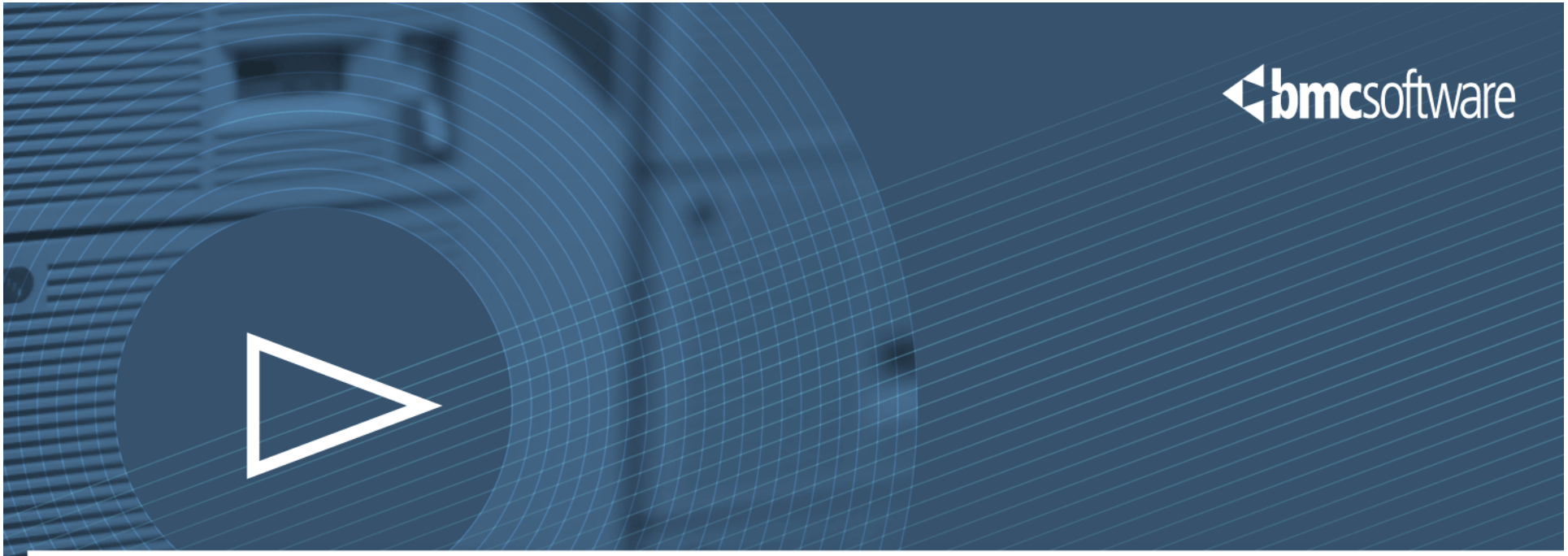
Best Practices: BSA Patching

INTERNATIONAL TOLL FREE: Participant Code: 704371

Argentina: 0800 444 6440
Australia: 1 800 612 415
Austria: 0800 295 780
Bahamas: 1 800 389 0491
Belgium: 0 800 75 636
Brazil: 0800 891 0266
Bulgaria: 00 800 115 1141
Chile: 123 0020 6707
China, Northern Region: 10 800 714 1509
China, Southern Region: 10 800 140 1376
Colombia: 01 800 518 1171
Czech Republic: 800 700 715
Denmark: 80 883 277
Dominican Republic: 1 888 752 0002
France: 0 800 914 176
Germany: 0 800 183 0299
Greece: 00 800 161 2205 6440
Hong Kong: 800 968 066
Hungary: 06 800 112 82
India: 000 800 1007 613
Indonesia: 001 803 017 6440
Ireland: 1 800 947 415
Israel: 1 80 925 6440
Italy: 800 789 377
Japan: 00348 0040 1009
Latvia: 8000 3523
Lithuania: 8 800 3 09 64
Luxembourg: 800 2 3214
Malaysia: 1 800 814 723
Mexico: 001 800 514 6440
Monaco: 800 39 593
Netherlands: 0 800 022 1465
New Zealand: 0 800 451 520
Norway: 800 138 41
Panama: 00 800 226 6440
Peru: 0800 54 129
Philippines: 1 800 111 010 55
Poland: 00 800 112 41 42
Portugal: 800 827 538
Russian Federation: 810 800 2915 1012
Singapore: 800 101 2320
Slovenia: 0 800 80439
South Africa: 0 800 982 304
South Korea, Korea, Republic Of:
003 0813 2344
Spain: 900 937 665
Sweden: 02 079 3266
Switzerland: 0 800 894 821
Taiwan: 00 801 127 186
Thailand: 001 800 156 205 2068
Trinidad and Tobago: 1 800 205 6440
United Kingdom: 0 808 101 7156
Uruguay: 0004 019 0348
Venezuela: 0 800 100 8540

