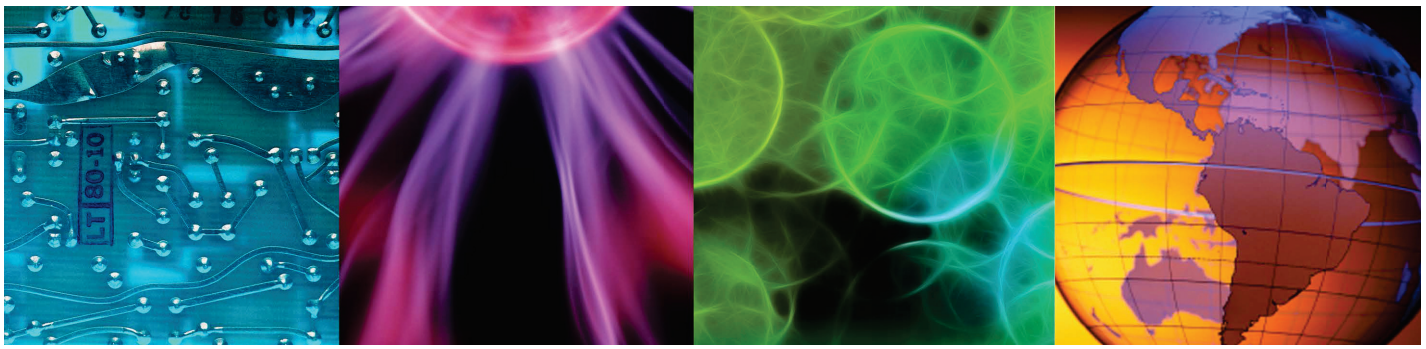
IBM Training

IBM SmartCloud Control Desk 7.5 Configuration, Change, and Release Management

Student Notebook

Course code TP370 ERC 1.0

June 2013



Cloud & Smarter Infrastructure

ibm.com/training

Authorized IBM Training

Contents

About this course

This 3-day instructor led course introduces students to the core functions for configuration, change, and release management in IBM SmartCloud Control Desk 7.5. Through lectures and extensive hands-on exercises, attendees will learn how use IBM SmartCloud Control Desk 7.5 to manage configuration item configurations throughout their lifecycle, and request, plan, implement, and verify changes to these configurations. In addition, students will experience how the IBM SmartCloud Control Desk 7.5 release management functions can be used to control, and perform mass deployment of new software releases to multiple target systems in a controlled fashion.

IBM SmartCloud Control Desk is a tool that provides comprehensive functions to support the management of the following resources:

- Service catalog and services requests (IT and non-IT)
- Incidents and problems
- IT Assets and software licenses
- Configurations, changes and releases

Highlights

- Introductory training for configuration, change, and release mangers and administrators.
- CI lifecycle management and audit.
- End-to-end change processing with impact analysis.
- Control mass deployment of critical software components.
- Extensive hands-on exercises

This course focuses on the configuration, change, and release management features, and teaches the fundamental skills to use the functions, understand how they work, and are integrated with one another.

Throughout the course, you will practice your knowledge through extensive hands-on exercises that emphasizes the skills taught in the lectures.

The lab environment for this course uses the Microsoft Windows Server 2003 platform.

For information about other related Tivoli courses, visit the Tivoli Education Training Paths website:

ibm.com/software/tivoli/education/paths/

	Details
Delivery method	Classroom or instructor-led online (ILO).
Course level	ERC 1.0
	This course is a new course.
Product and version	IBM SmartCloud Control Desk 7.5
Duration	3 days
Skill level	Basic

About the student

This course is designed for resource managers and administrators who need to understand how the various features of IBM SmartCloud Control Desk 7.5 work in order build the fundamental skills necessary to use them, and prepare for more advanced courses in administration and configuration of each of the functional areas. Before taking this course, make sure that you have the following skills:

- A good understanding of the ITIL processes for configuration, change, and release management.
- Familiarity with the core functionality of IBM SmartCloud Control Desk 7.5 and Tivoli's process automation engine similar to the topics taught in the IBM SmartCloud Control Desk 7.5 Foundations course (TP350G).

Learning objectives

Objectives

Upon completion of this course you will be able to:

- Describe the purpose and business value of IBM SmartCloud Control Desk configuration, change, and release management features.
- Explain the basic functions for configuration management including creating, updating, and auditing configuration items.
- Discuss Change Management processes and procedures used to control changes to the IT infrastructure, including change requests, and change specification, impact analysis and assessment, scheduling, authorization, implementation, and review.
- Understand how to manage complex changes and software roll-outs through the Release Management module.

1-2

Course agenda

The following outline is a high-level description of the contents of this course. Each unit has an overview presentation, and most have a series of student exercises designed to reinforce the concepts presented. The course contains the following units:

The course contains the following chapters:

1. Introduction to IBM SmartCloud Control Desk 7.5 configuration, change, and release management

   This chapter provides an overview of the functionality and business value of the IBM SmartCloud Control Desk CI update configuration, change and release management features.

   There are no exercises associated with this chapter.

2. Organization of configuration item information

   Understanding the way configuration item information is organized is key to understanding how and why the various features of IBM SmartCloud Control Desk configuration and change management work. This chapter introduces the data layer, and provides a quick overview of the main concepts of relating different representations of the same resource to one another.

   There are no exercises associated with this chapter.

3. Configuration management with IBM SmartCloud Control Desk 7.5

   Configuration management is the core discipline of service management. This discipline is responsible for ensuring the trustworthiness of the data that are the foundation for the change and release management processes. This chapter introduces the configuration management discipline, and processes, and teaches you how to effectively manage your configuration items.

   The exercises for this chapter takes you through the various ways to create and maintain configuration item configurations, assign lifecycle states, perform promotion and synchronization, and work with configuration topologies.

4. Configuration auditing

   This chapter introduces configuration auditing, a critical component of configuration management, which provides the basic functions for verifying changes and identifying unauthorized changes.

   In the exercises for this chapter you define and perform a CI audit to confirm that the actual configurations of your CIs are consistent with your expectations as they are defined in the authorized CI configurations.

5. Change management with IBM SmartCloud Control Desk 7.5

This chapter introduces you to the basics of change management, and takes you through the phases of the three main change processing models supported by IBM SmartCloud Control Desk.

The exercises for this chapter introduce change processing step-by-step. First you will work with an emergency change to learn the basic concepts of change processing. Then you will create, classify, assess, schedule, authorize, implement, and verify a normal change and focus on advanced change topics such as assessments, impact analysis, scheduling, and verification.

6. Release management with IBM SmartCloud Control Desk 7.5

   This chapter focuses on how the release management features in IBM SmartCloud Control Desk can help you manage the implementation complex changes, such as composite changes that need to be coordinated across a number of CIs, or mass roll-out of software updates. These types of changes are commonly referred to as releases.

   The exercises related to this chapter focus on the mass distribution of a middleware fixpack. Using the release management capabilities in IM SmartCloud Control Desk 7.5 you will experience how to define Definitive Media Libraries, create, design, develop, test, plan, approve, and implement a release, and associate changes with a specific release.

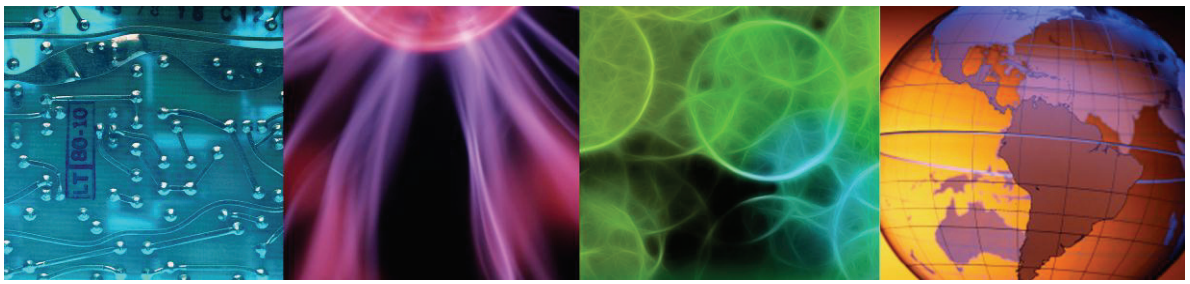
7. IBM SmartCloud Control Desk 7.5 summary

   This chapter summarizes the benefits of using IBM SmartCloud Control Desk to establish a CMDB, and manage your configurations, changes, and releases using its advanced facilities.

   There are no exercises for this topic.

1 Introduction to IBM SmartCloud Control Desk 7.5 configuration, change, and release management

Introduction to IBM SmartCloud Control Desk 7.5 Configuration, Change, and Release Management



What this chapter is about

This chapter provides an overview of the functionality and business value of the IBM SmartCloud Control Desk CI update configuration, change and release management features.

Objectives

- After you complete this unit, you will be able to:
- Articulate the main purposes of the configuration, change, and release management disciplines.
- Distinguish the responsibilities between the configuration, change, and release management teams.
- Discuss the main features of IBM SmartCloud Control Desk that support configuration, change, and release management.
- Describe the interactions between the three management disciplines.

Objectives

The purpose of IBM SmartCloud Control Desk

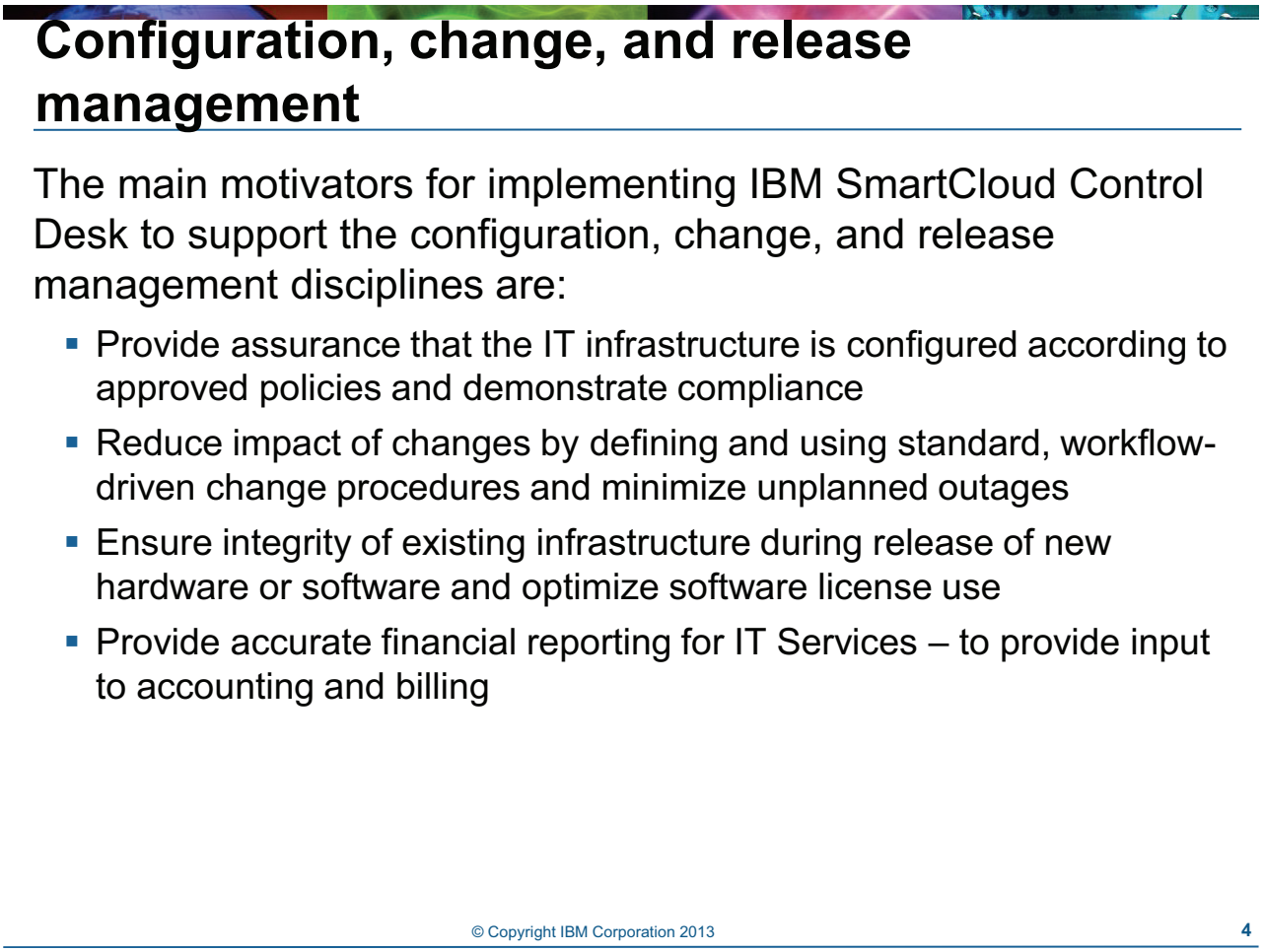
- IBM SmartCloud Control Desk is a comprehensive IT Service Management solution that helps **reduce cost** and **minimize service disruptions** through automated service request handling, efficient change management, optimized asset lifecycle management across IT and enterprise domains
- IBM SmartCloud Control Desk is a **planning tool** that maintains the Configuration Management Database (CMDB)
- IBM SmartCloud Control Desk does not interact directly with your IT resources – however, configuration and status information may be imported from OMPs through the Maximo Enterprise Adapters or IBM Tivoli Integration Composer (ITIC)

The purpose of IBM SmartCloud Control Desk

The capabilities in IBM SmartCloud Control Desk for Configuration, Change, and Release management allows your organization to verify that the actual configurations of the resources within your IT infrastructure are well documented and in compliance with your policies. Once you have established a trustworthy CMDB, you can leverage this information to control changes to the infrastructure, and using ITIL based processes, you can plan, assess, schedule, and authorize the change. Once a change has been properly authorized, it is implemented, and you can verify that the intended modifications have been applied to the infrastructure resources. Using these processes will help minimize disruptions to your operation, and thereby reduce costs and improve your service delivery.

The main purpose IBM SmartCloud Control Desk is to provide a platform in which you can implement standard processes, and controls. As a starting point, IBM SmartCloud Control Desk delivers template process workflows that are ITIL compliant, which can be tailored to meet the particular needs of your organization

The information used to manage configuration items in IBM SmartCloud Control Desk is typically gathered by the IBM Tivoli Application Dependency Discovery Manager product, and is uploaded to IBM SmartCloud Control Desk using the IBM Tivoli Integration Composer tool.



Configuration, change, and release management

The main purpose of configuration management is to ensure that the information that is stored in the configuration management database (CMDB) is consistent and compliant with your organizations policies and guidelines.

Maintaining a trustworthy CMDB is crucial because most of your operational and planning tasks rely on this information, and will most likely fail if the information in the CMDB is incorrect. The CMDB contains information that most likely is used by everyone in the IT Organization in order to perform tasks such as service provisioning, software deployment, incident management, problem determination, change and release planning and scheduling, as well as accounting and service delivery.

Once the information, on which you base your processes, is correct, and you apply (and adhere to) stringent processes for assessing, scheduling, and authorizing changes, you will most likely experience that the number of unplanned outages will fall, and that your service delivery will improve. By basing your decision making on solid information, you eliminate a most (if not all) of the guesswork which normally is involved in managing complex IT infrastructures. Using the information in the CMDB you can understand dependencies between resources, determine which

resources will be impacted by a change, and verify that the implementation of a change has been performed in accordance with the plan.

In addition to supporting the management of changes to the infrastructure, the information in the CMDB is also used to manage software licenses, perform analytics, for example look at how the available capacity is used, and perform financial reporting to support accounting and billing.

Main capabilities

IBM SmartCloud Service Desk provides capabilities that will enable your organization to:

- Manage and audit the IT configurations in your environment in order to verify compliance with your policies and identify discrepancies.
- Request, plan, analyze, schedule, authorize, implement, and verify changes to your IT environment in a controlled manner in order to minimize outages caused by changes, and implement changes in accordance with business priorities.
- Plan, test, and deploy releases in a controlled way in order to synchronize and control the implementation of multiple changes to a single resource, or changes to multiple resources.
- Manage IT service assets to provide accurate reporting of financial, organizational, and logistical information.

Main capabilities

Many organizations can attest to the fact that most outages are the un-welcomed result of unplanned changes. For that reason, the industry has seen an increased focus on properly planning and assessing changes prior to implementation over the last few years. One reason that this focus has not happened earlier, is the increased complexity of the IT Infrastructures that is the result of the increased adoption of server consolidation techniques, virtualization, and cloud delivery models. As more and more resources are virtualized, more layers of management are introduced, and combined with the dynamics provided in cloud-based delivery models, it is not humanly possible to keep track of your configurations. In order to understand how your infrastructure is composed, you need tooling that can discover all the configurations and relationships, and maintain the information in a central CMDB which then can be used as the basis for analysis and decision making.

One such analysis is configuration item auditing. This is one of the most important tasks in configuration management. The audit allows you to identify configuration items that are not configured the way you think. Auditing CIs allow you to verify compliance with the policies applied

by your organization, and helps you to raise the awareness of the resource owners about the inconsistencies, in order for the owners to decide which action to take to correct the issue.

Another type of analysis in which the CMDB plays a key role, is the assessment of the impact of a change. Using the known relationships between resources, you can determine if the planned outage of a resource (to perform an update) will affect other resources. By applying change windows to any resource you can specify when outages are accepted, and this enables you to schedule the change implementation for a point in time that causes the least amount of disturbance to your business.

Most organizations have well-defined periods (for example the second weekend every month) in which major changes, also known as releases, are rolled out. Planning which changes to include in which releases can be a cumbersome and complex task. By combining the (accurate) information about the how IT infrastructure components are currently configured and related with the planned changes, the release management team will have much better foundation for serializing and combining changes. This will lead to better utilization of the implementation resources, and perhaps even faster release implementation.

As resources are virtualized, and workloads are dynamically moved around in the infrastructure, accounting becomes a nightmare. Especially if your costing model is based on the amount of resources allocated to a workload at any given time. The CMDB that is maintained in IBM SmartCloud Control Desk will help you provide accurate financial reporting, by enabling you to view and report on past configurations. Using the history, you can determine how many resources were allocated to a specific business application at any point in time, and also help you analyze how configurations over time drift away from a baseline.

Key features and benefits

Feature	Benefit
CI auditing and remediation	▪ Immediately remediate an audit violation by: • Updating an authorized CI to reflect the Actual value • Create a Change or service request • Sending an email to the CI owner ▪ View approved changes for a CI when viewing an audit variance to help determine if there was an approved change that caused the variance ▪ View CI attribute history while viewing an audit variance ▪ View the last audit results for the same CI.
Compliance policy enforcement	▪ Track and record changes across the organization ▪ Manage desired states of resource configurations to validate compliance with internal and external policies
Calendaring capability	▪ Schedule Changes to minimize impact – change windows, resource scheduling can help identify exposures to planned changes, thus protecting critical business services
Blackout period identification	▪ Blackout periods identify critical business periods when outages would be expensive. Automated Change scheduling can help avoid blackout periods
Change and Release authorization	▪ Prevent unauthorized changes by verifying authorization access based on views
Impact Analysis	▪ Complete technical and business impact analysis capabilities. Based on thorough relationships, analysis can be performed to spot direct relationship impact as well as associated impacts to prevent unacceptable outages due to changes.
Deployment of approved images	▪ Save on support costs by deploying approved images from the Definitive Media Library. ▪ Supports a number of media libraries, and integrates with IBM Rational Asset Manager

Key features and benefits

The key benefits provided by IBM SmartCloud Control Desk are related to increasing the quality in the delivery of IT services.

By applying ITIL aligned processes, and improving the quality of the information on which decisions are made, errors and mistakes can be avoided, and change implementation processes can tracked and be optimized.

ITIL definitions

Term	Definition	Example
Configuration Item	Any Component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the configuration management system and is maintained throughout its lifecycle by configuration management.	▪ A Computer System ▪ A Db2 Instance Configuration Value ▪ A business application
Configuration	A generic term, used to describe a ***group of configuration items*** that work together to deliver an IT Service, or a recognizable part of an IT Service. Configuration is also used to describe the ***parameter settings*** for one or more configuration items.	▪ Specification attributes that describe the identify, relationships, and operational characteristics of a resource ▪ A group of related configuration items
Change	The addition, modification or removal of anything that could have an effect on IT Services. The scope should include all IT services, configuration items, processes, documentation etc.	▪ Addition of an additional node to an application cluster ▪ Deployment of a virtual system ▪ Replacement/upgrade of hard- or software
Release	A collection of hardware, software, documentation, processes or other components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, tested, and deployed as a single entity.	▪ Deployment of Application System across multiple platforms ▪ Mass deployment of software, for example update of antivirus signatures
Asset	Any Resource or Capability. Assets of an IT Service Provider include anything that could contribute to the delivery of a Service. Assets can be one of the following types: Management, organization, process, knowledge, people, ***information, applications, infrastructure***, and financial capital.	▪ A Router ▪ A business application

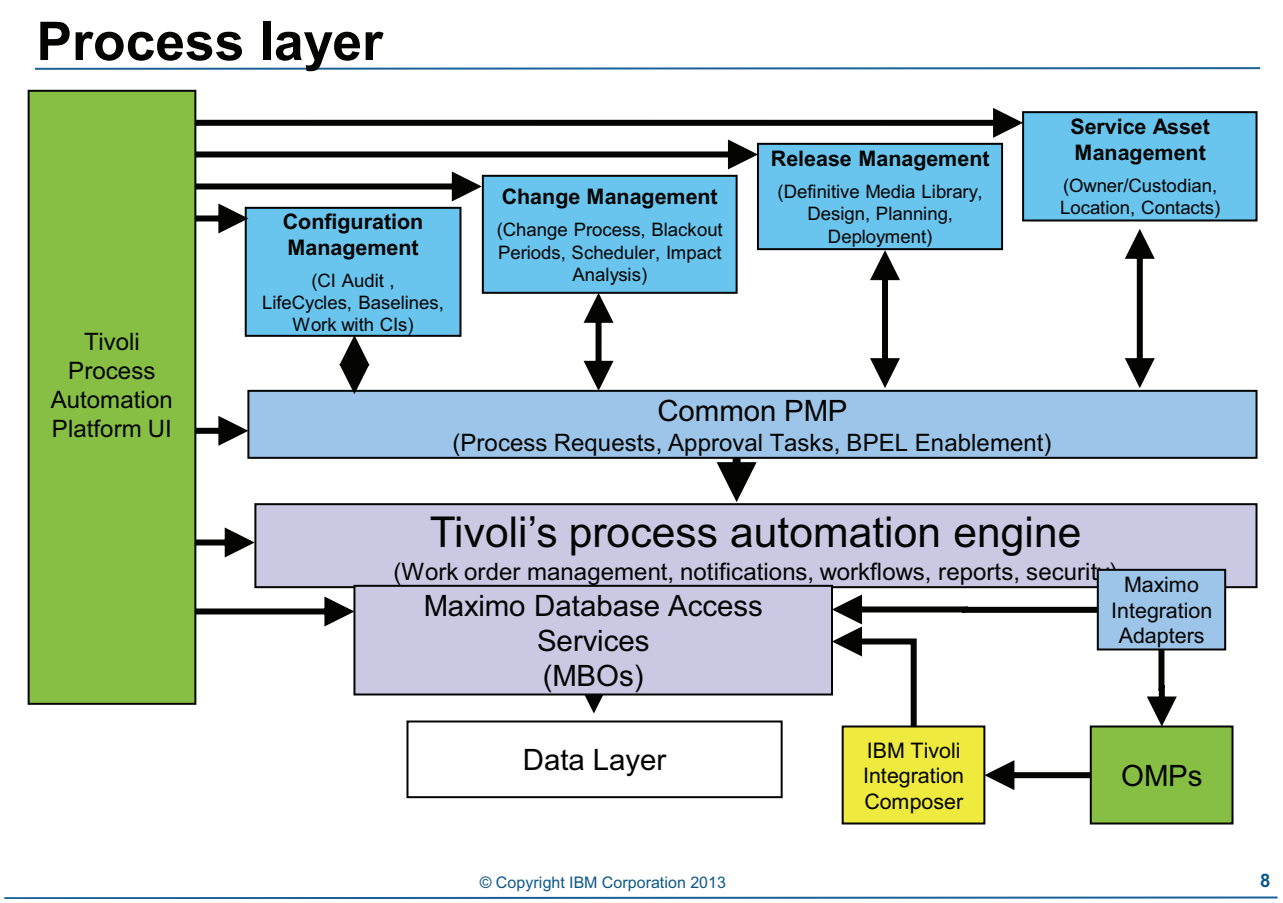
 7

ITIL definitions

When discussing configuration, change, and release management, these terms are used with a very specific meaning.

The key terms are:

- Configuration Item
- Configuration
- Change
- Release
- Asset



Process layer

In IBM SmartCloud Control Desk, the processes for change, configuration, and release management are implemented in the process layer.

The process layer:

- Provides a set of roles, interfaces, job plans, and workflows. These enable a defined set of inputs and outputs for the configuration, change, and release processes.
- Is expected to be tailored to match the outcome that is expected in a particular implementation
- Leverages the capabilities of the Tivoli's process automation engine (Tpae).

OMP is an Operation Management Product or MSS. These products are outside of the IBM SmartCloud Control Desk product.

