How can you ask your question?

- Type your question in the GoToMeeting Chat
- From time to time, I will stop to answer them
- If you have a burning question, you can also raise your hand to indicate that you need an answer quickly!
- For offline questions, send them to training@kaseya.com
Important Notes

• Please Follow the Presentation
  – Don’t worry if you can’t complete the LABs.
  – You can finish the labs as homework.

• Review Steps
  – Watch the streaming videos (Step 1)
  – Work with the Interactive Videos (Step 2)
  – Practice in Your Virtual Lab (Step 3)
    • Check the correctness of your work by looking at
      the screenshots included lab review slides at the
      beginning of the next slide set.
  – Scan the Book Chapter & Take the Quiz (Step 4)
Progress Check

• Are you logged into www.it-scholars.com? If not, please login now.

• Have you started your virtual lab? If not, please start your virtual labs for the next 3.5 hours.
Questions?

• Please type your questions in the chat section of your GoToMeeting window.

• Remember that you can always send your questions to training@kaseya.com too.

• If you are falling behind the steps in the lab, please just watch the presentation, take some notes, and perform your labs after the lecture.
Roadmap!

1. **Monday, Day One**
   - Overview
   - System Architecture
   - Agents

2. **Tuesday, Day Two**
   - LAB Review
   - Agent Template and Policy Management Concepts
   - Audit
   - Patch Management

3. **Wednesday, Day Three**
   - LAB Review
   - Monitor
   - Ticketing

4. **Thursday, Day Four**
   - LAB Review
   - Agent Procedures
   - Remote Control
   - Live Connect

5. **Friday, Day Five**
   - LAB Review
   - Agent Template vs. Policy Management
   - System
   - Info Center

www.kaseya.com
Audit Lab Review
Part 1

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

• Create three agent templates
  – “Server”
  – “Instructional”
  – “Guest”

• Put the agent template in the template machine group.
Agent Templates

Screenshot taken after Part 1
Please Skip Part 2 to 4

- Baseline Audit and System Info should be executed only once.

- Baseline Audit, System Info, and Latest Audit are done by default when an AGENT is installed on a machine.

- You can safely skip Part 2, 3, and 4 of the Audit Lab.
Part 5

• Prepare an audit report that contains a list of all the computers within each building.
Inventory Report

Screenshot taken after Part 5

<table>
<thead>
<tr>
<th>Quantity</th>
<th>H/W Type</th>
<th>Vendor</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PCI Network</td>
<td>Advanced Micro Devices</td>
<td>Am79C970/1/2/3/5/6 PCnet LANCE PCI Ethernet Controller</td>
</tr>
</tbody>
</table>

**Machine.Group ID**
- dc.mr.fiu-sadjadi
- guest1.gl.fiu-sadjadi
- laptop1.cec.fiu-sadjadi
- pc1.cec.fiu-sadjadi
Patch Management Lab Review
Part 1

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

Screenshot taken after Part 1
Part 2

- Create a patch policy for servers
  - Name it W2K3-PM-Policy-<USERNAME>.
  - Approve all future Security Updates.
  - Pending Approval for everything else.
  - Deny patches that are optional and have not been superseded by other updates.

- Create a patch policy for workstations
  - Name it XP-PM-Policy-<USERNAME>
  - Approve all future Security Updates.
  - Pending Approval for everything else.
Patch Policies and Membership

Screenshot taken after Part 2

Assign machines to a patch policy.
Each machine must be a member of at least one patch policy in order to install only approved patches via Initial Update and A Update. All patches will be installed regardless of policy settings if a machine is not a member of a patch policy.

Add
Kaseya_SaaS_Patch_Policy
W2K3-PM-Policy-sadjadi
XP-PM-Policy-sadjadi
Remove

Select All
Unselect All

<table>
<thead>
<tr>
<th>Machine Group ID</th>
<th>Policy Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>guest.templates.fi u-sadj...</td>
<td>XP-PM-Policy-sadjadi</td>
</tr>
<tr>
<td>instructional templates....</td>
<td>XP-PM-Policy-sadjadi</td>
</tr>
<tr>
<td>server.templates.fi...</td>
<td>W2K3-PM-Policy-sadjadi</td>
</tr>
</tbody>
</table>
Windows 2003 Patch Policy

Screenshot taken after Part 2
Note

• If the links on this page are not available or some of the patch categories are not listed, it basically means that you have not yet done any patch scan on your machines.

• Make sure to perform a patch scan on dc and one of the XP machines before defining the patch policies.
Windows XP Patch Policy

Screenshot taken after Part 2
Part 3

• 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
  – \192.168.0.10\PatchTemp

• The local directory should be
  – C:\PatchTemp
Patch File Source

Screenshot taken after Part 3

**Patch Management**

- **Manage Machines**
  - Scan Machine
  - Patch Status
  - Initial Update
  - Pre/Post Procedure
  - Automatic Update
  - Machine History

- **Manage Updates**
  - Machine Update
  - Patch Update
  - Rollback
  - Cancel Updates

- **Patch Policy**
  - Create/Delete
  - Membership
  - Approval by Policy
  - Approval by Patch
  - KB Override

- **Configure**
  - Windows Auto Update
  - Reboot Action
  - File Source
  - Patch Alert
  - Office Source

**Machine Group 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.
  - Delete package after install (from working directory)
  - Download from Internet
  - Pulled from system server
    - **Clear Cache**

- **Pulled from file server using UNC path** \192.168.0.10\PatchTemp

- **File share located on**: [dc.mr.fiu-sadjadi](#) → **Machine Group Filter**: fiu-sadjadi.mr

- **in local directory**: c:\PatchTemp

- File server automatically gets patch files from **the Internet** or **the system server**
  - Download from Internet if machine is unable to connect to the file server.

**NOTE:** Requires a Credential for the agent to get access to network drives.
Set Credentials

Screenshot taken after Part 3

<table>
<thead>
<tr>
<th>Machine Group ID</th>
<th>Username</th>
<th>Domain</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>dc.mr.fiu-sadjadi</td>
<td>sadjadi</td>
<td>FIU</td>
<td>Passed</td>
</tr>
<tr>
<td>guest.templates.fiu-sadjadi</td>
<td>sadjadi</td>
<td>FIU</td>
<td>Passed</td>
</tr>
<tr>
<td>guest1.gl.fiu-sadjadi</td>
<td>sadjadi</td>
<td>FIU</td>
<td>Passed</td>
</tr>
<tr>
<td>instructional.templates.fiu-sadjadi</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>laptop1.cec.fiu-sadjadi</td>
<td>sadjadi</td>
<td>WORKGROUP</td>
<td>Passed</td>
</tr>
<tr>
<td>pc1.cec.fiu-sadjadi</td>
<td>sadjadi</td>
<td>WORKGROUP</td>
<td>Passed</td>
</tr>
<tr>
<td>server.templates.fiu-sadjadi</td>
<td>sadjadi</td>
<td></td>
<td>Passed</td>
</tr>
<tr>
<td>ws1.scis.fiu-sadjadi</td>
<td>sadjadi</td>
<td>FIU</td>
<td>Passed</td>
</tr>
</tbody>
</table>
Patch File Source

