Kaseya Fundamentals Workshop

DAY TWO

Developed by

Kaseya University

Powered by

IT Scholars

Kaseya Version 6.5

Last updated March, 2014

Day Two Overview

- Day One Review
  - IT-Scholars Virtual LABS
  - System Management
    - Organization
    - Users
    - Scopes and Roles
  - Agent Deployment
- Patch Management
- Remote Control
- Live Connect
  - Desktop Access


Kaseya
Kaseya Fundamentals Workshop
REMOTE CONTROL

Remote Control Overview

- Desktop Control
- Configure Remote Control Type and Parameters
- Notification Policy
- Files/Processes
- Message with Users
- Agent Menu
- Summary

Remote Control

- *Remote Control*, also called *Remote Desktop and sometimes Virtual Network Computing (VNC)*, is a graphical desktop sharing system that uses the *Remote Framebuffer (RFB)* protocol to remotely control another computer.
- It transmits the **keyboard** and **mouse** events from one computer to another, relaying the **graphical screen** updates back in the other direction, over a network.

Remote Control (cont.)

- You can use *Remote Control* to provide immediate technical support.
- A *Remote Control Client* on your local machine connects to a *Remote Control Server* on a remote machine.
- The *Remote Control Server* is the program on the remote machine that shares its screen.
- The *Remote Control Client* (or *Viewer*) is the program on the local machine that watches and interacts with the remote machine.

Remote Control (cont.)

- Using *Remote Control*, you can remotely view and operate managed machines as if they were right in front of you, independent of any gateway or firewall configurations, even behind NAT.
- You can work independently on the remote machine or with the user to solve problems interactively where both parties can see what is happening in real time.
- Supported tools are WinVNC, pcAnywhere, RAdmin, and RDP.

Remote Control (cont.)

- You can set policies that allow users to block remote control or require users to ask permission before accessing a machine.
- You can FTP to any managed machine and access files.
- You can direct chat with any managed machine.
- You can remote control even without an agent installed. (*on-premise only*)

Firewalls & Port Blocking

- In setting up a remote control or FTP session, gateway and port blocking problems are eliminated by always initiating outbound connections from both the target machine and the user machine.
- If a direct connection is not possible then the helper applications route the remote control traffic through the Kaseya Server on the same port used by agents to check-in (default 5721).

Desktop Control

- Control Machine
  - Desktop access
  - Utilize Active X control
    - Non Internet Explorer browser must download a non-ActiveX application before continuing.
- Reset Password
  - Create a new local user account
  - Change a local user account password

Remote Control Configuration

- Configuration
  - Select Type
  - Set Parameters
  - Preinstall RC
  - Uninstall RC
- Notification Policy
  - User Role Policy
  - Machine Policy

Preinstall RC

- Setting up the agents so that they preinstall the selected remote control package will speed things up when you perform the first remote connection.
- Workstations
  - Preinstall K-VNC.
- Servers
  - Since *Terminal Server* is distributed by Microsoft as part of it Windows Server OS, you do not have the option to preinstall it. You need to make sure that it is enabled though.

Notification Policy

- Notification Type by User Role or Machine
  - How to interact with your end user?
  - Option to Record the remote control session
    - Create a video file under the Kaseya Working Directory folder.
  - This settings also effects the Desktop Access function under Live Connect

Files/Processes

- FTP
- SSH
- Task Manager

File Transfer Protocol (FTP

- FTP is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol.
- The FTP server is the program on the target machine that listens on the network for connection requests from other computers.
- The FTP client is the program on the VSA user's local machine that initiates a connection to the server.
- The FTP client machine requires user access rights to the FTP server machine..

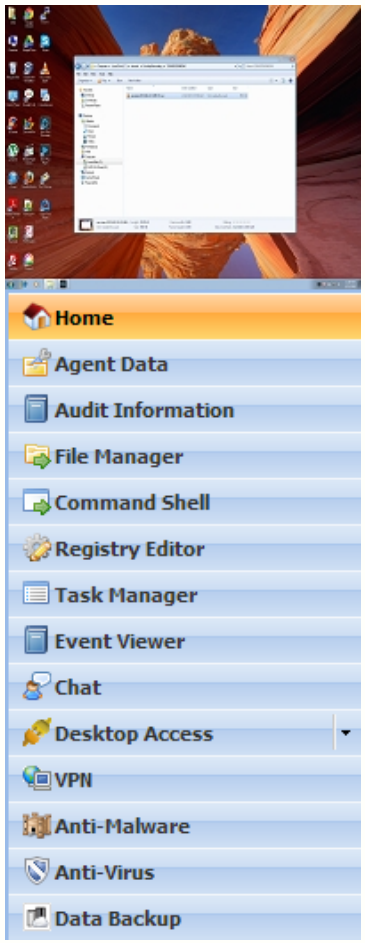
File Transfer Protocol (FTP)

- Once connected, the client can upload files to the server, download files from the server, rename or delete files on the server and so on.
- Virtually every computer platform supports the FTP protocol.
- Since Kaseya FTP sessions are relayed through the Kaseya Server, all FTP sessions are protected by the Kaseya 256 bit rolling encryption protocol.


