Best Practices: BSA Compliance

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

BSA Best Practices Webinars
Compliance & Change Tracking

Sean Berry

Agenda

- Compliance:
  - Overview
  - Running
  - Building
  - Out of the Box & SCAP
  - Change Tracking
  - Reporting

Overview

Compliance Overview

- What is Compliance?
  - Determining whether systems meet a standard
- What kinds of compliance are there?
  - Regulatory and Security compliance
    - Defined by 3rd parties like CIS, DISA, PCI
    - Internal corporate standards
  - Build Compliance
    - Is the system starting out in a known good state? (built correctly)
  - Configuration Compliance
    - Is the system still in a known good state after being in production for a while?
  - Patching Compliance
    - Does the system have the proper set of patches installed (see last session's preso)
  - Change Tracking
    - Does the system today look like it did yesterday (except for authorized changes)

Compliance Overview – Audits vs. Rules

- What does Compliance mean in BladeLogic ?
  - Two primary methods to determine compliance:
    - Audit Job
      - As few as one configuration, up to many
      - One to n comparison of state
        - » Live Server -> Live Server(s)
        - » Snapshot -> Live Server(s)
      - Requires an example ‘gold master’ (live system or snapshot)
      - Targets must match Master exactly
      - Very quick to get running, moderately flexible
    - Compliance Job
      - Rules-based: conditional evaluation
      - No master required
      - More than one “right” answer
        - » Ranges
        - » Boolean logic
        - » If..then..else, foreach, counts

Compliance Overview – Remediation Options

- After determining a lack of compliance, what are the options?
  - A failure is expected and can be excepted (allowed): common when required due to application limitations
    - Audit
      - Limited exception handling
    - Compliance
      - An 'exception' can be set on the component for the particular rule and the next compliance run this will be counted as compliant.
  - Failure needs to be fixed/corrected
    - Audit Job
      - Sync-to-master
        - » Makes targets look like masters for one or more items
        - » Creates a "remediation" blpackage that deploys whatever configuration is on the master to the target.
    - Compliance Job
      - Deploy "remediation" blpackage that brings system in line with standard
        - » Blpackage must be created and associated w/ each rule

Compliance Overview – Where do Policies Come From

- Compliance Policies for many common standards are provided Out-of-Box by BMC
  - Regulatory policies, very helpful for auditors
    - CIS, DISA STIG, SOX, HIPPA, PCI, NSA
- Compliance policies can be custom built by the customer, by BMC Professional Services or a Partner for the specific customer requirements
  - Typically for Build Compliance or other custom Configuration Compliance
  - Doesn't need to be "whole-server", common to build for specific applications
- Compliance Quickstart:
  - https://communities.bmc.com/communities/docs/DOC-18473

Compliance Development Workflow

- Define / Acquire Compliance Policy (what are the rules?)
- Determine how to evaluate the policy conditions in a programmatic, automated fashion
  - What configurations are native to BladeLogic?
    - Config file entries, applications, services, users, groups, etc.
  - What checks require a script or some extension ?
    - Extended Objects, 3rd party executables
  - What checks cannot be done programmatically?
    - Eg 'Server is in a locked room'
- Determine what conditions can be fixed and how to fix them
- Create a Component Template Object in BladeLogic ("Compliance Policy")
  - Define the parts and rules
  - Create Remediation packages and associate to the rules
- Test the rule conditions to ensure no false positive/negative
  - Useful to have a "red/bad" server and a "green/good" server
- Test the remediations
- Scale up!

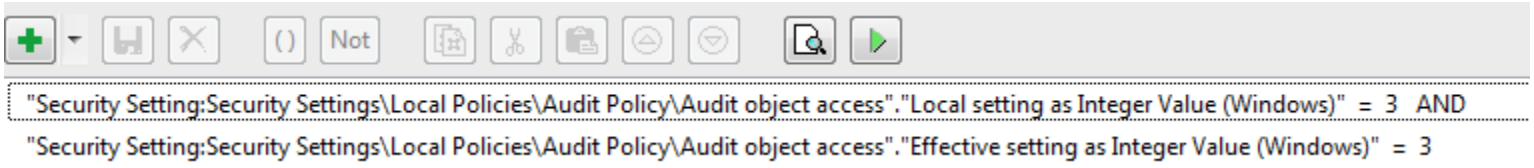
Compliance Execution Workflow

- Run ‘Component Discovery’ Job for the Component Template(s)
  - Custom or Out-of-Box
  - Creates Components
- Create a Component Smart Group for the discovered objects
- Create a Compliance or Audit Job targeting the Component Smart Group
- Run the Compliance Job
  - Identify environment-wide noncompliance vs. specific host noncompliance
  - In a Windows AD environment it’s beneficial to get the Domain GPO compliant before checking the member servers
- Review Results
  - Set Exceptions in Compliance Job as necessary (can expire!)
- Remediate
  - Sync to master for Audits
  - Remediate for Compliance
- Re-run Compliance or Audit to verify remediation/ newly compliant state

Building

Building Compliance

- Building/modifying content
  - BladeLogic has a rule editor that lets you build and test the rule conditions
  - Rules can be very simple or very complex



