SMIII-204 – BMC Change and Configuration Management Tech Talk

Darius Wallace and Pritpal Singh
BMC
Agenda

› UserWorld Change and Configuration Management (CCM) Sessions
› Brief BMC® CCM Overview
› CCM Architecture
› Components/Features of BMC CCM Solution
› How Does It All Work?
› Documentation
› Q&A
UserWorld Change and Configuration Management Sessions

› SMIII-102 - Compliance-Friendly Change Management: Closing the Loop on Your Change and Configuration Management  
  – Wednesday: 11:30 a.m.

› SMIII-103 - Configuration Management (Marimba) Best Practices and Troubleshooting  
  – Wednesday: 2:00 p.m.

› SMIII-201 - Change and Configuration Management in the Data Center  
  – Thursday: 10:15 a.m.

› SMIII-203 - Configuring BMC® Configuration Management for a Service Provider Environment  
  – Thursday: 2:00 p.m.

› SMV-302 - Improving Change Management with v7.0  
  – Friday: 11:00 a.m.

› ARSI-304 - Task Management Subsystem and Command Automation  
  – Friday: 2:45 p.m.

› SMIII-301 - BMC® Configuration Management Roadmap: The Roadmap to the Future  
  – Friday: 9:45 a.m.
Agenda

› UserWorld Change and Configuration Management (CCM) Sessions
› Brief BMC® CCM Overview
› CCM Architecture
› Components/Features of BMC CCM Solution
› How Does It All Work?
› Documentation
› Q&A
What’s The Value of CCM?

- When performing a change to the IT configuration managed resources, it is critical to maintain consistency and control through the entire process.

  - Manage the change lifecycle from request and planning through implementation and verification.
  - A “Closed-loop” approach ensures that the change is properly documented, assessed, tracked, implemented and ultimately verified.
CCM Integrates Change Management with Configuration Management

CCM: Closed-loop Change Management

- Request
- Plan
- Implement
- Verify

Configuration Management

Change Management

Key Benefits of CCM

- Control and auditability of changes
- More efficient and accurate hand-offs
- Accurate asset configuration information
Elements of Change Management Lifecycle Process

› Request
  – Ensures there is accountability for changes and that changes are woven in IT Service Processes

› Planning/Scheduling
  – Ensures there is proper assessment of resources, costs and risks for the change and that this information is visible to accountable parties

› Approval (Governance)
  – Ensures prioritization, resource plans, assessment of risks (business and technical) and attainment of proper approvals from the Change Advisory Board (CAB)

› Implementation/Verification
  – Ensures proper resources and activities are conducted, changes are kept on track, verified and meet goals with minimal disruption to the infrastructure

› Evaluation/Review of Changes
  – Ensures that changes are reviewed to determine if they were done in an effective and efficient manner
Change Management v7.0

Change Planning
› Change Calendar
› Risk Assessment
› CI Viewer
› Availability/Unavailability
› Multi-Stage Approvals

Change Efficiency
› Consoles
› Templates
› Process Flow Visualization
› Task Management & Viewer
› DSL

Change Productivity
› Change Dashboard
› Closed-loop Verification
Configuration Management v7.0 Can Now Address Key IT Operations Questions

Key IT Operations questions:

“How do you verify that the implemented change matches the approved change?”

“How can you trace changes on a machine back to the decision process that caused it?”

“How do you avoid the manual steps and data entry of transcribing change tasks?”

“How do you ensure that asset information is accurate and ‘normalized’?”
Agenda

› UserWorld Change and Configuration Management (CCM) Sessions
› Brief BMC CCM Overview
› **CCM Architecture**
› Components/Features of BMC CCM Solution
› How Does It All Work?
› Documentation
› Q&A
CCM Architectural Overview

- Automated Systems
  - Requester Console
  - Change Management
    - Support Console
    - Manager's Console
- Task Management
- Advanced Functions
- Business Users
  - Change Manager Change Assignee
- CIO
  - Change Management
    - CCM Calendar
    - Dashboards
- Investigation & Analysis
  - BMC Configuration Management
- Discovery
  - BMC Configuration Management
  - Topology Discovery
- Automated Tools
  - BMC Configuration Management