Kaseya
Kaseya Fundamentals Workshop
LIVE CONNECT & COMPUTER QUICKVIEW

Live Connect

- *Live Connect* is a related module of VSA that performs tasks and functions **solely for one managed machine at a time**.
- In many cases, *Live Connect* is superior to *Remote Control*.
- With Live Connect you have access to:

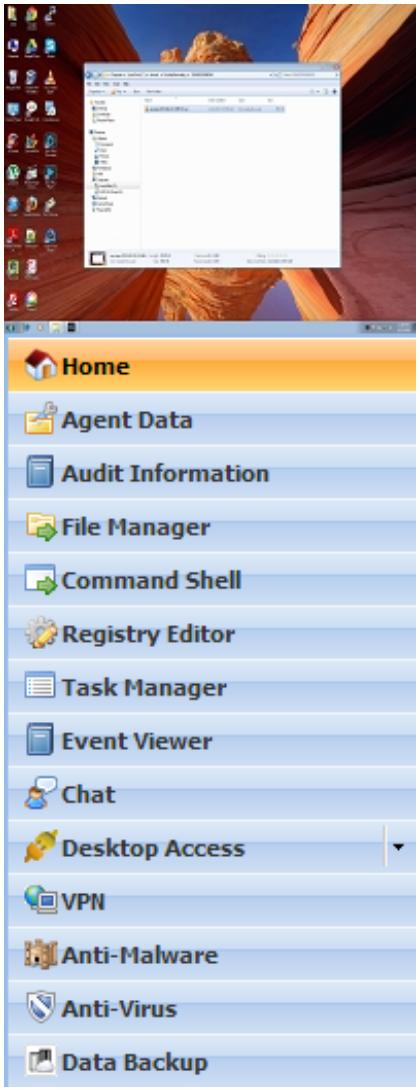


Why Live Connect?

- Sometimes, quick and simple system related tasks are needed to be done on a single machine.
- Physically being present at the machine or logging into it remotely to access system tasks, can waste valuable time.
- Instead, an easy accessible module can be used when quick access to basic system tools is needed.
- Live Connect enables you to perform system level tasks on a single managed machine.

Live Connect Solution

- In most cases, the tasks can be done without any interruption to the local user.
- Also Live Connect allows you to view, and sometimes edit, basic functionality given by the Kaseya VSA.



Add on Modules

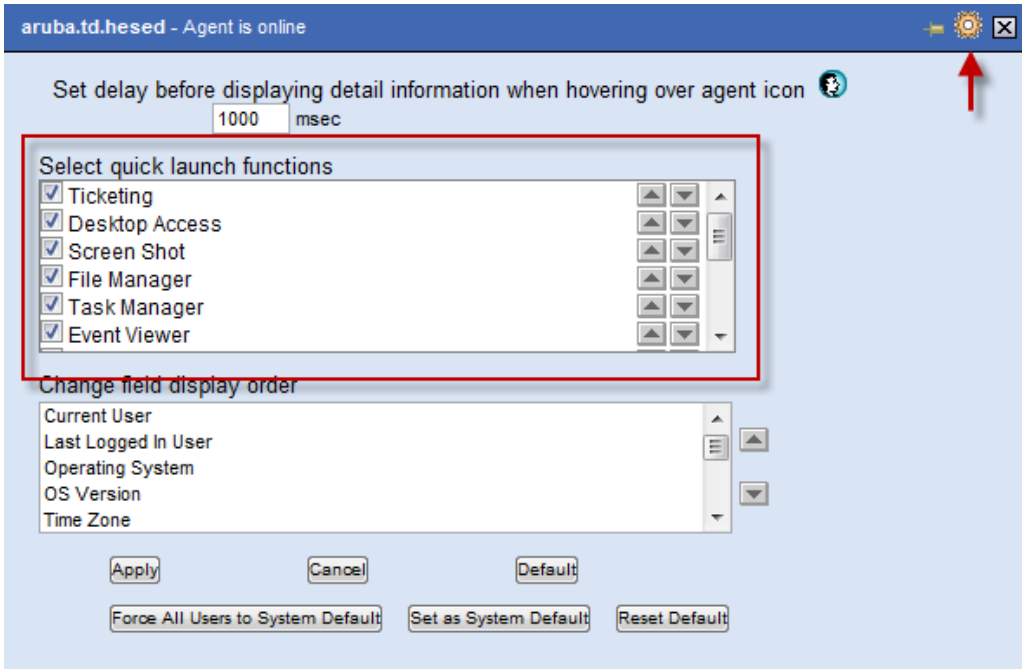
- Both Live Connect and Remote Control have add-ons that need to be installed.
- Pre install these add-ons to shorten the time when initiating Remote Control or Live Connect for the first time.
  - *Remote Control – Preinstall RC*
  - *Agent Procedure – Live connect endpoint plugin installer*
- Assign these task to the Agent Templates
- NOTE: Use *Agent - Copy Settings* to push the add-ons module installation during agent installation.

