

David Frye
Lawrence
Livermore
National
Laboratory
LANDESK PROCESS
MANAGER

Workflow for desktop configuration
management

Title: LANDesk Process Manager at LLNL
UCRL: UCRL-PRES-231385
Author: David Frye
Issued: June 1, 2007
Presented: June 13, 2007, Albuquerque, NM

This work was performed under the auspices of the U.S. Department of Energy by University of California, Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Agenda:

- The need for a new approach to configuration management: Patch Management
- Workflow tools in general
- LANDesk Process Manager (LPM)
- Preview of LPM at LLNL

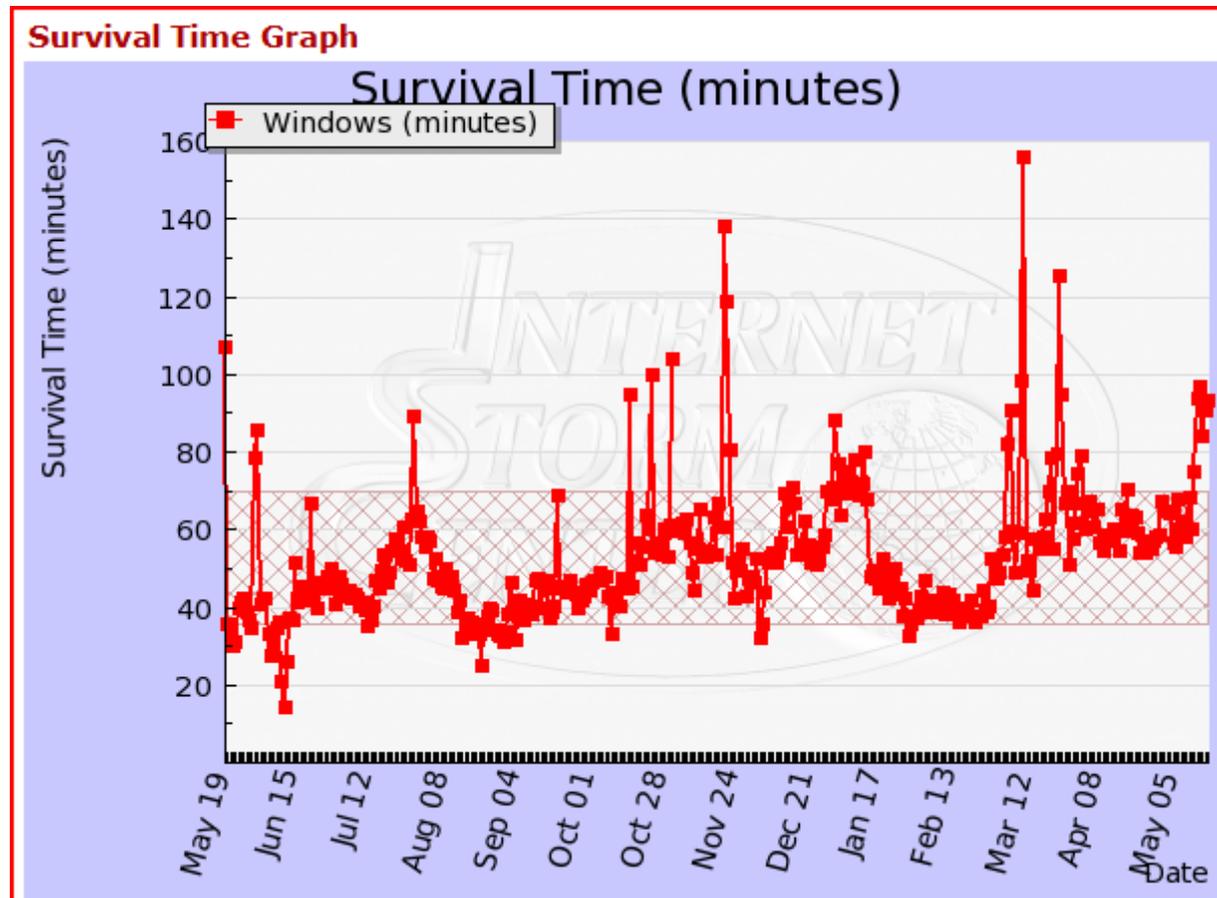
Problem: Patch Management

- Critical: Too important to get wrong
- Complex: Tedious, repetitive, and error prone
- Ubiquitous: Needed everywhere
- Impactful: Errors can have serious consequences to mission