Screenshot taken after Part 3
Part 4

• 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.
Patch Reboot Action

Screenshot taken after Part 4
Part 5

• Now that we have setup the patch policies to our liking, we need to schedule automatic update on the agent templates too.
Patch Automatic Update

Screenshot taken after Part 5

**IT Scholars Kaseya Fundamentals Workshop**

- **Machine ID:** [Field for Machine ID]
- **Machine Group:** fiu-sadjadi.templats
- **View:** < No View >

### Machine Management

**Automatic Update**

- **Machine ID**:
  - guest.templates.fiustadjadi
  - instructional.templates.fiustadjadi
  - server.templates.fiustadjadi

- **Next Run**:
  - guest.templates.fiustadjadi: 5:54:00 am 25-Jan-12
  - instructional.templates.fiustadjadi: 5:29:00 am 25-Jan-12
  - server.templates.fiustadjadi: 5:20:00 am 25-Jan-12

- **Recurrence**:
  - Daily every 1 day(s)

**WARNING**: Automatic Update is suspended for a machine while Initial Update is being processed. Automatic Update will automatically resume when Initial Update completes.

**Schedule**

- **Skip if machine offline**

**Kaseya**

- **Scan Machine**
- **Patch Status**
- **Initial Update**
- **Pre/Post Procedure**
- **Manage Machines**
- **Machine History**
- **Manage Updates**
- **Machine Update**
- **Patch Update**
- **Rollback**
- **Cancel Updates**
- **Patch Policy**
- **Create/Delete**
- **Membership**
- **Approval by Policy**
- **Approval by Patch**
- **KB Override**
- **Configure**
  - Windows Update
  - Reboot Action
  - File Source
  - Patch Next
Part 6

• 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.
Patch Copy Settings

Screenshot taken after Part 6

Copy agent settings from `instructional_templates/fiu-sadjadi` to all selected machine IDs.

Select which settings to copy from `instructional_templates/fiu-sadjadi`

Select the settings you want to copy from specialized template accounts. Select the Add option to add settings to target machines without replacing existing settings.

- Credential
- Agent Menu
- Checkin Control
- Working Directory
- Logs
- Machine Profile
- View Collections
- Portal Access
- Remote Control Policy
- Patch Settings
- Patch File Source
- Patch Policy Memberships
- Fixed Alerts
- Event Log Alerts
- Monitor Sets
- Distribute Files
- Protection
- Agent Procedure Schedules

Select All

Select All

Select All

- Do Not Copy
- Replace
- Add

60 min

Spread agent procedure schedules when copying to multiple machines

Done
Cancel
### Patch Scan

*Screenshot taken after Part 6*

#### IT Scholars Kaseya Fundamentals Workshop

**KServer - Operational**  
**Role:** System  
**System:**  
**Scope:** System  

**09:30:00 No Timer Running**  
**sadjadi@cs.fiu.edu**  
**LogOff**

#### Manage Machines
- **Scan Machine**
  - Machine ID:  
  - Machine Group: flu-sadjadi

#### Manage Updates
- **Machine Update**
  - Patch Update
  - Rollback
  - Cancel Updates

#### Patch Policy
- **Create/Delete**
  - Membership
  - Approval by Policy
  - Approval by Patch
  - KB Override

#### Configure
- **Windows Auto Update**
  - Reboot Action
  - File Source
  - Patch Alert
  - Office Source

### Schedule Scans for Missing Patches and Updates
- **Check boxes to select machines for patch scan**
- **Select All**  
- **Deselect All**  
- **Done**  
- **Cancel**  
- **Run Now**

<table>
<thead>
<tr>
<th>Machine Group ID</th>
<th>Last Scan</th>
<th>Next Scan</th>
<th>Recurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>do:mr.fiu-sadjadi</td>
<td>24-Jan-12 6:14:49 pm</td>
<td>25-Jan-12 3:58:00 am</td>
<td>Daily every 1 day(s)</td>
</tr>
<tr>
<td>guest.templates.fiu-sadjadi</td>
<td>24-Jan-12 3:33:00 am</td>
<td>25-Jan-12</td>
<td>Daily every 1 day(s)</td>
</tr>
<tr>
<td>guest1.gl.fiu-sadjadi</td>
<td>24-Jan-12 6:25:17 pm</td>
<td>25-Jan-12 3:40:00 am</td>
<td>Daily every 1 day(s)</td>
</tr>
<tr>
<td>instructional.templates.fiu-sadjadi</td>
<td>24-Jan-12 3:15:00 am</td>
<td>25-Jan-12</td>
<td>Daily every 1 day(s)</td>
</tr>
<tr>
<td>laptop1.cec.fiu-sadjadi</td>
<td>24-Jan-12 6:24:53 pm</td>
<td>25-Jan-12 3:04:00 am</td>
<td>Daily every 1 day(s)</td>
</tr>
<tr>
<td>pc1.cec.fiu-sadjadi</td>
<td>24-Jan-12 6:24:37 pm</td>
<td>25-Jan-12 3:07:00 am</td>
<td>Daily every 1 day(s)</td>
</tr>
<tr>
<td>server.templates.fiu-sadjadi</td>
<td>24-Jan-12 3:45:00 am</td>
<td>25-Jan-12</td>
<td>Daily every 1 day(s)</td>
</tr>
<tr>
<td>ws1.scis.fiu-sadjadi</td>
<td>24-Jan-12 6:28:43 pm</td>
<td>25-Jan-12 3:17:00 am</td>
<td>Daily every 1 day(s)</td>
</tr>
</tbody>
</table>
Patch Status

Screenshot taken after Part 6

The system resets test results every time File Source or Set Credential changes.

**NOTE:** Machines that are being processed by Initial Update will NOT be tested.

<table>
<thead>
<tr>
<th>Machine Group ID</th>
<th>Installed Patches</th>
<th>Missing Approved</th>
<th>Missing Denied</th>
<th>Missing Manual</th>
<th>Pending User Not Ready</th>
<th>Failed Patches</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>dc.mr.fiu-sadjadi</td>
<td>54</td>
<td>-</td>
<td>7</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Untested</td>
</tr>
<tr>
<td>guest1.gl.fiu-sadjadi</td>
<td>118</td>
<td>25</td>
<td>31</td>
<td>-</td>
<td>-</td>
<td>25</td>
<td>Untested</td>
</tr>
<tr>
<td>laptop1.cec.fiu-sadjadi</td>
<td>142</td>
<td>-</td>
<td>31</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Untested</td>
</tr>
<tr>
<td>pc1.cec.fiu-sadjadi</td>
<td>143</td>
<td>-</td>
<td>31</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Untested</td>
</tr>
<tr>
<td>ws1.scis.fiu-sadjadi</td>
<td>140</td>
<td>2</td>
<td>31</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Untested</td>
</tr>
</tbody>
</table>
Verify the File Source Settings

Screenshot taken after Part 6
Part 7

• Disable Windows Automatic Update for all computers.
Patch Windows Auto Update

Screenshot taken after Part 7

Configure Windows Automatic Update.