Computer Quick View Window

- Quick access to specific machine information.
- Execute Live connect and Remote Control functions from Quick View window.
- Screen snapshot and recording
  - Recordings is stored under the local machine Agent Working Directory Folder \ Desktop Recording
  - Snapshots are stored on the Kaseya Server under Kaseya\UserProfiles\AgentGUID\GetFiles
- Run common agent procedures tasks.

Quick View Settings

- You have the ability to control which quick launch functions to display and the order of how they are displayed.



- You can also set System Defaults for other users.

User Roles and Machine Roles

- Live Connect, Remote Control, and Computer Quick View functionality can be limited by User Roles Access Rights.
- End user Live Connect access is controlled by Machine Roles Access Rights.
- Limit access to ensure privacy is upheld for your end users and meet company privacy policy.

Kaseya

Our Automation. Your Liberation.™

Kaseya Fundamentals Workshop

SUMMARY

Summary

- *Remote Control* enables the VSA users to remotely control and provide immediate support to users of managed computers.
- Supported tools are WinVNC, pcAnywhere, RAdmin, and RDP.
- You can set policies that allow users to block remote control or require users to ask permission before accessing a machine.
- You can FTP to managed machines and access files. You can send message to the end users or direct chat with them.

Overview: The *Video Streaming* Page

- The *Video Streaming* page establishes a remote control session between the VSA user's local machine and a machine without an agent.
- Use it to help someone quickly on an infrequent basis.
- If you plan to provide continuous support we recommend you install an agent.


Kaseya
Kaseya Fundamentals Workshop
PATCH MANAGEMENT OVERVIEW

Patch Management

- Patch Data Collection
  - Patch Scan
- Methods of Deploying Patch Updates
  - Initial Update
  - Automatic Update
  - Machine Update
  - Patch Update
- Configure Patch Deployment Settings
  - Patch Policy
  - Windows Auto Update
  - Reboot Action
  - File Source
- Patch Views
- Summary

Patch Management

- System and network security depends on all your machines having the latest security patches applied.
- Use the *Patch Management* module to scan and update Microsoft patches on Windows managed machines.
- *Patch Management* automates the process of keeping all your Windows machines up to date with the latest patches.
- You can configure how and when updates are applied on a per machine basis.

Supported Operating Systems

- Patch Management supports all OS's supported by Windows Update, which includes:
  - Microsoft Windows 2000 (SP3)
  - XP
  - 2003, 2003 R2
  - Vista
  - 2008, 2008 R2
  - 7
  - 8
  - 2012
  - (Office 2003 or newer)


Kaseya
Kaseya Fundamentals Workshop
INITIAL UPDATE
vs.
AUTOMATIC UPDATE

Patch Management Process

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

Scan Machine

- The *Scan Machine* page schedules scans to search for missing patches on each managed machine.
- Scanning takes very little resources; therefore, technically, it can be run at any time of day.
- However, it is recommended to run it at less busy times.

Scan Source

- When Microsoft cannot be reached for patch scan, Kaseya uses Microsoft's **WSUSSCN2.CAB** data file.
- Microsoft publishes this CAB file as needed. It contains a sub-set of the Microsoft Update Catalog; only the high priority updates and occasionally for service packs are included in the CAB file.
- The Kaseya Server automatically downloads the CAB file on a daily basis to make it available for those machines needing this type of scan.