Criticality of Patch Management

Un-Patched XP – Hacked in an Hour:

(source: SANS Internet Storm Center)



Patch Management: Traditional Approach

Review

- Review new patch content
- Determine which clients need patching

Test

- Deploy to QA Systems
- Deploy to Production Pilot Systems

Deploy

- Deploy to Typical Users
- Deploy to Sensitive Users
- Track Progress / Resolve Failures

Patch Management: Current Tools

“Traditional” PM Tools at LLNL:



Patch Management: Current Tools

- PROS of current tools:

 - Flexible

 - Scalable

 - Powerful Administrative Consoles

 - With diligence, they work!

Patch Management: Current Tools

- **CONS of current tools:**

 - Administrators **MUST** use them

 - 40 “active” patch administrators

 - Simple Deployment: 15 steps, 50 options

 - Consoles are not automatable and are difficult to document

Patched By Exception Model

Patch Management & The Deep Blue Sea

- At Best:

- Lots of talented people working the same problem

- Performing the same sets of tasks

- Over and over

-OR-

- At Worst:

- It doesn't get done

- Machines go un-patched

- End users don't know

Patch Management: A New Approach

What's Needed?

- Automated, process-driven approach
QA, Pilot, and Production deployment cycles
- Admins must act to PREVENT patch deployment
- Support for our diversity
- Extensibility
- End user visibility?

Patched By Default Model

LANDesk Process Manager



Workflow Tools

What is a Workflow?

Workflow is the operational aspect of a work procedure:

- How tasks are structured
- Who performs them
- What their relative order is
- How they are synchronized
- How they are tracked

(source: wikipedia)

What are Workflow Tools?

Workflow tools provide the following services:

- Automation
- Coordination
- Visualization & Design
- Auditing & Reporting

What are Workflow Tools?

Typical Elements of a Workflow Tool:

- Actions (task specific application code)
- Rules Engine
- Graphical Designer
- End User Interface(s)
- Programming Interface (API)

What are Workflow Tools?

Commercial Examples:

- IBM WebSphere Workflow
- Microsoft BizTalk, Office Sharepoint Server and .NET Runtime 3.0
- LANDesk Process Manager (LPM)

Key benefits of a Workflow Tool

- Decouples design and implementation
- Provides common framework for designers and implementers
- Self-Documenting
- Reactive

LANDesk Process Manager



LPM In Detail

What is LPM?

Typical Elements Plus Workflow Support For:

- Patch Management
- Software Distribution
- Inventory Control
- License Management
- Remedy/HEAT integration
- OS Provisioning

What is LPM for Patch Mgmt?

Patch Management Capabilities:

- Automatic Download of Patch Content
- Automatic Patch Grouping
- Patch Approval Requests
- Automatic Patch Deployment
- Deployment Success/Failure Notification

LPM – The Designer

The screenshot displays the 'Process Designer' application interface. The main window, titled '4 SMSG Desktop Patching', shows a workflow diagram on the 'Drawing Surface'. The workflow starts with a task '4 SMSG Desktop Patching', which leads to a decision 'Repair SMSG Desktops'. This decision branches into 'Success' and 'Failure'. The 'Success' path leads to 'Success Notification'. The 'Failure' path leads to 'Add vulnerabilities to a group', which then leads to 'Send e-mail'. After 'Send e-mail', the workflow proceeds to a 'Completed' state, followed by a '7 Days' timer, and finally a 'Timed out' state. The 'Tools Palette' on the right lists various actions such as 'Active Directory', 'HEAT', 'LANDesk security management', 'Add vulnerabilities to a group', 'Autofix vulnerabilities', 'Create custom security group', 'Delete custom security group', 'Get vulnerabilities', 'Scan/repair vulnerabilities', 'LANDesk service management', 'Add assignment', 'Add note', 'Add task', 'Close incident', 'Create incident', 'Get incident info', 'Resolve incident', 'LANDesk system management', 'System', 'Assign manual task', 'Decision', 'Execute JavaScript', 'Execute program', 'Execute SQL', 'Execute VB script', 'Get approval', 'Modify approvals', 'Modify manual tasks', 'Modify request information', 'Placeholder', 'Request information', 'Send e-mail', 'Timer', 'Update request', and 'Web service'. The 'Workflow explorer' on the left shows a tree view of workflows, including '4 SMSG Desktop Patching'. The 'Attributes' pane at the bottom left is empty. The status bar at the bottom indicates 'Missing or incorrect information:' and 'Resume error check>>'. The text 'Drawing Surface' is overlaid on the workflow diagram.