Housekeeping

- Please ask questions in the “Q&A” section:
  - Many “Q&A” questions can be addressed during the session by our experts, while Chat is not seen by the Presenter until the very end of the session
- BSA BP Webinar Series:
  - https://communities.bmc.com/communities/docs/DOC-21692



BMC Server Automation (BladeLogic) v8.2

Best Practices
Patching with BSA (BladeLogic)

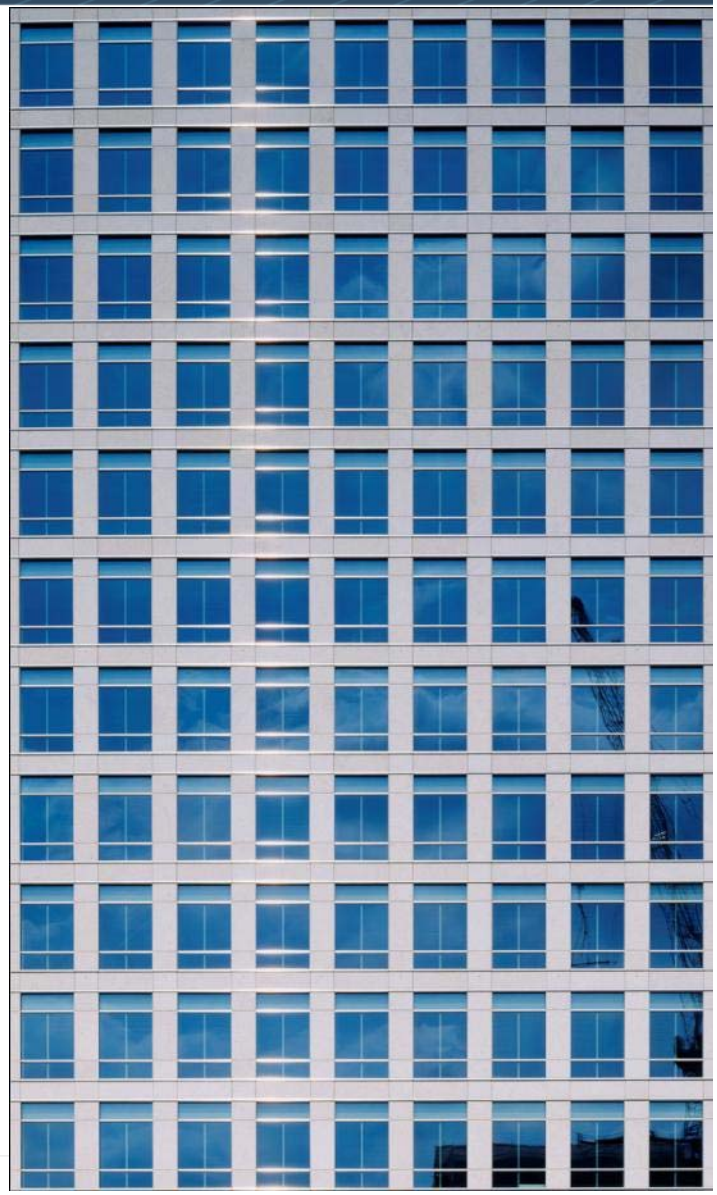
Sean Berry
Lead, Customer Engineering Operations

Disclaimers

- First Level Training
- Best Practice vs. How To
- Covers Most Common Tasks
- Does not address every scenario
- Assumes prior knowledge of BSA components and terms

Agenda

- Language, Terms and Concepts
  - Patch Catalogs
  - Policies
  - Analysis & Deployment
- Use Cases
  - Basic Patching
  - Align by Deployment
  - Fully Realized Use Case
  - Advanced Cases
- Where to Start
- Questions & Feedback