Patch Scan Frequency

- Microsoft typically releases patches on Tuesdays.
- Security and critical patches are typically released on **the second Tuesday of the month (Patch Tuesday)**.
- Non-security and non-critical patches are typically released on **the third and/or fourth Tuesdays of the month**.
- To ensure you are aware of the latest missing patches, we recommend that you scan all your machines on **Wednesdays**.

Patch Status / Patch Update Tips

- How to avoid Patch Update Problems
  - Most patch problems are the result of configuration and/or permission issues.
  - Before starting any patch update on your machines, it is recommended to first use the test function to exercise the entire patch deployment process without actually installing anything on the target machine or causing any reboots.
  - Also, you need to make sure that the right credentials are registered with the agents to successfully update machines.
  - Create an exception for CURL.EXE and CURL-NOSSL.EXE with Anti Virus software and Firewalls.

Initial Update

- To bring a newly managed machines up to speed with all approved Microsoft patches, you can utilize the *Initial Update* function.
- It should only be performed on machines that are not in production or currently being use by an end user.
- The *Reboot Action* policy are ignored and the managed machine will reboot without warning the user as often as necessary until the machine has been brought up to the latest patch level.

Automatic Update

- This is the preferred method of updating managed machines with Microsoft patches on a recurring basis.
- Use the *Initial Update* if you are installing patches for the first time on a managed machine.
- Patches that require manual intervention are not included in *Automatic Updates*.

Automatic Update

- Patch installation only occurs when a new missing patch is found by Scan Machine.
- Automatic Update obeys both the *Patch Policy* and the *Reboot Action* policy.
- Automatic Update is suspended for a machine while an Initial Update is being processed.
- Automatic Update automatically resumes when an Initial Update is completed.

Automatic Update Scheduling

- Workstations
  - Microsoft typically release new patches on Tuesdays and we recommend you schedule patch scan on Wednesdays, it makes sense to update your machines on **Thursdays**.
  - As workstations are typically powered on during the daytime and are powered off during night time, schedule *Automatic Updates* from **6am-6pm on Thursdays or during business hours**.
  - Ensure you enable the power management option on so that any machines powered off during the day can be woken up.
- Servers
  - Servers are more sensitive to Patches, because it effects multiple users and services when a Patch conflict arises.
  - Before you utilize the *Automatic Update* to schedule patch installations, review your server applications and be aware of any published patch issues or conflicts.

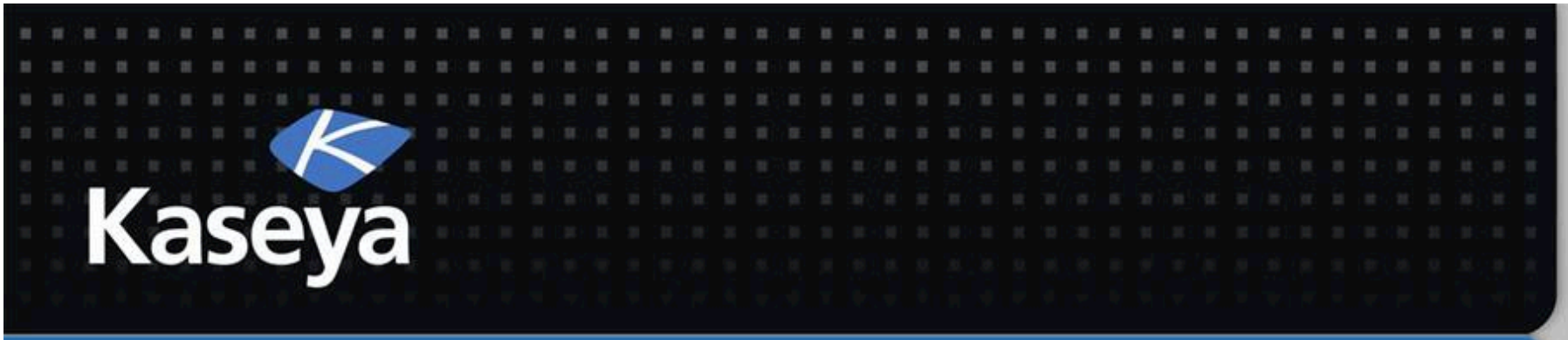
Pre/Post Procedures

- Use the *Pre/Post Procedure* page to run procedures either before and/or after Initial Update or Automatic Update.
- For example, you can run procedures to automate the preparation and setup of newly added machines before or after Initial Update.

Note: Post procedures will run even if there are patch installation failures.