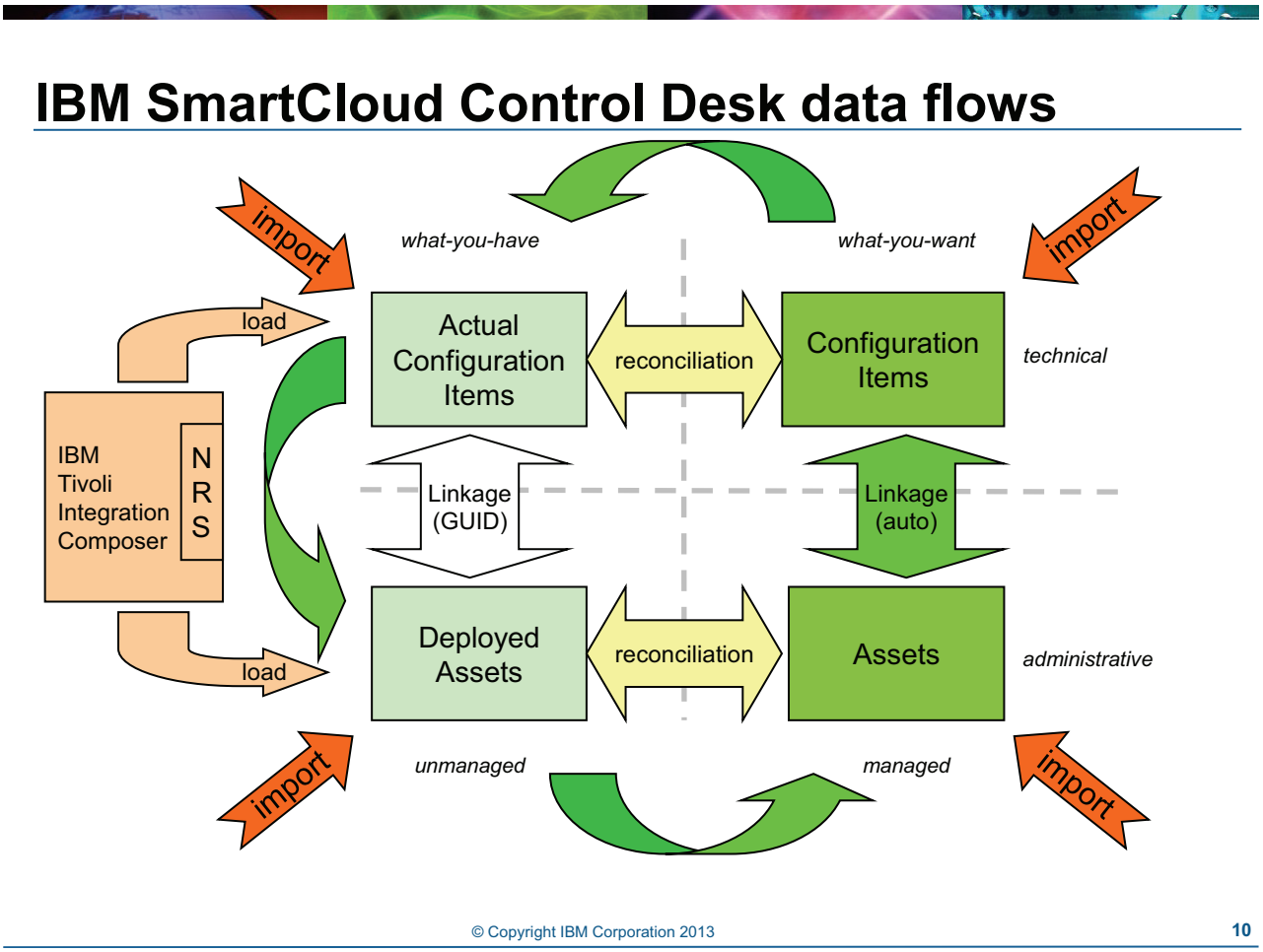
The data layer is normally populated from OMPs, which deliver configuration and relationship information to the CMDB. Optionally, operational state data can be dynamically linked to IBM SmartCloud Control Desk because the current operational state of a resource is not of interest when managing configurations, changes, and releases.

Processes

Discipline	Description
Configuration Management	The purpose of the configuration management process is to maintain the integrity of the configuration item (CI) employed in, or related to, IT systems and infrastructure, and to provide accurate information about CIs and their relationships.
Change Management	The purpose of the Change Management process is to achieve the successful introduction of changes to an IT system or environment. Success is measured as a balance of the timeliness and completeness of change implementation, the cost of implementation, and the minimization of disruption caused in the target system or environment. The process also ensures that appropriate details of changes to IT resources (assets, CIs) are recorded. Basically, a change is anything that alters the status of a configuration item (CI). This typically includes anything that adds to, deletes from, or modifies the IT environment. The definition of a change is the addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.
Release Management	The purpose of the Release Management process is to prepare and finalize release packages that are fit for deployment so that optimal business value will be attained when deployment occurs.

Processes

The IBM SmartCloud Control Desk facilities for configuration, change and release management are specifically built to support these ITIL processes.



IBM SmartCloud Control Desk Data flows

If you take full advantage of all the capabilities in IBM SmartCloud Control Desk, you will have both asset and CI records for most hardware and software resources.

The asset information contains administrative, financial, and organizational details such as owner, location, lifecycle status, related contracts, warranty information, accounting information and so on.

The Configuration Item information contains the technical details such as configuration item attributes, and relationships

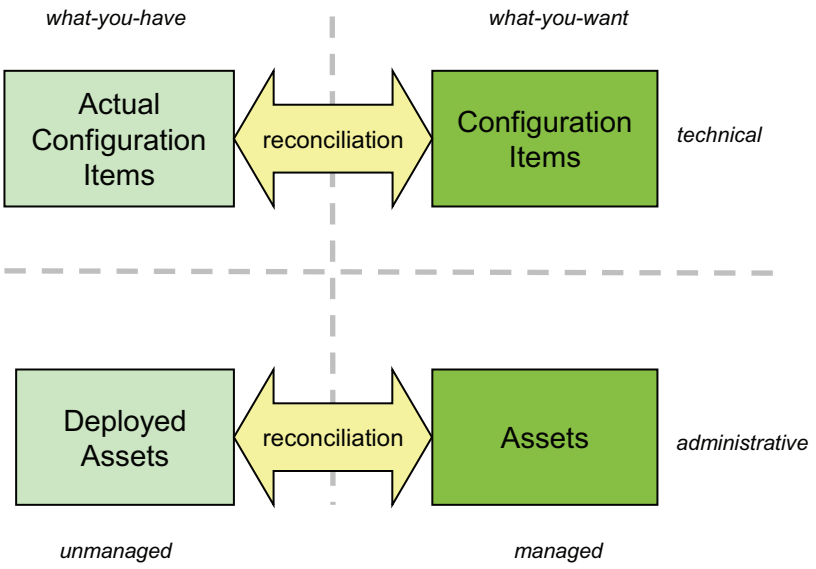
IBM SmartCloud Control Desk maintains two sets of data for both assets and CIs.

"What-you-have":Actual CIs and Deployed assets represent the current implementation of the resources. Sometimes this information is also referred to as actual, or unmanaged CIs and Assets. This information is typically loaded into the CMDB through the IBM Tivoli Integration Composer (ITIC) tool.

"What –you-want"CIs and Assets represent the planned implementation. Sometimes, this information is referred to as authorized, or managed CIs and Assets.

As changes are planned, the information in the “what-you-want” sets of data are updated. Once the changes have been implemented, the information in the “what-you-have” data should be refreshed from ITIC.

Data flows: reconciliation



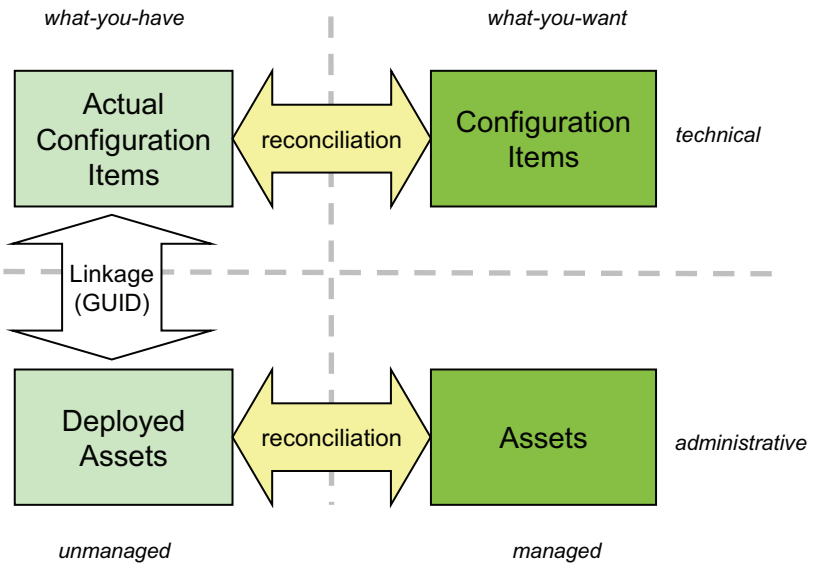
Data flows: reconciliation

Reconciliation is the term used to describe the process of comparing specific records in the authorized (managed) set to specific records in actual (unmanaged) set, and optionally synchronize the information automatically or create notifications that highlight the differences.

The purpose of reconciliation is to match-up actual (unmanaged) and authorized (managed) information for a specific resource so the two sets of data can be analyzed to find discrepancies. This is the core function of the Configuration Audit process

Commonly, you will not manage all the actual (unmanaged) CIs, so many actual (unmanaged) CIs will not have authorized (managed) siblings. For that reason, reconciliation is performed from the authorized (managed) side. However, once the two sets information for a single resource are reconciled, both sets contain references to the sibling.

Data flows: actual linkage

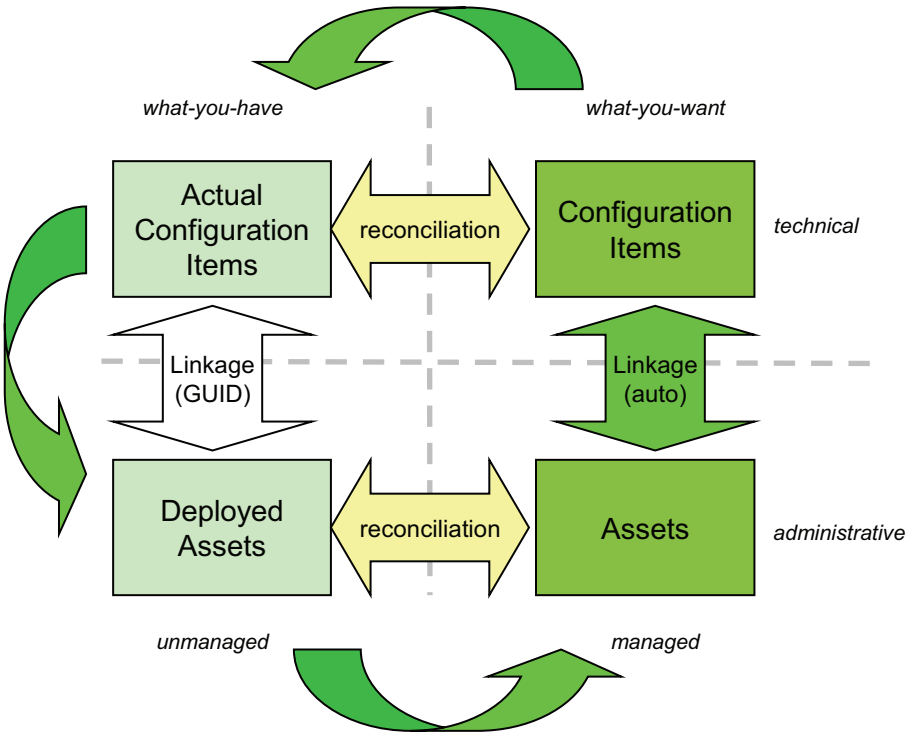


Data flows: actual linkage

The term linkage is used to link the CI information to asset information, so you have easy access to administrative information when you work with CIs, and access to the technical details when looking at assets.

The linkage is performed automatically by IBM SmartCloud Control Desk by comparing the Globally Unique Identifier (GUID) which is assigned to any resource that is imported through ITIC. ITIC looks at the naming rule attributes for the specific resource types, and uses this information to generate a GUID. Since the same naming attributes are used for corresponding resource types (ComputerSystem assets and ComputerSystem CIs) the GUIDs will be identical. When linking actual CIs and deployed assets, IBM SmartCloud Control Desk simply uses the GUID to create the link.

Data flows: authorized linkage



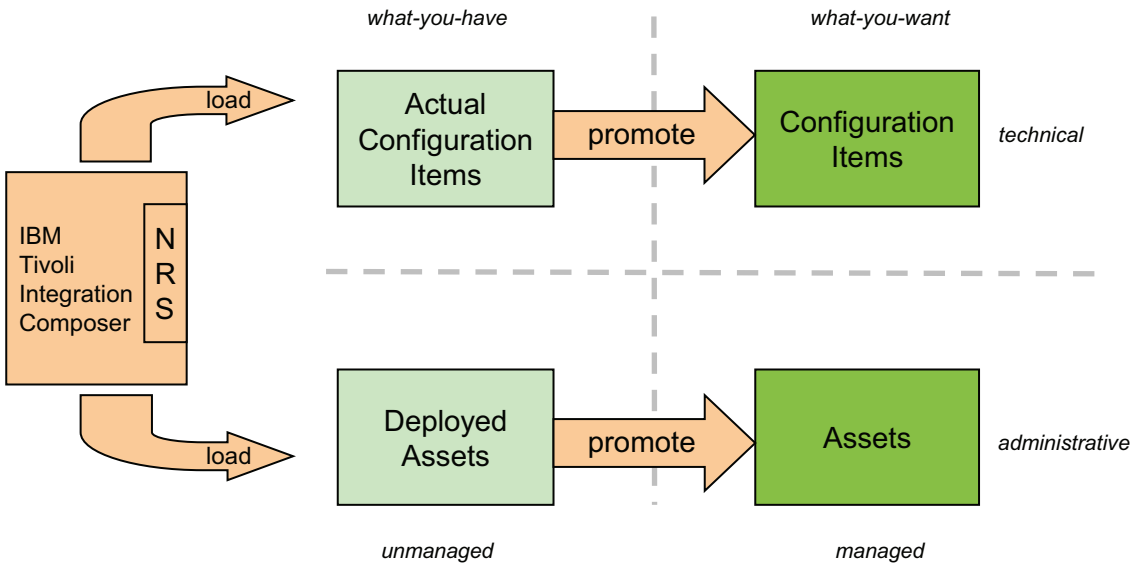
Data flows: authorized linkage

To close the loop the authorized (managed) information for specific asset/CI pairs must be linked. This is achieved in one of two ways by a background task in IBM SmartCloud Control Desk.

1. The task analyzes an authorized (managed) CI to find the actual (unmanaged) sibling. Then the linked asset is identified from the GUID, and finally the related authorized (managed) asset is located, and the link between the authorized (managed) CI and asset can be created.
2. The task inspects the authorized (managed) assets, and uses specific attributes to see if an authorized (managed) CI with the same key attributes exist. If one is found, the link is created.

The reason for having both types of linking is, that both authorized (managed) assets and CIs can be created before the actual (unmanaged) siblings are known to the system. During planning of, for example, the deployment of a new application system, assets may be created before they are purchased (to be included in budgeting) or when they are physically received. Similarly, new CIs can be created during planning of a change, before they are actually implemented. This implies that the link between the authorized (managed) siblings cannot be automatically established unless they share common attributes that can be used to identify matching pairs.

Data flows: loading, and promoting

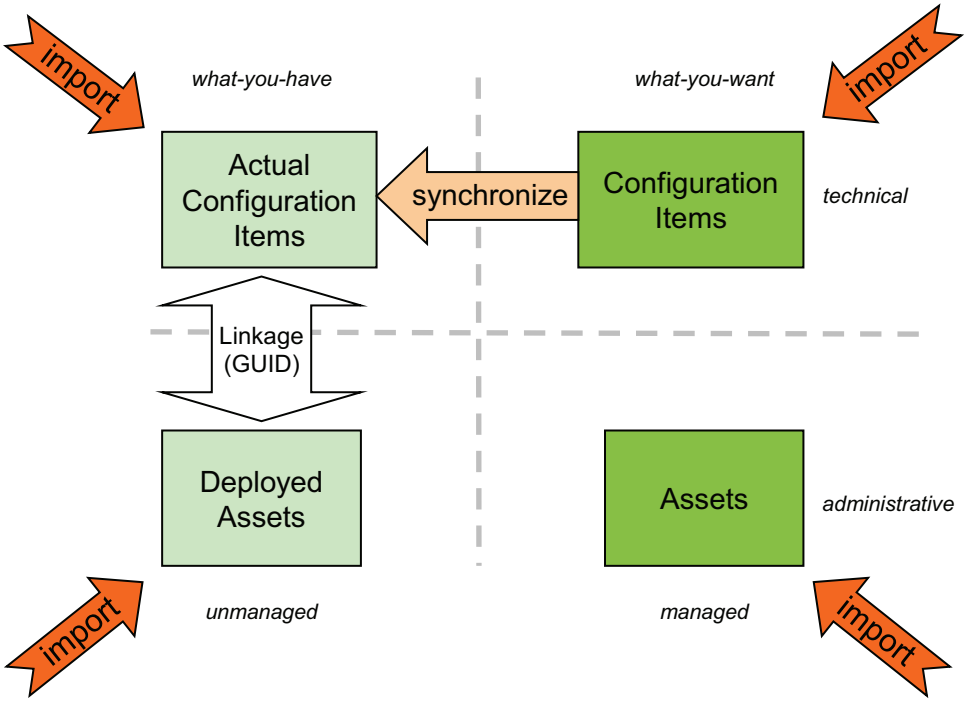


Data flows: loading and promoting

Typically actual (unmanaged) resources are loaded into the IBM SmartCloud Control Desk CMDB through the ITIC tool. ITIC can collect the actual information from a variety of sources, such as TADDM and IBM Tivoli Asset Discovery for Distributed (TAD/D). During the loading, the Naming and Reconciliation Services (NRS) component of ITIC inspects the naming rule attributes of the resources, and assigns a GUID to the CIs or assets that are created.

Once the actual (unmanaged) resources exist, they may be promoted in order to create the authorized (managed) resources.

Data flows: import



Data flows: import

You may also import any type of information from comma-separated or xml files. The main purpose of this feature is to enable you to import small sets of data, or augment existing resources with information that is not loaded through ITIC.

By default, IBM SmartCloud Control Desk does not allow you to update the actual (unmanaged) information. If you really have to, the export/import feature allows you to extract information about existing resources, update them manually, and import them back into the IBM SmartCloud Control Desk CMDB.

You should use this feature with caution, because the import does not generate a GUID, and therefore, the automated linkage of actual (unmanaged) resources will not work correctly.

In addition to the reconciliation tasks used to link authorized (managed) resources to actual (unmanaged) siblings, IBM SmartCloud Control Desk includes a facility that uses naming rules to link authorized CIs to actual CIs. This feature can be used from the user interface, and includes synchronization of all related CIs. You can say, that it operates like a reverse-promotion.

Configuration management

- Configuration management identifies, controls, and maintains all elements in the IT infrastructure called configuration items
- IBM SmartCloud Control Desk provides features to perform the following tasks:
  - Configuration item creation
  - Management of relationships between CIs
  - Configuration item lifecycle management
  - Configuration item baselining and drift analysis
  - Configuration item reconciliation and audit
  - Automated asset and configuration item linkage
  - Collection management

Configuration management

The main activities of the Configuration management discipline help you ensure that the information in the CMDB is accurate. This implies that it is the responsibility of the configuration management team to create, update, and audit the CIs. These activities include manipulating CI attributes, and relationships, as well as metadata such as lifecycle, linkage to assets, collection association, and managing baselines.

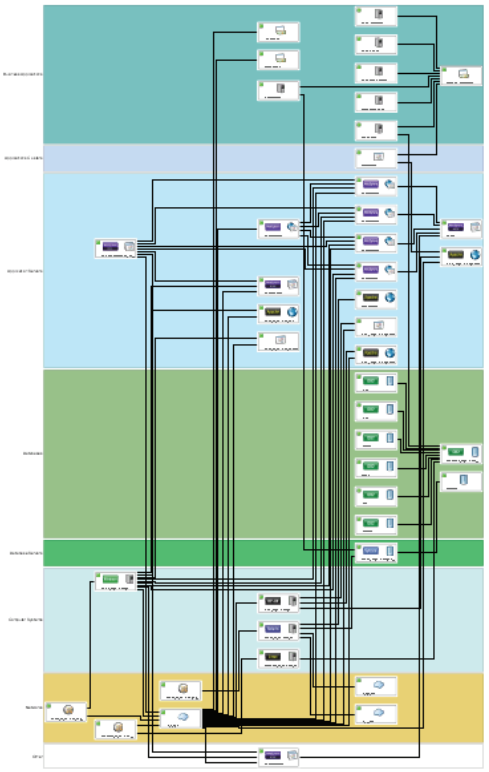
IBM SmartCloud Control Desk provides specific applications to manage different aspects of a CI configuration. These are all located in the IT Infrastructure application group.

To control system tasks for audit and linkage, the configuration management team uses the applications in the Reconciliation application group. These include facilities to define, maintain, and view results from reconciliation tasks.

Visualizes topologies

Helps Incident, Problem, Change and Release Management understand complex relationships for both Actual CIs and CIs.

- Business and Detail views
- Filtering, and search capabilities
- Shows status, planned changes, and impacts



Visualizes topologies

The topology viewer in IBM SmartCloud Control Desk enables you to view resource topologies to assist problem determination, or change impact analysis.

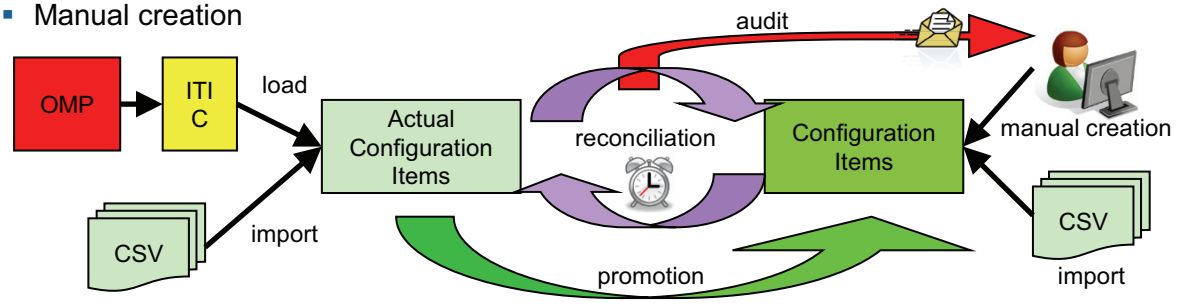
The topology viewer organizes different resource types in swim lanes. The swim lanes can be configured to group several related CI types, such as all databases, all application servers, or, for example, all z-related classification types.

The topology viewer has two views. The Business view shows only resources for which the classification specifically specifies that the resource type should be included in the view, and the Details view shows all resources.

The topology viewer provides filtering, search and zoom facilities to ease navigation, and hot-links to the resources in the view, allow you to quickly jump to any resource shown in the view.

Configuration item creation, reconciliation, and audit

- Configuration Items can be crated through:
  - Promotion of actual configuration items (includes related CIs)
  - Import from CSV files
  - Manual creation



- Reconciliation compares actual CIs to CIs and can invoke automated actions such as:
  - Linkage
  - Promotion
  - CI update
- Reconciliation tasks can be scheduled to automate the process
- Configuration Item auditing is performed by comparing attributes of actual CIs with the related attributes of the authorized CIs.

Key configuration management functions

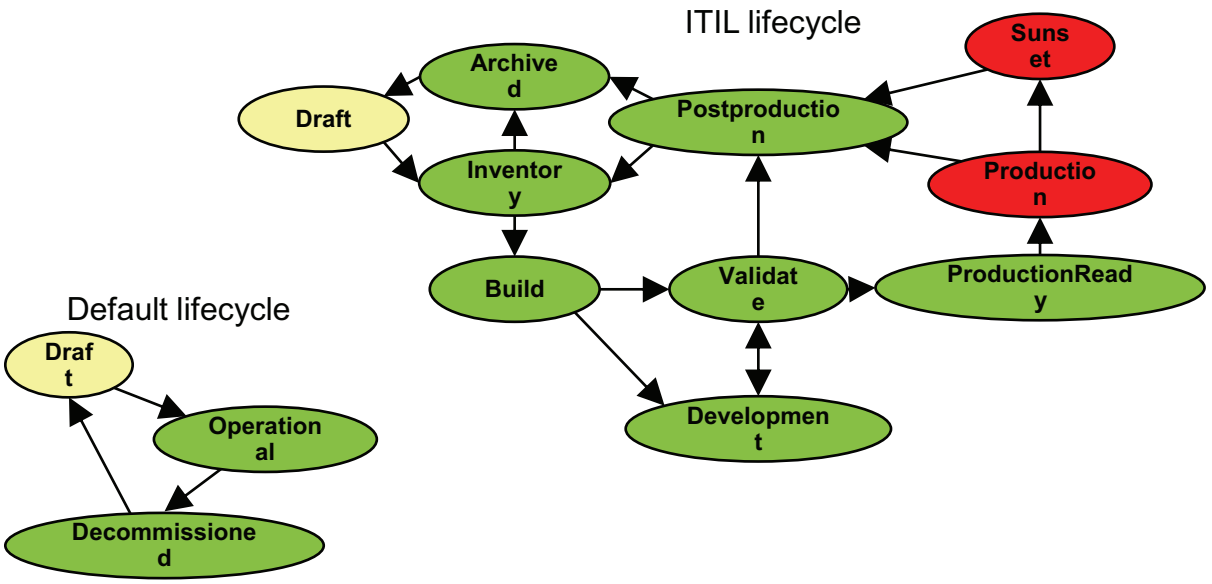
The main responsibility of the configuration management team is to manage the CI configurations and relationships, as well as the CI metadata. Examples of meta data are lifecycles and base lines.

