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. 4.1, 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, maintenance work on individual computers is done by a technician who must physically go to each computer needing maintenance and perform the required tasks on them. This method denies computer access to the users during the maintenance and does not utilize the technician’s time efficiently – the technician must physically go to each computer and remain idle, for example, during long installation periods. You have therefore decided to perform most of the maintenance tasks remotely so that first, the users can continue their work during the maintenance, and second, the technician can utilize otherwise idle time on other tasks. Kaseya’s Remote Control module allows technicians log into computers in all four buildings from inside or outside the network. To be able to utilize Kaseya’s Remote Control, you first need to set up remote control policies.
Technical Information

Your dedicated virtual environment includes the computers and network devices depicted in Fig. 4.1 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

To keep yourself as flexible as possible, you decide to set up remote control policies to allow yourself, and future technicians, to log into computers remotely via Kaseya’s VSA. This strategy will help you in diagnosing computers when you are off-site and an emergency arises. Since you want to involve the network technician as little as possible, using RDP (Remote Desktop Protocol) outside the network to access all the computers is not a reliable option as the port may be blocked by the firewall and the remote control may not be enabled on all machines under your management. Kaseya’s Remote Control module addresses this issue and in addition will help in sending files across the network, via FTP, when it is needed. This will allow you to send files to users by placing the files directly on their computers. It will be best to set the policies to the agent templates to be prepared for the possible future deployment of computers.

Part 1

For security reasons, Remote Control policies are needed to allow or restrict certain actions when attempting to remotely connect to a computer. The policy to be implemented is:

For the servers and instructional lab computers, if a user is logged into a computer, then the user must be prompted to either approve or deny remote access. If no user is logged in, access should be given automatically. Remote access to guest computers will take place silently without approval. Note that guest computers are public access computers. The policies will be based on the machine group to which each machine belongs. We will assign such settings in corresponding agent templates to keep track of the policies for the corresponding machine groups. Later, we will use the templates to distribute the settings for each machine group to the corresponding agents.

- Create a Machine Policy that will be established in the Instructional and Server templates to make sure that an administrator must gain permission first from a user logged on to the system at the time of remote connection. If the user is not logged in, access will be given automatically.

1. Open the Remote Control module. Go to *Notification Policy* > *Machine Policy*.

2. Select the checkboxes next to “Instructional” and “Server” templates.
3. Select *Ask permission. Approved if no one logged in* from the dropdown box under *Select user notification type*.

4. Check the box next to *Require admin note to start remote control*.

5. Click on *Apply*.

- Create a Machine Policy that will be established in the Guest template to make sure that access of the computer will be given silently and not require user permission.


7. Select the checkbox next to “Guest” template.

8. Select *Silently take control* from the dropdown box under *Select user notification type*.

9. Click on *Apply*.

Choosing the right remote control package for each computer will help in doing different things when attempting to make a remote connection. Since K-VNC allows copy and paste functionality, it will be best to use this package for all the machines in the SCIS, GL and CEC buildings. Since DC is a server, using Terminal Server is best as there would be no need for installing any remote control software on the server. Terminal Server will force the computer to initiate RDP.
Chapter 3 – Remote Control Hands-On Exercises

**Note:** Setting up the agents so that they preinstall the selected remote control package will speed things up when you perform the first remote connection. If you select Terminal Server, you do not have the option to preinstall as the Terminal Server is expected to be already available on the remote machine.

-Configure all the Instructional and Guest templates to use the K-VNC remote client. Then configure the Server template to use Terminal Server client for remote connection.

10. Open the Remote Control module. Go to Configure > Select Type.
11. Select the checkboxes next to “Guest” and “Instructional” templates.
12. Select K-VNC in the Select remote control package to use with selected machines dropdown box.
13. Click on Select.

**Note:** Once the new settings are applied to the agents in the following parts of this exercise, we will verify the correctness of the setting.

**Part 3**

Now that all three agent templates contain all the remote control 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.

15. Open the Agent module. Go to Configure Agents > Copy Settings.
16. Click on select machine ID link and a new window will open up.
17. Select “Templates” from the Group ID dropdown list.

18. Click on “Server” from the list of templates shown.

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

20. Select all the computers in the MR building and click on the Copy button.
21. Repeat steps 15-20 for the Instructional and Guest templates.

**Part 4**

One of the instructors has requested administrative access to install Chrome in his laptop. Not only does he need access but the install file as well. This request is time sensitive and must be implemented promptly.

- Using **Reset Password**, create a new administrator account on laptop1 with the username “ksmith” and your password (same as your other password to help remembering it in the future).