  - Or more complex

```
foreach "File:/var/yp/**"
   "Group Owner (Unix) (Unix)" = "Configuration File Entry:/etc/group//root"."Value2 as Integer (All OS)"  OR
   "Group Owner (Unix) (Unix)" = "Configuration File Entry:/etc/group//sys"."Value2 as Integer (All OS)"  OR
   "Group Owner (Unix) (Unix)" = "Configuration File Entry:/etc/group//bin"."Value2 as Integer (All OS)"
end  AND
foreach "File:/var/nis/**"
   "Group Owner (Unix) (Unix)" = "Configuration File Entry:/etc/group//root"."Value2 as Integer (All OS)"  OR
   "Group Owner (Unix) (Unix)" = "Configuration File Entry:/etc/group//sys"."Value2 as Integer (All OS)"  OR
   "Group Owner (Unix) (Unix)" = "Configuration File Entry:/etc/group//bin"."Value2 as Integer (All OS)"
end
```

  - Try to collect the highest level object that would be present, eg ‘Services’ or ‘Applications’, not ‘Application XZY’ if your check is that ‘Application XYZ’ is present.

Building Compliance

- How do I define what I want to check?
  - **Server Asset** based Audits are great for fast, ad hoc checks
    - "I found something wrong"
    - "I'm not sure what our standard is"
  - **Template** based checks for Audit and Compliance are for re-usable policies, checks.
  - After defining rules for compliance, should create blpackages to fix a rule failure, may not be first step
- **For a check of a documented compliance policy Component Templates and rules-based compliance are the way to go**

Building Compliance

- What is a template?
  - Sometimes called a “Policy”
  - Parts
    - Template contains the ‘parts’ you want to evaluate.
    - Typically you check a subset of parts (signal vs. noise!)
    - The parts are mostly just assets on the server
- Templates have many uses
  - Browse/limited access to server (access control use case)
  - Discovery/Inventory (find in-house apps, capture configs for reporting)
  - Audit/Compliance/Snapshot
- Where Rules Come From
  - Audit will use Template as the list of things to compare
  - Compliance requires creation of rules with conditions to evaluate the assets you list in the template

Building Compliance – Uses & Terminology

- What else can templates do?
  - Template lets you parameterize things like the path to the asset to account for server differences – eg /C/Windows vs /C/Winnt -> ??TARGET.WINDIR??, hostnames
  - With the use of the Properties can model multi-instance applications, eg in-house, or something like Oracle database, on the same or multiple servers
  - Templates can be used to give limited (browse) access to a server for example to grant a DBA access to only the Oracle assets on a server
  - Used for inventory tracking – determine if a set of objects exists on a target server like an application that doesn't show up in 'Add/Remove Programs'
- Component Template, Inventory Template, Compliance Template, Policy?
  - These are all the same object type, just used for different purposes.
  - A single template can be used concurrently for all of its functions and each function (snapshot/audit, compliance, etc) can act on different parts of the template

Building Compliance - Discovery

- Discovery: I have the template, now what?
  - Should define '**discovery conditions'** in the template to determine that set of 'stuff' applies to a particular system – No point in using Windows 2008 Policy on RHEL 6
  - **Discovery process** lets you set it and forget it – as new servers get added, discovery automatically associates any servers that meet the discovery conditions with the template (creates a component) on the new servers and the next compliance check will include those objects
  - If a server is changed so that it no longer meets the discovery condition, the component will be **marked invalid** and can be excluded from the Component Smart Group used as the job target.
  - **Servers must have components** created/discovered to be a used with a Compliance Job even if you target the server directly