Lifecycles contain well-defined states for which your organization applies specific meaning and processing. The processing includes valid transitions that define how you are allowed to move a CI from one lifecycle state to another. Some lifecycle states are defined as protected. If changes are planned against a CI that is in a protected lifecycle state, authorization is required to implement the change. CIs which support production workloads normally are in a protected lifecycle state.

Baselines can be used to capture configurations at any point in time. These are used as references that define how the included CIs were configured and related when the baseline was captured. At any point, you can compare the current configuration and relationships to the baseline to see how the CIs configurations have changed over time. This is also known as *drift*. This information is vital for example to verify that your planned disaster recovery environment is adequate to handle the load, or to verify that the information you use for billing is accurate.

Configuration item lifecycles

- Lifecycles determine the operational state of CIs and the valid transitions between them
- Protected lifecycle stages require changes to be authorized



Configuration item creation, reconciliation, and audit

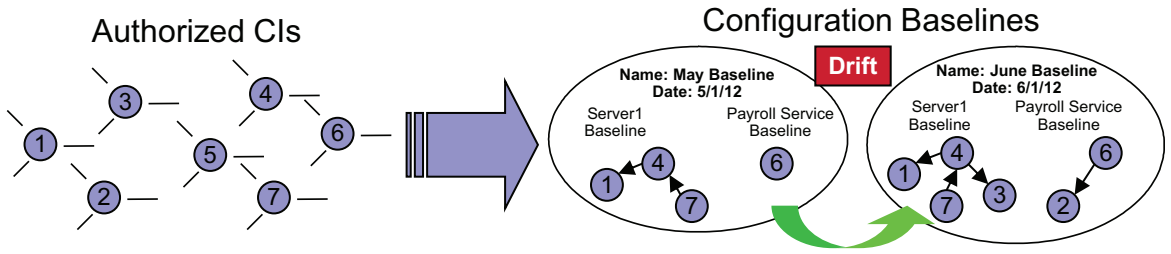
Configuration items can be created in several ways: manually, of through import. These are the typical ways new CIs, which have not yet manifested themselves physically, are created.

The most common way to create CIs is to promote actual CIs that have been loaded into the IBM SmartCloud Control Desk CMDB through ITIC.

Auditing compares the attributes and relationships of actual CIs to authorized CIs. When discrepancies are found, the change librarian is notified, so the proper action to resolve the issue can be initiated.

CI baselining

- Enables IT standardization by easily taking a snapshot, at any time, of CIs to produce an approved configuration.
- Ability to quickly detect changes to those approved configurations.



What is a Baseline:

"A configuration baseline is a snapshot that represents an approved configuration at a particular time that people can reference, compare to, and apply changes to in a manner that is understandable."

Configuration item lifecycles

Lifecycles are used to control the administrative state of a CI.

The lifecycle defines several valid states, some of which may be protected, and the allowed transitions from one state to another.

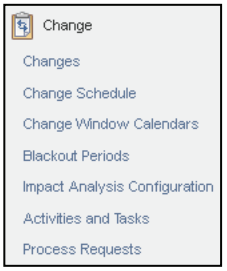
These states can be used to apply special processing for resources in a particular state. For example, events can be suppressed or escalated based on the lifecycle state, and work order priority may be assigned based on the state.

States may also be used to automate processing, for example the release of software licenses, when a resource moves from Production to Postproduction.

IBM SmartCloud Control Desk provides only one case of special processing based on lifecycle states. For states that are protected, IBM SmartCloud Control Desk enforces the requirement for authorization of changes before they can be implemented.

Change management

- Change management receives a change request and either approves or rejects it.
- IBM SmartCloud Control Desk provides features to perform:
  - Change acceptance and assignment
  - Change assessment
  - Change impact analysis
  - Scheduling
  - Authorization
  - Verification
  - Closure



- The change process can be automated, fully or in part, by adaptive workflows that use key attributes such as *classification*, *type*, and *priority* to determine which workflow to use.
- The change process describes the implementation tasks, but does not automatically interact with the target systems to implement changes.
- The change process can leverage configuration management to ensure that CIs are updated correctly and to verify the change implementation.

CI baselining

CI baselines allow you to capture the configuration and relationships of one or more authorized CIs at any point in time. Later you can compare the baseline to the current information if order to determine how the CIs and their relationships have changed.

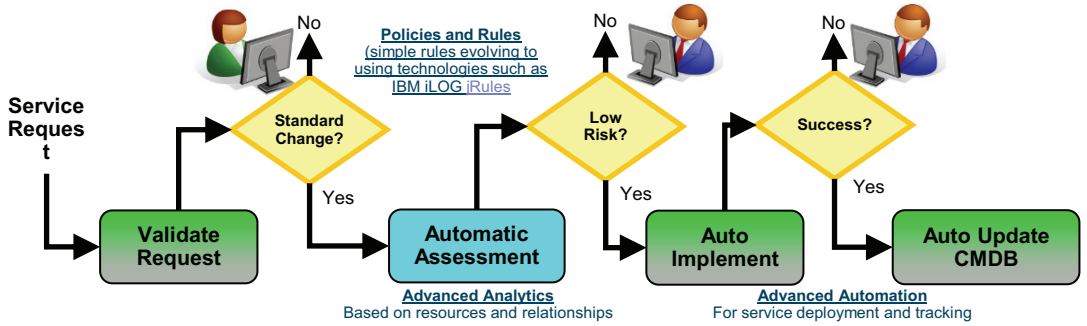
You can use this information to analyze how the group of CIs have drifted. This may prove useful for example to verify that your disaster recovery environment is adequate, if your basis for billing is up to date, if unwanted relationships have been introduced, or if dependencies have been obsoleted.

The baselining works in conjunction with the CI attribute and relationship history feature to allow you to track how your CIs change over time.

Automated and standardized change processing

- Change are processed in one or more phases

- IBM SmartCloud Control Desk provides capabilities to standardize and automate change processing to save on labor cost
- These functions allow change owners to focus on determining policies, managing risk, and reviewing and validating tool recommendations.
- Change processing standardization is implemented through response plans and job plans.
- Change processing and implementation of pre-approved (standard) changes can be fully automated by associating automation scripts with the implementation tasks.
- Workflows can be employed to govern the change processing, and can be instrumented to provide change processing similar to this example: “Standard / pre-authorized changes” - can be fully automated, with full change records – as long as the conditions are met. Else, queued for human assessment / review / scheduling / approval / implementation / corrective action.



24

Change management

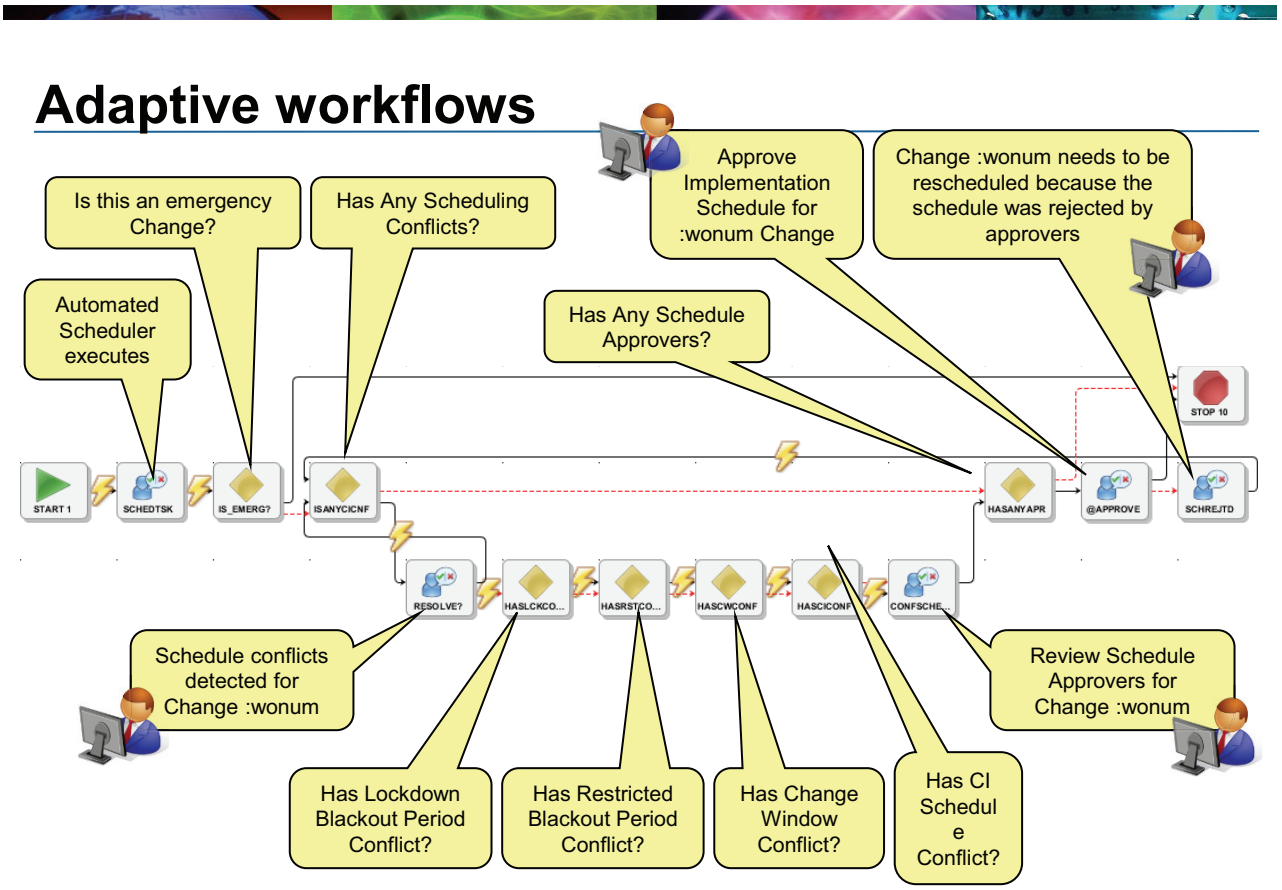
In the Change application group, the change management team can find all the application links they need to perform the tasks for which they are responsible.

These tasks include acceptance and assignments of RFCs, change assessment, impact analysis, scheduling, authorization, implementation, verification, and closure.

For trivial changes, such as password changes, or deployment and decommissioning of test systems, the change processing can be automated through workflows or automated job plans.

A job plan can be thought of as a template that defines a standard set of tasks that must be performed in order to implement a specific type of change.

Response plans may be developed to standardize the change definitions based on specific RFC attributes such as classification, type or priority. Response plans are basically change templates, which may include references to standard job plans, as well as standard assessment, and authorization requirements.

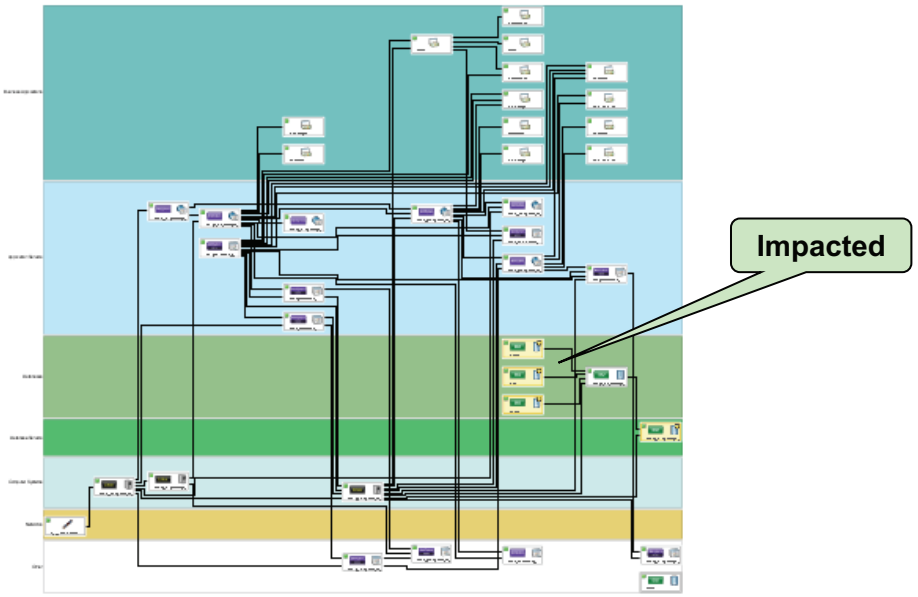


Automated and standardized change processing

IBM SmartCloud Control Desk allows you to automate a number of trivial tasks related to change management. For example large-volume changes such as security key updates for a group of servers, or provisioning/deprovisioning of related virtual systems.

Impact analysis

An integral part of the assessment phase in the change processing is the automated impact analysis which highlights the managed resources that will be impacted by the modifications contained in a change.



Adaptive workflows

IBM SmartCloud Control Desk uses workflows to control and automate processing of processes and records, such as requests, or changes. Within the workflows, the record can be routed trough different paths based on the available information.

Workflows are used in conjunction to automated tasks, to automate the processing, including implementations.

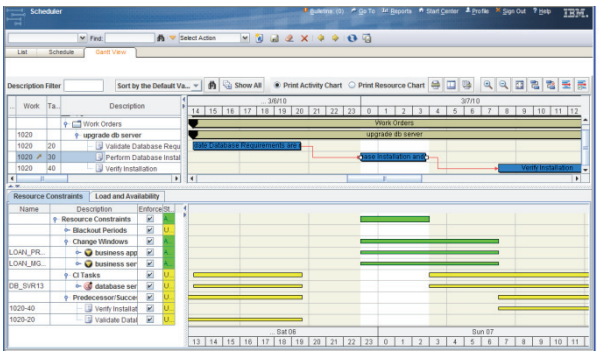
IBM SmartCloud Control Desk provides several ITIL compliant workflows, which can be modified to meet specific needs.

Change scheduling

- In the scheduling phase of the change processing, all implementation tasks of the change are considered, and attempted scheduled inside:
  - *Change Window Calendars* that apply to the target CIs and all impacted CIs

  and outside:
  - *Blackout Periods*
- Non-implementation tasks are scheduled around the implementation tasks as needed.
- Group and Person calendars are also taken into consideration if specific resources have been assigned as task owners.

- Scheduling conflicts are raised if a time slot in which all required resources are available, and with a minimum duration of the implementation task cannot be found.
- In the scheduling, only the current change is taken into account. The Change Schedule is used to identify scheduling conflicts across changes.



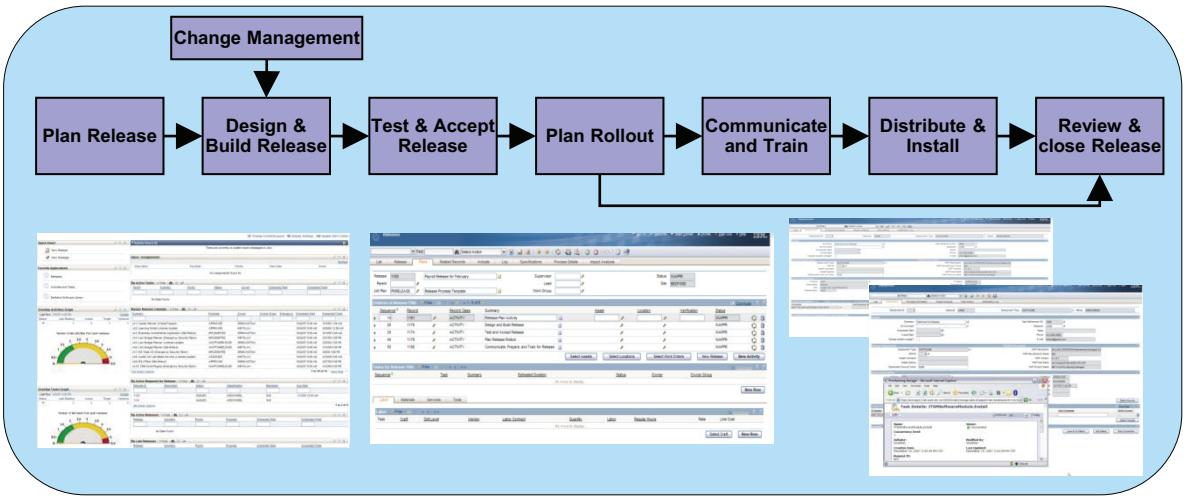
Impact analysis

The automated impact analysis uses the relationship information for the CIs to deduce which resources will be impacted by an outage, or service degradation, to a CI that is the target of a change.

Impacted CIs are highlighted, and tagged, in the topology viewer, to make it easy for you to identify the impacted resources.

This analysis is used in the scheduling process, to ensure that the change is implemented at a point in time when service degradation or outage is allowed for all impacted CIs.

Release management



- Ability to plan and oversee the successful roll-out of new and changed software and associated hardware, including documentation and training.
- Role-based start centers, workflows, scheduling and analytics
- Integration with deployment tools like Tivoli Provisioning Manager and Tivoli Configuration Manager, and to repositories like the Rational Asset Manager

28

28

Change scheduling

The scheduling feature of IBM SmartCloud Control desk provides a visualization of the Gantt chart representing the change. In the scheduler you see all the related tasks as well as the availability of target and impacted CIs, and the availability and resource requirements for implementation resources.

Using drag-and-drop, you can modify the schedule to meet your requirements.

The scheduler does not enforce scheduling within change windows and outside blackout periods. However, depending on the classification of the change, scheduling outside of the ‘allowed’ time slots, will require special authorization. The authorization is provided by the approver associated with the blackout period that is violated.

Summary

At this point, you should be able to:

- Articulate the main purposes of the configuration, change, and release management disciplines.
- Distinguish the responsibilities between the configuration, change, and release management teams.
- Discuss the main features of IBM SmartCloud Control Desk that support configuration, change, and release management.
- Describe the interactions between the three management disciplines.

Release management

You may think of release management as an extension to change management. Release management manages the coordination and deployment of multiple changes that are part of a release, or changes that involves updates to multiple resources. The nature of a release is often much more complex than a change, and may include documentation updates and training.

Typically you deal with three types of releases:

1. Complex, multi-resource changes that require synchronization and coordination. For example roll-out of a new application system.
2. Periodic releases, in which major updates to multiple resources are only allowed at certain periods of time. In this scenario, non-critical changes are accumulated in the release, and deployed *en block* at a pre-authorized point in time.
3. Mass deployment of software updates, for example fix-packs or antivirus signature updates.

Release management can leverage OMPs such as Tivoli Provisioning Manager, Tivoli Configuration Manager for implementation of the changes, and TADDM for access to CI details that may not have been uploaded to the IBM SmartCloud Control Desk CMDB.

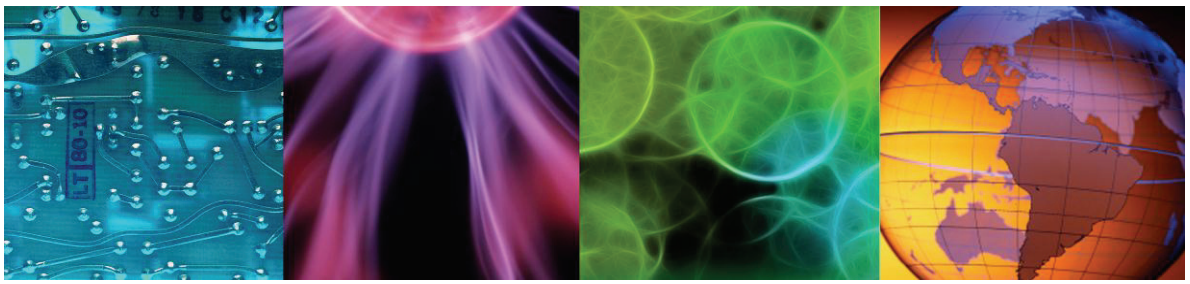
Release management often use Definitive Media Libraries (DML) that contain approved deployment images and documentation. Management of the DMLs is the responsibility of configuration management team.

Terminology

Summary

2 Organization of configuration item information

Organization of configuration item information



What this chapter is about

Understanding the way configuration item information is organized is key to understanding how and why the various features of IBM SmartCloud Control Desk configuration and change management work. This chapter introduces the data layer, and provides a quick overview of the main concepts of relating different representations of the same resource to one another.

Objectives

After you complete this unit, you will be able to:

- Articulate the main purpose of the Common Data Model (CDM)
- Describe how assets and configuration items are represented in the CMDB
- Explain reconciliation between actual and authorized resources
- Discuss asset and configuration item linkage

Objectives

CDM overview

- The Common Data Model is a logical model which is used to describe CIs, their attributes, and their relationships.
- CDM is leveraged by multiple IBM products including:
  - IBM SmartCloud Control Desk
  - IBM Tivoli Application Dependency Discovery Manager
  - IBM Tivoli Asset Discovery/Distributed
  - IBM Tivoli Business Services Manager

3

CDM overview

- The Common Data Model is IBMs strategic IT resource model which is an extension to the Common Information Model developed by the Desktop Management Task Force.
- It provides a logical representation of IT resources, their attributes and relationships.
- The CDM is object oriented.

The Common Data Model

- The Common Data Model has the following features:
  - A standardized definition of how system solutions and technologies represent resources and their relationships.
  - A logical data model that brings together various industry data models, acting as the dictionary and grammar for consistently describing details and the identity of resources.
- The Common Data Model provides consistent definitions for managed resources, business systems, processes, people, and other data and the relationships between those elements.
- The Common Data Model uses the *Unified Modeling Language* (UML) and is designed to work seamlessly with other development efforts based on UML.
- The Common Data Model can be used as the basis of data modeling and interactive design to foster integration among products.

4

The Common Data Model

Because the CDM is an information model, products are able to maintain their existing database schemas and also use the Common Data Model. When integrating with other products (such as when loading information into the CMDB), CDM definitions and terminology must be in use. This use fosters consistent, one-time integration that is re-usable across multiple solutions.

CDM and IBM SmartCloud Control Desk

In a IBM SmartCloud Control Desk context, the Common Data Model is an invaluable tool for the following reasons:

- It provides the logical reasoning to help you understand:
  - How CI information is organized
  - Which attributes are available for each class of CI
  - How CIs are named
  - The logical relationships between different types of CIs
- Having this basic knowledge helps you:
  - Understand how CIs are named and reconciled
  - Understand the relationships between CIs
  - Design and develop reports
  - Identify top-level CIs used to control import
  - Design and implement authorized CI hierarchies used in promotion

5

CDM and IBM SmartCloud Control Desk

The Common Data Model provides documentation and reference information for you to use to better understand how the CI information is organized in the IBM SmartCloud Control Desk.

Actual CIs are stored in strict accordance with the Common Data Model, so you can be assured that the necessary attributes, relationships and related CIs exist.

Authorized CIs can be organized in accordance with a custom classification hierarchy. This allows you to use only a subset of attributes and CI types when you are managing your CIs. The Deployers Workbench tool is used to define custom authorized CI classification hierarchies and the related promotion scopes that are used map actual CIs to authorized CIs during promotion.

CDM facts

- Approximately 900 resource types (class types), such as ComputerSystem, OperatingSystem, J2EEServer, BusinessService
- Approximately 120 relationship types, such as runsOn, installedOn, deployedTo, owns, controlsAccessTo…
- Originally based on Common Information Model (CIM) from the Distributed Management Task Force (DMTF)
- Integrating products allows for attribute extensibility, for example, the ability to store GPS coordinates

6

CDM facts

The Common Data Model defines IT resources at almost atomic level, and uses relationships to re-assemble them.

This allows for a very flexible structure in which new resource types can easily be added, and existing types can be augmented as technology evolves.

CI classes and types in the CDM

- All CIs are grouped within the CDM into entities that correspond to items in the real world.
  - These groups are called ***Classes*** in the CDM and in Tivoli Application Dependency Discovery Manager
  - Tivoli process automation environment refers to these groups as ***CI Classifications***
  - IBM SmartCloud Control Desk uses the term ***CI Type***
- Each class in the CDM contains:
  - Hierarchy
  - Attributes
  - Relationships
  - Naming rules

7

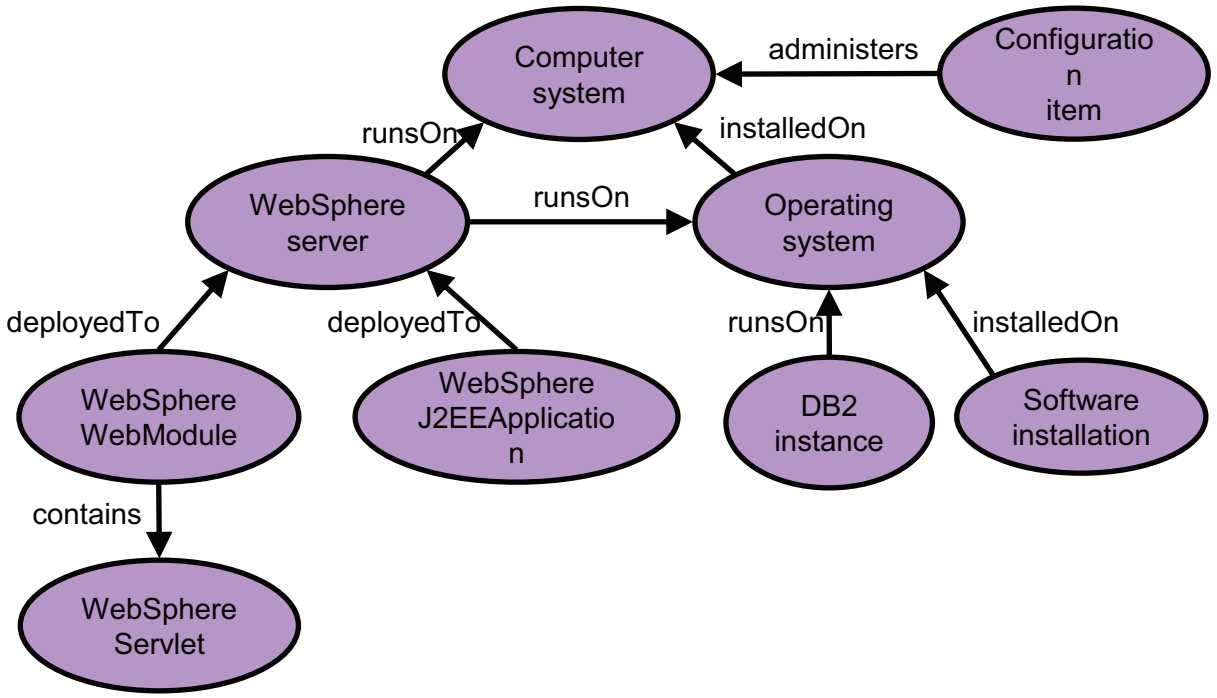
CI classes and types in the CDM

Each CI type is associated with a set of attributes that describe the properties of the CI.