- **Disable** - Disable Windows Automatic Update to let patch management control system patching.
- **User control** - Let machine users control Windows Automatic Update.
- **Configure** - Force Windows Automatic Update configuration to the following settings:
  - Automatic Update Options: Automatically download and schedule installation
  - Schedule on Every Day at 3:00 am
  - Force auto-reboot if user is logged on

<table>
<thead>
<tr>
<th>Machine Group ID</th>
<th>Machine Updated</th>
<th>Windows Automatic Update Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>dc.mr.fiu-sadjadi</td>
<td>Disabled.</td>
<td></td>
</tr>
<tr>
<td>guest1.gl.fiu-sadjadi</td>
<td>Disabled.</td>
<td></td>
</tr>
<tr>
<td>laptop1.cec.fiu-sadjadi</td>
<td>Disabled.</td>
<td></td>
</tr>
<tr>
<td>pc1.cec.fiu-sadjadi</td>
<td>Disabled.</td>
<td></td>
</tr>
<tr>
<td>ws1.scis.fiu-sadjadi</td>
<td>Disabled.</td>
<td></td>
</tr>
</tbody>
</table>
Part 8

- Prevent Internet Explorer from installing by using KB Override.
  - The KB article is KB944036.
Patch KB Override

Screenshot taken after Part 8
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

• Prepare a patch management report that contains a brief overview of the patches.
Patch Report

Screenshot taken after Part 8
Progress Check

- Are you done with all the Audit and Patch Management labs?

- Have you checked the correctness of your work?
Questions?

• Please type your questions in the chat section of your GoToMeeting window.

• Remember that you can always send your questions to training@kaseya.com too.

• If you are falling behind the steps in the lab, please just watch the presentation, take some notes, and perform your labs after the lecture.
Motivation

• Knowing that disk space utilization on a computer has reached a predefined threshold can trigger a few simple automated steps to prevent disastrous situations.

• Proactive and preventive system maintenance is only possible with accurate and easily accessible information regarding the key aspects of the states of all the computers and peripherals within the network.
Background

- **How?**
  - The required information must be collected
  - Categorized as to the severity of the issues
  - Be presented to the user

- **Warning!**
  - Too much info. is equivalent to no information.
  - Be very selective on what data to collect.

- **What is available?**
  - Commodity operating systems support facilities to collect the needed data on an ongoing basis.
What is an Alarm?

• An alarm is a warning of an existing or approaching danger

• We refer such situation by indicating that an alarm condition exists.

• For example, an alarm condition exists when a machine's performance succeeds or fails to meet pre-defined criteria.

• To check whether an alarm condition exist we need to *monitor* the environment.
How to Monitor?

1. Event-based
   - **Alerts**: Monitors events on agent-installed machines.
   - **System Check**: Monitors events on non-agent-installed machines.
   - **Log Monitoring**: Monitors events in log files.

2. State-based
   - **Monitor Sets**: Monitors the performance state on agent-installed machines.
   - **SNMP Sets**: Monitors the performance state on non-agent-installed devices.
How to monitor state?

• Using Monitor Sets or SNMP Sets, i.e., sets of counter objects, counters, counter instances, services and processes used to monitor the performance of machines.

• Basically we collect sample values of some counters associated with some performance object instances at a predefined interval.

• For example, to monitor the percentage of processor time, we collect sample values of the “% Processor Time” counter.
Performance Object

• A logical collection of counters that is associated with a resource or service that can be monitored.

• For example, processors, memory, and physical disks each have their own sets of predefined counters.
Performance Object Instance

• A term used to distinguish between multiple performance objects of the same type on a computer.
• For example, multiple processors or multiple physical disks.
• The VSA lets you skip this field if there is only one instance of an object.
Performance Counter

- A data item that is associated with a performance object, or if more than one instance of the object exists, the data associated with each instance of the object.
- Each selected counter presents a value corresponding to a particular aspect of the performance that is defined for the performance object and instance.
Windows Performance Monitor
Monitor Set

• Update Lists by Scan
  – Counters, Services, and Event Log Types

• Monitor Perfmon Object Counters

• Monitor Windows Services

• Monitor Windows Processes
LAB

• Assumptions
  – You have not put in place a way to monitor hardware and software performance on all computers simultaneously.
  – This prevents your IT technician from having an accurate way of knowing if all computers are at optimal performance.

• Tasks
  – Use the Kaseya Monitor module facilitates to develop a proactive maintenance solution.
LAB

• Tasks
  – Create a monitor set for servers
    • Monitor the DNS service
    • Total CPU usage
    • Available main memory
    • Page file usage
    • Free storage memory on C drive with trending
  – Create a monitor set for desktops
    • Monitor TermService service
    • Percentage of available storage memory space
    • Available main memory
  – Assign the monitor sets
1. Open the Monitor module. Go to Edit > Update Lists By Scan.
2. Select checkboxes for all machines.
3. Click on the Run Now button.
Monitor Set for Servers

4. Open the Monitor module. Go to Edit > Monitor Sets.
5. Select the folder “myMonitorSets - <USERNAME>”.
6. Click on the New MonitorSet button.
Monitor Set for Servers

7. Type in “Server Set - <USERNAME>” in Monitor Set Name.
8. Select System Check in the Group Alarm Column.
9. Click on Save.
Monitor Set for Servers

10. Click on the *Services Check* button.

11. Click on *Add*.
12. Select DNS in the Services dropdown box.
13. Type in 5 in the Re-start attempts textbox and leave the other options with their default values.
14. Click on Save.
15. Click on the *Counter Thresholds* button.
16. Click on *Add*.
17. Select *Processor Performance* in the *Object* dropdown box.
18. Select *% of Maximum Frequency* in the *Counter* dropdown box.
19. Select *Next*.

**Monitor Set for Servers**

- **17. Select Processor Performance**
- **18. Select % of Maximum Frequency**
- **19. Click Next**
Monitor Set for Servers

20. Select Over in the Collection Operator dropdown box, enter 10 in the Collection Threshold field, set Sample Intervals to 1 Minute, select Over in the Alarm Operator dropdown box, enter 50 in the Alarm Threshold field, set the Duration to 5 Minutes, and select Next.
Monitor Set for Servers

21. Select Save.

21.1 Click Save.
Note

• When setting the collection threshold, you need to make sure that the collected data range includes the alarm threshold.

• For example, in this exercise, as the collection operator is selected as Over, the Collection Threshold must be smaller than 50, which is set for the Alarm Threshold.
Note

• When setting the sample interval, you need to make sure that there is enough number of samples within the duration that you will be used to collect the data from the agent.

• For example, in this exercise, we set the Sample Intervals to 1 Minute so that there are 5 samples within each Duration of 5 Minutes.