KEY
- System to System Interaction
- Data Interaction
Agenda

› UserWorld Change and Configuration Management (CCM) Sessions
› Brief BMC CCM Overview
› CCM Architecture
› Components/Features of BMC CCM Solution
› How Does It All Work?
› Documentation
› Q&A
Primary Components/Features of CCM

› Components
  – Change Management
    • Task Management System
    • Command Automation Interface (CAI)
  – Configuration Management
    • Policy Manager Interaction Model
    • Deployment Manager
    • Task Receipts
    • Common Management Services (CMS)
  – Definitive Software Library
  – CMDB

› Features
  – Seamless Authentication
  – Closed-loop Verification
CCM Architectural Components

Change Management

- Change Request
  - Product Lookup
  - DSL Reference
  - Related CI Targets

Task Management System

CMDB

Definitive Software Library

Asset Management
- Software License Mgmt
- Approvals
...

Configuration Discovery

Policy Manager

Deployment Manager

Common Management Services

System to System Interaction

Data Interaction
Change Management and Configuration Management Integration Discussion

- Create new Change Request from Requester Console or RC Form
- Relate, check and update configuration data from change. Check affected CIs for change.
- Integration between applications
  - Data
  - Workflow
What is the Task Management System?

- Part of the Change Management application
- Primary Features/Goals
  - Manage workflow of tasks as they are implemented in an application
  - Provide comprehensive and extensive Task Management definition
  - Enable definition of simple, as well as complex, business process flows
  - Integrate with Automation Tools for Change Management Execution and Verification
  - Support automatic, as well as manual, Tasks
  - Support parallel Task operations
  - Enable passing data between Tasks
- Tasks are the smallest unit of work that need to be performed to fulfill a service request or a request for change.
  - Tasks facilitate the timely and accurate resolution of requests that are complex or need several steps completed before the request can be closed.
What is the Command Automation Interface (CAI)?

– Generic mechanism to abstract interfaces with external systems via application registry

**Diagram**

**Definition**
- Event Data Values

**Construction**
- Command Content

**Execution**
- Runtime Command

**Table**

<table>
<thead>
<tr>
<th>App Registry</th>
<th>Commands</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Name</td>
<td>Protocol</td>
</tr>
<tr>
<td>Command</td>
<td>Direction</td>
<td>Op. Type</td>
</tr>
<tr>
<td>Param</td>
<td>Data Type</td>
<td>Mode</td>
</tr>
</tbody>
</table>

**Protocol Stack**

- AR System
- URL
- Web Services
- Command Line

**Done**
What is Policy Manager?

- Web-application that runs on top of Configuration Management Services (CMS) used to edit policies.
  - CMS provides the foundation on which other components of the BMC CM console, such as Report Center run.

- A policy is the association between one or more targets, one or more packages, and the scheduled delivery of the packages to the targets.

- A target is where the policy will be enforced (e.g. user, machine, group of machines, etc. that are part of a Directory Service).

- A package is an application or data that can be installed on a target. You typically use Application Packager to create a package.
**Primary Components/Features of CCM**

**Configuration Management CCM Components**

**What is Deployment Manager?**

– Web-application

– Used to create, modify and monitor “deployments”

– A deployment is set of commands that distribute and manage applications on servers.

– Why people want Deployment Manager:
  • To deploy critical patches quickly
  • To deploy time-critical packages
  • To monitor installation in real-time
What are Task Receipts?

- Audit trail of the change request/task in the Configuration Management world
- As part of executing the task, policy service and deployment service write out task receipts on the endpoint
- A Task Receipt contains:
  - Timestamp, **Change ID, Task ID**, Receipt Provider (e.g. “Policy Service”), Status (e.g. “1” indicating success)
- Scanner service collects task receipts which are subsequently deposited into the Configuration Discovery (CD) database.
- Task receipts can be queried via the Query Builder in Report Center.
- Report Center provides several out of the box reports.
  - List of targets associated with a change ID and/or task ID
  - List of tasks performed for a period of time
  - List of tasks performed on machine X for a period of time
  - List of top X machines with most failed tasks in that last Y days
  - List of top X machines with most tasks executed in the last Y days
What are Common Management Services (CMS)?