Attributes can convey three different types of information:

- A value that describes a CI property (numCPUs).
- An implicit relationship to another CI (IpInterface).
- A group of related resources (fileSystems).

CDM example



8

CDM example

Instructor:

The various CIs that are found in a system are represented as related objects.

The relationships are enforced to ensure that CIs that by nature rely on other CIs (a WebSphere Server MUST run on an operating system) do not exist without the necessary relationships.

When resources are removed, the relationships are also used to remove dependent resources that rely only on the removed parent.

CDM facts

- It is a logical representation
- It is not a product
- Tivoli Application Dependency Discovery Manager provides an implementation of the CDM
- The CDM classifications are pre-loaded into IBM SmartCloud Control Desk
  - If you customize the model, you can import Tivoli Application Dependency Discovery Manager's representation of the CDM using IBM Tivoli Integration Composer (ITIC)

9

CDM facts

It is important to understand, that the Common Data Model represent the logical CI structures you work with in IBM SmartCloud Control Desk.

The TADDM product provides functions to discover your infrastructure resources and their relationships, so they can be loaded into the IBM SmartCloud Control Desk CMDB.

Working with the CDM

- Understand the CDM
  - Using appropriate object types
  - Knowing the required attributes to support naming
  - Traversing the relationships
- Where to find the CDM documentation
  - In the Tivoli Application Dependency Discovery Manager SDK
  - **<TADDM installation directory>\sdk\doc\model\CDMWebsite.zip**

10

Working with the CDM

Understanding how the CI information is organized in the Common Data Model is critical to create your own authorized CI classification hierarchies.

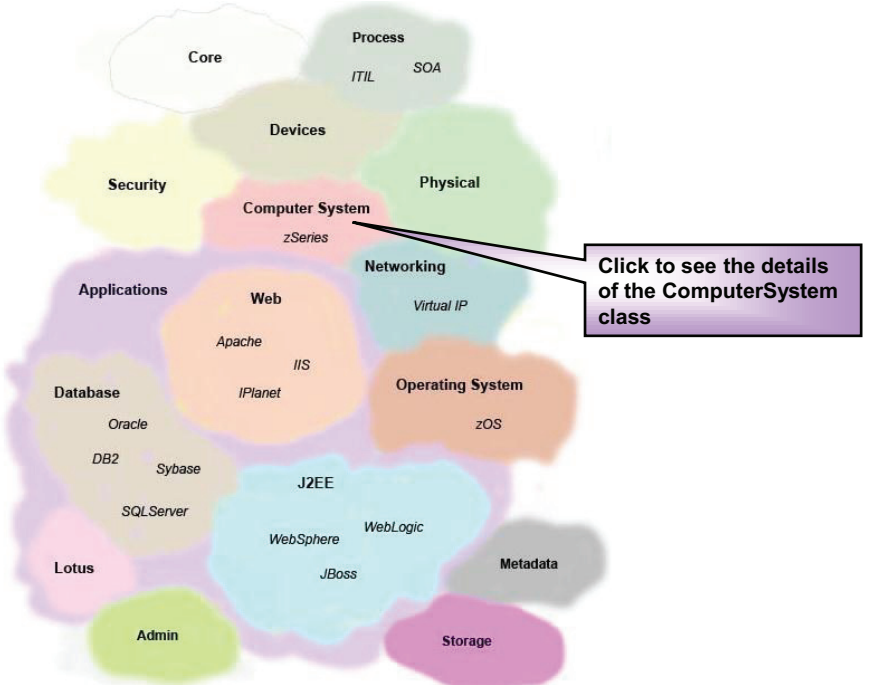
Most likely, you will not manage your IT resources to the level of detail provided in the CDM. The authorized CI classification hierarchy provides the means for you to define a simplified view of your resources. In this view, you can combine attributes from different CIs in you own classifications, thereby visualizing attributes of low-level CIs at the parent, or grand parent level. This helps you create a representation of your managed IT resources which is operational, and detailed enough to support your needs, yet not as detailed as the CDM.

CDM overview: <CDMWebsite.zip>WebsiteFiles/misc/cdm.htm

This diagram presents an abstract overview of the main sections of the CDM.

The important thing to understand from this diagram is what subsections exist in the CDM.

When you find a subsection that is interesting, click the label and a more detailed explanation of that section displays, from which you can dig deeper and investigate specific classes, interfaces, attributes, and relationships.



11

CDM overview: <CDMWebsite.zip>

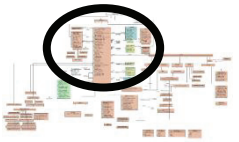
The Common Data Model documentation is provided with the TADDM product. The documentation consists of a number of web pages that provide all the details about the different configuration item types, their attributes, relationships, and naming rules.

The information is organized in logical groupings that are technology-based, but you can also navigate to a specific type by selecting it from an index.

In the Common Data Model, CI types are referred to as classes.

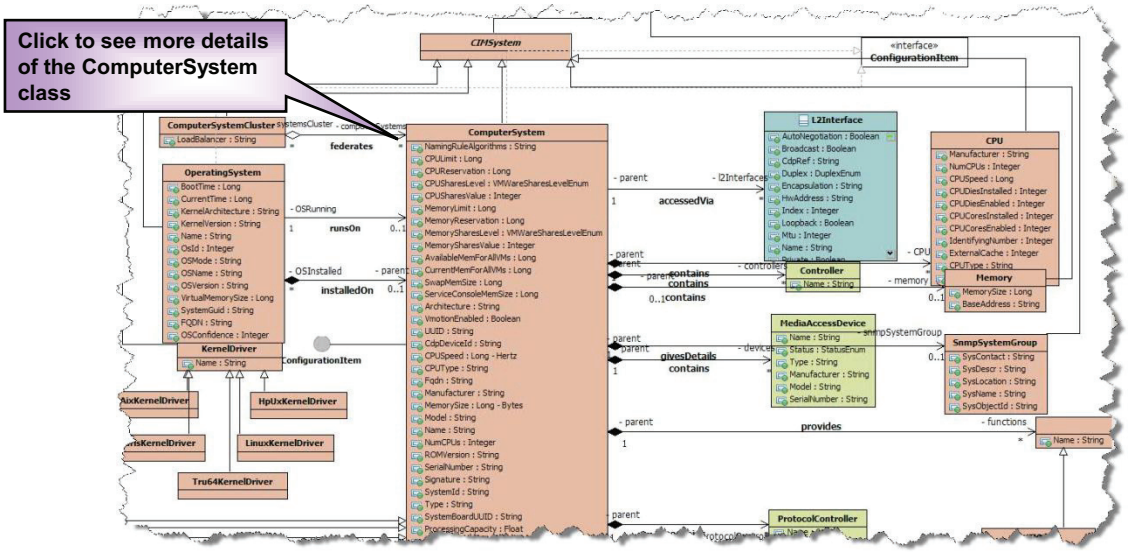
Computer system submodel

The computer system section of the model provides classes that represent the concept that we all know as a computer.



Primarily, this is a hardware-based definition, but relationships to all of the logical entities on the computer, as well as virtualization and clustering are represented in this section of the model.

For logical components of the computer, consult the *operating system* submodel.

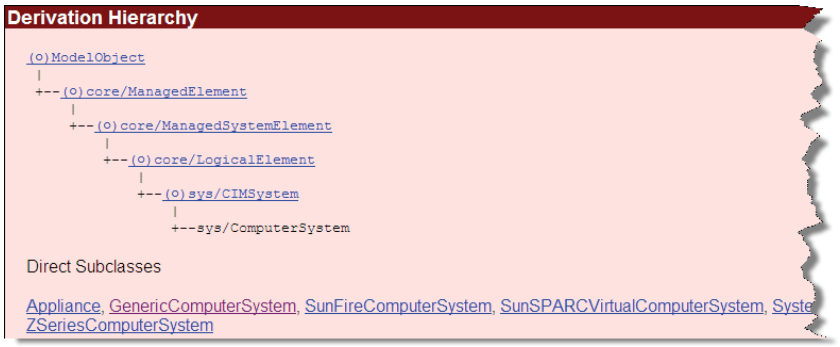


Computer system submodel

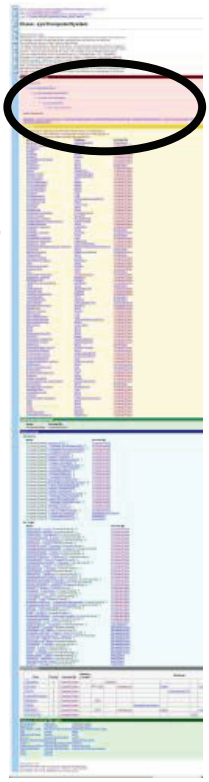
The Common Data Model includes UML diagrams that illustrate all the resource types, their attributes, and relationships. These diagrams can be very helpful if you want to better understand how the model works.

ComputerSystem: Derivation hierarchy

- Represents any resource instance that is a combination of some form of hardware and some form of software capable of manipulating data. (Where the physical devices are within the PhysicalElement section of the Common Data Model.)
- The logical representation of the physical device, ComputerSystem represents both the virtual and non-virtual computing environments. All non-physical, logical relationships relating to how the logical system is setup are associated with this class. This includes but is not limited to the logical resource representations on the ComputerSystem (for example, StorageExtent, CPU, and L2Interface).



- Examples of ComputerSystem instances include: servers, workstations, networking hardware (switches, routers, telephony), virtual computers (running virtual machines and LPARs), storage systems (IBM DS8000), even refrigerators (if they have supporting software and hardware).



13

ComputerSystem: Derivation hierarchy

All resource types defined in the Common Data Model inherits specific behavior or attributes from their parent. The only exception to this is the ModelObject. However, ModelObject, MangedElement, ManagedSystemElement, and CIMSystem are all transient classes, tagged with (o), which means that they are helper classes only. You will never see CIs in IBM SmartCloud Control Desk or TADDM of those types.

Attributes that are inherited from transient classes cannot be updated. You can say that they are managed by the system.

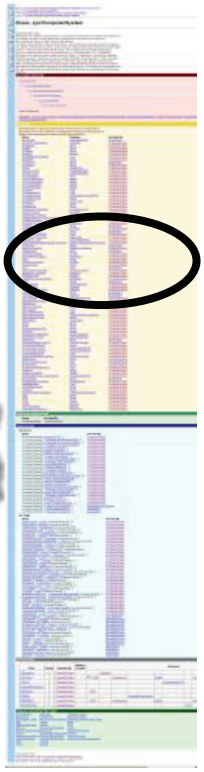
ComputerSystem: Attributes

- Attribute definitions might be inherited from upper level objects, in this case the ComputerSystem class exposes several attributes defined in the *ModelObject* class.
- Attribute values exposed by an instance of the ComputerSystem class might also expose attributes owned by related objects. These are called *implicit* attributes.

Attributes

In the following list, attributes that are listed with the name of a relationship in parentheses are *implicit* attributes, meaning that the reference in that attribute to another object represents an instance of the listed relationship.

Name	Datatype	Included By
AdminState	AdminStateEnum	ModelObject
Admininfo (administers)	AdminInfo	ConfigurationItem
Architecture	String	ComputerSystem
AssetID	String	ConfigurationItem
AssetTag	String	ConfigurationItem
AutoStart	Boolean	ComputerSystem
AvailableMemForAllVMs	Long	ComputerSystem
BootOrder	String	ComputerSystem
CDMSource	String	ModelObject
CICategory	String	ConfigurationItem
CIRole	CIRoleEnum	ConfigurationItem
CISource (uses)	ConfigurationItem	ConfigurationItem
CITarget (uses)	ConfigurationItem	ConfigurationItem



- For example, the *Admininfo* attribute is owned by an instance of the *ConfigurationItem* class that is related to the ComputerSystem instance through an *administers* relationship.

14

ComputerSystem: Attributes

In the Common Data Model, attributes are used to describe a resource.

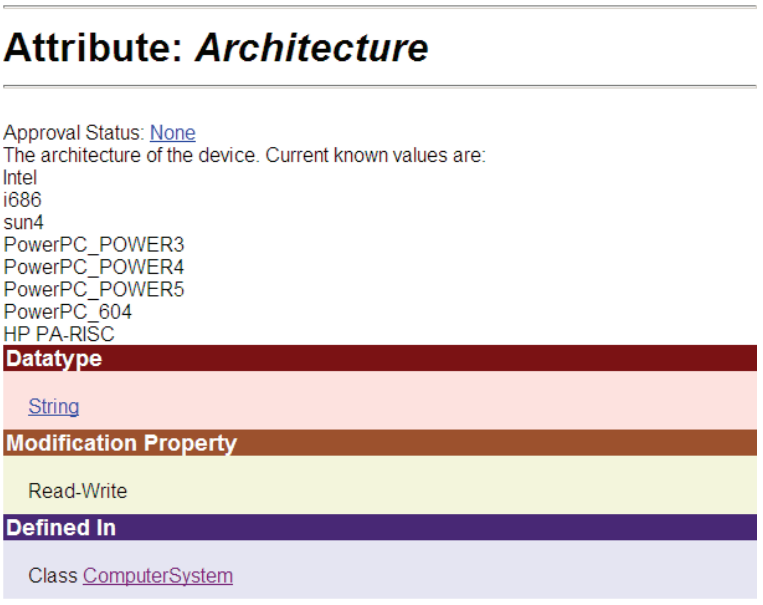
CIs many attributes, some of which contains pointers to related resourced. In this example, the Admininfo attribute contains a pointer to another CI, and implements an implicit relationship named administers.

Notice how the AdminState, and CDMSource attributes are inherited from the transient ModelObject.

When ComputerSystem CIs are loaded into IBM SmartCloud Control Desk as actual CIs, you will see the ComputerSystem as well as all the related CI types, depending on the depth that was used for the ITIC import.

ComputerSystem: Attribute details

Attribute definitions specify the datatype as well as related metadata (valid values for example) that define and control the value of and use of the attribute



15

ComputerSystem: Attribute details

The attribute details show the type, length and possible fixed values for an attribute.

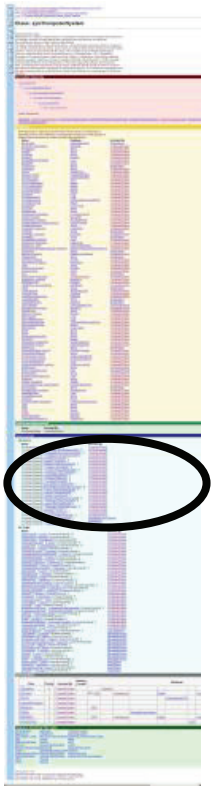
ComputerSystem: Relationships as source

Relationships define source class, target class, and cardinality

Relationships

As Source

Name	Included By
ComputerSystem[1] contains CPU[0..*]	ComputerSystem
ComputerSystem[0..1] manages WebSphereNode[0..1]	ComputerSystem
ComputerSystem[1] configuredUsing LogicalContent[0..*]	ComputerSystem
ComputerSystem[0..*] virtualizes ComputerSystem[1]	ComputerSystem
ComputerSystem[1] provides Function[0..*]	ComputerSystem
ComputerSystem[1] contains Controller[0..*]	ComputerSystem
ComputerSystem[1] contains ProtocolController[0..*]	ComputerSystem
ComputerSystem[0..*] realizes MsCluster[0..1]	ComputerSystem
ComputerSystem[0..1] runsOn PhysicalPackage[0..1]	ComputerSystem
ComputerSystem[0..1] manages J2EEDomain[0..*]	ComputerSystem
ComputerSystem[1] contains IpInterface[0..*]	ComputerSystem
ComputerSystem[0..1] contains Memory[0..1]	ComputerSystem
ComputerSystem[0..*] locatedAt SiteInfo[0..1]	ComputerSystem
ComputerSystem[1] accessedVia L2Interface[0..*]	ComputerSystem
ComputerSystem[1] givesDetails SnmpSystemGroup[0..1]	ComputerSystem
ComputerSystem[0..*] uses VMWareDataStore[0..*]	ComputerSystem
ComputerSystem[1] contains StorageExtent[0..*]	ComputerSystem
ComputerSystem[1] contains FileSystem[0..*]	ComputerSystem
ComputerSystem[1] contains MediaAccessDevice[0..*]	ComputerSystem
ComputerSystem[0..1] manages JBossDomain[0..1]	ComputerSystem
ComputerSystem[1] realizes MsClusterNode[1]	ComputerSystem
ComputerSystem[0..1] manages WebSphereCell[0..1]	ComputerSystem
ComputerSystem[1] contains FCPort[0..*]	ComputerSystem
ComputerSystem[0..*] provides Service[0..*]	ComputerSystem
ComputerSystem[0..*] uses ConfigurationItem[0..*]	ConfigurationItem
ComputerSystem[0..*] advertises Capability[0..*]	ManagedSystemElement
ComputerSystem[0..1] relates Relationship[0..*]	ModelObject
ComputerSystem[0..*] memberOf Collection[0..*]	ModelObject



16

ComputerSystem: Relationships as source

For each type of CI, you can see which relationships the CDM allows.

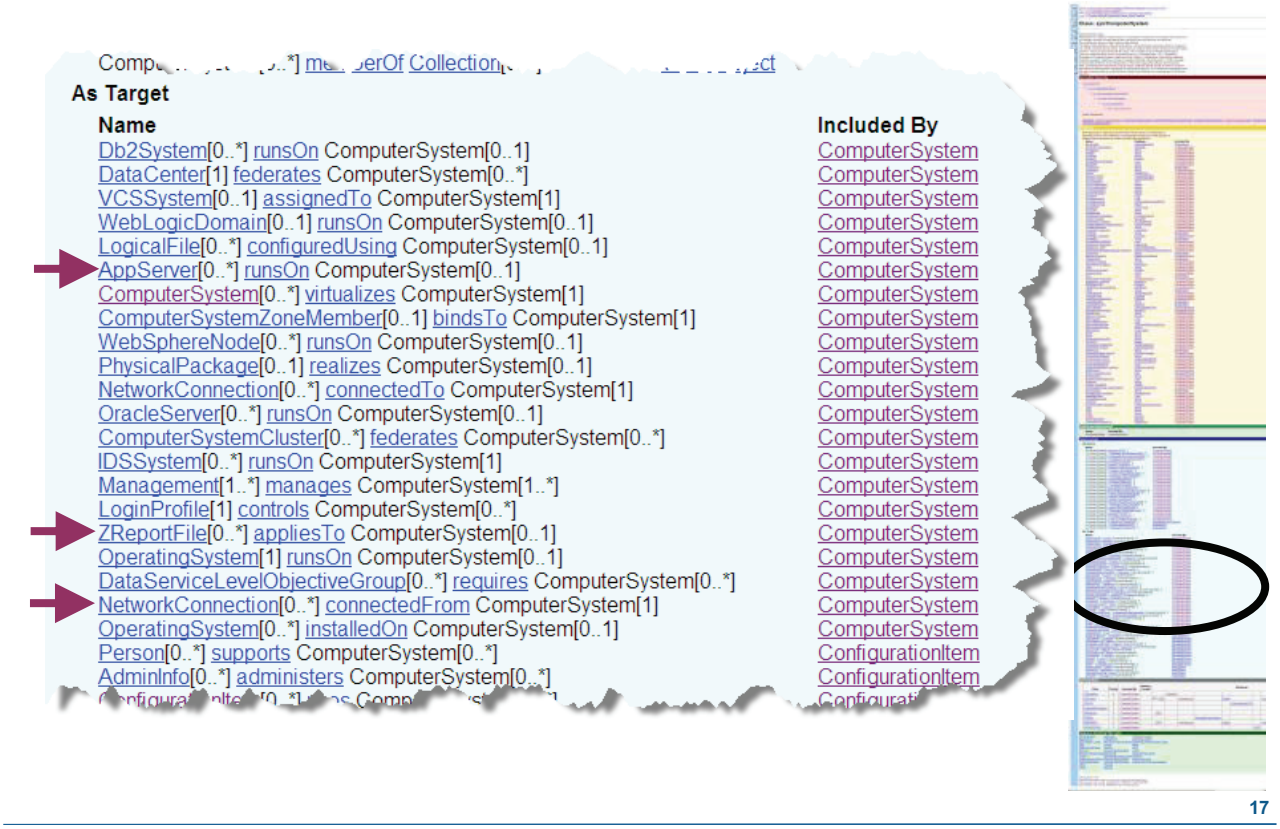
Relationships are uni-directional. They and are used to combine CIs in a logical structure, so you can easily navigate from one to the next.

Relationships that are implemented as attribute pointers are called implicit relationships. These relationships that are dictated by the model, and typically represent dependencies that MUST exist in order for a CI to exist. For example, the contains relationship between a ComputerSystem and an IpInterface tells you that an IpInterface CI cannot be created unless it is contained by a ComputerSystem.

The CDM also contains explicit relationships. These are relationships that represent communication, or interdependencies between CIs that are not implicitly related. For example, the uses relationship that represents that a WebSphere Application Server communicates with a DB2 Database Instance is an explicit relationship. There are no logical requirements for the two CIs to be related to one another, but the dependency has been discovered, and stored.

Relationships are used both when loading data into IBM SmartCloud Control Desk to automatically include dependent CIs, and when promoting actual CIs to authorized CIs in order to include child CIs in the promotion.

Relationships also play a key role in impact analysis, since they identify the dependencies between resources. In this case, the explicit dependencies are by far the most interesting ones.



ComputerSystem: Relationships as target

The Common Data Model also defines the cardinality of relationships.

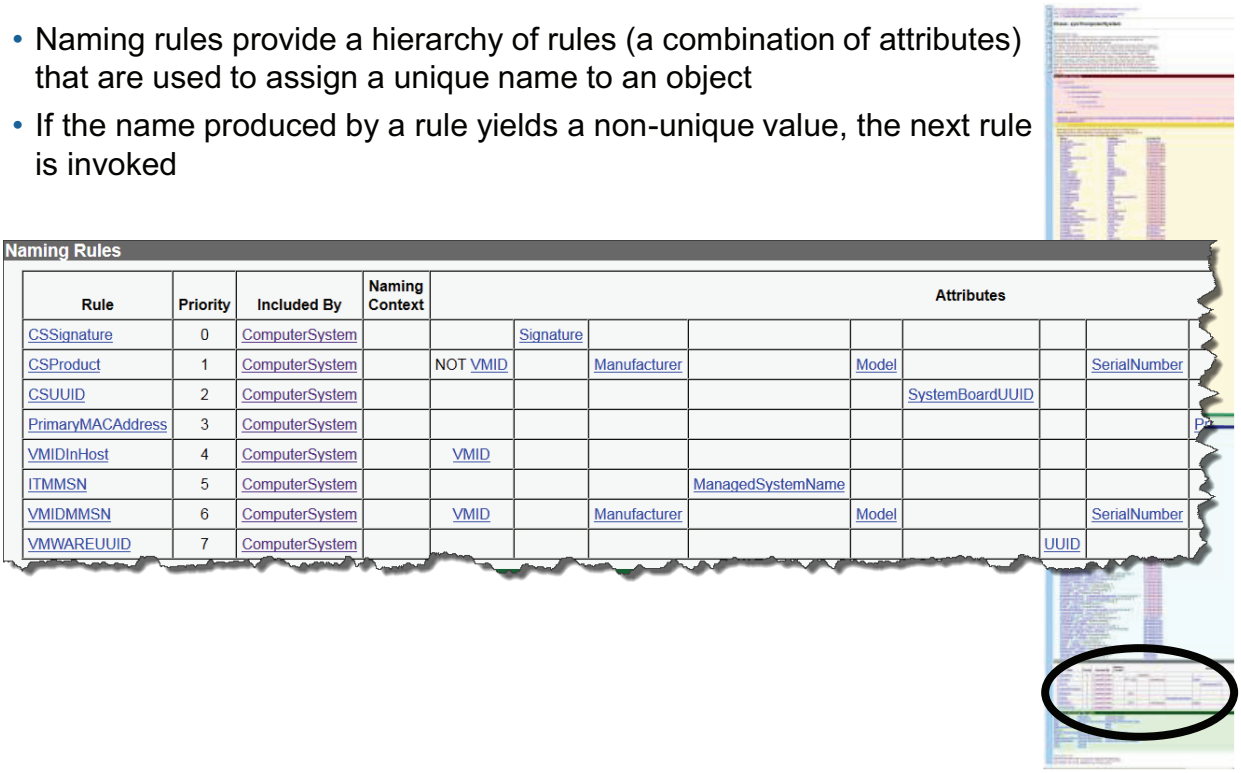
Notice that to support virtualization, the Common Data Model allows a ComputerSystem to virtualize another ComputerSystem instance.