• WHAT IS THE OPTIMAL SAMPLING INTERVAL?
22. Click on **Add**.
Monitor Set for Servers

23. Select *Memory* in the *Object* dropdown box.
24. Select *Available MBytes* in the *Counter* dropdown box.
25. Click *Next*. 

*Select the Object you wish to monitor. Specify the related counter and instance (some objects do not have instances). Counters to notify you when system objects fall out of desired operational range.*

*Optionally change the name used to refer to this counter object. The default name is the object name from step 1.*
Monitor Set for Servers

26. Set *Sample Intervals* to 1 Minute, set the *Duration* to 5 Minutes, leave everything else as its default value, and click *Next.*

26.1 Set *Sample Interval* to 1 minute

26.2 Set *Duration* to 5 minutes

26.3 Click *Next*
Monitor Set for Servers

27. Click Save.

Warning Level: When the counter is within this percent of the alarm level, the system displays a warning. Warnings only appear on the status displays and are not logged.

Warn when within X% of alarm threshold:

10

Warning will be at: 45 (alarm at: 50)

Trending Alarm: Uses historical counter data to predict when the next alarm occurs. Generate trending alarm when predicted alarm happens in Trending Notice seconds/minutes/days.

Trend Activated?:

No - Trending is not needed

Trending Window:

14 Days

Ignore additional 'trending' alarms for:

1 Hours

27 Click Save
28. Click on *Add*.
29. Select *Paging File* in the *Object* dropdown box.
30. Select *% Usage* in the *Counter* dropdown box.
31. Click *Next*. 
32. Set Sample Intervals to 1 Minute, set the Duration to 5 Minutes, leave everything else as its default value, and click Next.
Monitor Set for Servers

33. Select Save.

Warning Level: When the counter is within this percent of the alarm level, the system displays a warning. Warnings only appear on the status displays and are not logged.

Warn when within X% of alarm threshold:

<table>
<thead>
<tr>
<th>%</th>
<th>Warning will be at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>45 (alarm at: 50)</td>
</tr>
</tbody>
</table>

Trending Alarm: Uses historical counter data to predict when the next alarm occurs. Generate trending alarm when predicted alarm happens in Trending Notice seconds/minutes/days.

Trend Activated? :

- No - Trending is not needed

Trending Window:

<table>
<thead>
<tr>
<th>Days</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td></td>
</tr>
</tbody>
</table>

Ignore additional 'trending' alarms for:

**27 Click Save**
Monitor Set for Servers

34. Click on Add.

| Object    | Counter             | Instance  | Counter Name | Description | Collection Operator | Collection Threshold | Sample Interval | Alarm Operator | Alarm Threshold |
|-----------|---------------------|-----------|--------------|-------------|---------------------|--------------------|-----------------|---------------|----------------|----------------|
| Processor| % of Maximum Frequency | ProcessorPerformance | ProcessorPerformance | Over | 10 | 1 min | Over | 50 |
| Memory   | Available MBytes    | Memory    | Memory       | Over       | 20 | 1 min | Over | 50 |
| Paging   |                     | Paging File | Paging File | Over  | 20 | 1 min | Over | 50 |

34 Click on Add
Monitor Set for Servers

35. Select *LogicalDisk* in the *Object* dropdown box.
36. Select *% Free Space* in the *Counter* dropdown box.
37. Select *C:* in the *Instance* dropdown box.
38. Click Next.
Monitor Set for Servers

39. Set Sample Intervals to 30 Minutes, set the Duration to 6 Hours, leave everything else as its default value, and click Next.

39.1 Set Sample Interval to 30 minutes

39.2 Set Duration to 6 hours

39.3 Click Next
Monitor Set for Servers

40. Select Save.

Warning Level: When the counter is within this percent of the alarm level, the system displays a warning. Warnings only appear on the status displays and are not logged.

Warn when within X% of alarm threshold:

10
Warning will be at: 45 (alarm at: 50)

Trending Alarm: Uses historical counter data to predict when the next alarm occurs. Generate trending alarm when predicted alarm happens in Trending Notice seconds/minutes/days.

Trend Activated?
No - Trending is not needed

Trending Window:
14 Days
1 Hours

Ignore additional ‘trending’ alarms for:

<<Back  Save  Cancel   * Required Field

40 Click Save
Monitor Set

- Collection Threshold sets the value limit for the Kaseya Agent to collect and store the value into the Database.

- Alarm Threshold sets the value limit for the Kaseya Server to create an alert. The duration is referencing the duration held by PerfMon. It does not refer to the Collection Threshold sampling interval.

Note: Remember that object dropdown names are as follows: CPU = Processor Performance, main memory = Memory, page file = Paging File, storage memory = LogicalDisk.
Trending Alarm

- If Trending Alarm is activated. The monitor set will predict that an alarm will occur in the future determine by Trending Window.

- In order for a Trending Alarm to be successful, you must have historical counters that have hit the alarm threshold values.
It Is Your Turn!

Progress Check

- Do you know these terms?
  - Alarm?
  - Alert?
  - Monitor Set?

- How can you develop a monitor set?

- How do you interpret the monitor logs?

- Do you know the different ways to respond to an alarming situation? Raise an alarm? Submit a ticket? Run an agent procedure? Or simply send an email?
Questions?

• Please type your questions in the chat section of your GoToMeeting window.

• Remember that you can always send your questions to training@kaseya.com too.

• If you are falling behind the steps in the lab, please just watch the presentation, take some notes, and perform your labs after the lecture.
Monitor Set for Workstations

HOMEWORK

• Create a Monitor Set that will be established in the desktop templates.
  – Monitor the TermService service
    • If the TermService services fails, immediately restart it.
    • NOTE: Microsoft Windows TermService services usually are not installed on Desktop workstation, unless RDP is enabled. If the Windows Service does not exist an alert will be triggered.
  – Monitor the total percentage of storage memory space.
  – Monitor the available main memory.
Monitor Set for Desktops

41. Open the Monitor module. Go to Edit > Monitor Sets.
42. Select the folder “myMonitorSets - <USERNAME>”.
43. Click on the New MonitorSet button.
Monitor Set for Desktops

44. Type in “DesktopSet - <USERNAME>” in the Monitor Set Name textbox.

45. Select System Check in the Group Alarm Column.

46. Click on Save
Monitor Set for Desktops

47. Click on the *Services Check* button.
48. Click on *Add*.
49. Select TermService in the Services dropdown box.
50. Type in 3 in the Re-start attempts textbox.
51. Click on Save.
52. Click on the *Counter Thresholds* button.
53. Click on *Add.*
Monitor Set for Desktops

54. Select LogicalDisk in the Object dropdown box.
55. Select % Free Space in the Counter dropdown box.
56. Select _Total in the Instance dropdown box.
57. Select Next.
58. Set Sample Intervals to 30 Minutes, set the Duration to 6 Hours, leave everything else as its default value, and select Next.

