

# KASEYA CERTIFIED TECHNICIAN (KCT)

The Kaseya Certified Technician Lab Guide provides hands-on exercises and a structured approach to building and administering automation and integrated systems management using the Kaseya Virtual Systems Administrator

*Managed Service  
Provider Lab Guide*

## Table of Contents

Lab Guide Overview .....	5
The Scenario and vLab .....	5
Instructions for Use.....	7
Hands-On Exercises.....	8
O1 and O2: Orientation.....	8
Exercise 1 .....	8
Exercise 2 .....	8
Exercise 3 .....	8
T5: Tasks: Import/Export.....	9
Exercise 4 .....	9
Bonus Activity 1 .....	9
Bonus Activity 2 .....	9
A2: Agent: Manual Deploy.....	10
Exercise 5 .....	10
Exercise 6 .....	10
A3: Agent Auto Discovery/Remote Deploy.....	11
Exercise 7 .....	11
Exercise 8 .....	11
Exercise 9 .....	11
AI4: Audit: View Assets .....	12
Exercise 10 .....	12
Exercise 11 .....	12
Exercise 12 .....	12
A5: Agent Endpoint (to Endpoint).....	13
Exercise 13 .....	13
Exercise 14 .....	13
Exercise 15 .....	13
AI1: Audit: Information Review .....	14

Exercise 16 .....	14	2
Exercise 17 .....	14	
Exercise 18 .....	14	
Exercise 19 .....	14	
RC2: Remote Access: Use.....	15	
Bonus Activity 3 .....	15	
Bonus Activity 4 .....	15	
Exercise 20 .....	15	
Exercise 21 .....	15	
Exercise 22 .....	15	
Bonus Activity 5 .....	15	
Exercise 23 .....	15	
Exercise 24 .....	15	
Bonus Activity 6 .....	16	
Exercise 25 .....	16	
Exercise 26 .....	16	
Exercise 27 .....	16	
Bonus Activity 7 .....	16	
Exercise 28 .....	16	
Bonus Activity 8 .....	16	
Exercise 29 .....	16	
Exercise 30 .....	16	
Exercise 31-39: Agent Data .....	16	
Exercise 40-47: Audit Information .....	17	
Exercise 48: File Manager .....	17	
Exercise 49: Command Shell .....	17	
Exercise 50: Registry Editor .....	17	
T3: Task: Views.....	18	
Exercise 51 .....	18	
Exercise 52 .....	18	
Exercise 53 .....	18	
Bonus Activity 9 .....	18	

P1: Patch: Create/Assign Policies.....	19
Exercise 54 .....	19
T2: Tasks: Schedule and Execute .....	20
P5: Patch: Scan and Status.....	21
Exercise 55 .....	21
Bonus Activity 10 .....	21
P6: Patch: Updates.....	22
Exercise 56 .....	22
Exercise 57 .....	22
Exercise 58 .....	22
Exercise 59 .....	22
Bonus Activity 11 .....	22
M1: Monitor: ATSE.....	23
M2: Monitor: Monitor Sets.....	23
Exercise 60 .....	23
Exercise 61 .....	23
Exercise 62 .....	24
Exercise 63 .....	24
Exercise 64 .....	24
Exercise 65 .....	24
M3: Monitor: Monitor Fixed Alerts.....	25
Exercise 66 .....	25
Exercise 67 .....	25
Exercise 68 .....	25
Exercise 69 .....	25
M4: Monitor: Monitor Event Logs .....	26
Exercise 70 .....	26
Exercise 71 .....	26
M5: Monitor: Alarms.....	27
Bonus Activity 12 .....	27
Exercise 72 .....	27
Exercise 73 .....	27

M7: Monitor: Reviewing Monitor Data.....	28	4
Exercise 74 .....	28	
PM2: Policy Management: Policy Assign .....	29	
Exercise 75 .....	29	
Bonus Activity 13 .....	29	
PM3: Policy Management: Policy Compliance.....	30	
Exercise 76 .....	30	
Exercise 77 .....	30	
Exercise 78 .....	30	
T7: Tasks: Logs.....	31	
Exercise 79 .....	31	
Exercise 80 .....	31	
Bonus Activity 14 .....	31	
Bonus Activity 15 .....	31	
D1: Dashboards.....	32	
Exercise 81 .....	32	
Exercise 82 .....	32	
Exercise 83 .....	32	
Bonus Activity 16 .....	32	
IC2: Info Center: Execute and Schedule .....	33	
Exercise 84 .....	33	
Exercise 85 .....	33	
Exercise 86 .....	33	
T6: Tasks: File Management.....	34	
Exercise 87 .....	34	
Exercise 88 .....	34	
Answer Key .....	35	