To support the fact that multiple OperatingSystems can be installed on the same ComputerSystem at the same time, CDM uses the installedOn. However, there can only be one runsOn relationship between an Operating System and a ComputerSystem.

ComputerSystem: Naming rules

ComputerSystem: Naming rules

- Naming rules provide a hierarchy of rules (a combination of attributes) that are used to assign a unique name to an object
- If the name produced by a rule yields a non-unique value, the next rule is invoked



Naming Rules

Rule	Priority	Included By	Naming Context	Attributes							
CSSignature	0	ComputerSystem			Signature						
CSProduct	1	ComputerSystem		NOT VMID		Manufacturer		Model			SerialNumber
CSUUID	2	ComputerSystem							SystemBoardUUID		
PrimaryMACAddress	3	ComputerSystem									
VMIDInHost	4	ComputerSystem		VMID							
ITMMSN	5	ComputerSystem					ManagedSystemName				
VMIDMMSN	6	ComputerSystem		VMID		Manufacturer		Model			SerialNumber
VMWAREUUID	7	ComputerSystem								UUID	

18

ComputerSystem: Naming rules

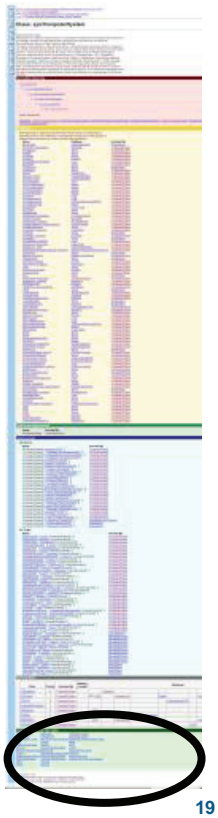
A naming rule is a combination of attributes that uniquely identifies a CI, When a CI is created, the attributes are validated from the lowest priority to the highest in order to correctly identify the CI and assign a GUID. This implies, that you must play close attention when importing CIs in order to avoid creating multiple instances (using different naming rules) that represent the same resource. When you load CI information using ITIC, the CIs have already been normalized and reconciled by the tools that own the data source ITIC reads from.

ComputerSystem: Diagrams

- This section in the CDM website includes links to related diagrams to help you navigate to related classes

Diagrams Including This Class

Administration	WebLogic	Computer System
Applications	WebSphere	Operating System
MS Failover Cluster	MQ Series Naming Rules	Operating System Naming Rules
DB2	Cluster	Blade
DB2 Naming Rules	Devices	i5OS
Informix	Devices Naming Rules	Virtual
Informix Naming Rules	Networking	Virtual Naming Rules
Oracle	Networking Naming Rules	VMWare
Oracle Naming Rules	Security Naming Rules	zSeries And zOS
HIS Naming Rules	Virtual IP Naming Rules	zSeries and zOS Naming Rules
J2EE	Physical	
JBoss	Storage	



19

ComputerSystem: Diagrams

At the bottom of the web page that documents the details of a CI type, you find links to the UML diagrams in which the CI type is referenced.

Asset and configuration item representations and linkage

- IBM SmartCloud Control Desk represent resources in both an actual and an authorized state.
- A tangible resource may be represented as both a CI and an asset.
- The CI and asset can be linked to provide a unified view of the resource

20

Asset and Configuration Item representations and linkage

A fundamental feature of IBM SmartCloud Control Desk is that CI and asset information is maintained in two states.

Actual This state represents the current configuration of your resources.

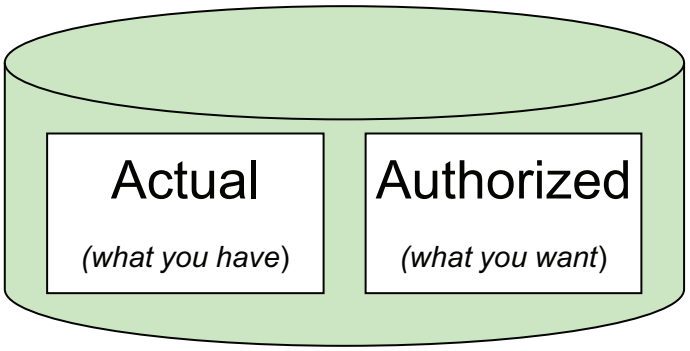
Authorized This state represents the planned state or the configuration of your IT infrastructure as you want it after implementation of all changes.

IBM SmartCloud also maintains separate data spaces for CI and asset information.

Linking Asset and CI information allows you to access both technical and administrative information for a resource.IBM SmartCloud Control Desk can be configured to automatically perform this linkage, provided all the necessary resource attributes are loaded into the IBM SmartCloud Control Desk CMDB.

Configuration items and assets in the CMDB

- Both assets and configuration items are represented in the CMDB in two *states*.
- Depending on the classification, resources are associated with different sets of attributes and relationships. The combination of attributes and relationships is commonly referred to as the *configuration*.



Actual resources represent what exists, and is loaded into the CMDB from discovered data.

Authorized resources represent how you want the resources to be configured.

21

Configuration items and assets in the CMDB

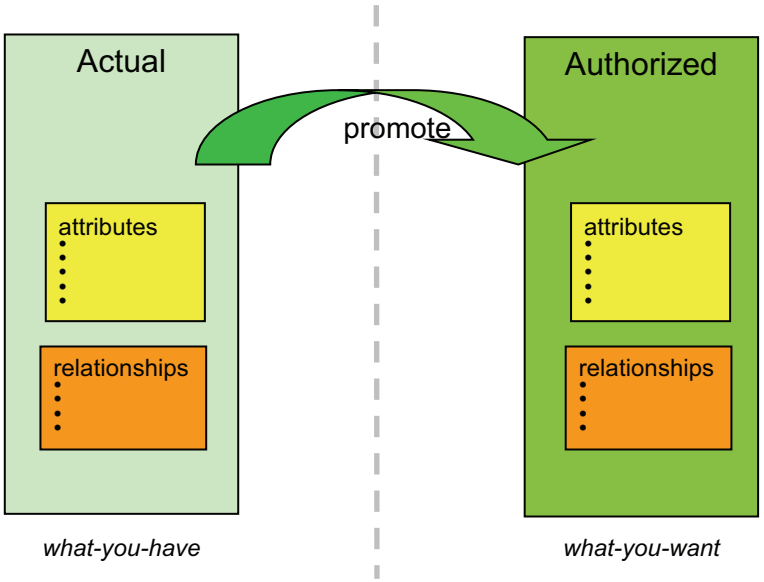
IBM SmartCloud Control Desk also keeps separate records for the current and the planned configuration of resources.

The current configuration, often referred to s the actual, or deployed configuration, represent the latest discovered configurations. This information is used by several tasks, primarily by the configuration management team, when they need information about what is actually implemented. CI audit, and promotion are some of the primary tasks that use the actual information

On the other side, the representation of the planned state of a resource, is primarily used by the change management team to plan changes, and document intended updates to the resource attributes. After all, a change is basically a set of configuration changes in which CI attribute values are modified, CIs created or removed, and relationships manipulated. The change documents the expected updates to the CI configurations, and after successful change implementation, it can be verified if the change was implemented correctly by comparing the new actual information with the planned (or authorized) information.

Promotion

- If you have discovered your actual resources, the authorized sibling can be created through promotion.
- To plan for upcoming events, you often create authorized resources before they have materialized.



22

Promotion

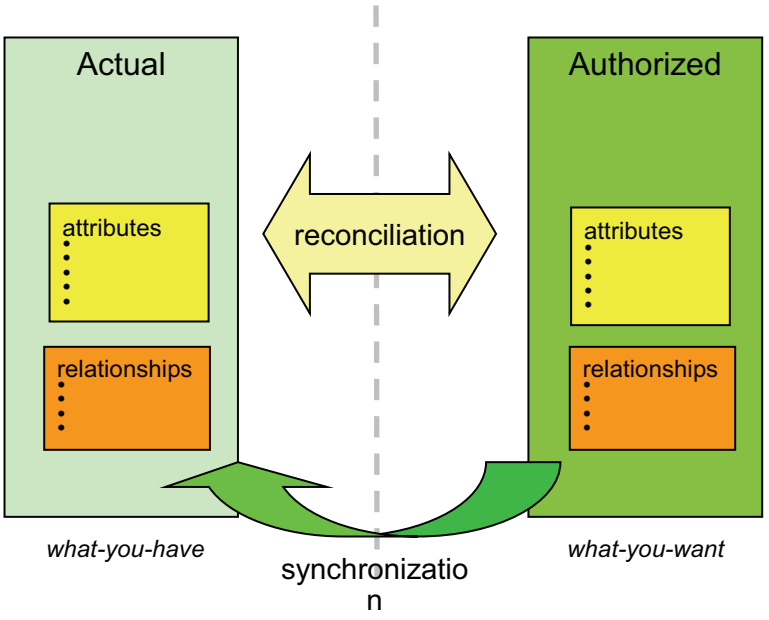
In order to manage your CIs, you must create authorized (managed) CIs.

When you create new authorized CIs to represent resources that have not yet been implemented, you use the IBM SmartCloud Control Desk user interface, or import facility. In this case you focus only on the key CIs and relationships, because it is not practical to enter all the details manually.

If your resources have been discovered and loaded into the IBM SmartCloud Control Desk CMDB, the most common way to create authorized (managed) CI is to promote the actual CIs. You normally promote top-level resources such as Applications, AppServers, ComputerSystems, and network devices. During promotion, CI that are dependent on the resource which is promoted, will be promoted as well. The fine-grained control of which dependent CIs to include is defined in the promotion scope for the promoted resource.

Actual and authorized linkage

- Actual and authorized resources are linked, when an attribute in each resource as been populated with the ID of the sibling.
- This ID is automatically maintained during promotion
- Reconciliation tasks can be created to automatically link unlinked resource pairs.
  This process is always initiated from the authorized resource



23

Actual and authorized linkage

Once both authorized and actual representations for a resource are represented in the IBM SmartCloud Control Desk they may be linked in several ways.

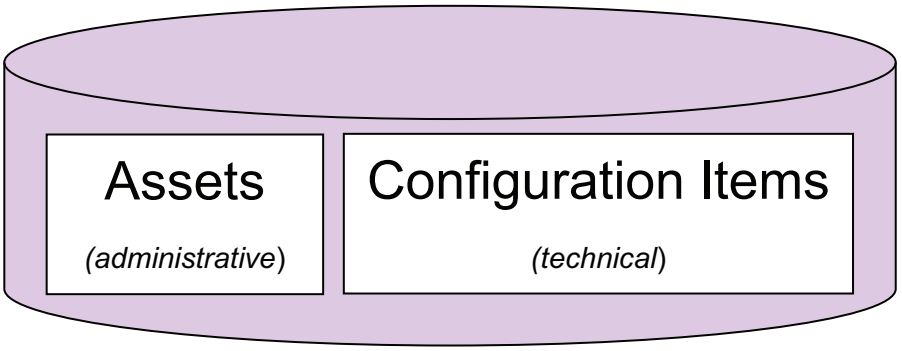
If the authorized CI was created by promotion, the information about the actual CI from which it was created already exists.

Reconciliation tasks can be defined to analyze the attributes of the authorized and actual CIs to find records that share a common set of attributes, and use this information to create the link.

From the user interface you can initiate a synchronization for an authorized CI. This works as a reverse promotion, where naming rules are used to identify the related actual CI, and its dependent children. When a match is found, the link is created, and (optionally) the dependent children are promoted so they appear as authorized CIs.

Configuration items and assets

- Administrative information about IT resources is represented in the CMDB Assets.
- Technical information about IT resources is represented in the CMDB as configuration items.



- Both assets and configuration items are classified to specify the specific resource type
- Depending on the classification, resources are associated with different sets of attributes and relationships. The combination of attributes and relationships is commonly referred to as the *configuration*.

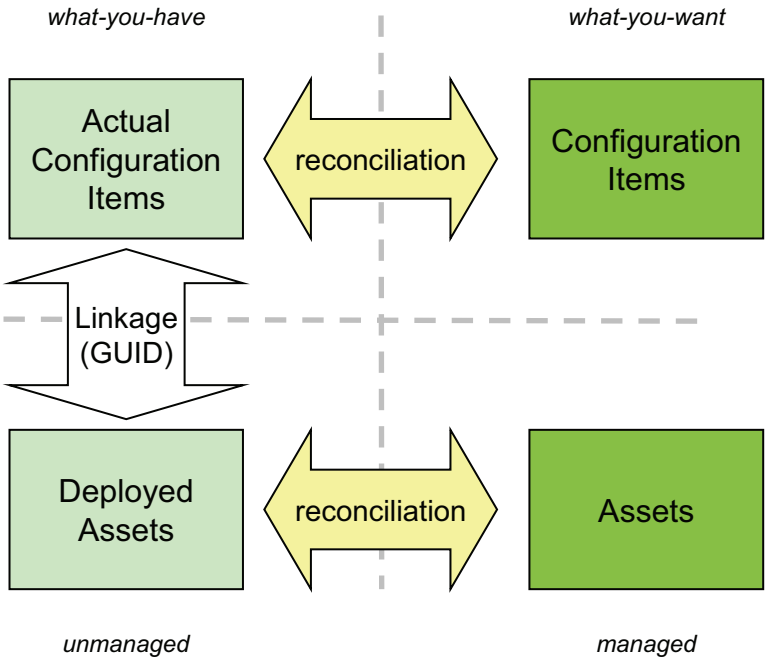
24

Configuration items and assets

In most cases, asset and CI information do not originate from the same source. Specialized tools discover Assets and Software License Information, and other tools discover CIs. For that reason, IBM SmartCloud Control Desk stores the information for the two different resource types in separately. Assets and CIs have their own unique set of attributes, but with some overlap. By using the overlapping attributes, the asset and CI records for the same resource can be linked to provide a unified view of the resource.

Actual and actual linkage

- The tool use to load discovered data, IBM Tivoli Integration Composer (ITIC)
  - Identifies all resources based on naming rules by inspecting the values in specific attributes
  - Associates each unique resource with a unique identifier named DISGUID or NRSGUID
- IBM SmartCloud Control Desk automatically links Deployed Assets and Actual CIs by comparing the NRSGUID and DISGUID values



25

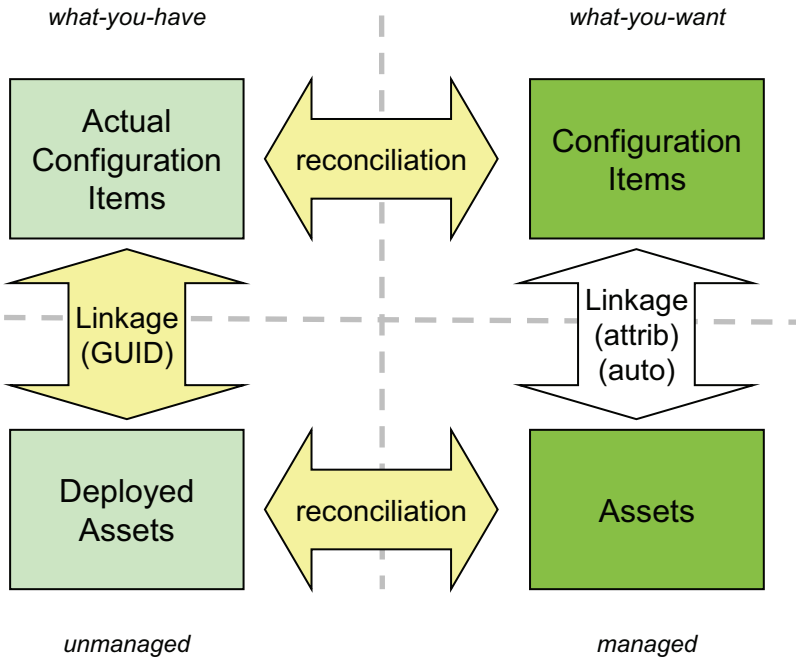
Actual and actual linkage

Asset and CI information for actual resources are automatically linked, if the resources have been imported via ITIC. ITIC populate GUIDs for both actual assets and CIs, and this information is used by a background task (escalation/action pair) to create the links.

If the GUIDs are not available, you must perform this linkage manually

Authorized and authorized linkage

- Reconciliation tasks can be defined to link authorized siblings based on identical values for common attributes
- IBM SmartCloud Control Desk automatically can be configured to automatically link authorized siblings for which the authorized-actual, actual-actual, and actual-authorized, link pairs already exist.



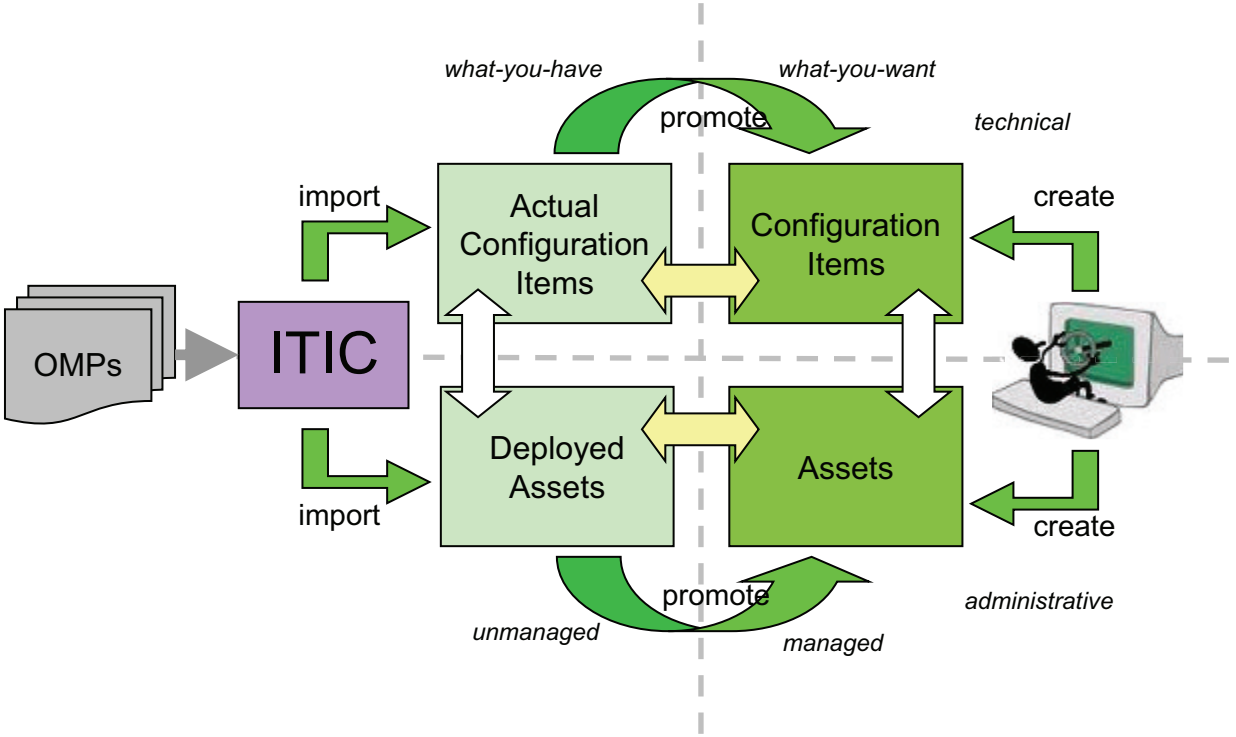
26

Authorized and authorized linkage

Once the actual-actual link has been created, a reconciliation task can be activated to use the available information in the authorized - actual - actual - authorized chain to create the missing authorized-authorized link.

For new resources, or in situations where the chain is broken (typically because the actual resources are not linked), you can configure the reconciliation task to compare specific attributes in the two types of resources to identify a match based on classification and attributes, and then create the link.

Data flows and link summary



Data flows and link summary

In Summary, both CI and asset information can be loaded into BM SmartCloud Control Desk from external sources (OMPs). IBM Tivoli Integration Composer is the component used to perform the load. Once actual resources have been created, they can be promoted to create their authorized siblings.

Authorized resources may also be created by an operator, and the reconciliation tasks built into IBM SmartCloud Control Desk are used to link authorized to actual resources (once the actual resources appear) and also link asset and CIs in both the actual and the authorized space.

Summary

At this point, you should be able to:

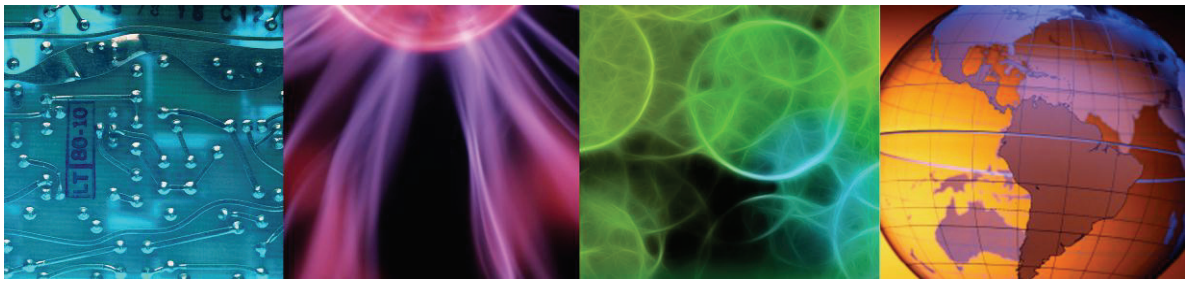
- Articulate the main purpose of the Common Data Model
- Describe how assets and configuration items are represented in the CMDB
- Explain linkage between actual and authorized resources
- Discuss asset and configuration item linkage

28

Summary

3 Configuration management with IBM SmartCloud Control Desk 7.5

Configuration management with IBM SmartCloud Control Desk 7.5



What this chapter is about

Configuration management is the core discipline of service management. This discipline is responsible for ensuring the trustworthiness of the data that are the foundation for the change and release management processes. This chapter introduces the configuration management discipline, and processes, and teaches you how to effectively manage your configuration items.

Objectives

After you complete this unit, you will be able to:

- Understand the purpose of the configuration management processes
- Describe the purpose of IBM Tivoli Unified Process and how it relates to the IT Infrastructure Library (ITIL)
- Define common configuration management roles and responsibilities
- Discuss differences and similarities between active and authorized configuration items
- Describe the purpose of naming rules
- Explain promotion, linkage, and synchronization
- Understand the purpose and use of configuration baselines
- Describe the use of configuration lifecycles
- Describe use and configuration of reconciliation tasks

Objectives

Agenda

- Configuration management overview
- CIs and assets
- Configuration item history and baselining
- Lifecycle management
- Configuration item reconciliation
- Summary

Agenda

Configuration management overview

The purpose of the configuration management process is to maintain the integrity of the configuration item (CI) employed in, or related to, IT systems and infrastructure, and to provide accurate information about CIs and their relationships.

Configuration management overview

Configuration management is focused on maintaining the trustworthiness of the CMDB.

Introduction to configuration management

- Configuration management is responsible for keeping the CMDB accurate.
- Its standardized methods and procedures are defined for efficient and prompt handling of all configuration requests, including:
  - Defining CI valid states and lifecycles
  - Creating and removing configuration items
  - Promoting, linking, and synchronizing actual and authorized CIs
  - Managing collections
  - Creating CI configuration baselines and identify drift
  - Auditing and reconciling actual and authorized CIs to identifying discrepancies and identify unauthorized changes
  - Linking CIs and assets
  - Creating workflows for handling configuration processes

Introduction to configuration management

The configuration management team focuses on maintaining configurations.

In this context, configurations represent the classification, attributes, and relationships of a resource, and also the metadata that describes the resource.

Descriptive metadata include properties such as:

- Related siblings (actual to authorized linkage)
- Related assets
- Lifecycle, and lifecycle state
- Membership of collections
- Access to view and manipulate the resource

ITIL and IBM Tivoli Unified Process (ITUP)

- ITIL (IT Infrastructure Library)
  - Best practices for service and support management.
  - Defines services, processes, roles, interfaces, functions.
  - Services such as configuration management are documented.
- IBM Tivoli Unified Process
  - ITUP provides detailed documentation of IT service management.
  - Tivoli documentation that uses ITIL as its foundation.
  - Documentation that is available to be used and customized to document a company's roles, processes, and services.
  - ITUP is based on ITIL Version 3.

 6

ITIL and IBM Tivoli Unified Process (ITUP)

The IT Infrastructure Library (ITIL) provides the theoretical description of the responsibilities of the configuration management team, and activities it performs. In addition, ITIL also provides a process model that describes the various tasks and roles related to configuration management.

The IBM Tivoli Unified Process (ITUP) is an IBM tool that summarizes ITIL and other process models, and relates the tasks and roles to IBM tools that support the various activities.

Configuration item management

Configuration management processes

- Identify CIs
- Control CIs
  - Update CI process
- Report configuration status
  - CI Lifecycles application
- Verify and audit CIs
  - Audit CI process

Configuration management roles

Configuration manager:
Performs the day-to-day overall management of the process. This role ensures that all process activities are being performed and that they are staffed adequately.

Configuration administrator:
Supports the Configuration Manager by managing records, tracking action items, and providing process-related reports.

Configuration librarian:
Is the custodian and guardian of all master copies of CIs registered with configuration management. The role is responsible for the integrity and accuracy of the configuration data.