58.1 Set Sample Interval to 30 minutes

58.2 Set Duration to 6 hours

58.3 Click Next
Monitor Set for Desktops

59. Click Save.
Monitor Set for Desktops

60. Click on Add.

Click on Add.
Monitor Set for Desktops

61. Select Memory in the Object dropdown box.
62. Select Available MBytes in the Counter dropdown box.
63. Select Next.
64. Set Sample Intervals to 1 Minute, set the Duration to 5 Minutes, leave everything else as its default value, and select Next.

64.1 Set Sample Interval to 1 minute

64.2 Set Duration to 5 minutes

64.3 Click Next
Monitor Set for Desktops

65. Click Save.

65. Click Save.
Monitor Set for Desktops

66. Go to Monitor module > Agent Monitoring > Assign Monitoring.

67. Select “serverSet - <USERNAME>” in the dropdown box.

68. Select the “Server” template.

69. Click on Apply.

70. Repeat steps 66-69 for the Instructional and Guest templates.
Progress Check

How does a monitor set for a workstation different than that of a server?
Questions?

- Please type your questions in the chat section of your GoToMeeting window.

- Remember that you can always send your questions to training@kaseya.com too.

- If you are falling behind the steps in the lab, please just watch the presentation, take some notes, and perform your labs after the lecture.
Assign Monitor Sets

• After defining monitor sets, you need to assign these monitor sets to machines.
• You can only assign monitor sets that you have edit rights to.
• Review the email alerts – Format Email button
  – Review the content help for variables used within the email
Why Alerts?

• Setting alerts is one good approach to staying informed when a certain event of interest is triggered.

• You can set the alert to generate an alarm, which will in turn be added to the Alarm Logs in Kaseya VSA, or you can set it up so that it sends an email to you if your quick attention is needed.
Why Alerts?

• Generating an alarm can be used mainly for logging and documenting an alarm condition, while alerting via email can be used if the issue is more important.

• Alerts can also create tickets, which will be discussed later; this feature is useful in cases that addressing an alarm condition would need creation of a service request that can be tracked.
Agent Alerts

- **Agent Status**
  - Alerts when Agent is offline

- **Application Changes**
  - Alerts when an application is installed or removed

- **Get Files**
  - Alerts when an agent procedure executes a Get File command and receive a different copy than previous Get File command.

- **Hardware Changes**
  - Alerts when a hardware configuration changes

- **Low Disk**
  - Alerts when free disk space falls below a specified percentage

- **LAN Watch**
  - Alerts when an AGENT-LAN Watch function detects new machines

www.kaseya.com
Agent Alerts

- **Agent Procedure Failure**
  - Alerts when an agent procedure failed to execute
- **Protection Violation**
  - Alerts when an access violation is detected
- **New Agent Installed**
  - Alerts when a new agent reports in for the first time
- **Patch Alert**
  - Alerts when a threshold is triggered for patch management events
- **System**
  - Alerts when selected system event occurred on the Kaseya Server
Creating Alerts

• For all server machines
  – Alert when an agent is not checked in for at least 5 minutes
  – Alert for all error events from both System and Application Log

• For all desktop machines
  – Alert when an agent has not checked in for at least 30 days
  – Alert for any hardware or software changes
    • exclude VMware and Windows update changes.
Creating Alerts for Servers

71. Open the Monitor module. Go to Agent Monitoring > Alerts.
72. Select Agent Status in the Select Alert Function dropdown box.
73. Click on the “server.templates.fiu-<USERNAME>” template checkbox.
74. Make sure that the Create Alarm checkbox and Email Recipients checkboxes are selected. Type in your email address in the textbox below the Email Recipients.
75. Click on Agent has not checked in for and set the time for 5 minutes. Rearm alert after 10 days.
76. Make sure that Create Ticket and Run Script checkboxes are NOT selected.
77. Click on Apply.
Creating Alerts for Servers

71. Click on Agent Monitoring > Alerts

72. Select Agent Status

74.1. Select Create Alarm

74.2. Select Email Recipients

75. Click on Agent has not checked in for and set the time for 5 minutes. Rearm alert after 10 days

76. Make sure Create Ticker and Run Script checkboxes are NOT selected

77. Click on Apply

73. Click on the “server” template
Creating Alerts for Servers

78. Select Agent Monitoring > Event Log Alerts.
79. Select Application in the Select Event log type drop-down list.
80. Select the Error checkbox.
81. Select the server.templates.fiu-<USERNAME> template checkbox.
Creating Alerts for Servers

82. Click on *Set Alert Actions* tab.
83. Check *Create Alarm*, *Create Ticket* and *Email Recipients*; enter your email address if it isn’t already present.
84. Click on *Apply*.
85. Repeat Steps 78 - 84 for System event log type instead of Application event log type.
Note

• To be able to monitor the Event Logs, it is necessary to set VSA to collect the required event logs.

• For this, you need to go to the Agent module and select the *Machine Status > Event Log Settings* page. Using this page, you can select the logs required for this exercise to be collected.
Note

• If you have not set the Event Log Settings correctly, you see "Note: Red letters indicate logging disabled." in the Monitor > Event Log Alerts page. Specifically, those event logs that are disabled and need your attention are shown in red under the EWISFCV column.

• For example, if you have set a monitoring alert on Error and Warning, and the corresponding event logs for Error are not enabled, you see EW------.
Capturing Event Logs

• **Under Agent > Event Log Settings**
  – Select the Event Log Types and the Event Categories to capture.
Windows Event Log

- **Source** - The application that produced the event log
- **Event ID**
- **Details** - The description of the event
- **Event Log Sets** define the Agent Alert to create an alarm for specific events.
Progress Check

- What are alerts?
- How alerts are different from monitor sets?
- How event-based monitoring is different from state-based monitoring?
- How can you collect some of the Event Logs from agents and create alerts based on the contents of the collected event logs?
Questions?

• Please type your questions in the chat section of your GoToMeeting window.

• Remember that you can always send your questions to training@kaseya.com too.

• If you are falling behind the steps in the lab, please just watch the presentation, take some notes, and perform your labs after the lecture.
Creating Alerts for Workstations

• Create alerts on the Instructional and Guest templates.
  – Set an alert that creates an alert and notifies the admin via email when an agent is not checked in for at least 30 days.
  – Set an alert that creates an alert that is triggered when there are any software changes.
    • For software alerts, exclude VMware and Windows changes.
Creating Alerts for Workstations

86. Open the Monitor module. Go to Agent Monitoring > Alerts.
87. Select Agent Status in the Select Alert Function dropdown box.
88. Click on the “guest.templates.fiu-<USERNAME>” and the “instructional.templates.fiu-<USERNAME>” template checkboxes.
89. Make sure that Create Alarm and Email Recipients checkboxes are selected.
90. Make sure that Create Ticket and Run Script are not selected. Type in your email address in the textbox below.
91. Click on Agent has not check in for and set the time for 30 minutes. Rearm alert after 1 hour.
92. Click on Apply
Creating Alerts for Desktops