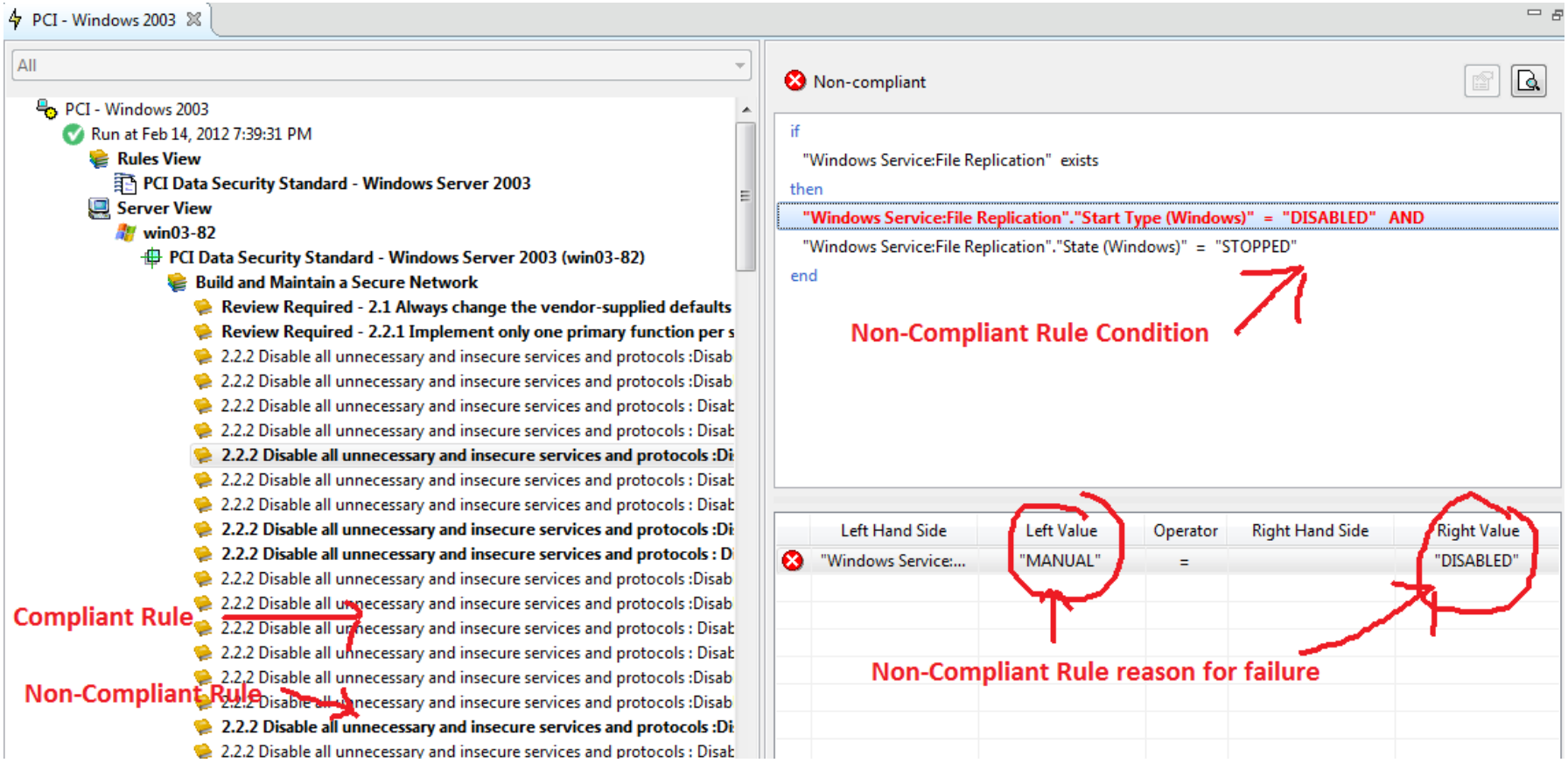
Building Compliance

- Extended objects
  - Extended Objects allow you to gather information that is otherwise not natively available in BSA.
    - Eg: output of a binary like ‘lspci’, eeprom, anything machine-readable
  - Typically are NSH scripts but others languages are usable (eg, shell, power shell, wmi/vb, perl/python/etc.)
  - Output should be formatted to be parsed by one of the formats, many common ‘grammar’ formats such as name = value, csv, XML (csv2xml!)
  - Poorly written Extended Objects can create a serious performance impact on the application server.
    - Remember that this script will run against every target server of the compliance/audit/snapshot job
    - Be careful with finds across filesystems
    - Trap errors wherever possible, return as much good information as possible

Running

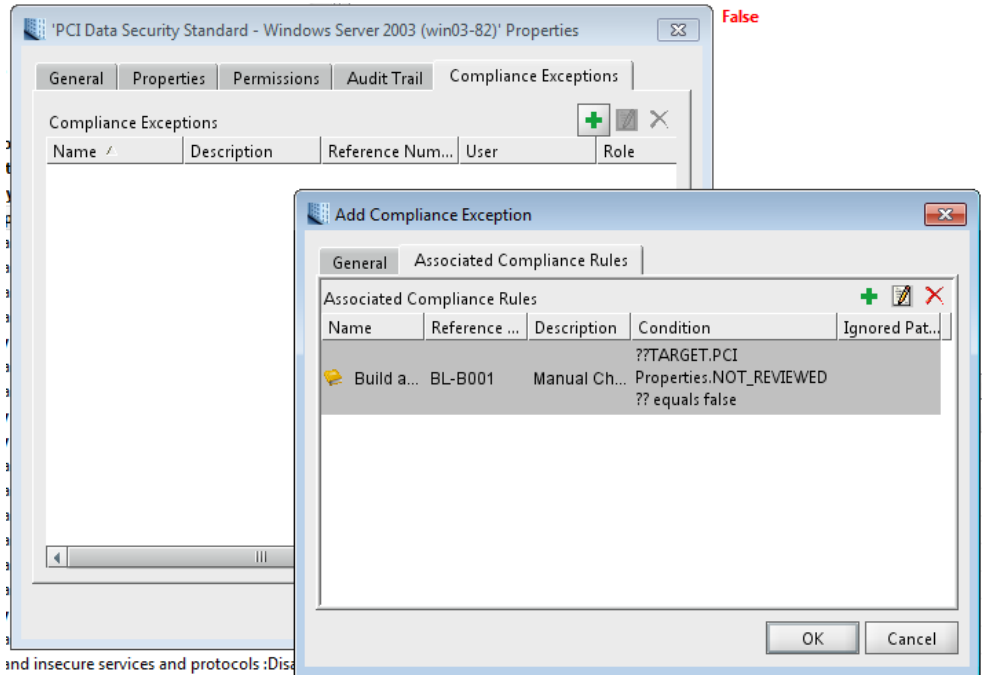
Running Compliance

- Run discovery job then run compliance or audit job
- Common to wrap in a Batch
- Review results



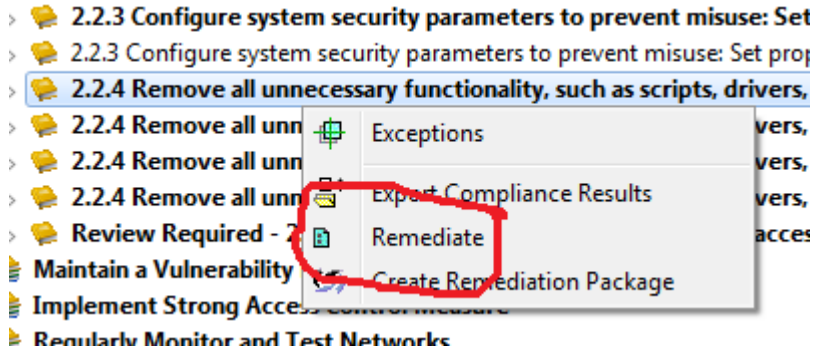
Running Compliance - Exceptions

- Set exceptions – allow a non-compliant system to “pass with documented exception”
- Exceptions can expire: “Ok, allowed for the next 3 months, until we expect underlying app to be fixed”
- Reportable!