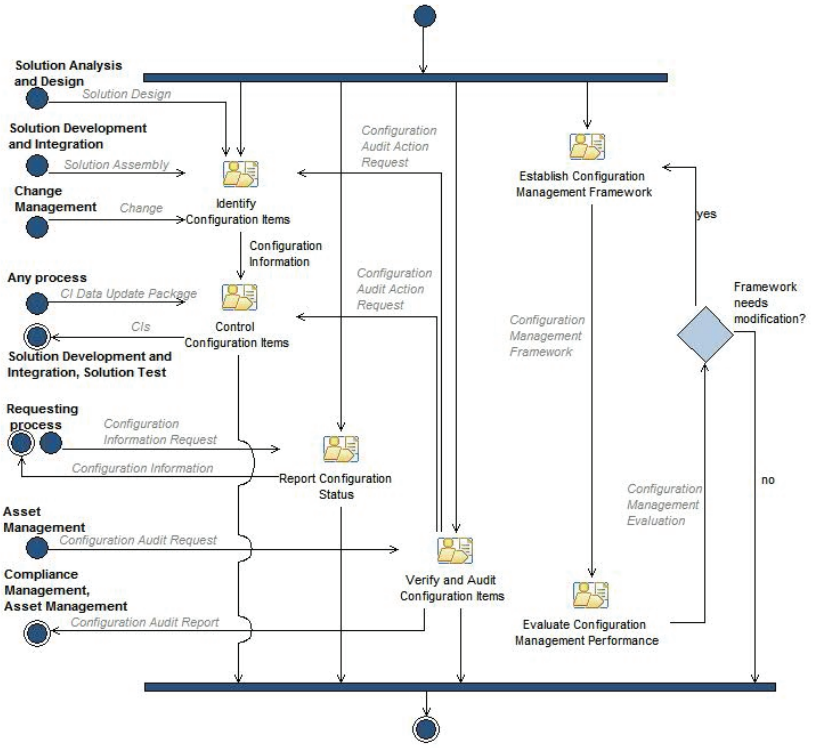
Configuration auditor:
Plans and executes the verification and audit of Configuration data and validates the accuracy of configuration management system content.

Configuration item management

From a high-level perspective, configuration management can be simplified to identifying, controlling, and verifying CI configurations, and providing reports that document the CIs as needed.

These activities are handled by four different roles. The key role that performs most of the day-to-day work is the configuration librarian. The work performed by the librarian is verified by the configuration auditor. Both the configuration manager and administrator roles are more involved with managing and administering the process, and tools used to perform configuration management.

The configuration management process



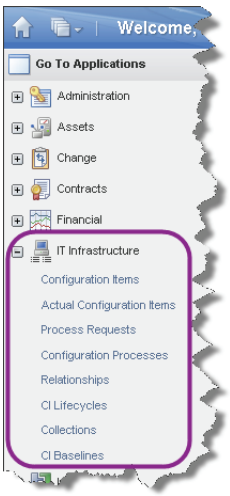
 8

The configuration management process

In ITUP you can find the outline of the configuration management process.

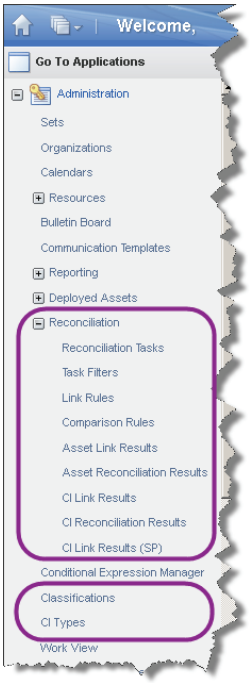
Notice how configuration management is interacting heavily with the other processes. This proves how much the whole organization relies on the information that is managed by the configuration management team.

Configuration management applications and roles



General tools used by most configuration management users

Role	Security Group	Start Center	Person Group
Configuration manager	PMCFGMGR	Configuration Manager (20)	PMCFGMGR
Configuration administrator	PMCFGADM	Configuration Administrator (19)	PMCFGADM
Configuration librarian	PMCFGLIB	Configuration Librarian (21)	PMCFGLIB
Configuration auditor	PMCFGAUD	Configuration Auditor (22)	PMCFGAUD



Administration tools used by the Configuration Administrator

 9

Configuration management applications and roles

In IBM SmartCloud Control Desk the tools used to manage configurations are found in the IT Infrastructure and Reconciliation application groups.

Each of the configuration management roles is implemented as a security group, and start centers that provide easy access to the main tools for the role are provided.

Configuration process requests

- The activities performed by configuration management are typically based on requests:
  - Asset management
    - Can request creation, updates, audits, and lifecycle changes
  - Change management
    - May request CI creation or promotion prior to implementing a change
    - Typically request CI verification after change implementation
- Automated configuration management activities include:
  - Asset management
    - Can create generic CIs when assets are created
    - Can update key attributes based on Asset and CI synchronization
  - Change management
    - Can update CI attributes after successful change implementation

Configuration process requests

Most of the daily activities performed by the configuration management team are initiated by requests from other parts of the organization. The one activity that configuration management initiates on their own is the audit of CIs. CI audit is critical to verify the trustworthiness of the information in the CMDB, which is so critical to accurately plan changes, evaluate incidents, manage problems and so on.

Configuration items

Any component that needs to be managed in order to deliver an IT service. Information about each CI is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by configuration management. Configuration items are under the control of change management. They typically include IT services, hardware, software, buildings, people, and formal documentation such as process documentation and service level agreements.

Configuration items

CIs and assets

- Configuration items are:
  - Any component that needs to be managed in order to deliver an IT Service
  - Information about each CI is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by configuration management.
  - CIs are under the control of change management.
  - CIs typically include IT services, hardware, software, buildings, people, and formal documentation such as process documentation and SLAs
- Assets are:
  - Any resource or capability.
  - Assets of a service provider include anything that could contribute to the delivery of a Service.
  - Assets can be one of the following types: management, organization, process, knowledge, people, information, applications, infrastructure, and financial capital
  - IT assets that are managed are typically tangible, such as hardware and software licenses
- The same resources are often represented as both an asset and a CI
  - The asset is used to manage financial, contractual, and logistical information
  - The CI is used to manage the configuration of the resource including planned and unplanned changes
- Assets and CIs each represent a unique set of information, which may be linked by a few common attributes. As such, assets and CIs each represent a different side of the coin.

CIs and assets

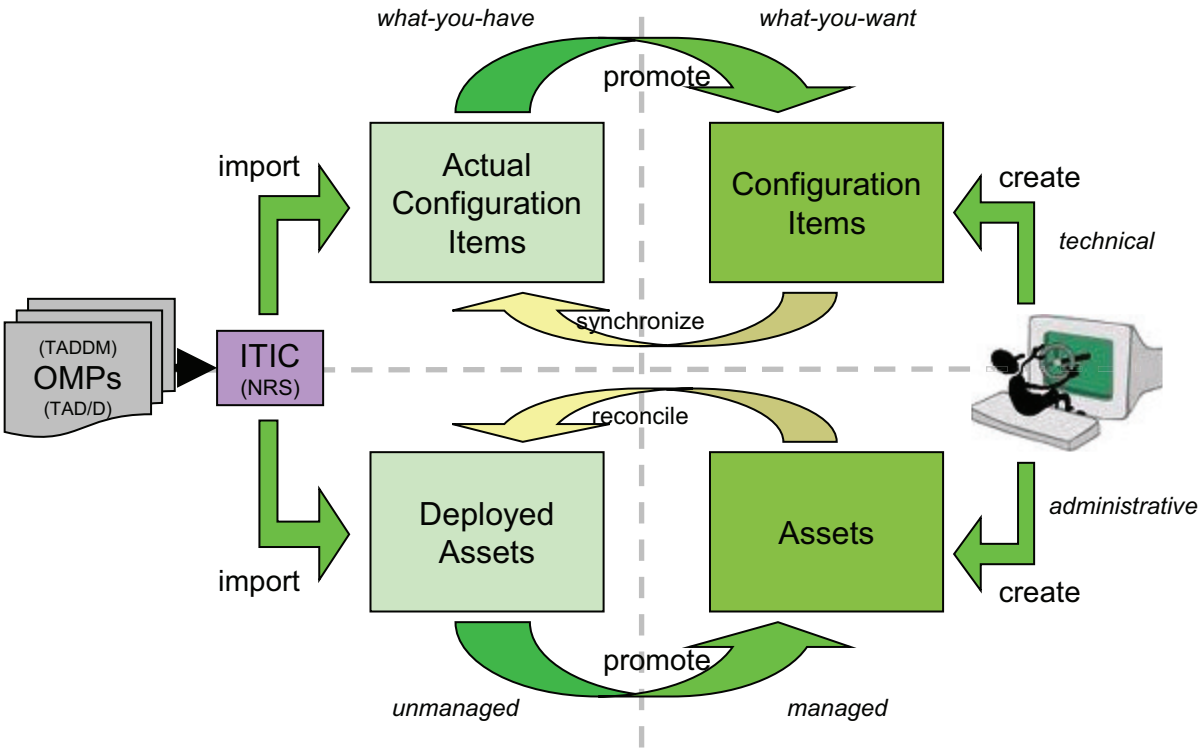
In essence, configuration management deals with management of configuration items (CIs). CIs represent the technical properties of a resource.

Administrative properties and metadata such as ownership, location, financial aspects, associated warranty or maintenance contracts, licenses and so on are all managed by the asset management team.

Naturally, both the administrative and the technical information is relevant when dealing with requests, changes, and incidents, so somehow the asset and configuration item information should be linked.

However, you must realize that for each asset, you may have thousands of related CIs. For example, a computer system can be treated as a single asset, but when looking at it through the configuration management glasses, it is made up of CIs for the computer system itself (top-level), and a lot of associated CIs that represent specific resources within the computer system. Resources such as CPU, memory, file systems, interfaces - just to name a few - are all individual CIs, for which there (rarely) are no associated assets.

Managing configuration items and assets



 13

Managing configuration items and assets

As already discussed, IBM SmartCloud Control Desk stores both active and authorized configurations - for both assets and CIs - in the CMDB, and provides facilities to promote and synchronize the two representations.

IBM SmartCloud Control Desk enables linkage of (top-level) CIs and assets I several ways:

1. Automatically, through GUIDs assigned at import (from ITIC). The GUID for a specific resource is assigned based on naming attributes, so the asset and CI records for the same resource will have the same GUID.
2. Automatically, through the periodic execution of a reconciliation task that compares specific, unique attributes (for example serial number) of the CI and asset records to identify related records.
3. Manually through the user interface.

How CIs are stored

- CIs are always associated with a classification
- Actual CIs are stored in the CMDB in accordance with the common data model
  - For each resource type the CDM defines classifications that determine:
    - Allowable attributes and types
    - Valid relationships to other actual CIs
    - Naming rules
  - The CDM classifications, attributes and relationships are preinstalled in IBM SmartCloud Control Desk, or loaded from TADDM via ITIC
- Authorized CIs are stored according to your custom CI classification hierarchy
  - Custom CI hierarchies contains
    - Custom classifications hierarchy
    - Promotion scopes that include:
      - Mappings between authorized classifications and actual classifications
      - Relationships between authorized classifications
    - Attributes for each resource type (a sub-set of the attributes defined for the actual CI)
  - Custom CI classification hierarchies are created and maintained in Deployer's Workbench

How CIs are stored

CIs, whether actual or authorizes, ad always associated with a classification. This classification, or CI Type, is used to associate the proper attributes and properties with the CI. Attributes are placeholders of configuration values, that provide the details about the configuration item.

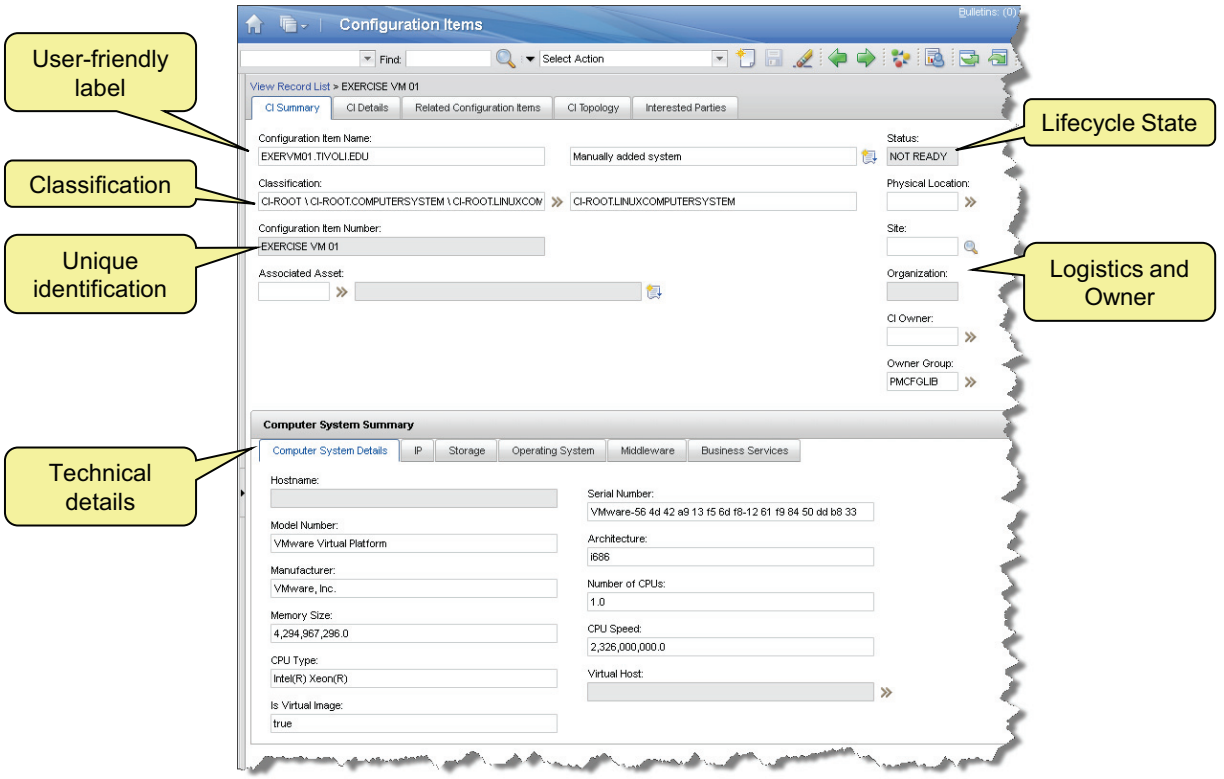
In addition, the classification also defined the valid relationships in which the CI can be a part. Some relationships, for example *runson*, are only allowed between specific classifications.

Implicitly, the classifications also determine the naming. Combinations of specific attributes are used to create a unique name of the CI. Naming rules associated with the classification defines, for each classification, which attributes in which combination should be used to uniquely identify the CI.

Actual CIs are always classified in accordance with the classification hierarchy defined in the Common Data Model.

Authorized CIs are classified in accordance with the authorized CI hierarchy of your choice. You can have several authorized CI classification hierarchies in order to differentiate between different lines of business, or customers. It is important to remember, that you cannot relate CIs in one classification hierarchy to CIs that belong to another CI hierarchy.

Configuration item summary



Configuration item summary

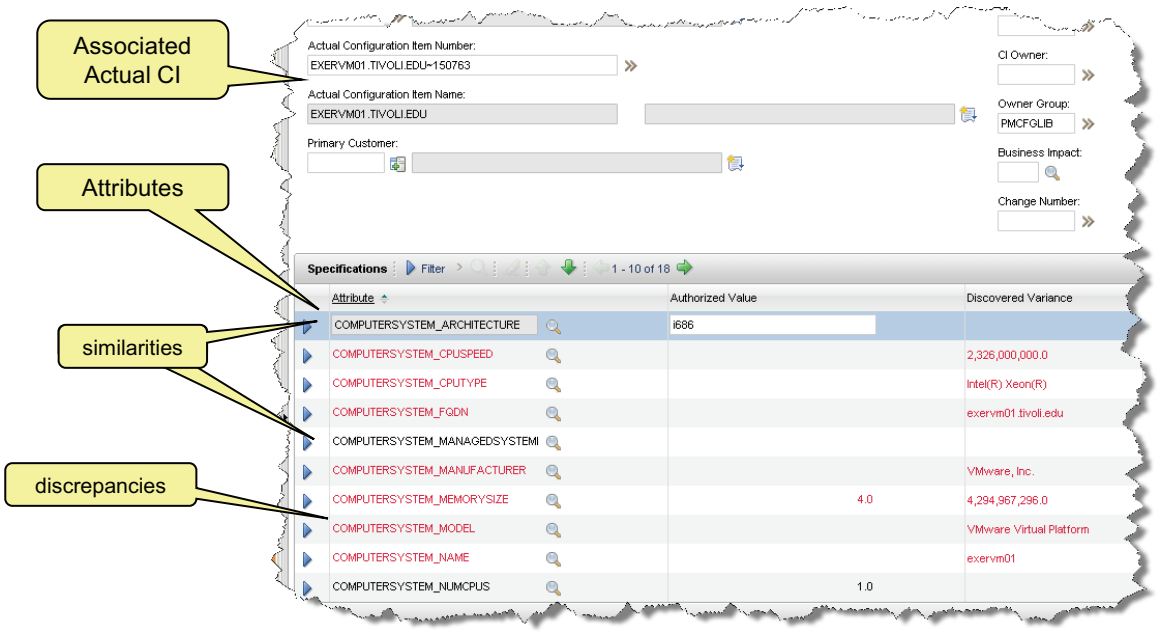
In the Configuration Items application you can see all the details for an authorized CI.

The CI Summary tab contains information that has been gathered from the attributes and metadata of the CI.

The CI Details tab shows all the attributes for the CI.

The Related Configuration Items tab shows the relationships in which the current CI is a part.

Configuration item details



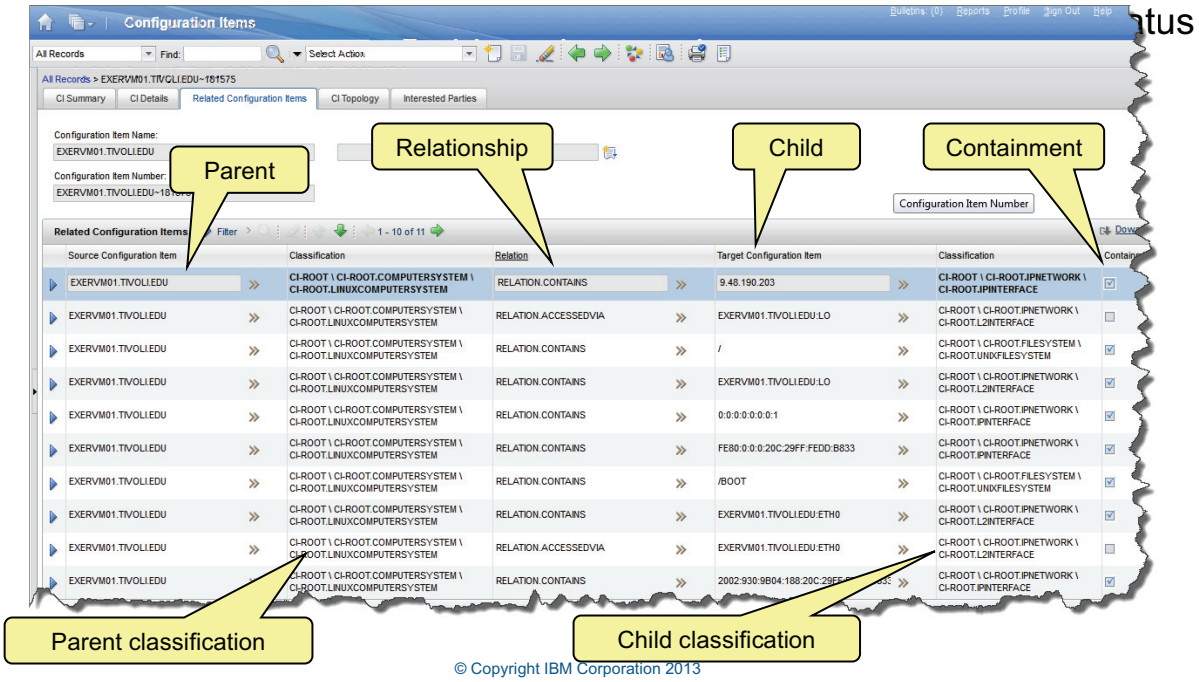
 16

Configuration item details

When looking at CI Details for an authorized CI which is linked to an actual CI, you can immediately see the discrepancies between the actual and the authorized CI.

Configuration item relationships

Configuration items are connected through uni-directional relationships.



Configuration item relationships

CI relationships are uni-directional. The Related Configuration Items shows you all the relationships in which the current CI is either the parent of the child. Remember that you only see one level of relationships.

You can drill down into the relationships for the children by opening a specific target.

Creating configuration items

- Actual CIs are created when they are imported from ITIC
- Authorized CIs can be created:
  - Manually, to represent a resource that does not yet exist
    - Population of specific attributes is not guaranteed
    - Relationships must also be created manually
  - By promoting top-level actual CIs, to represent an existing resource
    - Select attributes are populated from the actual CI
    - Relationships and related CIs are created automatically
  - By synchronizing an existing top-level CI, and include descendant CIs
  - Automatically from assets, to represent a computer system
    - A limited number of attributes are automatically populated
    - No relationships are created
- CIs are uniquely identified by the configuration item number
- Certain combinations of attributes, can also be used to uniquely identify the CIs. These combinations are identified by *naming rules*, and aids the promotion and synchronization between actual CIs and *existing* authorized CIs.

Creating configuration items

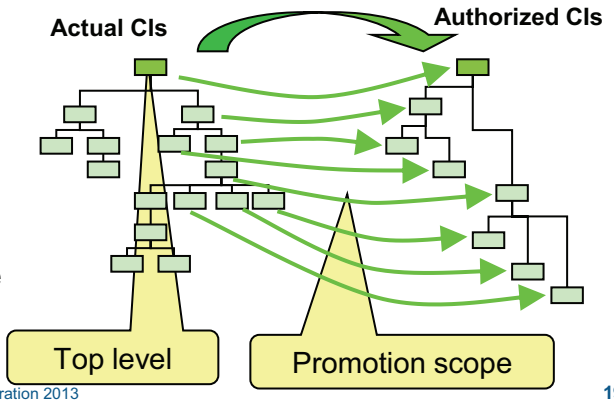
Actual CIs are created automatically when information from your discovery tool is loaded into the CMDB. If you do not use a discovery tool, actual CIs may be added by importing comma-separated or xml files. However, this is not the recommended path since the actual CI information reflects the current configuration of your data center, so by nature this information is updated very frequently. TO capture the changes to your infrastructure, you need a discovery tool that can capture all the details and relationships.

If you look closely at the description of the configuration management processes, you will not find any tasks that deals with the creation of authorized CIs.

Some organizations require change owners to submit a request for the creation of new CIs, which then are created by the configuration management team. Others allow the change owners to create new CIs as they see fit.

CI promotion

- Promotion creates or updates authorized CIs by cloning actual top-level CIs
  - Only actual CIs with a promotion scope can be promoted
  - Authorized CIs are linked to the actual CIs from which they were cloned
  - The actual CI configuration item number is used to name new CIs
  - The promotion process can leverage naming rules to identify existing CIs and link these to the actual CI
  - Identically named attributes copied to the authorized CIs
  - If any CI already exist, its attributes and relationships will be updated
- Promotion scopes are used to identify all related CIs that will be included, and map them to authorized classifications
  - Promotion scopes contain the mapping between actual and authorized CI classifications, as well as relationships to be created between the authorized CIs.
  - Think of a promotions scope as a template for authorized CI structures.



CI promotion

Authorized CIs are most commonly created by promoting actual CIs. During promotion, the actual CI classification is mapped to the desired authorized CI classification by means of a promotion scope. Only actual CIs for which one or more promotion scopes have been defined for the classification can be promoted.

Through the promotion scope, the actual CI is mapped to a particular classification in the authorized CI classification hierarchy, and anew resource of that type is created. The attributes for the new authorized CI are then cloned from the actual CI. Then, the relationships for the authorized CI classification are used to analyze if the actual CI has descendants that of the correct classification that are related through a similar relationship. If this is true, the child actual CI is promoted as well.

If the classification of the child that was promoted also has a promotion scope associated, this promotion scope will no be used to analyze if any more children should be promoted.

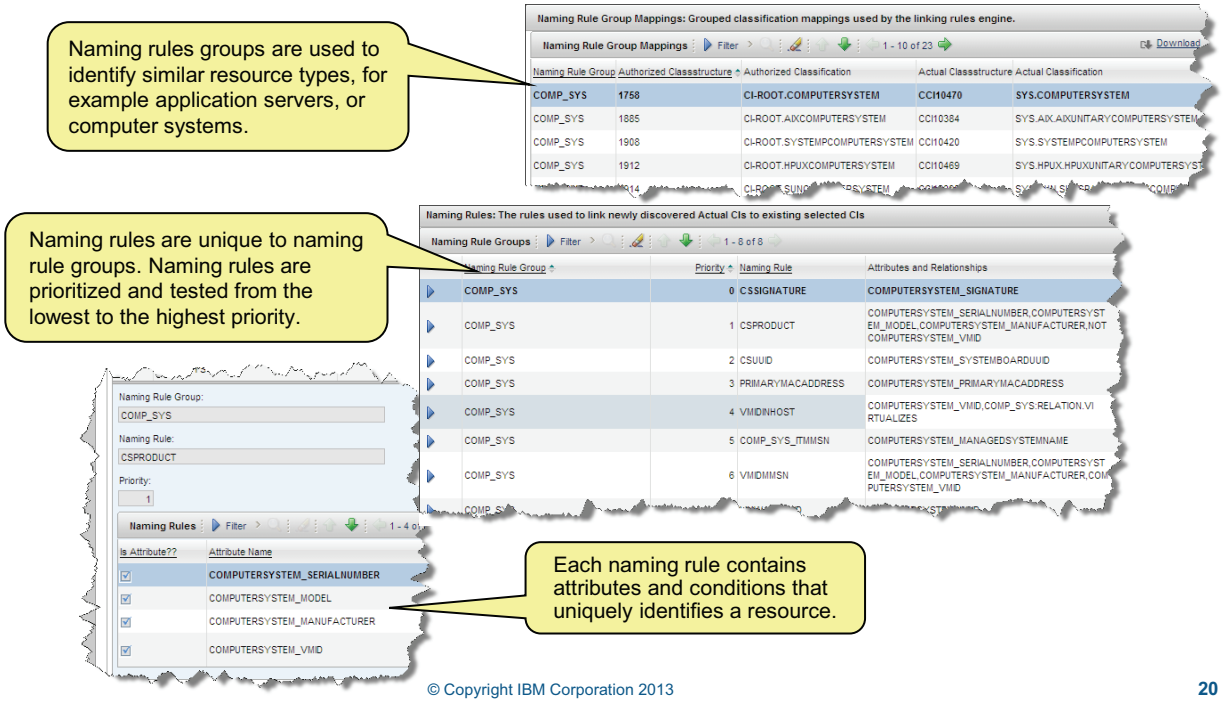
This behavior allows you to create many, related authorized CIs by promoting just a single actual CI. For example, using the default classification hierarchies that come with IBM SmartCloud Control

Desk, promotion of a business application will lead to the creations of the following types of authorized CIs (provided the actual CIs exist):

- Application
- Web Server (Apache, SunOne, IBM HTTP Server , etc.)
- Application Server (WebSphere Application Server, Tomcat, WebLogic, etc.)
- Database Server (DB2, Oracle, SyBase, etc.)
- Operating System
- Computer System
- IpInterface
- IpAddress
- And many more

Naming rules

Naming rules can be used in the promotion and linkage processes to identify existing resources based on combinations of attributes values.