Tools
Palette

LPM – Built In Actions

System

- System
- Assign manual task
- Decision
- Execute JavaScript
- Execute program
- Execute SQL
- Execute VB script
- Get approval
- Modify approvals
- Modify manual tasks
- Modify request information
- Placeholder
- Request information
- Send e-mail
- Timer
- Update request
- Web service

Patch

- LANDesk security management
- Add vulnerabilities to a group
- Autofix vulnerabilities
- Create custom security group
- Delete custom security group
- Get vulnerabilities
- Scan/repair vulnerabilities

- General & Special Purpose Actions
- Type Specific Properties
- Wizards For

Property Window

Attributes - Get approval

Auditing	Auditing template: Default audit
Comments	Approver's comments: <input type="text"/> Denier's comments: <input type="text"/>
Details	(Name): Get approval Action type: Get approval
Due date	Due date: <input type="text"/>
E-mail	Approvers: Contacts associated with this action E-mail template: Default E-mail Notification recipients: Contacts associated with this action
Auditing template Template to use for auditing this action	

LPM – Reporting

LANDesk® Process Manager

Filter: By request

Filter by request ID:

Request ID	External system ID	Status
10588	695425	Completed

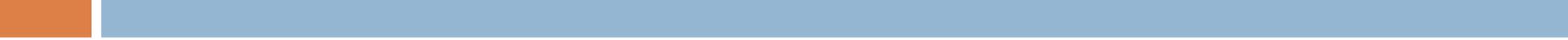
Cancel request | Pause request | Resume request

To do | Details | Requester | Action history | Audit history | Graphical history

```
graph TD; A[Update Status] --> B[Set State to Pending]; B --> C[Scan for vulnerabilities]; C --> D[Success]; C --> E[Failure]; D --> F[Set State to Complete]; E --> G[Set State to Failed];
```

Zoom in | Zoom out | Zoom to fit | Zoom 1:1 | Print...