Introduction

- Artifacts in the “Best Practices” franchise
  - BSA Best Practices Webinar Series:
    - https://communities.bmc.com/communities/docs/DOC-21692
  - Patching Best Practices Documents
    - Windows
    - Linux
    - Remote Deployments
    - Other Platforms Pending
  - BSA 8.3 base documentation:
    - https://docs.bmc.com/docs/display/bsa83/Home
  - Deployment Architecture:
    - https://docs.bmc.com/docs/display/bsa83/Deployment+architecture
  - Sizing and Scalability:
    - https://docs.bmc.com/docs/display/bsa83/Sizing+and+scalability+factors
  - Disaster Recovery and High Availability:
    - https://docs.bmc.com/docs/display/bsa83/High+availability+and+disaster+recovery
  - Large Scale Installations:
    - https://docs.bmc.com/docs/display/bsa83/Large-scale+installations
  - Agent Cleanup
    - blcli “Delete cleanup*” spaces

Why Patch?

- **Situation**: Most security breaches are due to known and patched vulnerabilities. The **challenge** is that patching is usually considered overhead. **As a result**, there's a need to manage patching as efficiently and effectively as possible.
- **By following best practices**, you can manage patching compliance at a minimum cost per host.
- As we go through this material, **consider** the current state of patching in your organization, and **look for what you can use** of this material, and what to try next. Feel free to **ask questions** in the Q&A: we have several experts available to respond.
- **The benefit to you**: faster, more efficient patch compliance, with minimum friction and efforts.

Typical Patching

- 1000s of servers per hour over several hours
- A few policies or many policies
- Tight control over execution: what patches get deployed when
- Efficient deployment and use of infrastructure
- Known data paths, highly auditable.

What Is It?

Basics

- Kinds of Patches
  - Maintenance
    - Security & Vulnerabilities
    - Bugfixes
  - New Features
- Methods
  - Individual Patches
  - Patch Clusters
  - Service Packs
- Patching Jobs vs. Other Ways to Patch

Standards & Policies

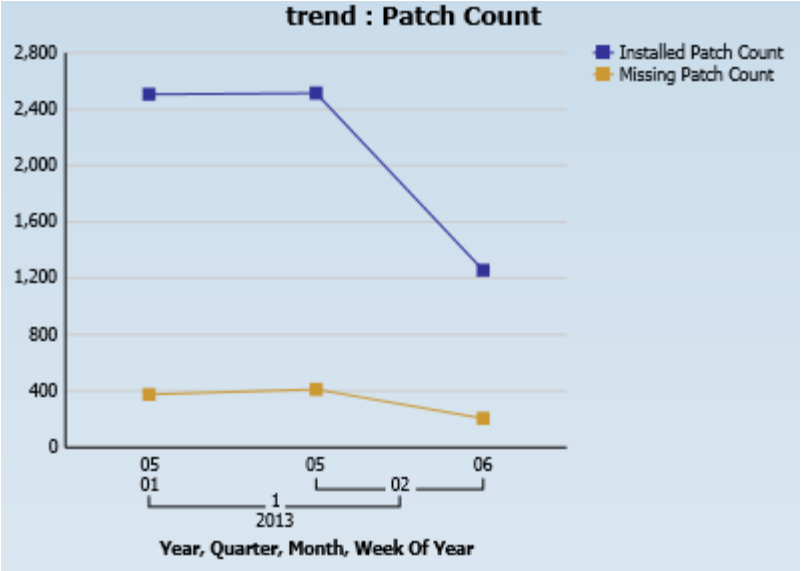
- Vendor specifications (metadata)
  - What you've got
  - What you need
- Catalogs
  - Filters
  - Patch Objects
  - Online/Offline
- Policies
  - Patch Smart Groups
  - Properties
  - Include/Exclude (white/black) Lists