## Lab Guide Overview

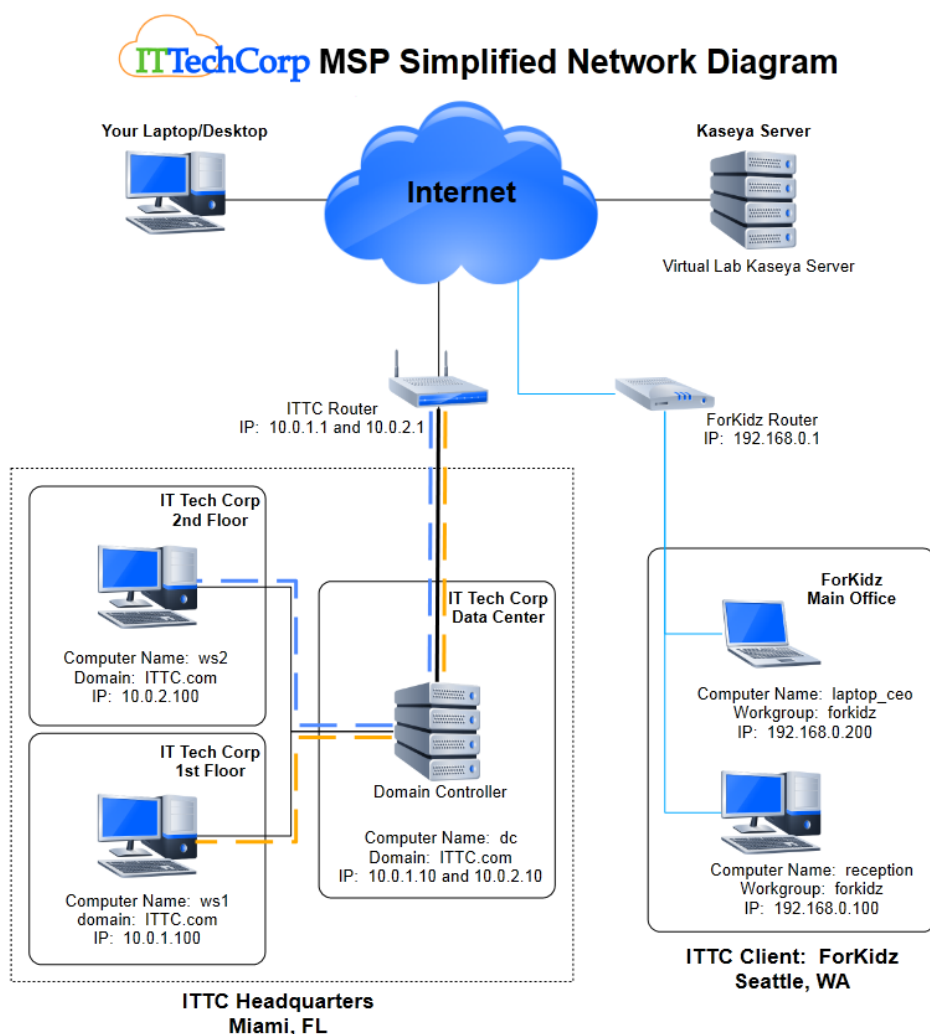
5

Welcome to the Kaseya Certified Technician (KCT) Lab Guide. The hands-on exercises presented in this guide align directly with the courses presented in the VSA Technician learning path and will help prepare students for the certificate exam. This lab guide uses a Managed Service Provider-based scenario. The exercises mirror those included in the Enterprise scenario, but the story has been customized to mimic an MSP-based Kaseya deployment.

## The Scenario and vLab

The exercises in this lab guide are scenario-based and tell the story of Jose, a Technician for IT Tech Corp. IT Tech Corp is a fictitious mid-sized Managed Service Provider which has recently purchased the Kaseya VSA to help them command centrally, manage remotely, and automate everything related to their own IT needs, as well to help enable them to provide services for their customers.

IT Tech Corp is a domain-based environment with a domain controller and several workstations. The vLab has two sample workstations and one Domain Controller representing the rest of the environment at ITTC. The client, ForKidz is a local small non-profit organization with a small number of computers. Their workgroup-based computers are all connected to each other via LAN and have access to the internet. They are not using a domain or any sophisticated network infrastructure. The vLab has two sample workstations representing this environment. (Network Diagram below)



Among other responsibilities, Jose is the lead technician for Desktop Support at IT Tech Corp. Jose was tracking the computers in his network, assisting in troubleshooting end-users computer incidents, and helping in onboarding of new endpoints for different clients' sites.

The Kaseya VSA is now the new platform Jose will use to help assist end-users' endpoints. Jose wants to convert his current daily tasks to Kaseya and minimize the amount of individual development he has to do on a regular basis. His primary goal is to automate as many of his routine tasks as possible.

Jose is responsible for:

- Using Kaseya to schedule and execute endpoint-side tasks and automation scripts
- understand the basic layout of the Kaseya VSA and know how to utilize it as a tool for troubleshooting

Jose is going to:

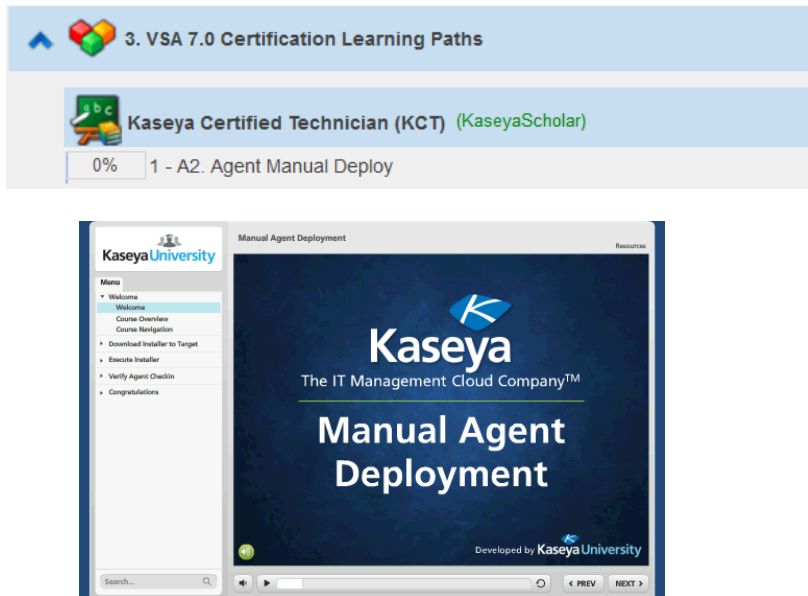
- install agents so he can remotely manage machines
- discover devices so he can install agents and remotely manage those devices
- schedule tasks to automate processes
- configure settings throughout the VSA to control how the agents behave and what info is visible, reportable, etc.
- know how to scan endpoints for patches and prevent any updates from installing that might be problematic or needs additional testing prior to release.
- create and assign pre-existing patch policies for patch management and deployment
- learn how to review monitor data to proactively asses endpoint performance
- understand how to remotely control into endpoints
- force compliance (Policy) and make changes on a scheduled basis (Agent Procedures)
- automatically assign settings, scripts, monitoring and other regular functions to existing machines and any new machines that are introduced into the environment.
- provide customers with regular reports on the status of devices, work accomplished, managed devices, etc.

## Instructions for Use

7

The exercises in this lab guide are designed to complement the course curriculum presented in the KCT learning path. Kaseya University recommends that you utilize this guide real-time as you work through the courses.

In order to optimize learning, in the Learning Center go to the Kaseya Certified Technician (KCT) Learning Path, and launch and complete a course. Before moving on to the next course in sequence, open this lab guide and apply that learning using the hands-on exercises associated with specifically with the completed course before moving on to the next.



### A2: Agent: Manual Deploy

Install one agent into the IT Tech Corp net can be used to locate additional machines machines will be accessed remotely, and c on user.

Hint: The path to the registry key is:

32 bit: HKeyLocalMachine\Software\I

64 bit: HKeyLocalMachine\Software\I

### Exercise 5

Log into DC

Download and execute the agent

**The exercises are intended to be completed IN-SEQUENCE.** There is no enforcement mechanism and so the vLab does permit you to skip around. However, some of the exercises in this guide assume that prior configurations have been completed.

Finally, Kaseya University wants you to be able to do more than click through step-by-step instructions, but rather actually understand what you are doing! Thus, the exercises in this guide are written in an open-ended fashion. Should you get stuck and need help, there is an **Answer Key** in the back of the guide. There is often more than one way to complete the exercise. The answer key utilizes the best practice or optimal approach.

You are encouraged to do as much as you are able to without having to consult the key!



## Hands-On Exercises

### O1 and O2: Orientation

Jose would like to have all machines and user records belonging to IT Tech Corp grouped together and have separate groupings for each client.

Create an organization structure for IT Tech Corp and one client, ForKidz. Each organization needs a machine group for the endpoints and each needs an "onboarding" group for new machines. The machine groups will mirror the physical locations. IT Tech Corp has machines spread in three physical locations: a data center and on two separate floors of an office building. ForKidz machines are located within the same physical HQ office.

A user role, Technician, and scope is in need of creation and assignment for the VSA User, Jose Pearlman (jpearlman). Jose will only be able to access the ForKidz organization access Audit and Patching configuration for the ForKidz organization.

**Notice about Name Clashing:** Some configurations on a Cloud VSA server must be unique across the entire shared server. Where this is a requirement, we ask that you include your username as part of the configuration. When you see -<USERNAME> indicated in the lab guide, enter your VSA login name in place of the <USERNAME>. For example, if your VSA login is ajackson and you are requested to create a VSA user named jose-<USERNAME>, you would create the user jose-ajackson.

#### Exercise 1

Rename myOrg to ITTC-<USERNAME>  
Create Machine Groups: "DataCenter", "FirstFloor", "SecondFloor", "onboarding"  
Create Departments: Accounting, IT, HR  
Create Staff record: Jose Pearlman in the IT department

#### Exercise 2

Create org ForKidz  
Create Machine Groups: "hq", "onboarding"  
Create Departments: MainOffice, FamilyServices, YouthOutreach  
Create Staff record: Samantha Jackson in the MainOffice department

#### Exercise 3

Create User Role: Technician with access to Audit and Patch functions  
Create Scope: ForKidz. Limit the scope to machines in the ForKidz organization  
Create VSA User: Create a login account for Jose Pearlman as jpearlman-<USERNAME> and assign to the Technician role and ForKidz scope

## T5: Tasks: Import/Export

---

9

---

Jose works with Alex. Alex is the Kaseya Administrator of IT Tech Corp and is responsible for building the framework of Kaseya so technicians like Jose can manage individual machines.

Alex has created a number of views, policies, reports, agent install packages, and other useful utilities for Jose and has provided those in an .xml. Jose needs to import the .xml to get all of these items available in the VSA.