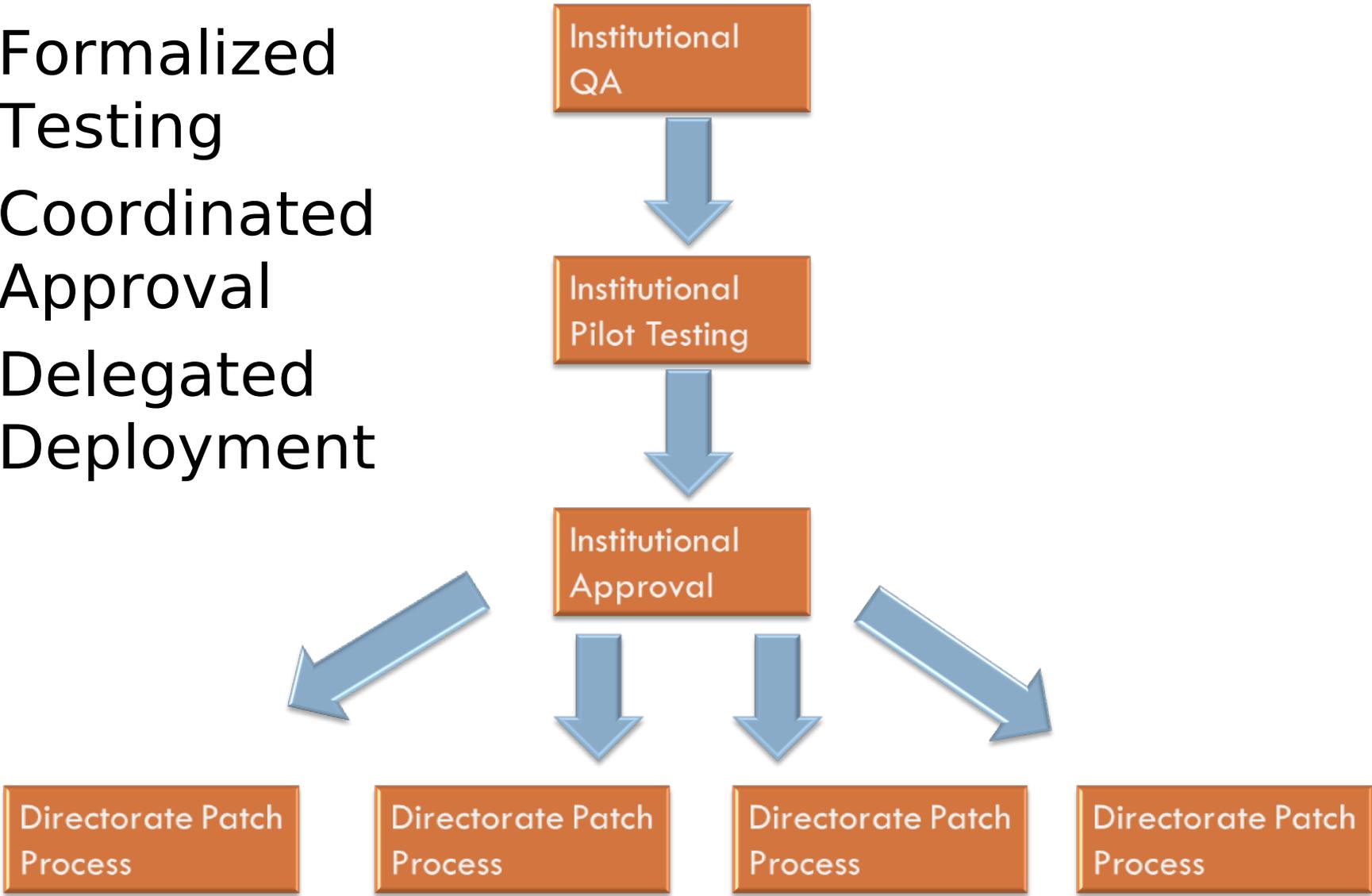
LANDesk Process Manager



Preview of LPM for Patch
Management @ LLNL

LLNL Patch Process – Overview

- Formalized Testing
- Coordinated Approval
- Delegated Deployment



LLNL Patch Process – Patch Download & QA

1 New Patch Download and Institutional QA

LANDesk Workflow - Start new Patch Management Workflow?

Idworkflow@llnl.gov

Sent: Fri 11/3/2006 12:40 PM

To: David J. Frye

LANDesk >>>

Download of
from

Check if any
new
was
down

LANDesk >>> **LANDesk® Process Manager**

[To do](#)

[Requests](#)

[Calendar](#)

Details	Action	Request ID
View details	<input checked="" type="checkbox"/> <input type="checkbox"/>	10401
View details	<input checked="" type="checkbox"/> <input type="checkbox"/>	10415
View details	<input checked="" type="checkbox"/> <input type="checkbox"/>	10450
View details	<input checked="" type="checkbox"/> <input type="checkbox"/>	10492