Machine History

- The Machine History page displays the results from the most recent patch scan of managed machines.
- All installed and missing patches applicable to a managed machine are listed, regardless of whether the patch is approved or not.



Kaseya Fundamentals Workshop

PATCH CONFIGURATION

Configure

- Windows Auto Update
  - Disable all other Patch Management
- Reboot Action
- File Source
- Patch Alert
- Office Source

Reboot Action Policy

- How to process Reboot Request after a Patch Update is performed.
- Reboot Action Policy does not apply to *Initial Update*
  - Workstations
    - If user logged in ask to reboot every 60 minutes until reboot occurs.
    - Reboot if user not logged in.
  - Servers
    - Do not reboot after update
    - When reboot required, send email to you

      Note: The KaUsrTsk.exe is the application that determines whether a user is logged in or not.

File Source

- Downloading all the patches to a file server and distributing it to all the machines on network will allow you to save bandwidth.

- For LAB environment
  - Set the file share on dc “C:\PatchTemp”.
  - Set the UNC path “\\192.168.0.10\PatchTemp”.
  - If the computer cannot access DC, it should then download from the Internet.

File Source – LAN Cache

- Configure a Local machine to be a file source.
- Select the machine to perform the LAN Cache.
- After assigning machines to the designated LAN Cache, they will connect using a UNC path mapping. i.e. \ \LANCacheServer\LANCacheName$
- The LAN Cache server will create a FSAdminxxxxxx user for other machines to use as credentials.
- LAN Cache server will create a VSAFileShare and Patch folder to store the shared files locally.

Patch Settings – Patch Alert

- Workstations
  - Generate an Alarm and Email when
    - Agent credential is invalid or missing
    - Patch install fails
    - Windows Auto Update changes
- Servers
  - Generate an Alarm and Email when
    - New Patch is Available
    - Agent credential is invalid or missing
    - Patch install fails
    - Windows Auto Update changes

Patch Management Review

- STEPS to configure an automated Patch scanning and deployment
  1. Patch Scan
  2. Patch Policy Configuration
  3. Reboot Policy
  4. File Source
  5. Disable Windows Automatic Update
  6. Schedule Patch Automatic Update


Kaseya
Kaseya Fundamentals Workshop
PATCH POLICY

Patch Policy

- Create/Delete
- Membership
- Approval By Policy
- Approval By Patch
- KB Override

Patch Policy

- Policies are like templates in which you can approve/deny a group of patches, or an individual patch.
- Patch policies contain all active patches for the purpose of approving or denying patches.
- An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA.

Patch Policy

- 3 levels of Default approval settings
  - Denied – highest precedence
  - Pending Approval -
  - Approved – lowest precedence
- 2 Views for Grouping Patches
  - Classification View
  - Product View
- A Patch will only be installed if Approved on all views and across all Patch Policy

Sample Patch Policy Settings

- Workstations Patch Approval

Workstation Patching	Default Approval Policy
Security Update - Critical (High Priority)	Approved
Security Update - Important (High Priority)	Approved
Security Update - Moderate (High Priority)	Approved
Security Update - Low (High Priority)	Approved
Security Update - Non-rated (High Priority)	Approved
Critical Update (High Priority)	Approved
Update Rollup (High Priority)	Pending Approval
Service Pack (Optional - Software)	Pending Approval
Update (Optional - Software)	Pending Approval
Feature Pack (Optional - Software)	Pending Approval
Tool (Optional - Software)	Pending Approval

Sample Patch Policy Settings

- Servers Patch Approval

Server Patching	Default Approval Policy
Security Update - Critical (High Priority)	Pending Approval
Security Update - Important (High Priority)	Pending Approval
Security Update - Moderate (High Priority)	Pending Approval
Security Update - Low (High Priority)	Pending Approval
Security Update - Non-rated (High Priority)	Pending Approval
Critical Update (High Priority)	Pending Approval
Update Rollup (High Priority)	Pending Approval
Service Pack (Optional - Software)	Pending Approval
Update (Optional - Software)	Pending Approval
Feature Pack (Optional - Software)	Pending Approval
Tool (Optional - Software)	Pending Approval

Null Patch Policy

- A null patch policy is one that all its patches are set to the default *Pending Approval* status.
- Note that once this policy is applied to any machine, no patches would be approved, as *Pending Approval* acts like denied, and when combined with any other policies, the result is not applying any patches.
- This is useful when you want, for example, to temporarily not let any patches to be installed on a group of machines.