### Exercise 4

Download Learning Content Pack from <http://university.kaseya.com/KaseyaUniversity/KU-ContentPack.zip>

System > Import Center > Import > select content pack

Verify policies, views, reports, Aps, agent install packages were imported

### Bonus Activity 1

Visit <http://community.kaseya.com>

Find any procedure in the community and import to your lab VSA using the Import Center

Verify procedure imported

### Bonus Activity 2

Export a procedure from a lab server and import to preview or production server

## A2: Agent: Manual Deploy

10

While the ITTC Admin, Alex, is usually responsible for agent install configurations, there are times when Jose steps in to help. While automation is the ultimate goal, Jose must first manually deploy at least one agent into each network environment.

Install one agent into the ITTC network and a separate agent in the ForKidz network. Automated discovery can be used to locate additional machines once the "agent zero" machines have been introduced in each network. Jose also knows these machines will be primarily accessed remotely and wants to ensure the agent icon properly reflects a logged on user.

Hint: The path to the registry key is:

32 bit: HKeyLocalMachine\Software\Microsoft\Windows\CurrentVersion\Run

64 bit: HKeyLocalMachine\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

### Exercise 5

Log into DC

Download and execute the agent install package

Add -remote to registry key

Verify checkin showing logged in user

### Exercise 6

Log into PC1

Download and execute the agent install package

Add -remote to registry key

Verify checkin showing logged in user

## A3: Agent Auto Discovery/Remote Deploy

11

Now that there is an agent in each environment, Jose can use Discovery to locate other computers in each environment and automatically install the agent software to all other computers found within each network.

Use the option that caters BEST for each organization. (I.E. if Active Directory is predominantly used, use Discovery > Domains, if there is no Active Directory environment, use Discovery > Networks).

Configure the “Naming Policy” of the ForKidz environment to force endpoints in the ForKidz organization to join its appropriate machine grouping based on the Default Gateway and IP Address range.

### Exercise 7

Create Network using LAN Watch to scan the ForKidz network and execute the scan. LAN Watch should be configured to discover devices and install the default agent package.

### Exercise 8

Configure Naming Policy to automatically move all ForKidz devices into the appropriate machine groups.

### Exercise 9

Configure Domain Watch to discover devices and users in the ittc.com domain. Domain watch should automatically install the default agent package on discovered machines. Execute the scan.

## AI4: Audit: View Assets

---

12

---

A number of agents have been installed, and Kaseya has become aware of other components of the network Infrastructure, as well.

Jose would like to review the devices found so he can be certain he's aware of all network devices on the ITTC and ForKidz networks. He would also like to assign a credential to the machine group floor1.ittc so he can have a centralized place for him, and other technicians, to retrieve the password to the environment's endpoints if they need to troubleshoot.

### Exercise 10

Explore the Audit > View Assets function

### Exercise 11

Explore the Audit > Managed Credentials page

### Exercise 12

Add a managed credential to the ForKidz Router. (Hint: IP address of 192.168.0.1)  
Username: svc\_rc Password: \$Super\$Secret.

## A5: Agent Endpoint (to Endpoint)

13

With all endpoints discovered and agents installed, Jose would like to customize some of the basic settings on the agents.

Change the Working Directory to C:\ITTC and configure the Agent Menu to hide the *Exit* and *Disable Remote Control* options. Modify the Credentials used on the agent to a username of 'ittcadmin' and password of '\$uper\$ecret' for the IT Tech Corp agents only (Omit the single quotes).

### Exercise 13

Configure the Working Directory to c:\ITTC for all machines

### Exercise 14

Configure the Agent Menu to hide *Exit* and *Disable Remote Control* on all machines

### Exercise 15

Configure the Set Credential to ittcadmin/\$uper\$ecret on the IT Tech Corp machines only

## AI1: Audit: Information Review

---

14

---

With Agents installed, Jose would like to review some of the information about the individual workstations.

### Exercise 16

Schedule all audits via Run Now

### Exercise 17

Find Disk Space for DC (Machine Summary > Hardware > Disk Shares)  
Explore available tabs

### Exercise 18

Find sol.exe (Solitaire) on endpoints  
Select DC  
Machine Summary > Software > filter grid to sol.exe (no results on DC)  
Switch view to different machine (note filter remains in place; sol.exe listed)

### Exercise 19

Create Custom Column Set  
(Current User, Time Zone, Contact Name, Contact Email, IP Address, Connection Gateway, Used Space)  
Navigate to Audit > Column Sets, select custom set, explore available data

## RC2: Remote Access: Use

Technicians at IT Tech Corp sometimes need to remote to workstations to assist end users. Periodically connecting to servers may also be required. Jose needs to ensure that he knows how to utilize Kaseya Remote Control to remotely access endpoints.

### Bonus Activity 3

Configure User Role Policy for the System role with the following settings:

- If user is logged in, display alert (use the default alert or optionally customize)
- Require admin note

### Bonus Activity 4

Configure Machine Role Policy for laptop-ceo

- If user is logged in, require permission
- Require admin note
- Optionally enable recording

### Exercise 20

Use the Agent Icon to connect to WS1

Download and Install Kaseya Remote Control Application (If prompted, install the Remote Control package.)