LANDesk
Deployment
Group
Created

005, MIS03-027, MIS03-007, MIS06-052, WXP-SPTa, WXP-SP2

Workflow ID: 74

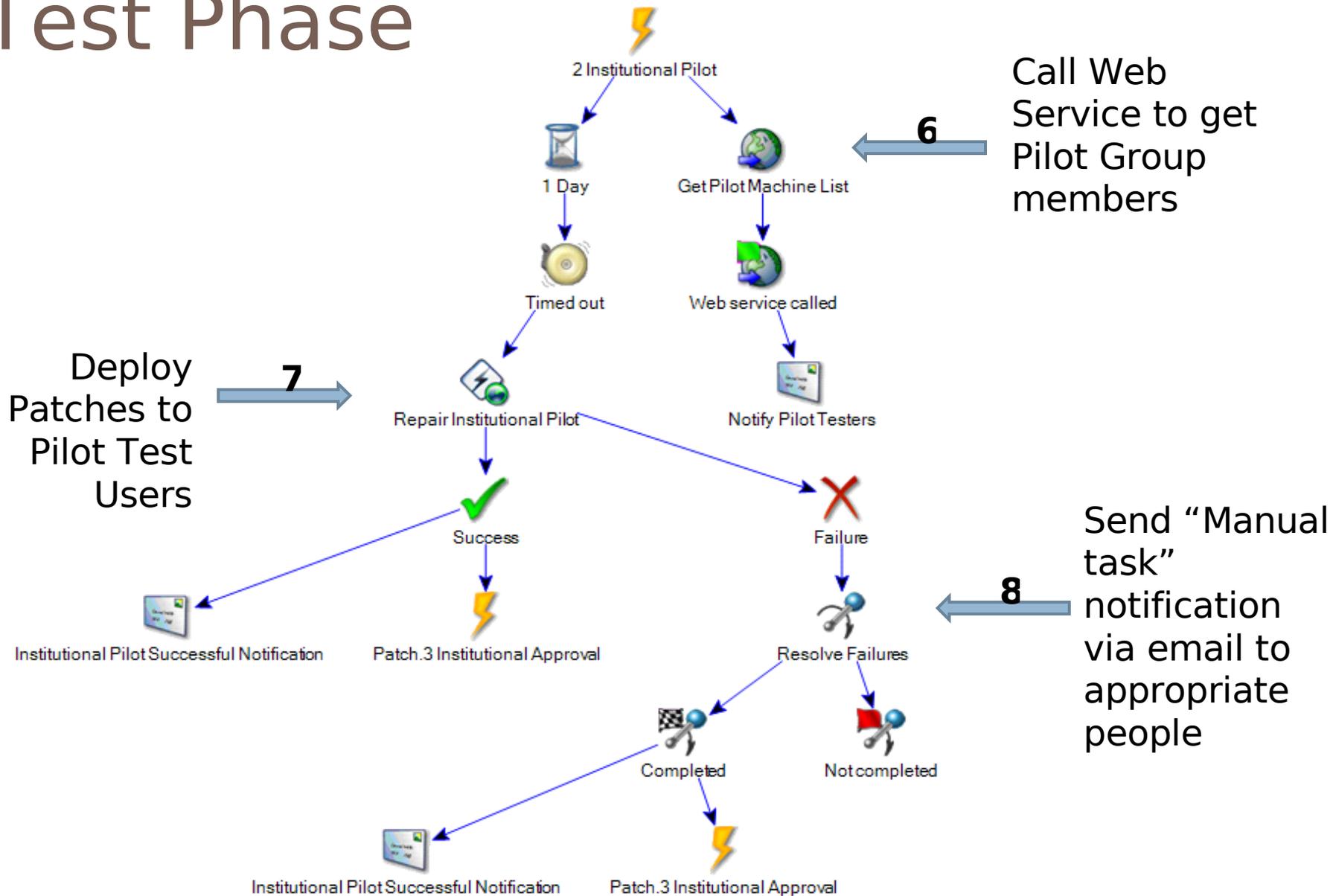
[Click here to see the details.](#)