- Foundation element of the BMC CM console that allows other components of the BMC CM console, such as Report Center and Policy Manager, to run

- Acts as a gateway to interact with the BMC® Remedy AR System over a Web-services interface for all Configuration Management components

- Provides a shared Web-services client module required by both Policy Manager and Deployment Manager

- Provides seamless authentication support between BMC AR and CMS Web-applications
What is the Definitive Software Library?

- Repository of authorized and approved software
- Contains or provides a reference to the “golden image(s)"
- The DSL gives an IT professional the following advantages
  - Keeps track of software location
    - Configuration Management can automate this activity via Distribution Servers (transmitters)
  - Software you register in the DSL is linked with the normalized names to enable making “apples-to-apples” comparisons across the enterprise.

- Thus, IT always refers to an application as one canonical thing, whether IT is buying it, associating license contracts with it, packaging it, deploying it, discovering it or referring to its usage.
Normalizing Configuration Discovery Data

- BMC CM Configuration Discovery
  - BMC CM tables
  - BMC CM views
  - DB Connector

- BMC Remedy Action Request System
  - Atrium Configuration Management Database (CMDB)
  - Reconciliation Engine
    - Asset Management dataset
      - Asset Management application
      - Change Management application
      - Problem Management application
    - Incident Management application
      - Incident Management application
    - Service Level Management application
      - Service Level Management application

- Definitive Software Library (DSL)
Primary Components of CCM
Configuration Management Database (CMDB)

How does the CMDB fit in the equation?
– Normalized Configuration Discovery Data is transferred into the CMDB
Primary Components/Features of CCM

Seamless Authentication

What is Seamless Authentication?

- Transparently authenticate an AR user when launching the BMC Configuration Management console (and Web-apps) from AR applications so that users don’t have to type in their user name and password again.

- CMS provides a common security service
  - Static Web-service in CMS
  - Network security using SSL is required to secure user-credentials
  - Opaque security ticket generated based on User ID and Password
  - Security ticket contains User ID, Password, Timeout, Salt, Hashed MAC Code
  - The security ticket is encrypted and sent back to the AR server.
  - CMS uses the “Security Token” Tuner service to generate authenticators (security tickets).

- How is the Security Ticket used?
  - AR Server adds the Security Ticket to all out-going requests to the Configuration Management console.
  - Ticket is processed by one of the in-built authentication filters in CMS.
  - If the validation of the ticket succeeds, the user is automatically logged into CMS without having to go through a login screen.
  - If the validation fails for any reason, the user is prompted with usual CMS login screen.
What is Closed-loop Verification?

- **Policy Compliance**
  - Target-based (“Does Jamie have everything his policy says he should have?”)
  - Package-based (“Has everyone who is supposed to receive PowerPoint actually received it?”)
  - Target- and Package-based (“Did all of Engineering get Visio like they were supposed to?”)

- **Verification Tasks**
  - Manual
  - Automatic

- **Viewing Compliance Information in Real-Time**
Agenda

› UserWorld Change and Configuration Management (CCM) Sessions
› Brief BMC CCM Overview
› CCM Architecture
› Components/Features of BMC CCM Solution
› How Does It All Work?
› Documentation
› Q&A
How Does This All Work?

› **Architectural Diagram**

› **Closed-loop Verification**

› **Predefined Task Templates**
  – Create and Modify Policy with Closed-loop Verification
  – Deploy Package
  – Create and Modify Policy
  – Closed-loop Verification (automatic)
  – Execute Remote Command
  – Execute Remote Script
  – Verify Target Status

› **Key Configuration Areas**
  – Task Management
  – Configuration Management
How Does This All Work?