Initiate connection

Control ws1 from your own computer

### Exercise 21

Connect as a Technician User Role to WS2

Initiate connection (Note no Remote Control package needs installation if previous exercise completed)

Log into ws2 to view/accept notification (Will appear if Bonus Activity 3 is completed)

Control ws2 from your own computer

### Exercise 22

Connect as System User Role to laptop-ceo

Initiate connection

Log into laptop-ceo to view/accept notification (Will appear if Bonus Activity 4 is completed)

Control laptop-ceo from your own computer

### Bonus Activity 5

Initiate connection to laptop-ceo

Log into laptop-ceo to view notification. Deny permission.

Review what occurs within VSA when permission is not granted

### Exercise 23

Using FTP, copy any file you'd like from your computer to the working directory of the reception computer

### Exercise 24

Using FTP, copy the file c:\CopyMe.txt from the dc machine.



### Bonus Activity 6

Review processes available in Remote Control > Task Manager. You do not need to terminate any processes as part of this lab, but be sure to know how you could do so, if necessary.

### Exercise 25

Send Message to WS1 “now” as dialogue box to notify the user the machine is scheduled for maintenance tonight at 5 pm. Log into WS1 to review the message.

### Exercise 26

Send Message (blink icon) “now” as dialogue box to WS2. Log into WS2 to view the message.

### Exercise 27

Send Message as browser to Reception to the URL [community.kaseya.com](http://community.kaseya.com).

### Bonus Activity 7

Schedule a message to any machine to display in the future

### Exercise 28

Initiate a Remote Control session to reception using Control Machine function. Optionally enable record session

### Bonus Activity 8

Preinstall KVNC on WS1. Remote using Control Machine. After session completes, uninstall KVNC.

### Exercise 29

Using Live Connect (Ctrl + Click Agent Icon), remote control to any machine

### Exercise 30

Access Live Connect via Quick View

KLC LABS WITH NOTICE: The lab exercises you are about to conduct is intentionally trivial, showing you how most of the tasks performed using other modules of the VSA can also be performed using Live Connect

### Exercise 31-39: Agent Data

31. User Profile: Use Live Connect to set the logon and profile of the end user of WS1

- a. Username: Jill-<username>
- b. Password: user the same password as you’ve used throughout your lab
- c. Contact Name: Jill Matthews
- d. Email Address: Jill-<username>@itcc.com
- e. Phone Number: 305-000-0001

32. Verify Schedules: Use Live Connect to verify Audit and Patch schedules on WS1. You can find these functions on the Pending Procedures tab. Verify the Pending Procedures schedules for these functions match what you configured in your Audit exercise.

33. Review Agent Log: Use Live Connect to determine how frequently the agent on WS1 is checking into the KServer. The entries will look similar to: Received n OOB requests to checkin in the last x min y sec.

34. Review Configuration Changes Log: Use Live Connect to determine who has changed the password for the User Portal (aka Access Portal) on WS1.

35. Review Agent Procedure Log: Determine when the most recent Latest Audit was executed on WS1

36. Patch Status: Use Live Connect to determine whether WS1 is fully patched. If not, manually deploy any remaining patches but be sure to follow the corresponding Patch Policy.

37. Agent Settings: Using Live Connect, check the version of the agent installed on WS1. Verify the Working Directory is configured as c:\kworking.
38. Agent Documents: Create a text file for WS1 that includes some information about WS1. Using Live Connect, upload this document to the KServer so it can be later referenced by you and other VSA users.
39. Get File: Using Live Connect, check what files, if any, have been uploaded from WS1 to the KServer.

### Exercise 40-47: Audit Information

40. Machine Info: Using Live Connect, determine the following information about WS1. If the data is more than a day old, run Latest Audit immediately.
- OS
  - RAM
  - IP Address
  - Connection Gateway
  - Last Reboot
41. Installed Apps: Using Live Connect, determine if 7-Zip has been installed on WS1
42. System Info: Using Live Connect, determine the maximum possible RAM for WS1
43. Disk Volumes: Using Live Connect, determine the disk volumes on WS1
44. PCI & Disk Hardware: Using Live Connect, determine the PCI cards on WS1
45. Printers: Using Live Connect, determine what printers are available to WS1
46. Software Licenses: Using Live Connect, determine the license code and product key of the OS on WS1
47. Add/Remove Programs: Using Live Connect, determine the number of Kaseya agents installed on WS1 and the uninstall string for 7-zip.

### Exercise 48: File Manager

Using Live Connect, copy a file from your local machine to the working directory on WS1

### Exercise 49: Command Shell

Using Live Connect, try to ping kaseya.com and google.com from WS1 without interrupting the machine user's work.

### Exercise 50: Registry Editor

Using Live Connect, and without interrupting the machine user's work, verify the registry key value related to the Kaseya agent icon in the system tray has been updated to show the icon when connected via RDP. If not, add the "–remote" to the end of the value of this key.

## T3: Task: Views

Jose regularly needs to locate machines that have similar configurations or meet specific criteria. He wants to be able to find specific machines and then configure settings or assign tasks to all machines that meet the defined criteria. The creation of Views will help Jose to easily filter to specific agents.

Use a Machine Group Filter to filter to all machines in ForKidz. Once filtered to ForKidz, further filter to only machines containing "laptop" in the name.

Create a view to filter to All Workstation OSs, a view for All Server OSs, and finally a view to filter to machines with the Solitaire application (sol.exe) installed.