LANDesk Process Manager

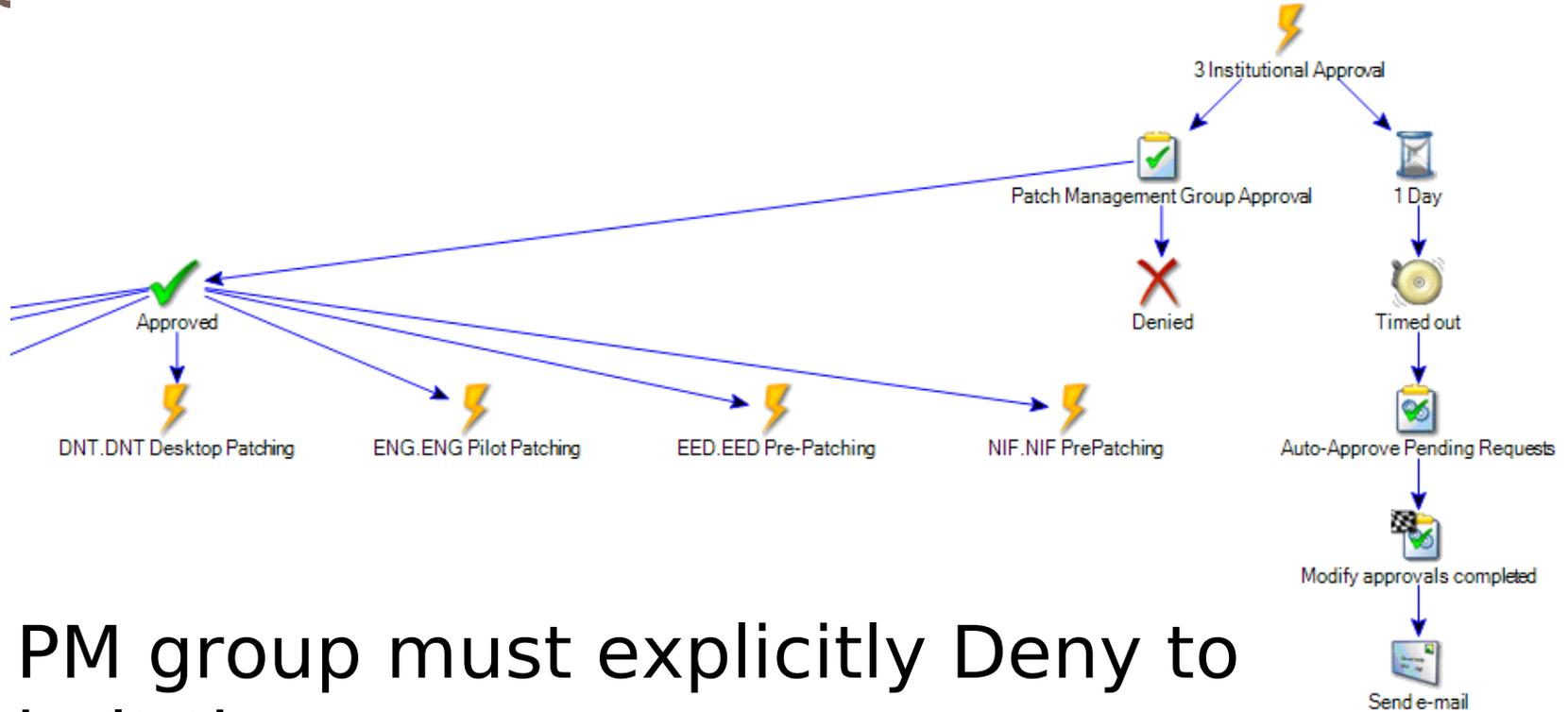


5 New Patches added to Deployment Group and deployed to QA

LLNL Patch Process – The Pilot Test Phase



LLNL Patch Process – Institutional Approval



- PM group must explicitly Deny to halt the process
- Non-responders will auto-approve
- On Approval, Control passes to Directorates

Patch Management: Benefits of LPM

What does this buy us?

- ✓ Automated, process-driven approach
 - ✓ QA, Pilot, and Production deployment cycles
- ✓ Admins must act to **PREVENT** patch deployment
- ✓ Support for diversity
- ✓ Extensibility

Importance of End User Visibility in CM

But, What Happens If:

- ❑ Systems will fall through cracks
- ❑ Unresolved patch installation failures
- ❑ Bugs in the Process design

LANDesk Process Manager



Prototype: LPM & End User Visibility

LPM & End User Visibility



- Custom Written Application
- System Tray Icon
- Application communicates with LANDesk Process Manager
- Retrieves health information about itself
- Green Logo Indicates Health

LPM & End User Visibility

The screenshot displays the 'SeverityCenter - Self-Service Management Portal' window. The window title is 'SeverityCenter' and the main heading is 'Severity Center - Self-Service Management Portal'. Below the heading are four tabs: 'General Information', 'Patch Severity', 'Software Severity', and 'Configuration Severity'. The 'General Information' tab is active, showing the 'Overall Severity Level' as 'Critical'. A progress bar below this indicates the severity levels: 'OK' (green), 'Warning' (yellow), and 'Critical' (red). The 'Critical' level is selected, and a red triangle points to the '4' mark on the bar. Below the progress bar, the 'Severity Index' is 10. The 'Patch Severity Level' is 'Critical', the 'Software Severity Level' is 'OK', and the 'Configuration Severity Level' is 'Critical'. At the bottom of the window are three buttons: 'Fix Now', 'Refresh', and 'Close', along with a help icon (?) in the bottom right corner.

SeverityCenter

Severity Center - Self-Service Management Portal

General Information Patch Severity Software Severity Configuration Severity

Overall Severity Level: **Critical**

Severity Index: 10

Patch Severity Level: **Critical**

Software Severity Level: **OK**

Configuration Severity Level: **Critical**

Fix Now Refresh Close ?

Summary: A Combined Solution

- **LANDesk Enterprise Suite** – Core Services for vulnerability detection and remediation
- **LANDesk Process Manager** – Workflow Services
- **User Visibility** - Custom LLNL app for end user visibility and control



Questions?



THANK YOU!