86. Click on Agent Monitoring > Alerts

87. Select Agent Status

88.1 Click on the “guest” template

88.2 Click on the “instructional” template

89.1 Select Create Alarm

89.2 Select Email Recipients

90. Make sure Create Ticker and Run Script checkboxes are NOT selected

91. Click on Agent has not checked in for and set the time for 30 days. Rearm alert after 1 hour

92. Click on Apply
Creating Alerts for Workstations

93. Select *Application Changes* in the *Select Alert Function* dropdown box.

94. Select the “*instructional.templates.fiu-<USERNAME>*” and “*guest.templates.fiu-<USERNAME>*” template checkboxes.

95. Make sure that the *Create Alarm* and *Email Recipients* checkboxes are selected.

96. Make sure that *Create Ticket* and *Run Script* are not selected.

97. Type in “*\Windows\*” in the *Exclude directories* text box.

98. Click on *Apply*. 

www.kaseya.com
Creating Alerts for Workstations

93. Select Application Changes

94.1 Click on the “guest” template

94.2 Click on the “instructional” template

95.1 Select Create Alarm

95.2 Select Email Recipients

96. Make sure Create Ticker and Run Script checkboxes are NOT selected

97. Type in “Windows”

98. Click on Apply
Creating Alerts for Workstations

99. Type in "*\VMware\*" in the Exclude directories text box.

100. Click on Apply.

101. Repeat steps 93 - 98, exclude step 97, for the Hardware Changes.
Note

• Using (*) is considered a wildcard.
• To include using all subdirectories within the folder, use (\*) following the folder name.
LAB

• Assumptions
  – All the three agent templates contain all the alert settings.

• Tasks
  – Push the settings captured in the templates to all the currently deployed agents with the similar roles.
Copy Settings to Assign Monitor Sets

102. Select all the computers in the MR building.

103. Click on the Copy button.

104. Repeat steps 108-112 for the Instructional and Guest templates.
Note

• Monitoring alerts can be assigned to the agents directly.

• We ask you to add them to the templates, however, this is not a requirement in a real world environment where you may have a limited number of machines with similar monitor sets.
Alarm Remediation

• Creating Alerts allows you to use the Alarm Summary and the Dashboards.

• The Alarm Summary page displays alarms for all machine IDs that match the current machine ID / group ID filter. You can include additional filtering for listed alarms using fields in the Alarm Filters panel.

• You can also close alarms or re-open them and add notes to alarms.

• Tickets can be created from an alarm with all the alarm notes and messages.
Alarm Remediation

- Using the Filters to find the issues
Dashboard List

• The Dashboard is a visual tool that filters out the alerts generated from your assigned monitoring
  – You can set up Group Alarm Columns to further define the types of issues.
  – The monitor set is assigned to the specific group alarm column so that when the condition is met the filter is applied.
### Define Monitor Sets

**Monitor Set Name**
- critical.diskspace1gb.alldrives.counter

**Monitor Set Description**
- Counter-based Disk Space Monitoring, \( \leq 750 \text{MB} \) Free Space Alarm

**Enable Counter Matching**
- Checked

### Group Alarm Column Name:

- Other

### Counter Name

<table>
<thead>
<tr>
<th>Object</th>
<th>Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogicalDisk</td>
<td>Free Megs</td>
</tr>
</tbody>
</table>

### Table

<table>
<thead>
<tr>
<th>Counter Name</th>
<th>Description</th>
<th>Collection Operator</th>
<th>Collection Threshold</th>
<th>Sample Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogicalDisk</td>
<td>Monitors LogicalDisk obj...</td>
<td>Over</td>
<td>0</td>
<td>20 min</td>
</tr>
</tbody>
</table>
Monitor Dashboard

- Status view of OPEN Alerts in Alarm Summary
Progress Check

- How do you perform alarm remediation?
- What would be a good monitor dashboard for your company?
Questions?

• Please type your questions in the chat section of your GoToMeeting window.

• Remember that you can always send your questions to training@kaseya.com too.

• If you are falling behind the steps in the lab, please just watch the presentation, take some notes, and perform your labs after the lecture.
Kaseya Fundamentals Workshop

TICKETING
Background Story

• While deployed agents provide extremely useful information regarding the state of all managed machine, facilitating regular automated system maintenance tasks, your team must still perform sporadic maintenance tasks, based on random user requests and daily server problems reported by agents.
Background Story

• In addition, all such tasks must be performed in a manner that minimizes overall disruptions in the work environment.

• However, the large number of managed machines and users, and different levels of severity associated with reported problems has forced you to adopt an ad-hoc respond approach, which has proven not to be efficient when it comes to providing adequate and timely user support.
Background Story

- Without an automated system to organize and prioritize user support requests, the user support task becomes tedious and unmanageable.

- In addition, relying on email as the only communication medium between the user and maintenance technicians creates an unorganized environment where the number of service requests greatly exceeds the technicians’ capacity to handle the requests.
Background Story

• Therefore, you decided to use the Kaseya’s ticketing system and pair it up with your already in-place email system to keep requests organized and prioritized, and to document the progress towards the completion of each request.

• Kaseya’s Ticketing module enables you to manage service requests.

• It also allows you to create, distribute, edit, or resolve ticket submissions.
LAB

• Management wants a ticketing system implemented to facilitate user support requests.
• The ticketing system must be customized to adequately fit into the rest of your support environment.
• The individual tickets must have two status fields: “Awaiting Customer Feedback” and “Awaiting Customer Approval”.

www.kaseya.com
LAB

• In addition, priority or urgency of tickets must be set to medium by default and the ticket creation process must allow the submitter to select the priority of the ticket.

• The submitter should also be allowed to view the SLA (Service Level Agreement) type to select whether the issue is server or workstation related.

• You need to be notified when new tickets are created.
LAB

• The submitter must be notified when a note has been added to their ticket.
• Support-request emails must be directed to the corresponding support group.
• If a ticket is created, or if a new note was added to a previous ticket, the submitter should automatically receive an email.
• Due dates should be automatically set to expedite tickets, especially server tickets due to their importance.
LAB

• If any ticket is overdue, Kaseya should automatically send an email to you, as the head technician.

• To test the ticketing system you are to create five tickets reporting different issues on different machines.

• Creating the tickets will make sure the settings are working and will give you a general understanding of how the ticketing module works.
LAB

• Tasks
  – Add two status fields into the ticketing system
    • “<USERNAME>-Awaiting Customer Feedback”
    • “<USERNAME>-Awaiting Customer Approval”
  – The default value of Priority must be “Medium”.
  – Allow ticket submitters
    • to select the priority level themselves
    • to choose the SLA type
  – Configure Kaseya
    • to send you an email when a new ticket is created
    • to inform thesubmitter when a note is added
Note

- As the new fields added into the ticketing system by any technician will have a global impact (all the other technicians and end users will see that too), to make sure that you were able to finish this exercise, we are asking you to include your username (indicated as <USERNAME>) to the beginning of the fields that you add.