### Exercise 51

Use Machine Filter toolbar to filter to all machines in ForKidz

Once filtered to ForKidz, further filter to only machines containing "laptop" in the name

Reset the filter to display all machines

### Exercise 52

Create a View to filter to All Workstation-type Operating Systems

Create a View to filter to All Server-type Operating Systems

Create a View to filter to machines with the Solitaire application (sol.exe) installed

Explore each of the Views created

### Exercise 53

Create an Advanced View to show all machines in PST time zone (HINT: Use time zone offset in hours to create this filter)

### Bonus Activity 9

Edit the Solitaire View to filter to specific version of the app (HINT: Check Audit to verify the version currently installed on at least one machine)

## P1: Patch: Create/Assign Policies

19

In order for Jose and his team to define which Microsoft Update patches will be applied to endpoints, he needs to create and assign Patch Policies. The Patch Policies should have been already created by Alex, but Alex wasn't sure which machines should get which policies. There are some patches that should be blocked for all machines across the board.

Create a "Base" policy for all workstations and servers, and name them "Base Workstations" and "Base Servers" respectively.

Jose also wants servers to have Service Packs tested before they are deployed.

Create a patch policy that blocks all service packs but allows all other patch types through.

Finally, the ForKidz client is using a web-based application that must run on IE8. These machines cannot have Internet Explorer updated beyond what they are currently running. Jose must block all IE updates from all ForKidz machines but be sure to allow all other "base" patches through, and will need a patch policy to specifically accomplish this.

NOTE: Patch Policy Containers and default approval status should have been imported during the Import/Export course.

### Exercise 54

Assign the patch policies to the appropriate machines:

- DC: Base Servers, No Service Packs
- WS1: Base Workstations
- Guest1: Base Workstation
- Laptop1: Base Workstation, No Internet Explorer, No Service Packs
- PC1: Base Workstation, No Internet Explorer

## T2: Tasks: Schedule and Execute

---

20

---

Jose knows he will be scheduling several functions throughout his work in the VSA, but he's not familiar with the scheduler utility and the variances that exist for some modules. He needs to understand the various options available and how he can best schedule tasks in ways that are healthiest for the KServer and network environments.

NO HANDS-ON LABS (scheduling will be explored in future labs)

## P5: Patch: Scan and Status

---

21

---

Both the IT Tech Corp and ForKidz machines need to have Microsoft patches installed on them. In order to determine which patches are available to the machines, Jose needs to execute a patch scan.

Run a patch scan. Also schedule the patch scan to run automatically every Wednesday, during business hours, so any patches released by Microsoft that are applicable to the endpoints can be discovered.

### Exercise 55

Schedule a patch scan on all machines with the following configuration:

- Every Wednesdays
- During business hours for the respective location
- Run an immediate patch scan on all machines

### Bonus Activity 10

Review Patch Status to identify the installed and missing patches

## P6: Patch: Updates

22

Jose has completed the foundation for patching and he's ready to install patches on the machines in his environment. He wants to be sure that the Windows built-in patch utility does not run to install patches - he wants Kaseya to be responsible for all install cycles.

He would also like to verify the machines are configured properly for successful patching and then wants to install updates on the machines. Finally, he would also like to schedule the machines to automatically install all Missing Approved patches on a regular basis.

### Exercise 56

Set Windows Auto Update to Disabled for all machines

### Exercise 57

Run a Patch Test on all machines

### Exercise 58

Schedule an Initial Update on Laptop1 to run immediately.

### Exercise 59

Schedules Automatic Update on all workstations to run weekly on Thursdays. Suspend the schedule on DC.

### Bonus Activity 11

Configure the machines in the ForKidz organization to default to the offline scan source. Attempt to install a patch (approved or denied) using any install method. Check Patch Status to determine if the patch failed. If failed, clear the failure and reattempt install. If patch continues to fail, ignore the patch. Reset the default scan source to Online.

**M1: Monitor: ATSE**

NO HANDS-ON LABS

23

**M2: Monitor: Monitor Sets**

Note: Many of the Monitor-related labs will instruct you to use an email address as part of the alert notifications. For the purposes of these labs, please use your business email address with “.fake” at the end. This will prevent emails from continually flooding an inbox. For example, if Jose’s email address is jose@ittc.com, he would use the email address jose@ittc.com.fake.

Jose must configure monitoring of managed endpoints within the Kaseya VSA for both Internal ITTC machines and the ForKidz computers. He would like to avoid the need to connect to the endpoints in order to check the status of services, processes, and free space on endpoints. He has decided that he will deploy monitor sets for both Workstations and Servers within these environments. On Workstations, he must configure a monitor set to monitor available disk space (<10% free), the Windows Firewall service, and the SNMP process. On Servers, he must configure a monitor set to monitor disk space (<20% free), the windows event log service, and the SNMP process.

**Exercise 60**

Run Update List By Scan on DC and WS2

**Exercise 61**

Create Server Monitor Set

- Counter Thresholds
  - Object: Logical Disk
  - Counter: % Free Space
  - Instance: C:
  - Collection Threshold: The % Free Space data must be collected for Servers once more than 10% of the total disk space has been used. (When there is 90% free space available start collecting data)
  - Alarm Threshold: An Alarm must trigger when the alarm threshold reaches below 10% free space on the total drive of the machine. (Alarm when there is less than 10% free space available on the machine.)
- Services Check
  - Configure a Service Check for the Windows Firewall Service, which will try no attempts with a 0 minute restart interval. The re-arm for this service check must be six hours.
- Process Status
  - Create a Process Status check to alarm when the snmp.exe process is down, the re-arm period must be specified to create additional alarms every 1 hours.