Analysis & Remediation

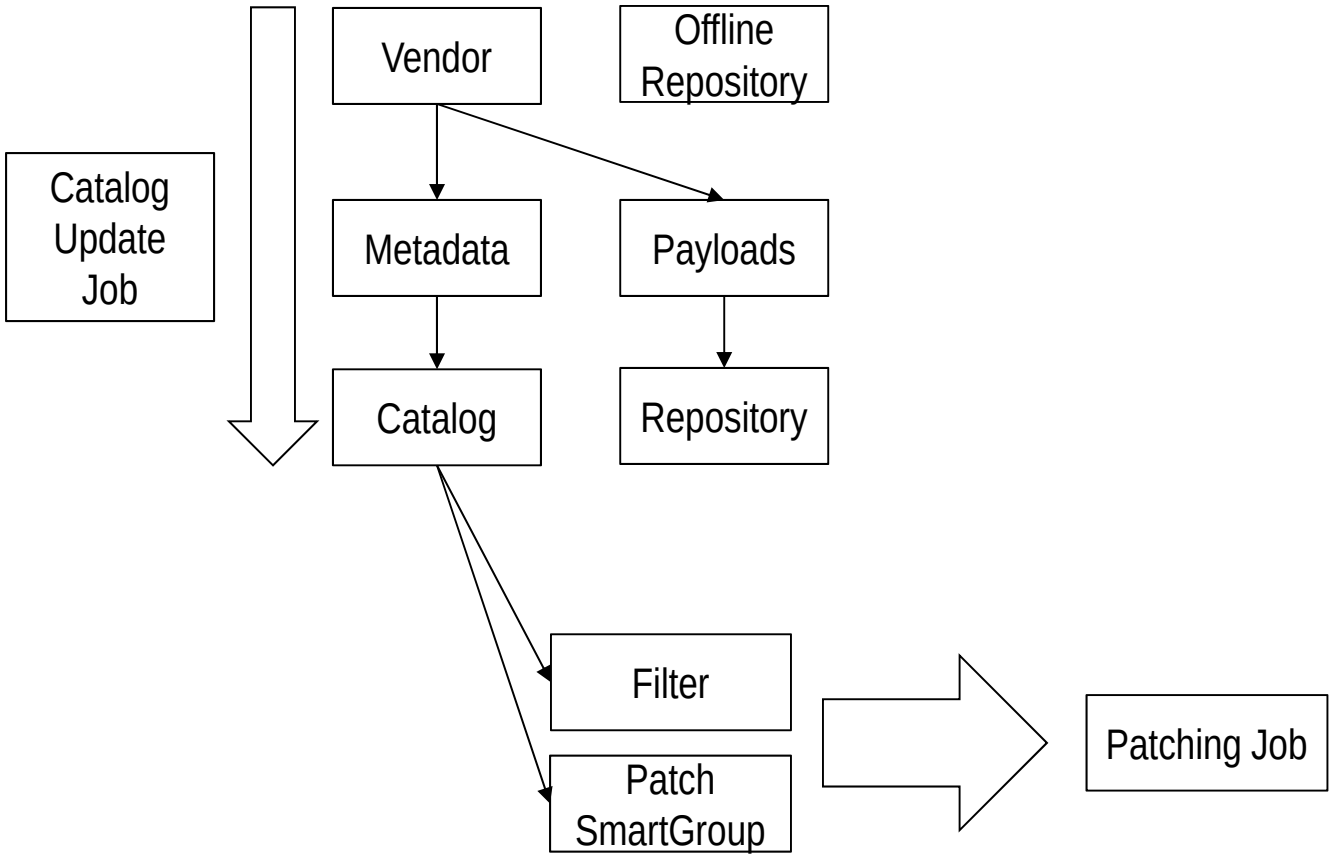
- Analysis
  - Policies
  - Include/Exclude/List
  - Check boxes
- Payloads
  - Acquisition / Downloading
- Packaging, Scheduling
  - Dependencies
- Deployment & Reboots
  - Platform specifics