Running Compliance - Remediation

- Sync to master or remediate
- Can remediate:
  - one rule on one server,
  - one rule on many servers,
  - whole server,
  - all servers under a given Compliance or Audit Job
- BE CAREFUL: axes vs. chain saws



- Some fun with parameterized remediation
  - https://docs.bmc.com/docs/display/bsa83/How+to+pass+local+parameter+values+to+a+compliance+remediation+package+%28user+contribution%29

Running Compliance – Auto-Remediation

- Auto-Remediation
  - Once you are confident in your remediation packages and identify those that are safe across the environment, consider enabling auto-remediation
  - Useful for initial server provisioning, or use cases where policies are very well understood and socialized
  - This will automatically push remediation for failed rules after compliance run
  - Auto-Remediation must be enabled in both the General tab of the Template and on the specific rule.
  - Easy to just execute remediation via CLI/API

Running Compliance – At Scale

- Running Large Scale Compliance Jobs
  - Work done on appserver, not on the edge
    - CPU and memory hungry on the appserver
  - Typically one job per policy (template), and one template per OS/platform
  - May want to group targets together by function, customer, etc
- Sizing and Scalability
  - Need to consider available WorkItemThreads in the env, other jobs going on, etc
  - Ensure proper jvm heap sizes on the appserver(s)
  - Enable (in blasadmin) the process spawner
    - This offloads EO runs (and nsh script) to another process and out from under the appserver process to improve performance
  - Look at the job parallelism, sometimes running w/ a lower parallelism can improve overall performance, must be balanced w/ other jobs
  - For the OOB content, we provide NSH Scripts that can pre-seed some of the results.
    - These can run on a schedule so results are available to CJ. (“find files across filesystems”, etc)

Out of The Box Content & SCAP

Out of the Box (OOTB) Content

- If we don't have a standard, where can I start?
  - BMC provides Templates based on industry standards like:
    - CIS
    - DISA STIG
    - PCI
    - HIPPA
    - SOX
  - Includes remediation
    - BMC provided updates to this content will overwrite the existing objects and any changes
  - Copy content for local use: many customers start with an OOTB policy & customize based on what they find in their environment, feedback from InfoSec teams
- How to load the OOTB Compliance Content
  - (covered in a separate Howto Video here: https://communities.bmc.com/communities/docs/DOC-18468)
- When using this content should first evaluate it checks what you want. Always test remediation first on a small scale
- Remediate ALL is something to be used with **caution**: know what you're doing!

SCAP Compliance

- What is SCAP?
  - SCAP is a protocol for authoring content based on a collection of specifications(xccdf/oval/cpe/cve).
  - Maturing standard.
  - Most prevalent in the US Government area (DISA, DHS, etc.).
  - Read more here: http://scap.nist.gov/
- SCAP in BSA
  - Support introduced in BSA 8.2.
  - Certified for SCAP v1.0 . Details available at (http://nvd.nist.gov/validation_bmc_impl_statements_8.2.0.html).
  - Supported platforms include(Windows, Linux, Solaris)
    - AIX and HPUX support forthcoming.
  - Leverages ovaldi for oval check evaluation on agents.
  - Can export results in different formats (xccdf results, asr/arf)
  - Analyze feature - export detailed SCAP result in a html format (to assist with troubleshooting issues).

SCAP Compliance - Running

- Running SCAP
  - Download SCAP bundle from vendor
    - SCAP content publically available at
      - http://web.nvd.nist.gov/view/ncp/repository
      - http://iase.disa.mil/stigs/os/index.html
  - Import SCAP into BSA.
  - Create job definition.
  - Run Job.
  - View/Analyze Results.

Running SCAP

- Download SCAP bundle from vendor, upload to the BSA application server and run
  - Some what of a 'Black Box' – no direct editing of the policy via BSA
- SCAP is a parallel engine to the aforementioned BSA compliance engine.
  - Because of lack of remediation, exceptions and reporting most customers are primarily using w/ BSA compliance
  - Will use BSA's SCAP capability to produce output for their auditors
  - Will use BSA's native compliance to check and remediate their servers