- Of course, in a production environment, only one technician would need to configure the ticketing system.
New Fields in the Ticket Form

- Allow tickets to contain the status fields, “<USERNAME>-Awaiting Customer Feedback” and “<USERNAME>-Awaiting Customer Approval”.

1. Open the Ticketing module. Go to Configure Ticketing > Edit Fields.
2. Add a new empty Field Label textbox and type “<USERNAME>-Awaiting Customer Feedback”.
3. Select “List” in the adjacent dropdown box.
4. Select “<Edit List>” in the adjacent dropdown box.
New Fields in the Ticket Form

1. Go to Configure Ticketing > Edit Fields.

2.1. Click the New button.

2.2. Type john doe-Awaiting Customer Feedback in an empty Field Label textbox.

3. Select List in the adjacent dropdown box.

4. Select <Edit List> in the adjacent dropdown box.
New Fields in the Ticket Form

5. Click on “Add New” three times to create three separate textboxes.
7. Click on “Apply”.
8. Click on “Done”.
9. Repeat steps 2-8 for “<USERNAME>-Awaiting Customer Approval”
Default Values

- Set the default value of the *Priority* field to “Normal”. Allow the ticket submitter to select the priority themselves and allow them to view the SLA type.

10. Select “Normal” in the dropdown next to *Priority*. 
11. Open the Ticketing module. Go to Configure Ticketing > Access Policy.


13. Select “View Only” in the SLA Type dropdown box.
Email Notification Policy

- Define the email notification policy for all groups within the fiu organization. Also be sure to notify the ticket submitter when a note was added.

14. Open the Ticketing module. Go to Configure Ticketing > Notify Policy.
15. Select all groups within the “fiu-<USERNAME>” organization.
16. Select the Ticket Creation checkbox.
17. Select the Notify Ticket Submitter when note added checkbox.
18. Verify everything else is unchecked.
19. Type in your personal email in the Email List textbox.
20. Click on Update.
Email Notification Policy

14 Go to Configure Ticketing > Notify Policy.

15 Select all groups within the fiu-john doe organization.

16 Select the Ticket Creation checkbox.

17 Select the Notify Ticket Submitter when note added checkbox.

18 Verify everything else is unchecked.

19 Type in your personal email in the Email List textbox.

20 Click on Update.
LAB / Homework

• Create five tickets:

1. A closed ticket with one hour spent on server maintenance, which is assigned to you. The purpose of the ticket is to report a network problem.

2. A ticket awaiting customer feedback with two hours spent and assigned to you with a high priority on laptop1. The purpose of the ticket is an application problem.

3. A not resolved ticket with four hours spent and assigned to you on laptop1. The purpose of the ticket is workstation configuration.
LAB / Homework

• Create five tickets:

4. A not resolved ticket with four hours spent and assigned to you on pc1. The purpose of the ticket is workstation configuration.

5. An open ticket on guest1. The purpose of the ticket is printing problems.
Note

- When creating tickets, the *Summary* and *Note* textboxes are required before creating the ticket, feel free to choose on your own what should be included in the textboxes.
- Also, feel free to add in other information not required for this exercise.
Creating the First Ticket

- Create a closed ticket. Set the *Hours Worked* to one hour, assign the *Assignee* to you, assign the ticket to the dc machine, and assign the *Category* to “Network Problem”.

21. Open the Ticketing module. Go to *Manage Tickets > Create/View*.
22. Click on *Select association*. 

21 Go to Manage Tickets > Create/View.

22 Click on Select association.
Creating the First Ticket

23. Select “machine” in the dropdown box.
24. Select the “dc.mr.fiu-<USERNAME>” radio button.
Creating the First Ticket

25. Type in the ticket summary in the Summary textbox.
26. Select “<USERNAME>” in the Assignee dropdown box.
27. Select “Network Problem” in the Category dropdown box.
28. Type “1” in the Hours Worked textbox.
29. Type in the ticket notes in the Enter new note textbox.
30. Click on Submit.
31. Select “Closed” in the Status dropdown box.
Creating the First Ticket

25 Type in the ticket summary in the Summary textbox.

26 Select john doe in the Assignee dropdown box.

27 Select Network Problem in the Category dropdown box.

28 Type 1 in the Hours Worked textbox.

29 Type in the ticket notes in the Enter new note textbox.

30 Click on Submit.

31 Select Closed in the Status dropdown box.
LAB

• Creating automated tasks within the Ticketing module will greatly help in creating and organizing tickets.

• Kaseya provides a way to retrieve email from an account and organize the email requests into tickets.

• By creating a company email and asking ticket submitters to direct their requests to the designated email address, Kaseya can automatically create and store tickets in their group.
LAB

• To help in expediting tickets, due dates are required based on priority:
  – For servers, high priority requires completion within two hours, normal priority requires completion within four hours, and low priority requires completion within eight hours.
  – For workstations, high priority requires completion within four hours, normal priority requires completion within one day, and low priority requires completion within three days.

If a ticket becomes overdue, a notification will be sent to your email.
Due Date Policy

• Create a due date policy for all tickets.
  – For servers, high priority requires completion within two hours, medium priority requires completion within four hours, and low priority requires completion within eight hours.
  – For workstations, high priority requires completion within four hours, medium priority requires completion within one day, and low priority requires completion within three days.
85. Go to Ticketing > Configure Ticketing > Due Date Policy.
86. Type “<USERNAME>-server-high” in the Policy Name textbox.
87. Select “2 hours” in the Resolve Time dropdown.
88. Select “High” in the Priority dropdown.
89. Select “Servers” in the SLA Type.
90. Click on Create.
91. Repeat steps 86-90 for “normal” and “low” priorities.
92. Type “<USERNAME>-workstations-high” in the Policy Name textbox.
93. Select “4 hours” in the Resolve Time dropdown.
94. Select “High” in the Priority dropdown.
95. Select “Workstations” in the Priority dropdown box.
96. Click on Create.
97. Repeat steps 92-96 for “normal” and “low” priorities.
Notify Policy

- Edit the email notification policy for the scis, mr, gl, and cec groups within the fiu organization.

98. Open the Ticketing module. Go to Configure Ticketing > Notify Policy.
99. Select the scis, mr, gl, and cec groups within the “fiu-<USERNAME>” organization.
100. Select the Overdue Ticket checkbox.
101. Type in your personal email in the Email List textbox.
102. Click on Update.
Notify Policy

100 Select the Overdue Ticket checkbox.

101 Type in your personal email in the Email List textbox.

102 Click on Update.

98 Go to Configure Ticketing > Notify Policy.

99.1 Select the scis, mr, gl, and cec groups within the fiu-johndoe organization.

99.2 Select the scis, mr, gl, and cec groups within the fiu-johndoe organization.
Email Reader

- Examine the settings and the options available for Email Reader.

72. Open the Ticketing module. View the contents of Configure Ticketing > Email Reader. Note what settings can be set.
Creating a New Machine Group

- Under the organization name “FIU-<USERNAME>”, create machine group “support”.