Validation & Reporting

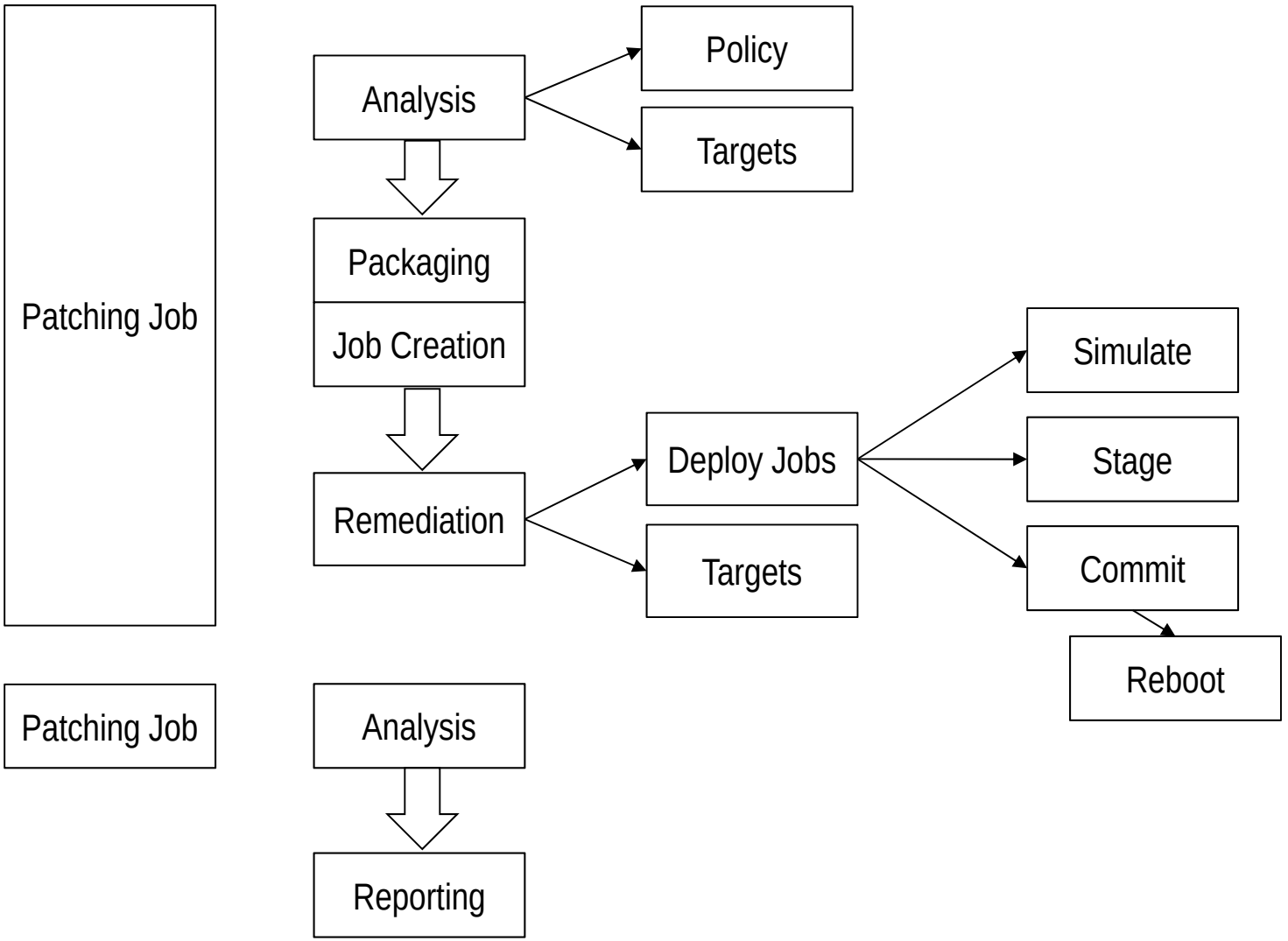
- Validation
  - Verify / Audit to original standard
  - Can Reuse Original Patching Job
- Reporting
  - Standard Reports
  - Custom
- Integration with ITSM Change
  - If a business service breaks after patching, event/impact/change will help to track it down pretty easily.



Patching Infrastructure Workflow Components



Typical Patching Job Workflow



Standing Up a New Service Offering

Standing Up a New Service Offering

- Define Process
- Test in QA
- Train Users
- Deploy into Production
- Monitor

Basic Use Cases

Server Specific Use Cases

- Live Browse Installed Patches
- Live Server 1:1 Audit
- Snapshot / Gold Standard
- Individual Patch Deployment
- Service Packs
- Reporting without Remediation
- Compliance Jobs & Firmware Deployments

Standard Use Cases

Standard Use Cases

- Cross-platform Patch Compliance Reporting (Single Pane of Glass)
  - Windows, Linux, AIX, Solaris, HPUX
- Patching and Remediation as a Regular Practice (monthly/quarterly)
  - Typically first 2-3 cycles are longer until converge on the same 5-12 patches per month
  - Many Best Practices
  - Some Training Required!
- Patching During Provisioning For Initial Quality
  - Use same policies for provisioning (day 1) as production (day 2-1500)
  - No “catch-up” after deployment
- Patching for Service Providers
  - Common catalog
  - Many PSGs