22. Open the Remote Control module. Go to **Desktop Control > Reset Password**.

23. Click on the checkbox next to laptop1.

24. Type “ksmith” in the textbox next to **Username**.

25. Type your password in the textbox next to **Password** and **Confirm**.

26. Click the checkbox next to **Create new account** and make sure **as Administrator** is checked.

27. Click on the **Apply** button.
-Download Chrome install file from the Internet. Then using FTP send the file to laptop1’s C: drive.

28. Download Chrome install file from the Internet. (Note: Any file can be used to mimic the process.)

29. Open the Remote Control module. Go to Files/Processes > FTP.

30. Click on “laptop1.cec.fiu-<USERNAME>”.

31. Select the radio button next to Select remote fixed drive to FTP To C:

32. Click Connect.

33. A new Explorer window will pop up.

34. Copy and paste the file into the Explorer window.
35. Send a text message to the instructor using Message with Users > Send Message (see Part 5 for more details on this function).

**Part 5**

The DC is causing some problems on the network and the network technician is going to take it off of the network and fix it tonight at 3:00am. Management has asked you to send a global message to all the computers and inform users about the emergency maintenance.

-Using Send Message send a global message telling users the server will be down for emergency maintenance tonight at 3am.

36. Open the Remote Control module. Go to Message with Users > Send Message.

37. Select all the computers in the SCIS, GL, and CEC buildings.

38. In the Enter message/URL sent to remote machines (dialog box or URL) write the message explaining the emergency maintenance.

39. Make sure “Dialog Box” is selected under Select display window.

40. Leave everything else as its default selection.

41. Click on Send Now.
A co-worker is having problems with his laptop. The co-worker has Internet access and is asking you to remotely log into his laptop to diagnose the problem. The laptop does not have an agent installed therefore Video Streaming should be used for remote login as it allows for direct remote access without need for agents.

- Using Video Streaming, remotely connect to laptop1 and take control of the computer.

42. Open the Remote Control module. Go to Desktop Control > Video Streaming.
43. Select K-VNC next to Select remote control package to us.
44. Click on Start.

45. Remotely login to laptop1 through RDP (use "mstsc.exe /admin /v:<NAT_ROUTER_IP>:<LAPTOP1_RDP_PORT>")

46. While logged into laptop1, through RDP, log into http://kaseya2.cis.fiu.edu/gethelp.asp.
47. Click on your user name hyperlink.
Chapter 3 – Remote Control Hands-On Exercises

48. A number of files will be downloaded and installed. Accept all requests to install downloaded software. (All installed software will automatically be uninstalled after completion of remote session.)

49. After the file is installed, a new K-VNC window will open up. This will give access to laptop1 and allow it to be used remotely.

**Note:** While you may try use Video Streaming on other browsers, besides Internet Explorer, this process may not be successful. Functionality of the Kaseya VSA is tested fully with Internet Explorer, so in the event of a function within the VSA not working as expected, please try again within Internet Explorer.

**Part 7**

First, verify that the remote control policies assigned to the machines have been applied as intended. Next, to make sure that the policies created in this exercise will not affect your performance when working on the exercises in the other Kaseya modules, we ask you to reverse some of the polices that you put in place in Part 2. Basically, you need to make sure that remote access will take place silently without approval for all the computers.

- Remotely connect to ws1 and dc machines, as two examples, to verify if all your remote control settings are correctly applied.

50. Open the Remote Control module. Go to Desktop Control > Control Machine.

51. Click on ws1.scis.fiu-<USERNAME> link and verify remote connection.

52. Once completed, close the connection and click on dc.mr.fiu-<USERNAME> and verify remote connection.

- Create a Machine Policy that will be established in the Instructional, Server, and Guest templates to make sure that access to all the computers will be given silently and not require user permission.

54. Select the checkbox next to “Instructional”, “Server”, and “Guest” templates.

55. Select *Silently take control* from the dropdown box under *Select user notification type*.

56. Uncheck the box next to *Require admin note to start remote control*.

57. Click on *Apply*.

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 "Templates" from the Group ID dropdown list.

61. Click on “Server” from the list of templates shown.
62. Leave everything as its default selection in the next page and click on *Done*.

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

64. Repeat steps 58-63 for the Instructional and Guest templates.
The management has now asked you to print out a report of your work. They need to see immediate progress and you only have a matter of hours to prepare the report. Going around to each computer will take too long, so you look to Kaseya to fulfill your reporting needs.

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

67. Choose Logs in the left column.
68. Choose the Remote Control report template.
69. Click Next.
70. Leave all the default options and choose Save.

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

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

73. Click on Submit.
74. Once the scheduled report is done, the report will open automatically.