## Exercise 62

Create Workstation Monitor Set

- Counter Thresholds:
  - Object: Logical Disk
  - Counter: % Free Space
  - Instance: C:
  - Collection Threshold: The % Free Space data must be collected for Servers once more than 20% of disk space has been used. (When there is 80% free space available start collecting data)
  - Alarm Threshold: An Alarm must trigger when the alarm threshold reaches below 20% free space on the machine. (Alarm when there is less than 20% free space available on the machine.)
- Services Check
  - Configure a Service Check for the Event Log Service, which will try three restart attempts with a 2 minute restart interval. The re-arm for this service check must be six hours.
- Process Status
  - Create a Process Status check to alarm when the snmp.exe process is down, the re-arm period must be specified to create additional alarms every 6 hours.

## Exercise 63

Assign the Server Monitor Set to DC

## Exercise 64

Assign the Workstation Monitor Set to all workstations

## Exercise 65

Individualize the Monitor Set assigned to the laptop-ceo machine. Change a setting such as the defined threshold for a counter or the number of restart attempts for a service. Commit the change and verify the monitor set appears as individualized for the machine.

### M3: Monitor: Monitor Fixed Alerts

25

Note: Many of the Monitor-related labs will instruct you to use an email address as part of the alert notifications. For the purposes of these labs, please use your business email address with “.fake” at the end. This will prevent emails from continually flooding an inbox. For example, if Jose’s email address is jose@ittc.com, he would use the email address jose@ittc.com.fake.

Jose needs to track some basic changes on all of his managed machines so he can be notified when configurations change, when agents fail to check in for extended periods of time, and whenever new agents are installed. He needs to make sure the router at ForKidz is active, but he does not have direct access to manage that network resource. He'll use Ping Check to ensure the IP address stays available and notify if it does not.

#### Exercise 66

Configure an Agent Offline alert

- Servers: Alert when offline for 1 minute with a 30 minute re-arm period
- Workstations: Alert when offline for 30 days with a 7-day re-arm period
- Set all alerts to create an alarm and a ticket and send an email

#### Exercise 67

Configure an alert to notify when an application is installed or removed on any machine. Set the alert to create an alarm and a ticket and send an email.

#### Exercise 68

Configure an alert to notify when a New Agent is installed in the ForKidz organization. Configure the alert to create a ticket.

#### Exercise 69

Create a System Alert to run a Ping Check on the router at ForKidz site

- Use a name of your choosing
- Only alarm when service does not respond for 1 day
- Ignore additional alarms for 1 day
- Ping 192.168.0.1
- Configure the alert to create an alarm and a ticket and send an email

## M4: Monitor: Monitor Event Logs

26

Note: Many of the Monitor-related labs will instruct you to use an email address as part of the alert notifications. For the purposes of these labs, please use your business email address with “.fake” at the end. This will prevent emails from continually flooding an inbox. For example, if Jose’s email address is jose@ittc.com, he would use the email address jose@ittc.com.fake.

Jose has been tasked to track any error that is generated on endpoints. He does not want to scan through the logs of each machine manually to find these errors. In order to accurately and efficiently identify these errors, he will need to create an Event Log Alert to generate alarms when the errors occur. He will also need to configure a specific Event Log Alert to identify a Kaseya related error.

### Exercise 70

Create Custom Event Log Alert to create a ticket, create an alarm, and send an email when an event is discovered that meets the following criteria:

- Service Filter: \*Kaseya\*
- Categories: All
- Event ID: 55
- Description filter: \*Kaseya Learning Error\*

### Exercise 71

Assign Custom Event Alert to all machines with the following configuration

- Enable Error Log Event Log Level
- Event Log Type: Application Log
- Alert when the event occurs once
- Ignore additional alarms for 10 days
- Actions: Create an alarm, Create a ticket, Send an email

## M5: Monitor: Alarms

27

Note: Many of the Monitor-related labs will instruct you to use an email address as part of the alert notifications. For the purposes of these labs, please use your business email address with “.fake” at the end. This will prevent emails from continually flooding an inbox. For example, if Jose’s email address is jose@ittc.com, he would use the email address jose@ittc.com.fake.

Jose has configured and applied monitor sets to perform critical server and workstation checks. He now needs to review the alarms created based on these checks. He will also require temporary suspension of these checks to eliminate false positives during upgrades and maintenance periods.

### Bonus Activity 12

Use the Alarm filter to view only some of the Alarms. If you do not have any alarms generated in your lab environment, try this task later (after alarms have had an opportunity to generate) or explore the Alarm filter in your production environment.

### Exercise 72

Suspend Alarms on all machines in the ForKidz organization every weekend (HINT: You can either create two separate alarms recurring once every seven days to capture both Saturday and Sunday, or create a single recurring alarm lasting 2 full days.)

### Exercise 73

Suspend Alarms on DC for 30 minutes due to emergency maintenance. Reboot DC and verify no alarms were generated during this period.