73. Open the System module. Go to Orgs / Groups / Depts > Manage.
74. Verify if the Organization “FIU-<USERNAME>” is checked.
75. Click on Machine Group on the right hand side of the module.
76. Click on New in this section.
Creating a New Machine Group

73.1 Open the System module.

73.2 Go to Orgs/Groups/Depts > Manage.

74 Verify if the Organization FLU-johndoe is checked.

75 Click on Machine Group on the right hand side of the module.

76 Click on New in this section.
Creating a New Machine Group

77. Create a group by typing its name "support" under **Machine Group Name**. Click **Save**.
Email Mapping

- Map emails to the “support” group if they come from your email address.

78. Go to Ticketing > Configure Ticketing > Email Mapping.
79. Click on Select association.
Email Mapping

80. Select *group* in the dropdown box.

81. Click on the “fiu-<USERNAME>.support” group.
Email Mapping

82. Type in your personal email in the Email Address or Domain textbox.
83. Select <USERNAME> in the Assignee dropdown box.
84. Click on Create.
Note

• For this exercise, your own personal email should be used.

• However, in a production environment application, a ticket submitter’s email would be used.
Creating the Second Ticket

• Create a ticket awaiting customer feedback. Set the Hours Worked to two hours, assign the Assignee to you, assign the ticket to the laptop1 machine, assign the Priority to “High”, and assign the Category to “Application Problem”.

32. Open the Ticketing module. Go to Manage Tickets > Create/View.
33. Click on Select association.
Creating the Second Ticket

34. Select “machine” in the dropdown box.
35. Select the “laptop1.cec.fiu-<USERNAME>” radio button.
Creating the Second Ticket

36. Type in the ticket summary in the Summary textbox.
37. Select “<USERNAME>” in the Assignee dropdown box.
38. Select “Application Problem” in the Category dropdown box.
40. Type “2” in the Hours Worked textbox.
41. Select “Yes” in the <USERNAME>-Awaiting Customer Feedback dropdown box.
42. Type in the ticket notes in the Enter new note textbox.
43. Click on Submit.
Creating the Second Ticket

36. Type in the ticket summary in the Summary textbox.
37. Select johndoe in the Assignee dropdown box.
38. Select Application Problem in the Category dropdown box.
39. Select High in the Priority dropdown box.
40. Type 2 in the Hours Worked textbox.
41. Select Yes in the johndoe-Awaiting Customer Feedback dropdown box.
42. Type in the ticket notes in the Enter new note textbox.
43. Click on Submit.
Creating the Third Ticket

- Create a ticket waiting to be resolved. Set the *Hours Worked* to four hours, assign the *Assignee* to you, assign the ticket to the laptop1 machine, and assign the *Category* to “Workstation Configuration”.

44. Open the Ticketing module. Go to *Manage Tickets > Create/View*.
45. Click on *Select association*. 

```plaintext
44 Go to Manage Tickets > Create/View.
45 Click on Select association.
```
Creating the Third Ticket

46. Select “machine” in the dropdown box.
47. Select the “laptop1.cec.fiu-<USERNAME>” radio button.
Creating the Third Ticket

48. Type in the ticket summary in the Summary textbox.
49. Select “<USERNAME>” in the Assignee dropdown box.
50. Select “Workstation Configuration” in the Category dropdown box.
51. Type “4” in the Hours Worked textbox.
52. Type in the ticket notes in the Enter new note textbox.
53. Click on Submit.
Creating the Third Ticket

48. Type in the ticket summary in the Summary textbox.

49. Select johndoe in the Assignee dropdown box.

50. Select Workstation Configuration in the Category dropdown box.

51. Type 4 in the Hours Worked textbox.

52. Type in the ticket notes in the Enter new note textbox.

53. Click on Submit.
Creating the Fourth Ticket

- Create a ticket waiting to be resolved. Set the *Hours Worked* to four hours, assign the *Assignee* to you, assign the ticket to the pc1 machine, and assign the *Category* to “Workstation Configuration”.

54. Open the Ticketing module. Go to *Manage Tickets > Create/View*.
55. Click on *Select association*. 
56. Select “machine” in the dropdown box.
57. Select the “pc1.cec.fiu-<USERNAME>” radio button.
Creating the Fourth Ticket

58. Type in the ticket summary in the Summary textbox.
59. Select “<USERNAME>” in the Assignee dropdown box.
60. Select “Workstation Configuration” in the Category dropdown box.
61. Type “4” in the Hours Worked textbox.
62. Type in the ticket notes in the Enter new note textbox.
63. Click on Submit.
Creating the Fourth Ticket

58 Type in the ticket summary in the Summary textbox.

59 Select joindoe in the Assignee dropdown box.

60 Select Workstation Configuration in the Category dropdown box.

61 Type 4 in the Hours Worked textbox.

62 Type in the ticket notes in the Enter new note textbox.

63 Click on Submit.
Creating the Fifth Ticket

- Create an open ticket. Assign the ticket to the guest1 machine, and assign the Category to “Printing Problem”.

64. Open the Ticketing module. Go to Manage Tickets > Create/View.
65. Click on Select association.
66. Select “machine” in the dropdown box.
67. Select the “guest1.gl.fiu-<USERNAME>” radio button.
Creating the Fifth Ticket

68. Type in the ticket summary in the Summary textbox.
69. Select “Printing Problem” in the Category dropdown box.
70. Type in the ticket notes in the Enter new note textbox.
71. Click on Submit.
Creating the Fifth Ticket

68 Type in the ticket summary in the **Summary** textbox.

69 Select **Printing Problem** in the **Category** dropdown box.

70 Type in the ticket notes in the **Enter new note** textbox.

71 Click on **Submit**.
Progress Check

- What are the different ways to create a ticket?
- How can you add custom fields to the tickets?
- How can you set the due date for the tickets automatically?
- How can you configure the notification policy for your tickets?
- How can you set Kaseya to receive tickets over email?
Questions?

• Please type your questions in the chat section of your GoToMeeting window.

• Remember that you can always send your questions to training@kaseya.com too.

• If you are falling behind the steps in the lab, please just watch the presentation, take some notes, and perform your labs after the lecture.
Kaseya Fundamentals Workshop

MONITOR WRAP UP
Monitor Wrap Up

• Monitor Results
  – Review Monitor Set for Server Logs
  – Review Alarm Summary
  – Review Windows Event Logs Sets

• Monitor Help Manual

• Work through the LABS
Roadmap!

1. Monday, Day One
   - Overview
   - System Architecture
   - Agents

2. Tuesday, Day Two
   - LAB Review
   - Agent Template and Policy Management Concepts
   - Audit
   - Patch Management

3. Wednesday, Day Three
   - LAB Review
   - Monitor
   - Ticketing

4. Thursday, Day Four
   - LAB Review
   - Agent Procedures
   - Remote Control
   - Live Connect

5. Friday, Day Five
   - LAB Review
   - Agent Template vs. Policy Management
   - System
   - Info Center

www.kaseya.com
THE END!