Change Tracking

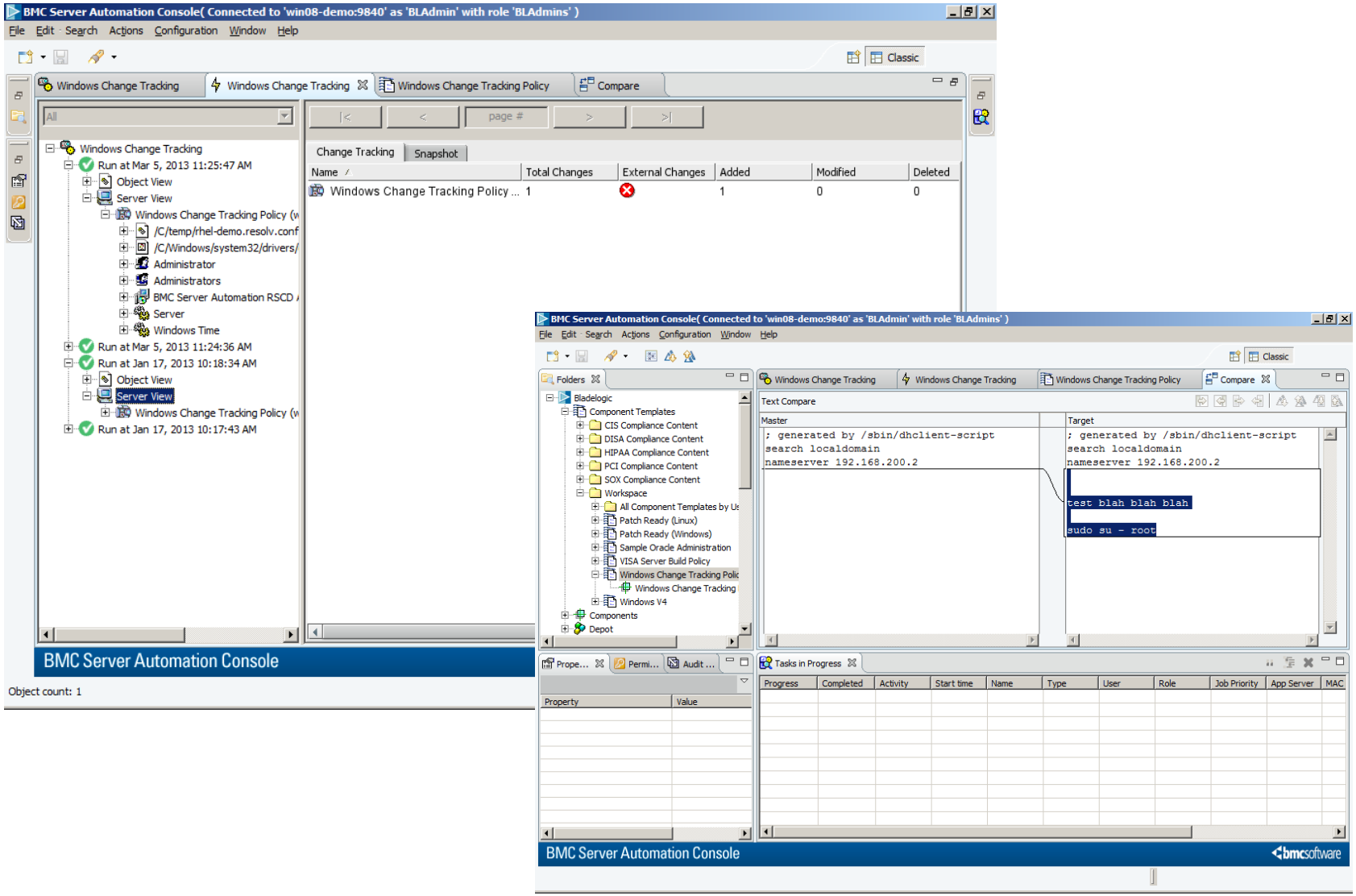
Change Tracking - Overview

- Change Tracking
  - As opposed to a comparison or evaluation this looks for what changed on a particular server between job runs
  - As easy as running a snapshot job on a daily basis
    - Results are on ‘change tracking’ tab in snapshot result
  - This is akin to creating a snapshot to snapshot audit and changing the audit master and target before every job run
  - Snapshots already operate by capturing the delta between the last run and current state, this exposes that in job results
  - limitations
    - Will tell you that the asset changed and what changed, not necessarily who changed it
    - Not real time
    - Asset can go from A to B to C and only A to C will be seen if job doesn’t run between A/B and B/C

Change Tracking – Use Cases

- What change tracking is used for
  - PCI File Integrity Monitoring (FIM)
    - Tracks changes made to critical / sensitive system files
  - Unauthorized Change
    - The /etc/hosts file may not be under configuration control because each box might need different things, but you still want to know if someone changes it from day to day on a particular host
    - Useful in environments with no compliance standards – getting started
  - Configuration Drift
    - Stuff gets changed during break fix
    - Take a snap before and after a change window
      - Deltas will show what changed