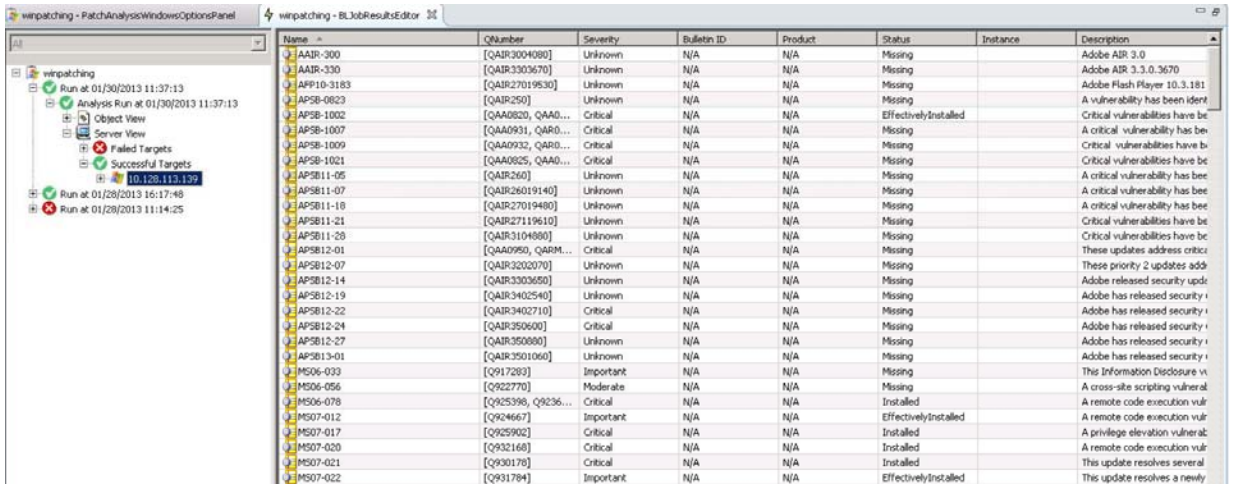
How to Do Standard Patching Efficiently

- Patching By Cohort/Group
  - Analyze servers together that will be patched/deployed together
  - Group together by datacenter, major OS version
  - Group together by server quality (well behaved vs. problematic)
- Patching in Short Maintenance Windows
  - Analyze well in advance of deployment (at least 4 hrs, usually at least a day)
  - Deploy phase by-server
  - Use Timeouts
  - Simulate immediately or ASAP
  - Stage patches in advance to save time once the maintenance window opens
  - Commit patch package installation as soon as the maintenance window opens
  - Re-analyze immediately after deployment

Specific Use Cases

Reporting-only Patching Compliance

- Audit to Policy
  - Potentially many tools used for remediation/deployment
  - Potentially many teams doing patch management
  - Competition/Co-opetition
  - Common first step to full cycle
- Centralized Compliance Visibility
  - Compare many server cohorts to their policies
  - Unified reporting



Time-Based Policies

- Biannual Patch Standards
  - Usually UNIX
  - “Winter 2012”
  - Policy Promotion & Job Reuse
- Policies
  - Quarterly Rolling Windows
    - (80% complete in Dev -> promote policy to QA)
  - Patches from specific date ranges (this month, last quarter)
- Platforms “frozen in time”
  - Patch Smart Group with DATE_POSTED* filter & end date
- Catalogs “frozen in time”
  - Software locked to a certain date or before
  - Offline catalog or single-run

Complex Change Environments

- Tight maintenance windows
  - 1-2 hour
  - Advanced Deploy Jobs
    - (scheduled simulate-stage-commit phases)
- Many maintenance windows / different patch policies
  - Analysis per window / policy
  - Overview reporting
  - Many different maintenance windows => re-use jobs, just change policies
- Individual servers that need to get pulled at the last minute
  - Scripts to create individual remediation processes
  - Higher costs
- Non-automated application start/stop
  - Anything that requires manual intervention is going to be painful!