Assigning Patches under Policy

- When you create a new Patch Policy, existing scanned or discovered patches will be set to Pending Approval
- After you change the Default Approval status, the patches do not automatically move to the Default Approval status.
- Select the Pending Approval Total and use Scan Selection Filters to group specific patches to either approve or deny for Patch Installation.


Kaseya
Kaseya Fundamentals Workshop
MANAGE UPDATE

Manage Updates

- Machine Update
- Patch Update
- Rollback
- Cancel Updates

Machine Update

- If you're using *Automatic Update*, then *Machine Update* is used on an exception basis to apply patches to individual machines.
- *Machine Update* is often used to test a new patch prior to approving it for general release to all machines.
- It is also used to install missing or failed patches from automatic updates.
- It overrides the *Patch Policy* but obeys the *Reboot Action* policy.

Patch Update

- *Patch Update* is used on an exception basis to apply individual patches, to **multiple machines** or for patches that originally were missed or failed on certain machines during the *Automatic Update* process.
- It overrides the *Patch Policy* but obeys the *Reboot Action* policy.

Rollback

- The Rollback page removes patches after they have been installed on a system.
- Not all patches may be uninstalled.
- The system only lists patches supporting the rollback feature.

Cancelling Updates

- The Cancel Updates page clears all manually scheduled patch installations on selected machine IDs.
- The Cancel Updates page can also terminate currently running patch installation processes.
- A Terminate button displays next to the machine name when a patch installation is being processed.
- Termination deletes existing patch installation procedures for the selected machine, and the installation process ends after the currently running procedure completes.

Kaseya Fundamentals Workshop

SUMMARY

Patch Views

- Create Patch Views for
  - **Patch - No Policy:** Displays all machines that are not a member of a Patch Policy.
  - **Patch - Pending Reboot:** Displays all machines that are pending a reboot due to recent patch updates.
  - **Patch - Scan Failed:** Displays all machines that failed the patch scan.
  - **Patch - Scan Not Scheduled:** Displays all machines that do not have a patch scan scheduled.
  - **Patch - Windows Auto Update Enabled:** Displays all machines that have Windows Automatic Update Enabled.

Analyzing Patch Status

- You can determine the patch status of managed machines using the following pages:
  - The *Scan Machine* page determines what patches are missing on managed machines.
  - The *Patch Status* page displays a summary view of installed, missing and denied patches for each managed machine.
  - The *Machine History* page displays a detailed view of patch scan results for each managed machine.

Methods of Updating Patches

The VSA provides five methods of applying Microsoft patches to managed machines:

1. Initial Update
2. Automatic Update
3. Machine Update
4. Patch Update
5. Patch Deploy (a function under Agent Procedures; explained later)

1. Initial Update

- It is a one-time processing of all approved Microsoft patches applicable to a managed machine based on Patch Policy.
- It should only be performed during non-business hours and is typically performed over a weekend on newly added machines.
- It ignores the *Reboot Action* policy (explained later) and reboots the managed machine without warning the user as often as necessary until the machine has been brought up to the latest patch level.

2. Automatic Update

- It is the preferred method of updating managed machines on a recurring basis.
- It obeys both the *Patch Policy* and the *Reboot Action* policy.

3. Machine Update

- If you're using Automatic Update, then Machine Update is used on an exception basis to apply patches to individual machines.
- Machine Update is often used to test a new patch prior to approving it for general release to all machines.
- It overrides the *Patch Policy* but obeys the *Reboot Action* policy.

4. Patch Update

- If you're using Automatic Update, then Patch Update is used on an exception basis to apply individual patches to multiple machines or for patches that originally failed on certain machines.
- It overrides the *Patch Policy* but obeys the *Reboot Action* policy.

5. Patch Deploy

- Microsoft releases many hot fixes as patches for very specific issues that are not included in the Microsoft Update Catalog or in the Office Detection Tool, the two patch data sources the Patch Management module uses to manage patch updates.
- *Agent Procedures > Patch Deploy* enables users to create a patch installation procedure for these hot fixes, via this wizard, that can be used to schedule the installation on any desired machine.

Non-Microsoft Applications

- You can install non-Microsoft applications using *Agent Procedures > Application Deploy*.
- When a pre-defined install solution cannot be used, use *Agent Procedures > Packager* to create a self-extracting file ready for automated distribution.

Note: *Agent Procedures* are explained later.

Kaseya Fundamentals Workshop

Wrap Up

Day Two Wrap Up

Q&A

Day Two Hands On Labs

- Day Three Topics
  - Monitor
  - Introduction to Agent Procedures