Change Tracking - Contents



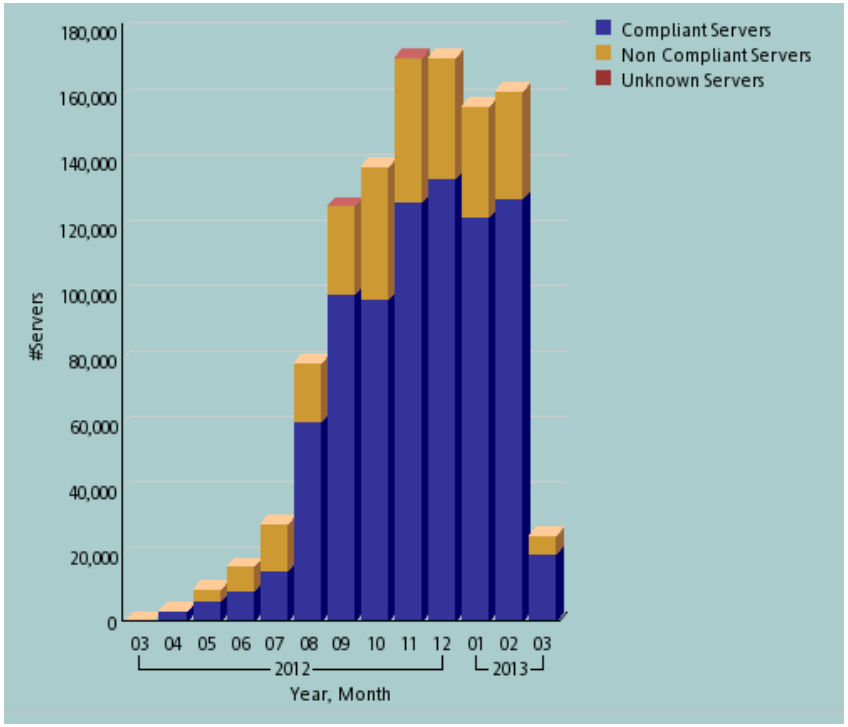
Change Tracking

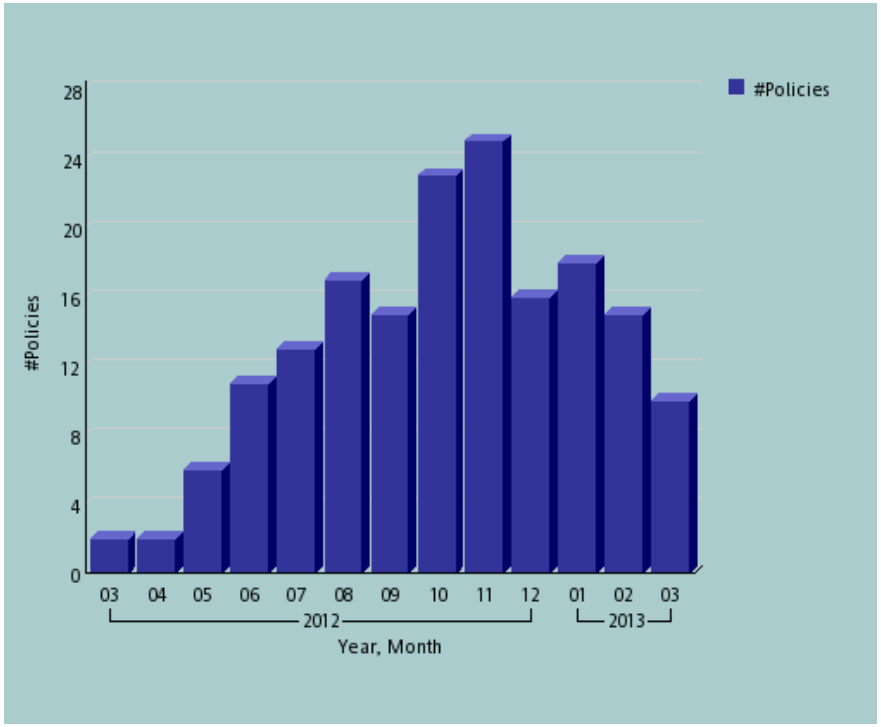
- How not to use snapshots
  - BladeLogic is a configuration management tool, this is not a bare-metal restore tool, not practical to take a snapshot of a whole box a la Ghost or other image restore tools
  - Snapshots should be targeted to particular application configurations
  - Snapshots of 'everything' will have too much noise to be useful
    - Whole registry
    - Whole filesystems
    - Be careful of "Files contents"
  - It's not a monitoring tool:
    - Only capture information you care about / plan to take action on
    - Only capture as often as is relevant: don't capture every few hours if you expect changes only every week, or someone's only going to look at the data once a month.

Reporting

Reporting

- OOB BDSSA Reports are available for Compliance, Audit and Change tracking
- Custom reports can be generated for these domains using Query Studio and Reports Studio