› Architectural Diagram
› **Closed-loop Verification**
› Predefined Task Templates
  – Create and Modify Policy with Closed-loop Verification
  – Deploy Package
  – Create and Modify Policy
  – Closed-loop Verification (automatic)
  – Execute Remote Command
  – Execute Remote Script
  – Verify Target Status
› **Key Configuration Areas**
  – Task Management
  – Configuration Management
Closed-loop Verification
Automatic Verification Task

› TMS can automatically kick-off a verification task when a previous task (such as “deploy software”) is closed.
Policy Manager leverages TMS Web-services and retrieves the following details about the verification task.

- Targets and packages URLs
- Desired compliance percentage (default is 100%)
- Window of time in hours (expiration timeout) by which Policy Manager should report back on compliance results (default is seven days)
  - Note: In the best practices templates, the expiration timeout is using the variable feature and not the Time Out feature that could be set up in a task template or a task group template.

A CMS “task” is then created with the Verification Task Details which runs on a schedule (default is once a day).

Policy Manager sends back a return code and work info either when the desired compliance level is reached or the next “task” invocation is past the timeout window.
Closed-loop Verification

Task Information

› Task Status is updated in the TMS task.
› Work Info data returned is added as a new work info record in the TMS Task.
› High level compliance information is sent back as well.
How Does This All Work?

› Architectural Diagram
› Closed-loop Verification
› Predefined Task Templates

- Create and Modify Policy with Closed-loop Verification
- Deploy Package
  - Create and Modify Policy
  - Closed-loop Verification (automatic)
  - Execute Remote Command
  - Execute Remote Script
  - Verify Target Status

› Key Configuration Areas
  - Task Management
  - Configuration Management
A change request is created from the Requester Console to deploy software to a target.
Create and Modify Policy with Closed-loop Verification

Adding Sources and Targets to a Task

› Source = Software Library Item (SLI)
› Target = Configuration Item (CI)
Policy Manager is invoked from within TMS using the “launch” button on the Task form.
Clicking on the “launch” button on the Task form invokes the following CMS URL:


where:
- `<cms_host>` is the host name of the machine hosting CMS.
- `<cms_port>` is the CMS HTTP(S) listener port.

Change ID and Task ID are passed in as URL parameters.

Policy Manager makes a Web-service call back into TMS and retrieves:
- Package URLs and Desired States
- Targets
  - Supported Machine Target Types: LDAP DN, CN, DNS name (retrieved from the CMDB)
  - Additional task details

A new policy is created if one doesn’t exist for the targets using these packages.

Otherwise, packages get added to the existing policy for the targets.

User is then directly taken to the “Edit Policy” page where s/he can see the policy already pre-populated with the target and package information in context of the change request.

- If one of the packages is a Patch Group, then you can see it listed under the “Patches” tab.
Change ID and Task ID are maintained within Policy Manager.
In the “Edit Policy” page you can modify additional attributes.
- Policy Service Schedule
- Reboot Settings

Preview

Save
- Policy is saved (committed) into LDAP.
  - Change ID and Task ID are saved as part of the policy.

Once the policy is saved, the user is directed back to the Task form in TMS.
Create and Modify Policy with Closed-loop Verification

Task Information

› Task Status is updated in the TMS task.
› Work Info data returned is added as a new work info record in the TMS Task.
› Work Info contains both old and new policy information.
How Does This All Work?

› Architectural Diagram
› Closed-loop Verification
› Predefined Task Templates
  - Create and Modify Policy with Closed-loop Verification
  - **Deploy Package**
    - Create and Modify Policy
    - Closed-loop Verification (automatic)
    - Execute Remote Command
    - Execute Remote Script
    - Verify Target Status
› Key Configuration Areas
  - Task Management
  - Configuration Management
A change request is created from the Requester Console to deploy software to a target.
Deployment Manager is invoked from within TMS using the “launch” button on the Task form.

Clicking on the “launch” button invokes the following DM URL:
http://<dm_host>:<dm_port>/ars/deployment.html?changeid=<ChangeID>&taskid=<TaskID&doredirect=1
-  `<dm_host>` is the host name of the machine hosting DM.
-  `<dm_port>` is the DM HTTP(S) listener port.

Change ID and Task ID are passed in as URL parameters.