 20

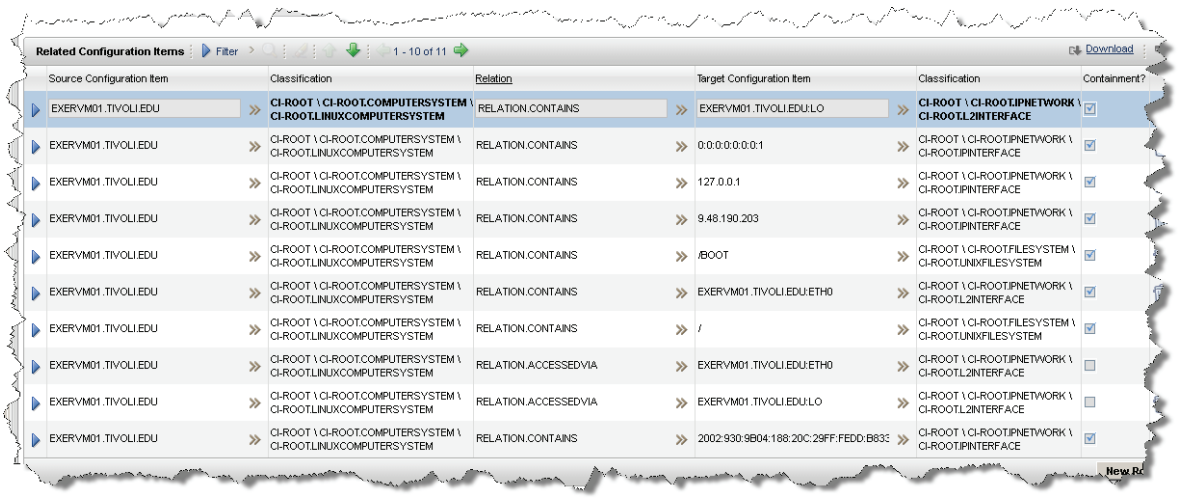
Naming rules

If you have created a new authorized CI, and provided values for a couple of key attributes, you can use the synchronize function to identify the actual CI for your resource if it exists.

Under the covers, IBM SmartCloud Control Desk uses the promotion scopes and naming rules to find the actual CI. The promotion scope that points to the classification of the authorized CI is used to find the classification of the actual CI to locate, and a combination of attributes from the authorized CI is used to find the correct actual CI that has the same values for the attributes.

Related configuration items

- Shows the immediate child configuration items for a CI
  - Indicates how the children are related to the CI
  - Indicates whether or not the child is *contained* in the CI



Related configuration items

The relationships that are allowed for an authorized CI, are also defined at the classification level.

Relationships are defined for all valid combinations of classifications in which CIs of the specific classification can be either the source (parent) or the target (child). Remember, relationships are unidirectional.

Relationships have a couple of properties, that determine how IBM SmartCloud Control Desk treats the relationship. The most important property is the Containment property.

The relationship properties and their meaning are:

Containment — Determines if the target of the relationship is treated as an individual CI, or as a member of the source CI.
This property is used to automatically perform the same actions on the target CI as the parent CI.
For example, if you change the lifecycle status of a source CI, the lifecycle status of all the target CIs that are related to the source CI through a relationship for which the contains property is true, will also be changed.

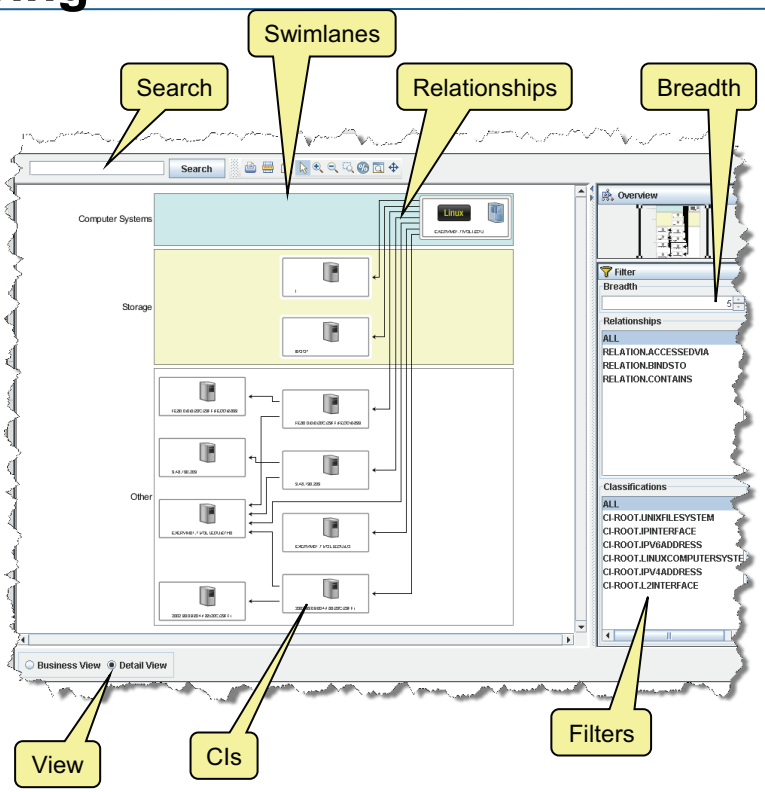
Target-is-parent	This property is used to create a (hidden) relationship in the reverse direction of the original relationship. This hidden relationship is used by the containment setting to allow IBM SmartCloud Control Desk to traverse the relationships top-down. For example, the runsOn relationship between an OperatingSystem and the ComputerSystem classifications points from the Operating System to the ComputerSystem. This means that the OperatingSystem cannot be included in the ComputerSystem (using the containment setting) so when the ComputerSystem is promoted, so is the OperatingSystem. However, if target-is-parent is true, IBM SmartCloud Control Desk assumes that a relationship exists between the ComputerSystem and the OperatingSystem, and this relationship can now be used to find the OperatingSystem to promote along with the ComputerSystem.
Cardinality	Specifies the nature of the allowed number of instances of the relationships between the CI and its targets. Valid values are: one-to-one, one-to-many, many-to-one, many-to-many. For example, the installedOn relationship between the OperatingSystem classification and the ComputerSystem classification is may-to-one. This means that you can install as many copies of an operation system as you like on a single computer system. On the other hand, the runsOn relationship between the same classifications has the one-to-one cardinality because you can only run one operating at a time on a computer system.
Propagate Change	This option is used to propagate changedDate and changedBy information to a parent if a CI is updated. If, for example, the name attribute of an IP address CI is modified, and the Propagate Change option is set, the changedBy and changedDate attributes of the CIs that use this IP address (computer systems, operating systems, application servers etc.) will e updated as well.
Imported	This option indicates if the relationship was imported from an external source or not. This is typically applies to relationships between actual CIs, as the relationships are imported from the CDM.

CI topology mapping

Visualizes the CI and its related CIs.

- Custom and Business views
  - CI Classification is used to determine if a CI is shown in the Business View
  - Business Views are built by the TopologyCacheCron cron task.
  - Actual CI topologies do not support the Business View
- Max 200 resources

  `pmgui.citopology.maxnodes`
- Level of relationships to follow (breadth) can be adjusted
- Organized in swim lanes
  - Classification groups are related to specific lanes
  - Similar resource types are grouped in classification groups
  - Swim lane assignments, color, and label can be customized
- From the topology you can jump directly to another CI



 22

CI topology mapping

When looking at CIs, you can (if your assigned role is properly authorized) see the CI Topology.

The CI Topology used the IBM SmartCloud Control Desk topology viewer to visualize the relationships between a CI and its related CIs.

The Topology Viewer allows you to view both business and detail view, and provides controls to filter and expand the topology.

Configuration item history and baselining

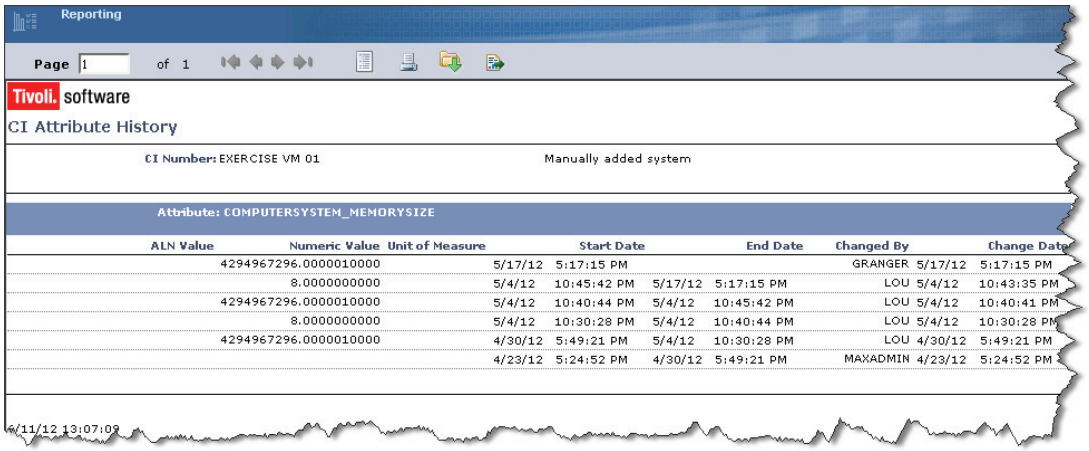
A baseline is "*a snapshot that is used as a reference point. Many snapshots may be taken and recorded over time but only some will be used as baselines. For example:*

- *An ITSM baseline can be used as a starting point to measure the effect of a service improvement plan*
- *A performance baseline can be used to measure changes in performance over the lifetime of an IT service*
- *A configuration management baseline can be used to enable the IT Infrastructure to be restored to a known configuration if a change or release fails."*

Configuration item history and baselining

Attribute and relationship history

- During the life of a CI, you can see the history of both attributes and relationships.
- This information is available in the console, as well as a report.
- This allows you to identify when specific changes was applied to the CI, which may be very helpful when troubleshooting technical issues.



Attribute and relationship history

As a CI matures, relationships may be added and removed, and attribute values may change. Updates to relationships typically imply that other CIs have been added or removed.

IBM SmartCloud Control Desk keeps track of the changes to CI configurations, including attribute values and relationships.

The history is available from the user interface as well as in reports that provides the full configuration history for a specific period in the life of the CI.

Removing CIs

- Authorized CIs can only be deleted from the CMDB if:
  - The current status of the CI, also known as the lifecycle state, is not protected.
  - The CI is not included in a baseline.
  - The CI is not, and has never been, related to a process request.
  - The CI is not, and has never been, the target of a change or configuration work order.
- From the Console, actual CIs cannot be removed
  - The only way to remove actual CIs is to enable ITIC to create records in the ‘To be deleted’ table, and remove them through an escalation/action pair.

Removing CIs

A fundamental feature if ITIL, and of IBM SmartCloud Control Desk, is, that the history for a CI is kept in the CMDB to provide an audit trail of the entire life of the resource.

At some point in time you may want to remove the CI, however, this would cause the history, which may need to be kept for legislative reasons, to be deleted to, so IBM SmartCloud Control Desk does not allow that.

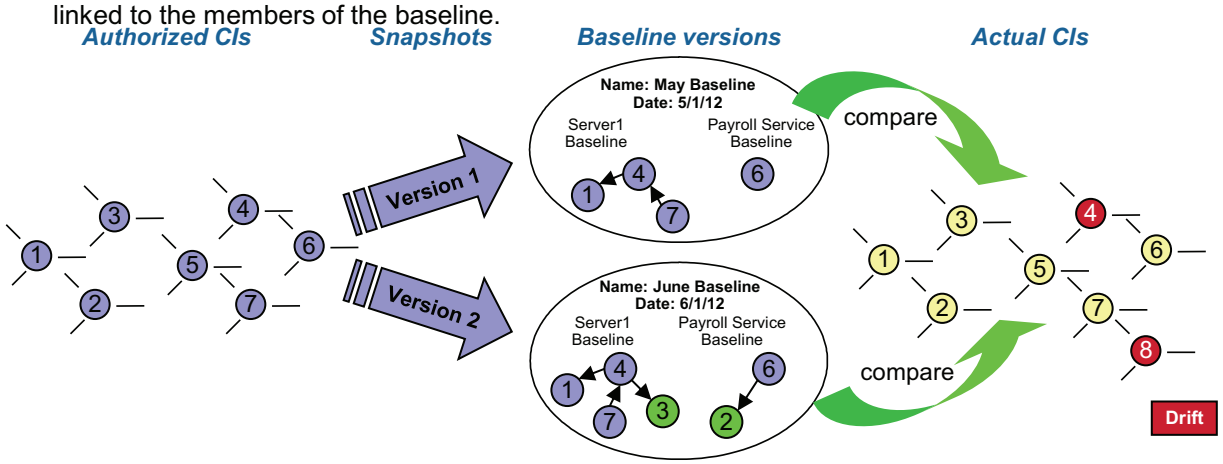
In general, IBM SmartCloud Control Desk does not allow you to delete CIs, that have been manipulated on way or another, to be deleted. Only pristine, authorized CIs can be deleted from the CMDB.

This deletion can be performed by the configuration management team members using the user interface.

Actual CIs can never be deleted manually. If a CI has been deleted from the database used by your discovery tool, the corresponding actual CI will be marked for deletion at the next actual CI load. Based on your preferences, you can then activate a background task, which removes all the actual CIs that have been marked for deletion.

Baselines

- A configuration baseline is a snapshot that represents an authorized (approved) configuration at a particular point in time.
- Multiple CIs can be members of a baseline.
- Baselines can at any point be compared to the current configuration of the actual CIs that are linked to the members of the baseline.



- Using baselines, you can quickly detect changes to your approved configurations.
- The changes you can detect are additions and deletions of CIs as well as modifications to CI attributes and relationships.

Baselines

When you deploy a new application system, you basically implement a large number of CIs. CIs for computer system (physical or virtual), operating system, web servers, application servers, clusters, databases, software modules, as well as all the CIs that represent the detailed configuration. Depending on the size and complexity of your application, this can literally be hundreds of thousands of new discovered CIs. After loading of actual CIs, many of these CIs will be registered in the IBM SmartCloud Control Desk CMDB as actual CIs, and depending on your processes and procedures the subsequent promotion used to create the authorized CI you use to manage the application system will create a significant number of authorized CIs. To see the topology of the application, you would use the topology viewer.

At this point in time you may want to capture a snapshot of the application and all its related CIs. This snapshot is called a baseline. The baseline documents the configuration of the application system (CIs, attributes and relationships) as it existed when you created the baseline.

As time passes, new application functionality may be added, other applications may start using services that are provided by the new application, the application infrastructure serves may be reconfigured to optimize performance, and the application itself may require more or less

resources to deliver its services in accordance with the SLA. In other words, it is highly likely, that over time the application configuration (as well as the topology) changes.

At any point in time, you can compare the current configuration, as it is represented by the actual CIs, to the baseline. This provides a list of initial and current CIs that are (or was) part of the application. This list will highlight discrepancies between the original baseline, and the current configuration, so you can identify how the application has drifted, since it was originally deployed.

Baseline information is particularly valuable to assess if you are using the correct information to staff application support, generate billing information, and whether your event automation needs to be modified to include events from resources that have been added or removed.

IBM SmartCloud Control Desk allow you to keep multiple baselines for the same CIs, so you can compare several versions of the application configuration.

Creating a baseline

- When creating a baseline, members can be included from:
  - All available CIs
  - Collections
  - Other baselines
  - CIs related to selected member CI
  - Child CIs of selected top-level member CI
    - For example, to add all resources that take part in provisioning a business application,
    - Add the top-level application from All available CIs
    - Add all children using Child CIs of Selected Top-level member CI
- When a baseline is activated, the current member configurations are captured, and the baseline can no longer be modified.
- To update the baseline, create a new version, and perform your alterations before you activate it.

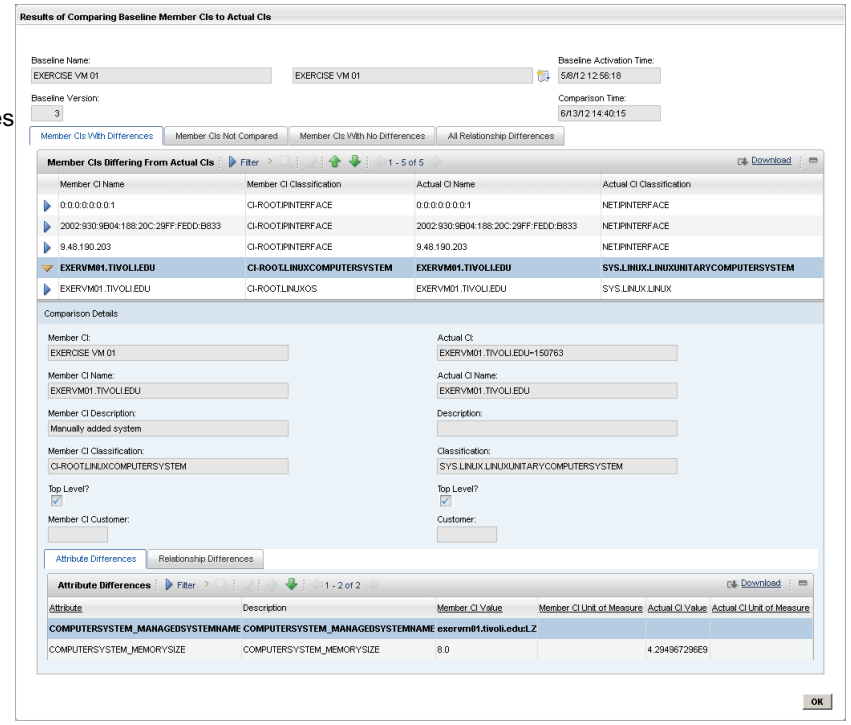
Creating a baseline

To create a baseline, all you do is to include the CIs that you are interested in, decide if children should be included, and save the baseline.

To create a new version of the baseline, you can reuse the definitions, and simply create a new version.

Comparing baselines to actual CIs

- Comparing a baseline to the actual CIs, you can see:
  - Member CIs with Differences
  - Member CIs Not Compared
  - Member CIs with No Differences
  - All Relationship Differences
- For members CIs with differences, you can see:
  - Attributes with different values
  - Discrepant relationships
- Unfortunately there is no facility available to compare baseline versions.



Comparing baselines to actual CIs

At any point in time, you can compare the baseline to the current actual configuration, as it is represented as actual CIs in the IBM SmartCloud Control Desk CMDB.

You can also use the reporting feature to create reports that can be distributed to a wider audience, and users that do not have access to the IBM SmartCloud Control Desk user interface.

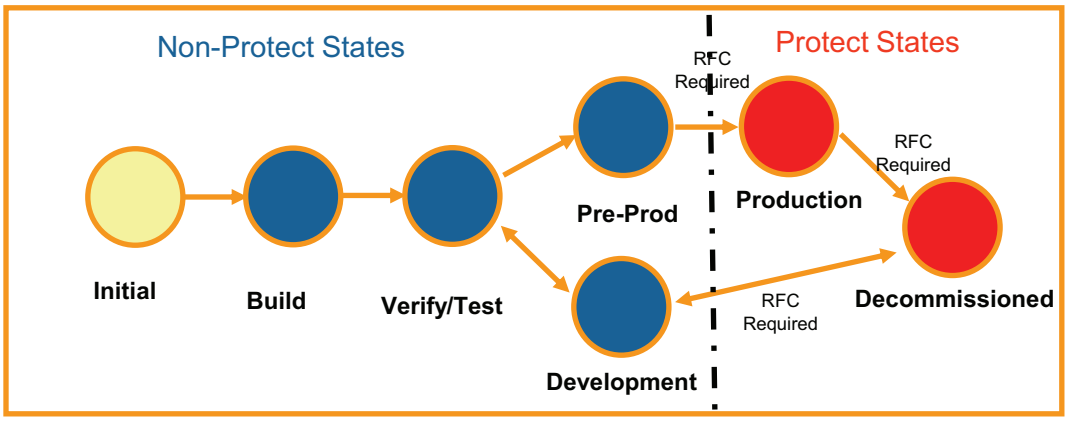
Lifecycle management

The various states in the life of an IT service, configuration item, incident, problem, change, etc. The lifecycle defines the categories for status and the status transitions that are permitted. For example:

- *The lifecycle of an application includes requirements, design, build, deploy, operate, optimize*
- *The expanded incident lifecycle includes detection, diagnosis, repair, recovery and restoration*
- *The lifecycle of a server may include: ordered, received, in test, live, disposed, etc.*

Lifecycle management

Configuration item lifecycle management



- A lifecycle can be described as the various stages in the life of a configuration item. Therefore, it can be used to identify and manage the configuration items.
- A lifecycle defines a set of ***states*** and authorized ***transitions*** that occur between them. Every lifecycle must have one state designated as the ***default*** state, and states can be defined as protected.
- Transitions involving ***protected*** states must be associated with a change request.
- Each CI classification can be assigned one lifecycle.
- IBM SmartCloud Control Desk supports the use of multiple lifecycles and customizable lifecycles.

 30

Configuration item lifecycle management

Lifecycles are used to associate information about the operational state of an authorized CI. The state provides information about how the resource is currently used.

Lifecycles are assigned to authorized CI classifications, not individual CIs.

Lifecycles define the states. In addition, the lifecycle definition contains valid transition paths that dictate how a resource can move from one state to another. These transitions can be used to control how the resource is being handled when certain, predefined events occur.

Image a server that is used for a production workload. It would be in the lifecycle state named Production. When the server is no longer needed in production, it should be cleaned up, sw licenses should be released so they can be used by other CIs, and the asset and accounting information should be updated. By placing the resource in a state, for example named PostProduction, processes can be initiated to ensure that the cleanup takes place. Only after the cleanup has been completed, the resource can be moved to the Available state, so it can be reused for another project. In this simple scenario, you would define transitions from Production to PostProduction, and from PostProduction to Available. Naturally you can react on this

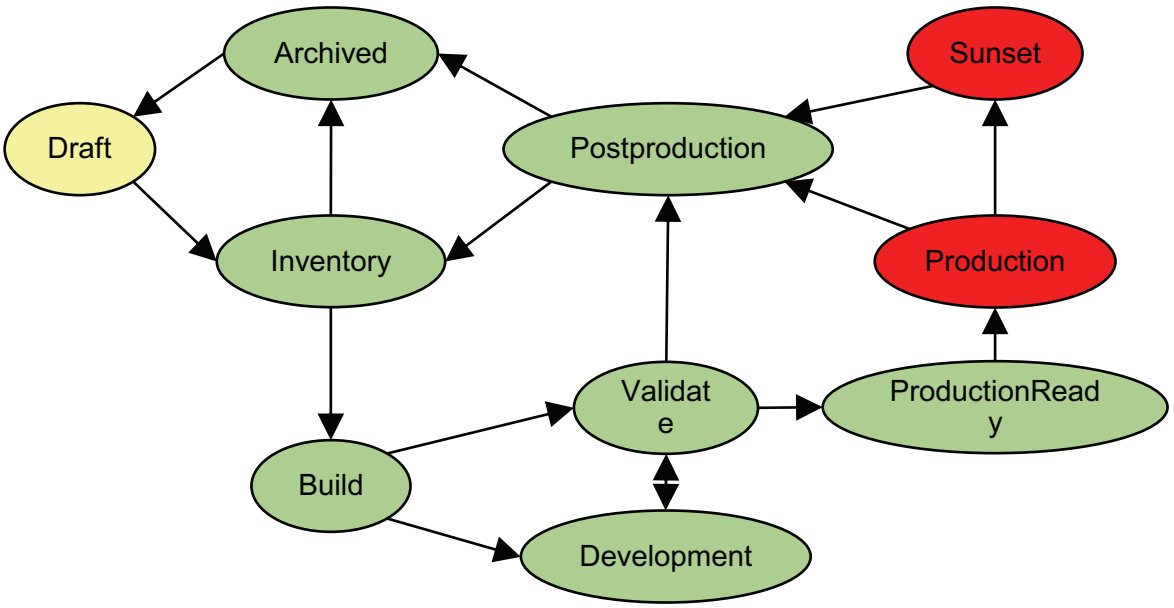
automatically, so you can trigger the cleanup process as soon as the state is changes to PostProduction.