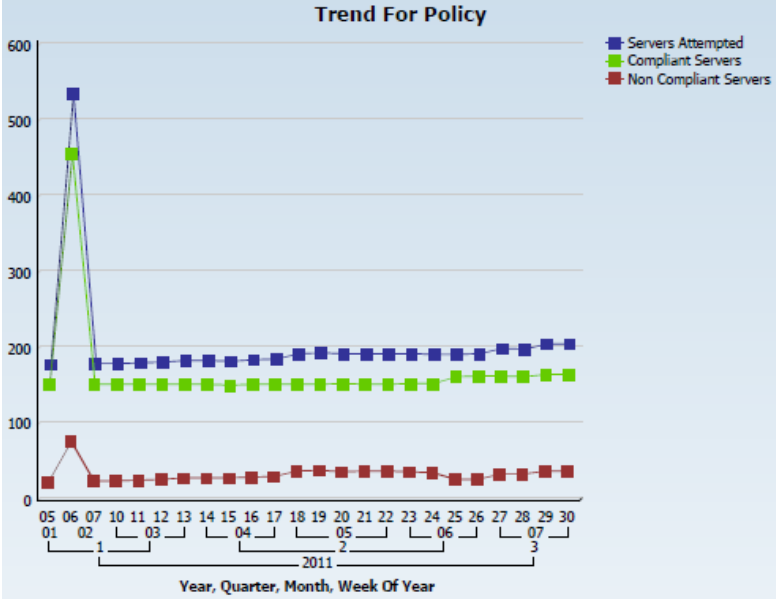


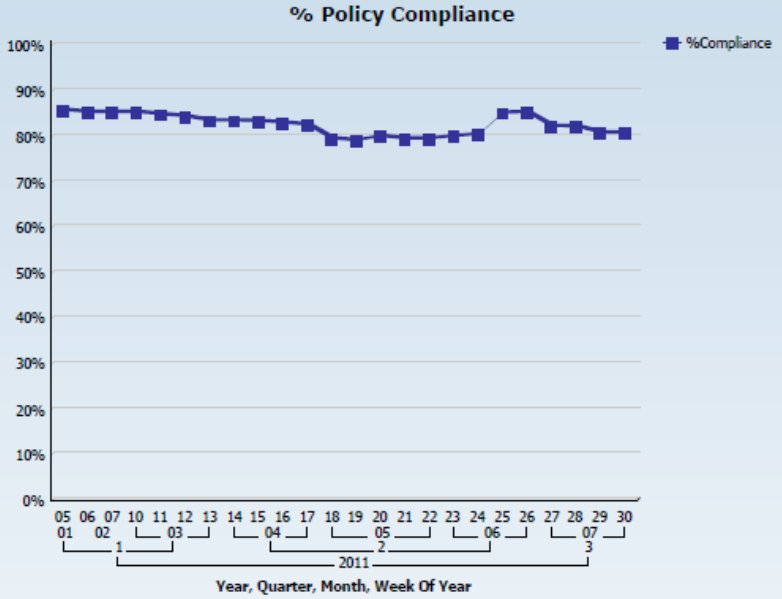
Compliance Trend By Policy

Compliance Trend by Policy

Site\User(Role) : Primary\BLAdmin(BLAdmins)

Date Range :	All Dates
Policy Name :	KeyStrokeLoggerDiscovery





Template(Policy) Name	Year	Quarter	Month	Week Of Year	Servers Attempted	Compliant Servers	Non Compliant Servers	%Compliance
KeyStrokeLoggerDiscovery	2011	1	01	05	177	152	25	85.88%
			02	06	534	456	78	85.39%
				07	178	152	26	85.39%
			03	10	178	152	26	85.39%
				11	179	152	27	84.92%
				12	180	152	28	84.44%
				13	182	152	30	83.52%
		2	04	14	182	152	30	83.52%
				15	181	151	30	83.43%
				16	183	152	31	83.06%
				17	184	152	32	82.61%

Compliance Exceptions

Detailed Exceptions Report

Site\User(Role) : Primary_Invent\Riju(GlobalReportAdmins)

Site	All
Date Range :	All Dates
Latest Run :	All Job Runs
OS Name	Windows

Template(Policy) Name	Job Name	Server Name	Job Run Start Time	Rule Group Name	Rule Name	Rule Definition	Exception Name	Expiration Date
20111201_1	20111201_RBAC	10.20.91.111	Dec 01, 2011 02:57:06 PM	(none)	Rule1	"Windows Service:*" count between [5 AND 10]	E_RBAC	
			Dec 01, 2011 02:10:01 PM	(none)	Rule1	"Windows Service:*" does not exist	E_RBAC	
Exception_Compliance_Template	Exception_Compliance_Job	localhost	Nov 25, 2011 06:45:07 PM	(none)	Rule_1	"Windows Service:ClipBook" does not exist	Exception_Rule	
Exception_Compliane_Template	Exception_Compliance_Job	vm-w23-rds898	Nov 24, 2011 05:35:17 PM	(none)	Exception_Rule	"Windows Service:/".Name equals "Server"	Exception_1	
New_Exception_Template	New_Exception_Compliance_Job	vm-w23-rds318	Nov 30, 2011 07:05:23 PM	(none)	New_Compliance_Exception_Rule_2	"Directory:/C" does not exist	New_Exception_1	
			Nov 30, 2011 07:05:23 PM	(none)	New_Exception_Rule	"Directory:/C".Name contains "Ashok"	New_Exception_1	
			Nov 30, 2011 07:01:48 PM	(none)	New_Exception_Rule	"Directory:/C".Name contains "Ashok"	New_Exception_1	Nov 30, 2019 6:04:00 PM
			Nov 30, 2011 06:05:17 PM	(none)	New_Exception_Rule	"Directory:/C".Name contains "Ashok"	New_Exception_1	Nov 30, 2019 6:04:00 PM

Change Tracking

Change Tracking Details By Asset

Site\User(Role) : Primary_OM_81_295_NEW\BLAdmin(BLAdmins)

Date Range :	All Dates
Latest Run :	All Job Runs
OS Name :	All

Physical Memory Device:

Full Name	Change Type	Change String
/Hardware/Memory/PhysicalMemoryDevices/Physical Memory 1	Removed	"Missing"

Physical Memory Array:

No Data Available

Processor:

Full Name	Change Type	Change String
/Hardware/Processors/CPU1	Modified	"Changed" [speed "(M: 2394,2433)"]
/Hardware/Processors/CPU3	Removed	"Missing"
/Hardware/Processors/CPU2	Modified	"Changed" [speed "(M: 2395,2394)"]

Network Card:

Full Name	Change Type	Change String
/Hardware/NetworkCards/8	Modified	"Changed" [macAddress "(M: E0:72:20:52:41:53,18:3F:20:52:41:53)"]
/Hardware/NetworkCards/10	Modified	"Changed" [manufacturer "(M: Intel,)"] [macAddress "(M: 00:50:56:BF:2B:52,)"]
/Hardware/NetworkCards/11	Modified	"Changed" [macAddress "(M: 00:50:56:BF:2B:52,)"]

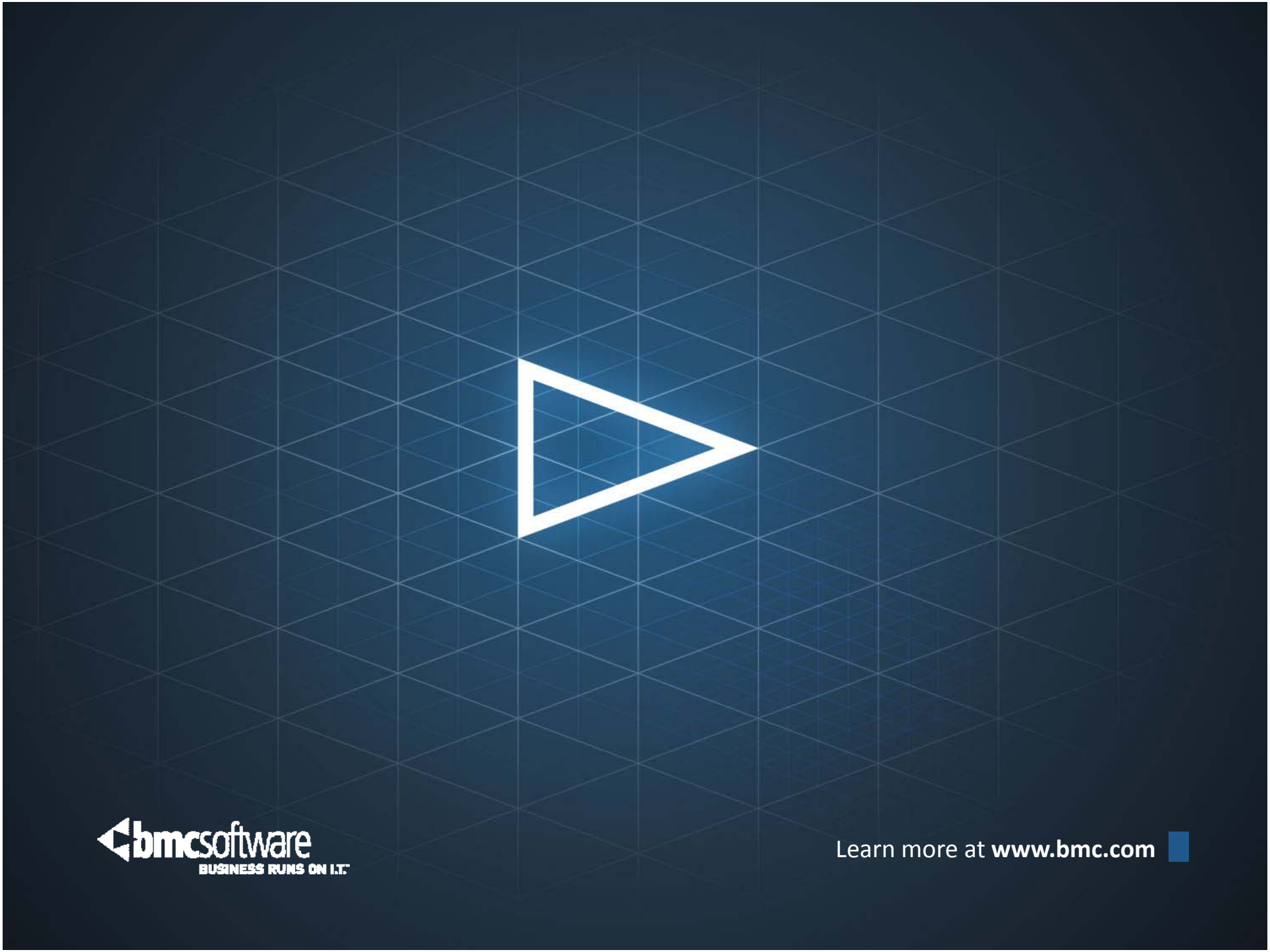
Physical Storage Device:

Config Compliance – Change Tracking

Software Full Name	Change Type	Change String
Adobe Flash Player 10 ActiveX	Modified	"Changed" [Version "(M: 10.2.153.1,10.3.183.55)"] [Install Date "(M: ,2013/02/08 00:00:00-0600)"] [Size "(M: 6291456,3113984)"]
Mozilla Firefox 14.0.1 (x86 en-US)	Removed	"Missing"
Mozilla Firefox 18.0.2 (x86 en-US)	Added	"Extra"
Mozilla Maintenance Service	Modified	"Changed" [Description "(M: Mozilla Maintenance Service 14.0.1 (x86 en-US),Mozilla Maintenance Service 18.0.2 (x86 en-US))"] [Ve 203776,337920)"]
Adobe Reader XI	Removed	"Missing"

Best Practices Webinars Home

- Best Practices Webinars
  https://communities.bmc.com/communities/docs/DOC-21692


bmcsoftware
BUSINESS RUNS ON I.T.
Learn more at **www.bmc.com**