Deployment Manager makes a Web-service call back into TMS and retrieves:
- Package URLs and Desired States
- Targets
  - Supported Machine Target Types: DNS name (retrieved from CMDB)
  - Additional task details

A new deployment is created.

User is taken to the Control and Monitoring page containing the deployment created for the corresponding Change ID and Task ID.
Change ID and Task ID are maintained within Deployment Manager.
Deployment Manager (DM) interfaces with the Transmitter to determine the channel types of the packages associated with the TMS task.
- Transmitter exposes channel types in the XML Listing.

DM hands off the job to the Deployment Service running on the endpoint Tuner.

Once the job is complete, DM gets notified with the results.

DM maintains the task context during this entire period and notifies TMS.
- Task Status is updated in the TMS task.
- Work Info data returned is added as a new work info record in the TMS Task.
How Does This All Work?

› Architectural Diagram
› Closed-loop Verification
› Predefined Task Templates
  – Create and Modify Policy with Closed-loop Verification
  – Deploy Package
  – Create and Modify Policy
  – Closed-loop Verification (automatic)
  – Execute Remote Command
  – Execute Remote Script
  – Verify Target Status
› Key Configuration Areas
  – Task Management
  – Configuration Management
How Does This All Work?
Configuring Task Management System for CCM

› Configure BMC® Remedy® Mid-Tier

› Creating User Accounts
  – Create People Entry for CMS AR System User (CMSUSER)
    • Keep the AR System User Name as CMSUSER, but change the password.
    • Change User permission.
    • License Type of AR Fixed
    • Account used by outbound and inbound Web services communication between the integration components
      • **Important:** This user is also configured in the AR Settings page of the BMC CMS and an equivalent account must exist in the CMS User Directory such as LDAP.

› Activating the Integration
  – Update CMS & DMS Host and Port via Administrator Configuration Console.
  – Indicate whether SSL will be used.

› Post-installation Tasks
  – Update CMS Host and Port references in the 2 XML files for Web Services Filters.
  – Import each xml file (filter) using BMC Remedy Administrator.
CMS Integration Tasks

- Set the AR System User (CMSUSER) to be a Primary Administrator.
- Set the Change Management Users to be at least an Administrator.
- Set AR mid-tier and server settings to enable CMS to communicate with AR via web-services.
- Make sure the Mid-Tier is reachable.
  - Default Mid-Tier port is 80
- The user account must have the correct permissions to access the AR System Change Management application and the Definitive Software Library (DSL).
- **Important:** This should be the AR System CMS User (CMSUSER) with the appropriate password.
Change and Configuration Management (CCM)

REQUEST
- Service Catalog
- Event Funnel Filtering
- Classification
- Assignment Notification

VERIFY
- Verify State
- Verify Configuration
- Track Drift
- 3rd Party Solutions

CCM CORE
- Network
- Configuration
- Topology
- CCM Reconciliation
- CCM Extensions
- Dashboards
- Flowcharts
- Reports

PLAN
- Prioritization
- Create Tasks
- Ordering
- Resource Management
- Implementation
- Preparation
- Analysis
- Testing
- Risk Analysis
- Approvals
- Activate Policy

IMPLEMENT
- Provision User
- Provision Resource
- Deploy SW
- Deploy Code
- Deploy Patch
- 3rd Party Solutions

I.T. INFRASTRUCTURE
Useful Documentation

› **Configuring CCM References**
  - BMC Remedy Task Management System v7.0 Administrator’s Guide
    • Appendix A
    • Appendix B
  - BMC Configuration Management Policy Management v7.0 Administrator’s Guide
  - BMC Configuration Management Server Management v7.0 Administrator’s Guide

› **General Supporting References**
  - BMC® Remedy® Change Management v7.0 User’s Guide
  - BMC Definitive Software Library v7.0 Administrator’s Guide
  - BMC Configuration Management Configuration Discovery Integration for CMDB 7.0 Implementation Guide
  - BMC® Remedy® v7.0 - What’s New in Release v7.0
  - BMC® Atrium CMDB v2.0 Concepts and Best Practices Guide
  - BMC® Atrium CMDB v2.0 User’s Guide
Questions?