registered Applications					
Copies	Application	Product Name	Description	Manufacturer	Version
1	TzFM.exe	7-Zip	7-Zip File Manager	Igor Pavlov	4.65.0.0
4	bckgzm.exe	Zone.com	Zone Datafile	Microsoft Corporation	1.2.626.1
4	chkzrm.exe	Zone.com	Zone Datafile	Microsoft Corporation	1.2.626.1
1	CluAdmin.exe	Microsoft® Windows® Operating System	Cluster Administrator	Microsoft Corporation	5.2.3790.1830
1	cluadmin.exe	Microsoft® Windows® Operating System	Cluster Administrator	Microsoft Corporation	5.2.3790.3959
1	conf.exe	Microsoft® Windows® Operating System	NetMeeting®	Microsoft Corporation	5.2.3790.1830



Notes

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.