Distributed Environments

- Remote data centers
  - Repeaters
- Very high latency remote sites
  - Remote Patch Repositories
  - Offline downloaders & File Deploy Job Auditing
  - Optional: Parallel Infrastructure
- Poorly behaved agents
  - JOB_PART_TIMEOUT
  - JOB_TIMEOUT
  - Keep agent versions current
- Integrating with:
  - ITSM Change
  - NIM, WSUS, RH Satellite, existing repos
  - Air-gapped environments

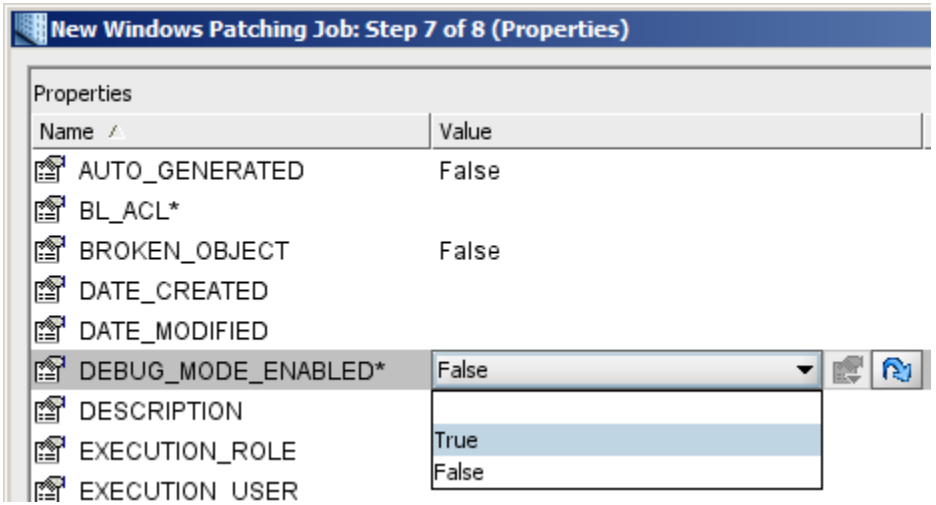
Reporting

- Pre-defined Standard Reports
  - Audit results
  - Trends
  - Multi-platform -> One report
- User Definable Reports
  - Ad-hoc queries
  - Customize formats, branding and calculations
- Job-related & effort-related metrics

Troubleshooting

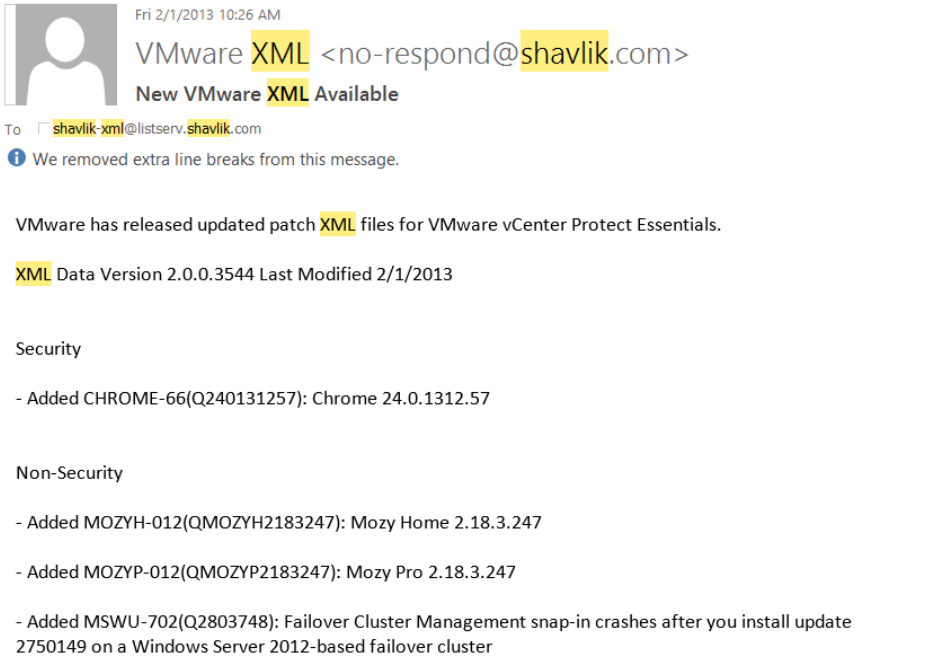
Troubleshooting

- Knowledge Base!
- Logging:
  - Deployment Logs
  - Enable Job Debug option to show more details on failures in analysis
- Job Logs
  - -40xx exit codes