## M7: Monitor: Reviewing Monitor Data

28

Note: Many of the Monitor-related labs will instruct you to use an email address as part of the alert notifications. For the purposes of these labs, please use your business email address with “.fake” at the end. This will prevent emails from continually flooding an inbox. For example, if Jose’s email address is jose@ittc.com, he would use the email address jose@ittc.com.fake.

Jose has would like to create a Dashboard so that he can keep open to monitor critical client’s environments. Every time he logs into the Kaseya VSA, he wants the Dashboard to open on login.

### Exercise 74

Create a Dashboard in Monitor. Add any three dashlets you would like. Configure the Dashboard to launch at Startup.

## PM2: Policy Management: Policy Assign

29

Along with the other configurations Alex provided were a number of Policy Management policies. Jose would like Kaseya to automatically assign several settings to machines so he doesn't have to manually configure all settings for new machines.

He'd also like to make sure that all machines, whether they're new or existing, are using standardized configurations. Using Policies will allow Kaseya to be responsible for assigning the appropriate agent settings based on the agent's membership in a view, organization, machine group, etc.

### Exercise 75

Assign Base Workstation, Base Server policies at Global level

Assign the imported *Logs and Working Directory* Policy, inside the Kaseya University\ITTC folder, to the ITTC organization

Assign imported folder *ITTC Floor1 Custom* to ittc.firstfloor Machine Group level

Assign imported folder *ITTC Floor2 Custom* to ittc.secondfloor Machine Group level

### Bonus Activity 13

Reorder policies within the ITTC org-level folder; check settings on machines

Reorder policies within the ITTC group-level folder; check settings on machines

## PM3: Policy Management: Policy Compliance

30

Jose would like to make sure that the policies he's applied are actually controlling the settings properly on the managed machines.

Also, the DC has been behaving oddly and Jose would like to capture the event logs for a longer period of time. The issue is sporadic. He would like the DC to remain "in compliance" but would like to have the logs retained for 90 days. A policy assigned directly to the DC should accomplish this "exception".

### Exercise 76

Explore Policy Management > Machines to review compliance

### Exercise 77

Set Event Log Settings to 90 days for DC (creates an override)

Check Policy > Machines > DC (Note Out of Compliance machine)

Check compliance status icon > note override

Clear Override

Reprocess Policies (Note: DC back in compliance.)

### Exercise 78

Assign imported individual policy to DC (log retention 90 days)

Check event log retention settings on DC

**T7: Tasks: Logs**

---

31

---

Jose has configured several settings on machines, and some of his team members have been running various processes. He would like to review what's been occurring on the machines to better understand who's been making changes and when. Reviewing several logs should help illuminate what's been occurring on the managed machines.

**Exercise 79**

Locate the time and sequence of scripts related to the Initial Update patch cycle on Laptop1 (Config Changes Log)

**Exercise 80**

Locate event ID 55 with the description of "Kaseya Learning Error" in the logs of DC

**Bonus Activity 14**

Create a quick event set from logs for Event ID 55

**Bonus Activity 15**

Review the logs for WS1 using Live Connect



## D1: Dashboards

32

With everything configured, Jose would like to review the environment at a higher level. He knows that there are several dashboards he can review, and would like to have information about the status of his machines presented to him immediately at login. He knows there is information he should look at first thing every day, but sometimes he gets so busy, he forgets. He would like Kaseya to present this information to him automatically.

### Exercise 81

Identify the triggered alarms for machines in ForKidz

### Exercise 82

Customize the dashboard skin

### Exercise 83

Create a custom dashboard to display group alarms and online status. Configure the dashboard to display at login. Verify this configuration (logout/in).

### Bonus Activity 16

Determine the number of Applied v. Not Applied policies

**IC2: Info Center: Execute and Schedule**

---

33

---

Jose needs to be able to gather some information about the state of the environment for his own knowledge. In fact, he plans to use the information in the report to help direct his weekly workload. He needs to determine if there are any patch install failures for any of his managed machines, what alarms have been triggered, and which Operating Systems are in use.

Additionally, ITTC's contract with ForKidz requires a report be provided every month, and Jose's manager just asked him for some data that's needed immediately.

**Exercise 84**

Run General Machine Health report immediately. Run the report against all endpoints.

**Exercise 85**

Schedule General Machine Health to run every Monday at 8am. Run the report against all endpoints.

**Exercise 86**

Schedule General Machine Health to run the last day of every month. Automatically email the results to Sam Jackson at ForKidz. The report should only include the client's machines.

## T6: Tasks: File Management

34

Jose has a contact list that includes all of the names, phone numbers, email addresses, etc. for ITTC Support. Clients should use these contacts when requesting assistance with any technology issues. He knows from past experience that if he emails the contact list to his clients, many will misplace or forget about the list and call him directly for every issue. While Jose doesn't mind helping, he isn't always the right person for every issue. He would like to make the contact list available to every client on their desktop. If they delete the file from the desktop, he would like the file to automatically repopulate. That way, there's no excuse for not knowing how to properly engage Support.

### Exercise 87

Download Contact List from <http://university.kaseya.com/KaseyaUniversity/KU-ContentPack.zip>

Remote Control > FTP > Copy Contact List from local machine to WS1

### Exercise 88

Agent Procedures > Distribute File > contact list to all machines (desktop)

## Answer Key

35

COMING SOON