Troubleshooting (cont'd)

- Windows
  - Trace.txt & other KB articles
  - https://docs.bmc.com/docs/display/bsa83/Troubleshooting+Windows+Patching+%28user+contribution%29
  - Subscribe for Shavlik XML notifications & updates at http://www.shavlik.com/support/xmlsubscribe.aspx)



Fri 2/1/2013 10:26 AM

VMware XML <no-respond@shavlik.com>

New VMware XML Available

To shavlik-xml@listserv.shavlik.com

We removed extra line breaks from this message.

VMware has released updated patch XML files for VMware vCenter Protect Essentials.

XML Data Version 2.0.0.3544 Last Modified 2/1/2013

Security

- Added CHROME-66(Q240131257): Chrome 24.0.1312.57

Non-Security

- Added MOZYH-012(QMOZYH2183247): Mozy Home 2.18.3.247

- Added MOZYP-012(QMOZYP2183247): Mozy Pro 2.18.3.247

- Added MSWU-702(Q2803748): Failover Cluster Management snap-in crashes after you install update 2750149 on a Windows Server 2012-based failover cluster

Tactical Techniques

- Reboot Extended Object: 1 hr / 4 hrs / 24 hrs
- Separated Reboot Process
- By-server deploy execution flow
- Stage-ahead (Short Maintenance)
- Re-use existing Patching Jobs
- Import Q-numbers list

Offline Downloader

- OS Platform sensitive
  - Linux supports most except Windows
  - Common to use a “helper” server to acquire metadata, build repos., run platform-specific code
- Storage footprint per platform, version, architecture (5-8GB typical)
- Sample config files
  - Includes some examples, could always use more.

Questions and Feedback

Additional Resources & Information

- BSA Best Practices Webinar Series:
  - https://communities.bmc.com/communities/docs/DOC-21692
- Online Documentation
  - BSA Deployment Architecture Best Practices
    http://docs.bmc.com/docs/display/public/bsa82/Deployment+architecture
  - Product Documentation
    http://docs.bmc.com/docs/display/public/bsa82/Home
- BMC Communities (public forum)
  - BMC website
    - documents
    - discussions
    - whitepapers
    - additional information
  - https://communities.bmc.com/communities/community/bmcdn/bmc_service_automation/server_configuration_automation_bladelogic
- What to do when you inherit a BSA installation, including “How to” videos:
  https://communities.bmc.com/communities/community/bsm_initiatives/optimize_it/blog/2012/06/15/taking-the-reins-server-automation

- Windows Patching Knowledge Articles:
  - https://docs.bmc.com/docs/display/bsa83/Troubleshooting+Windows+Patching+%28user+contribution%29

Howto Videos

- Initial Install – Database Setup: On BMCdocs YouTube at http://www.youtube.com/watch?v=91FEUDVD6sE
- Initial Install – File Server and App Server Installs: On Communities YouTube at http://www.youtube.com/watch?v=m7Y3SY23kuQ
- Initial Install – Console GUI and Appserver Config: On Communities YouTube at http://www.youtube.com/watch?v=uwqlj60Lvo0
- Compliance Content Install: On BMCdocs YouTube at http://www.youtube.com/watch?v=bXdaogDsCNc
- Compliance Quick Audit: On BMCdocs YouTube at http://www.youtube.com/watch?v=i8BLi4WAWEY
- BSA 8.2 Patching - Setting Up a Windows Patch Catalog: On Communities YouTube at http://www.youtube.com/watch?v=nfpFpOuub9k.
- Windows Patch Analysis: On Communities YouTube at http://www.youtube.com/watch?v=ODWhC01uEaQ.
- Patching in Short Maintenance Windows with BMC BladeLogic Server Automation: On Communities YouTube at http://www.youtube.com/watch?v=o6Lfzbb3JZg.
- Basic Software Packaging: http://www.youtube.com/watch?feature=player_embedded&v=dtOWTTFqsaY
- SOCKS Proxies: https://communities.bmc.com/communities/community/bmcdn/bmc_service_automation/server_configuration_automation_bladelogic/blog/2012/11/30/how-to-use-socks-proxies-with-bsa-to-deal-with-firewalls-and-overlapping-ip-ranges