Lifecycle states may be protected. For CIs that are in a protected state, it is required that changes are authorized. This provides an assurance that the changes have been properly reviewed, and that someone, with the proper authorization, has approved the change implementation. In addition, to transition into or away from a protected state, you must provide a valid change number.

Typically, you only define lifecycles for the classifications that represent your top-level resources. By means of the containment attribute of relationships to descendants of the top-level resources, the lifecycle state of the descendants will be updated when you change the lifecycle state of the top-level CI.

The ITIL CI lifecycle

The ITIL lifecycle that is preinstalled in IBM SmartCloud Control Desk supports all the statuses and transitions defined in ITIL V3.



The ITIL CI lifecycle

ITIL defines a comprehensive lifecycle that allows you to control almost any transition in the life of a resource. For each state, special processes can be invoked in order to perform checks and validations, ensure proper accounting and licensing, prepare operational procedures and so on.

Each organization is different, so the exact meaning of the states and the processes that will be performed on a resource in a particular state varies. You must apply your own interpretation, or create lifecycles that meet your particular needs.

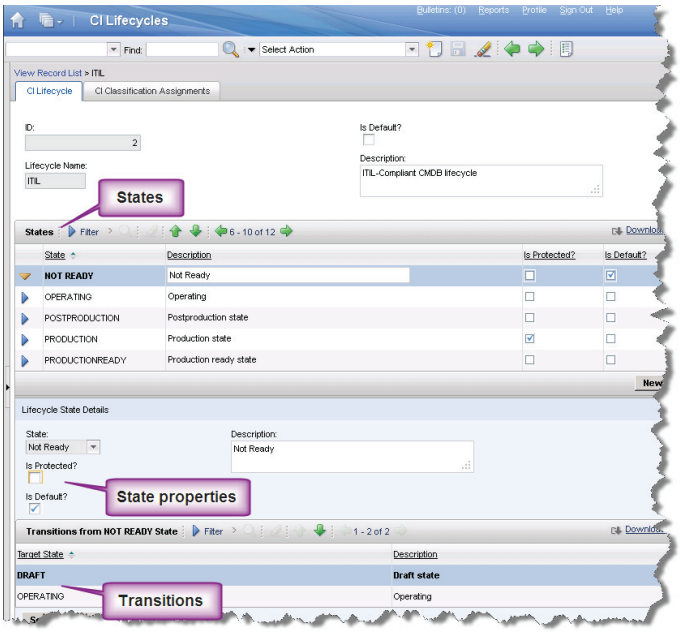
When an authorized CI is created, it is given the state that is defined as the default state for the lifecycle that is assigned to the classification. If no lifecycle is defined for the CI classification, the default lifecycle is assigned.

Working with lifecycles

Access the CI Lifecycles application from Go To > IT Infrastructure > CI Lifecycles

Each lifecycle contains:

- States
- State properties
  - Is Default?
  - Is Protected?
- Transitions
  - Defines a valid path to a new state from the current state



Working with lifecycles

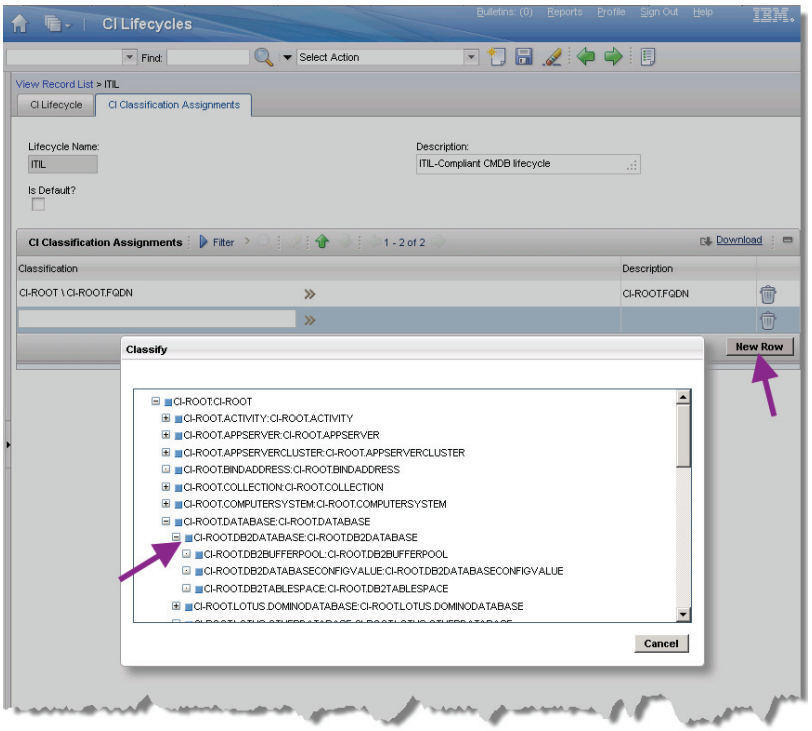
Lifecycles are defined in the IBM SmartCloud Control Desk user interface.

First you define the stated, and then you can apply transitions.

Once the lifecycle is defined, you can apply it to the authorized CI classifications, or individual CIs of your choosing.

Assigning lifecycles to CI classifications

- Lifecycles are assigned to CI classifications, not to individual CIs.
- Use the CI Lifecycles application to assign lifecycles to classifications.
- Classifications for which containment relationships exist should be assigned the same lifecycle, or lifecycles with the same states and transitions.



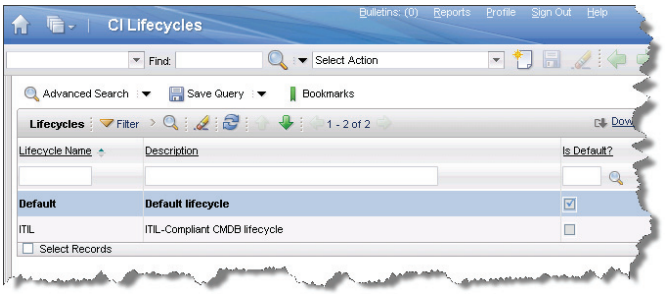
Assigning lifecycles to CI classifications

Lifecycles are assigned to CI classifications - not to individual CIs.

When assigning lifecycles, it is important to remember that descendant CIs (or classifications) should have the same lifecycle assigned - or as a minimum, a lifecycle that contains the same states and transitions. When the state changes, the state of descendent CIs (for which a containment relationship exists) is also changed, and if the new state, or the transition, is not represented in the lifecycle of the descendant CI, the update will fail.

Default lifecycle and state

- When CIs are created, they will automatically be assigned the default state from either the lifecycle associated with their classification, or the default lifecycle.



  - When you change the state of a CI, the states for all descendants that can be located through *containment* relationships will be changed too.

  - When changing the lifecycle associated with a CI classification, you must ensure that the new lifecycle contains the currently assigned state, and a transition to the new state you want to apply.

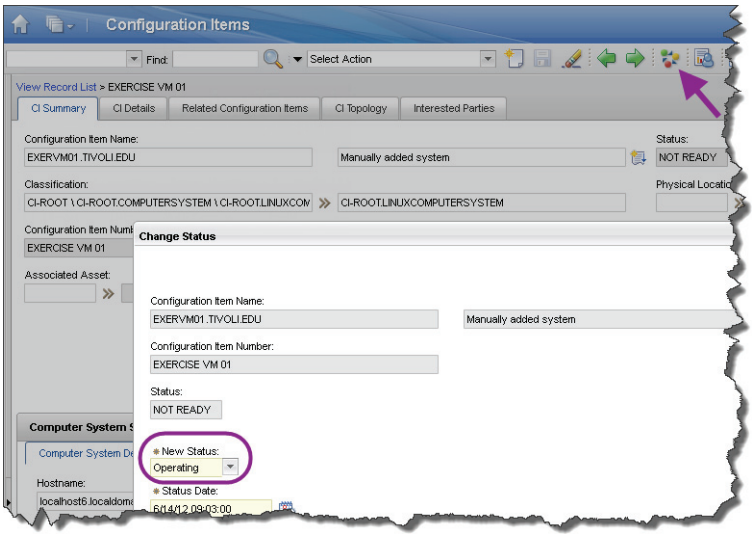
Default lifecycle and state

When creating authorized CIs it is the responsibility of the change management team to ensure that the appropriate lifecycle and state is assigned.

If no specific state is provided, the default state for the lifecycle associated with the classification is applied to the CI. If the classification is not associated with a lifecycle, the default lifecycle is used.

Changing the CI status

- Use the change status function ( ) in the Configuration Items application to change the status of a CI and its *contained* descendants.
- You can only choose new states that, in the lifecycle, are related to the current state through a transition.
- If you are transitioning in to or out from a protected state, you must provide a change number.
- For CIs in the same state, you can use multi-row operations to change the state of multiple CIs in a single operation.

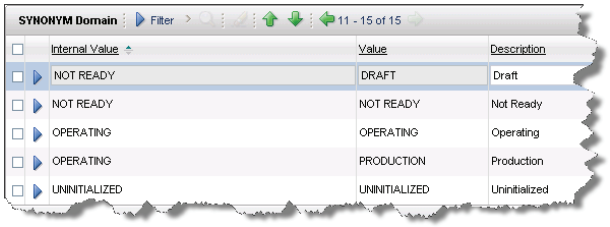


Changing the CI status

In the IBM SmartCloud Control Desk user interface, the lifecycle state of an authorized CI is known as the **status**.

Adding new lifecycle states

- IBM SmartCloud Control Desk 7.5 includes 15 available lifecycle states:
  - 5 System Management Platform default states
  - 10 ITIL-compliant states
- Users can define their own lifecycle states using the Domains application by adding them into the CISTATUS domain.
  - When adding new lifecycle states, you must use existing internal values in the domain.



  - Once the states are defined in the CISTATUS domain, they can be applied to a lifecycle.

Adding new lifecycle states

IBM SmartCloud Control Desk provides 15 predefined lifecycles states. These are all defined in the CISTATUS domain.

To add custom states, apply the new names to the CISTATUS domain, before you start defining the lifecycle, its states, and transitions.

Configuration item reconciliation

- IBM SmartCloud Control Desk provides a set of reconciliation functions that enable you to identify resource pairs that share common attribute values:
  - Authorized-actual CI pairs
  - Authorized-deployed asset pairs
- Reconciliation can be used to link active and authorized resources that otherwise are not logically related to one another.
- Based on this linkage you can automate actions such as synchronization or promotion.
- The reconciliation tasks identify successful matches as well as discrepancies and variances between two sets of data.

Configuration item reconciliation

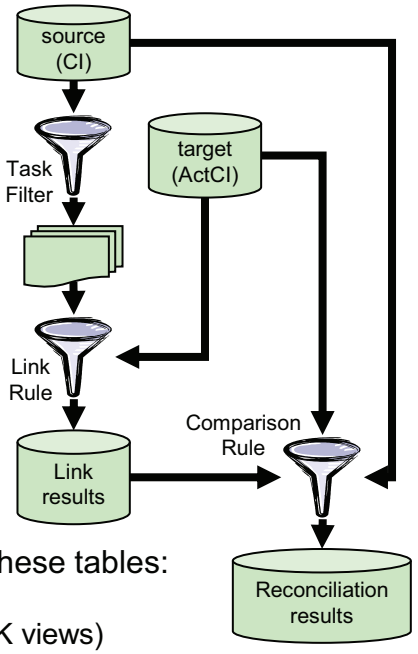
The basic functions used to link and compare actual and authorized resources in IBM SmartCloud Control Desk is that of the reconciliation task.

Reconciliation tasks provide the mechanism used to perform CI Audit, which is important to ensure that the CMDB can be trusted.

CI reconciliation

- When defining a reconciliation task, you can control the operation of the reconciliation through application of:

Task filter	Defines the subset of source resources (authorized) to analyze.
Link rule	Identifies a source attribute to match with a specific target attribute.
Comparison rule	Defines how to compare objects or attributes of a child or parent object in one data set with a child or parent object in another data set. A special *Full CI Comparison* rule also includes relationship comparison.
Schedule	Allows you to specify the frequency with which the reconciliation task is executed.



- The results from the reconciliation task are provided in these tables:

Linkage	RECONLINK (or RECONASSETLINK and RECONCILINK views)
Results	RECONRESULTS (or RECONASSETRESULTS and RECONCIRESULTS views)

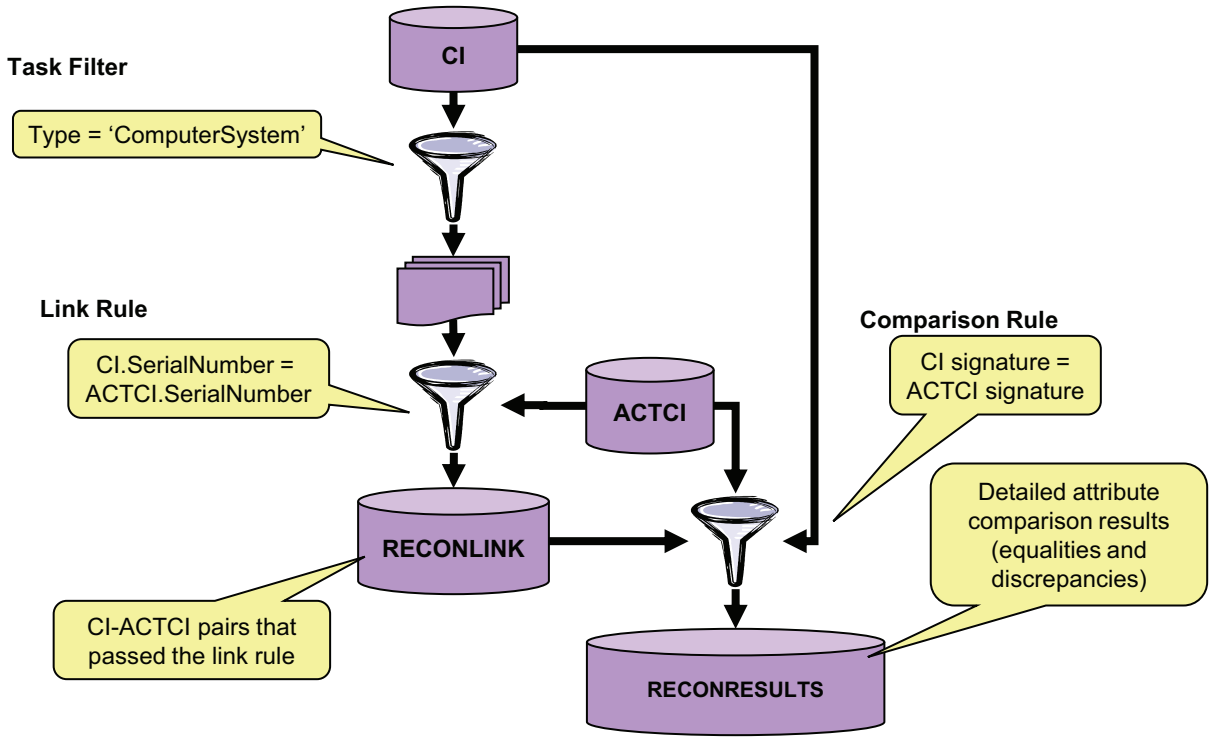
CI reconciliation

Reconciliation tasks are used to compare authorized and actual resources. The starting point is always the authorized resources, because they represent the resources you are actively managing.

When a reconciliation task has been activated, this happens:

1. The schedule determines when the reconciliation task is started.
2. The source records (authorized) are read, ad filtered based on the optional task filter.
3. For each authorized record identified by the task filter the link rules are applied to identify an actual resource that matches the authorized. Link rules use classifications and attributes to identify matches. The results are stored in the RECONLINK table.
4. When matches has been identified, the comparison rule is invoked to analyze the configurations (attributes and relationships) of the matching authorized-actual pair, and identify similarities and discrepancies. Results are stored in the RECONRESULTS table.

A reconciliation example



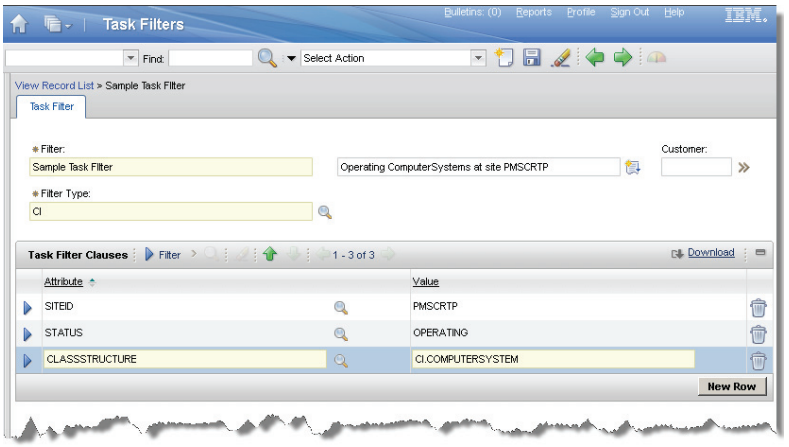
 39

A reconciliation example

This example, that compares authorized CIs to actual CIs, illustrates how to apply a task filter that includes only authorized ComputerSystem CIs. Then the SerialNumber attributes are used to identify actual CIs that will be linked to the authorized CIs, and finally the signature attributes are analyzed.

Task filters

- Task filters use resource metadata property values to limit the number of records to process.
- Task filters are managed through the Go To > Administration > Reconciliation > Task Filters application
- Valid metadata properties are:
  - CINUM
  - CLASSSTRUCTURE
  - COLLECTIONNUM
  - ITEMNUM
  - LOCATION
  - ORGID
  - SERVICE
  - SERVICEGROUP
  - SITEID
  - STATUS
  - WONUM



- Only one (optional) task filter can be applied to a reconciliation task

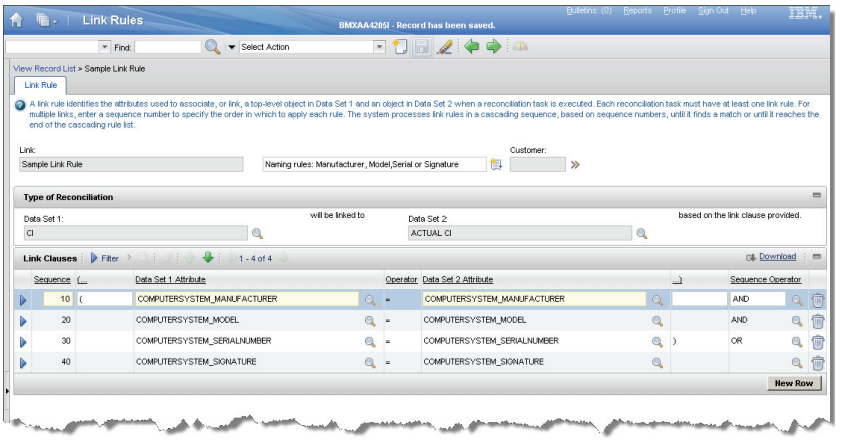
Task filters

Task filters are used to filter the authorized resources, so that only a specific subset of authorized resources is analyzed.

For CIs only a specific set of authorized CI metadata can be used in the filter.

Link rules

- Link rules define how to identify target resources that match a source resource included by the task filter.
- Link rules are managed through the Go To > Administration > Reconciliation > Link Rules application.
- Link rules contain one or more link clauses that when 'true' are used to identify resources that are linked.
- Attributes to use in link clauses may be selected directly from the source and target datasets, or by resource type (classstructure) from the related specification table.



- At least one Link Rule must be associated with a reconciliation task

 41

Link rules

Link rules are used to define the classification-attribute pairs that are inspected in order to identify matches.

Each link rule may contain multiple link clauses (combinations to inspect)

Multiple link rules can be applied to a single reconciliation task.

The results of the linkage are stored in the RECONLINK table (also accessible through the RECONASSETLINK and RECONCILINK views) which can be used in queries.

Comparison rules

- Comparison rules are used to specify which results to report (comparison of attributes).
- Comparison rules are managed through the Go To > Administration > Reconciliation > Comparison Rules application.
- If no comparison rule is specified, nothing will be compared or reported.
- For CIs, a special *Full CI Comparison* option is available. This compares all attributes as well as all relationships.
- Comparison rules can include:

Data Set 1 filter	Enables further filtering on input records
Data Set 2 filter	Enables filtering on records to find matches

and MUST include on of:

Full CI Comparison	This compares all attributes as well as all relationships.
Matched Found	Specifies the ratio of source resource instances to target resource instances to look for in the comparison.
Attribute Equality	Specifies how to compare a source attribute (or attributes of a child or parent object in Data Set 1) with a specific target attribute (or attributes of a child or parent object in Data Set 2)

- One or more (optional) comparison rules can be associated with a reconciliation task

Comparison rules

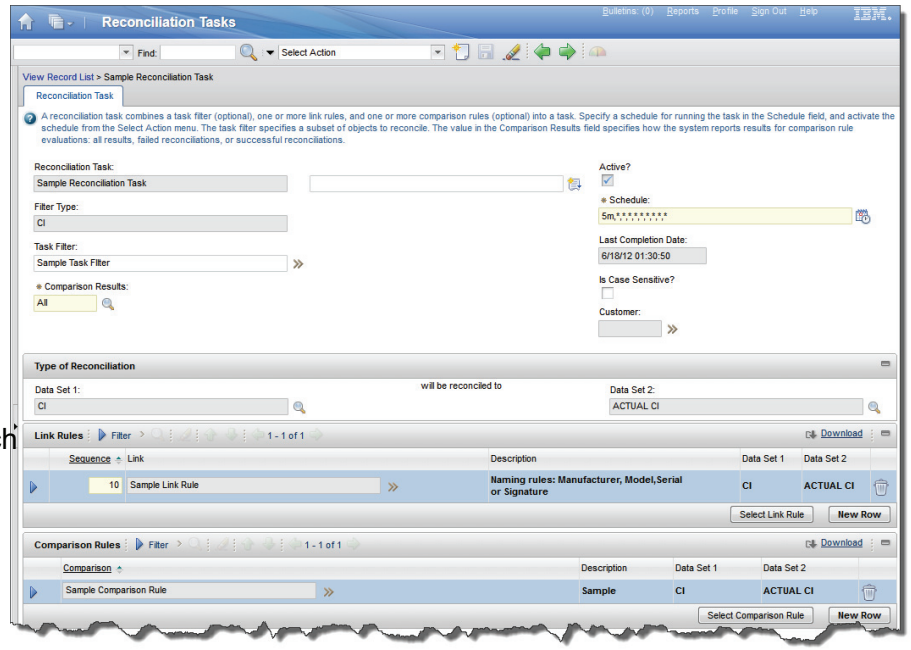
The comparison rules define to the reconciliation task, which configuration details to analyze in detail, in order to find discrepancies between the authorized and actual CIs.

For CI Audit, you will use the Full CI Comparison option.

Comparison results are stored in the RECONRESULTS table (also accessible through the RECONASSETRESULTS and RECONCIRESULTS views).

Reconciliation task definition and scheduling

- The reconciliation task references:
  - Task Filter
  - Link Rules
  - comparison rules (optional)
- In addition, the reconciliation task definition includes:
  - Schedule
  - Specification of which results to generate (SUCCESSFUL, FAILED, ALL)
  - Activation switch



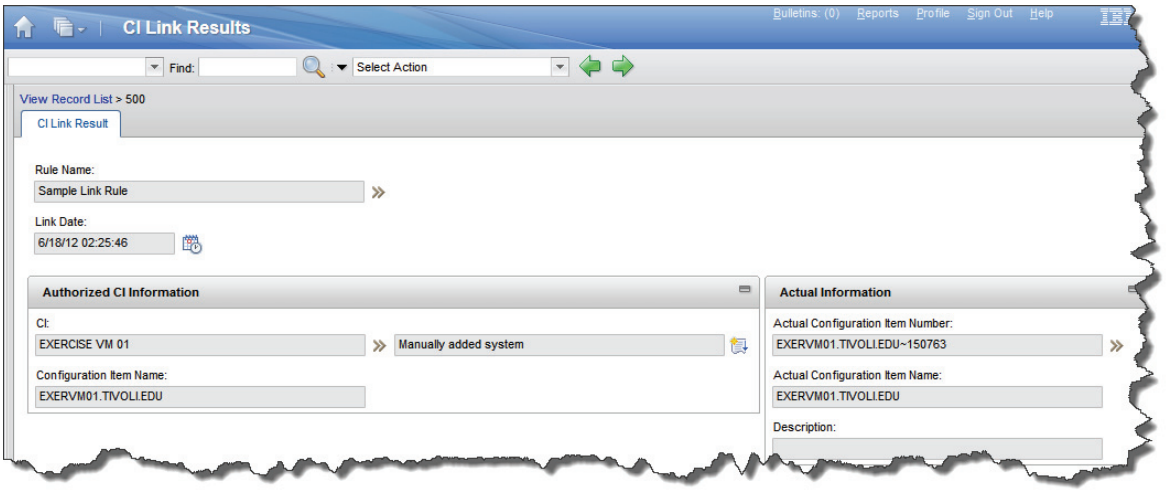
Reconciliation task definition and scheduling

Reconciliation tasks are scheduled, so they run periodically. There is no option to only run a task once, except deactivating the task after it has run once.

Notice that the reconciliation task must be activated before it will be executed. Under the covers, activation creates an instance of the ReconciliationCronTask cron task.

The CI Link Results window

- Shows the successful link results based on the Link Rule
  - CIs for which no links were found are shown in Reconciliation Results
- Accessible through Go To > Administration > Reconciliation > CI Link Results
- Links are stored in the RECONLINK table, and can be used to trigger automated operations through escalation/action definitions

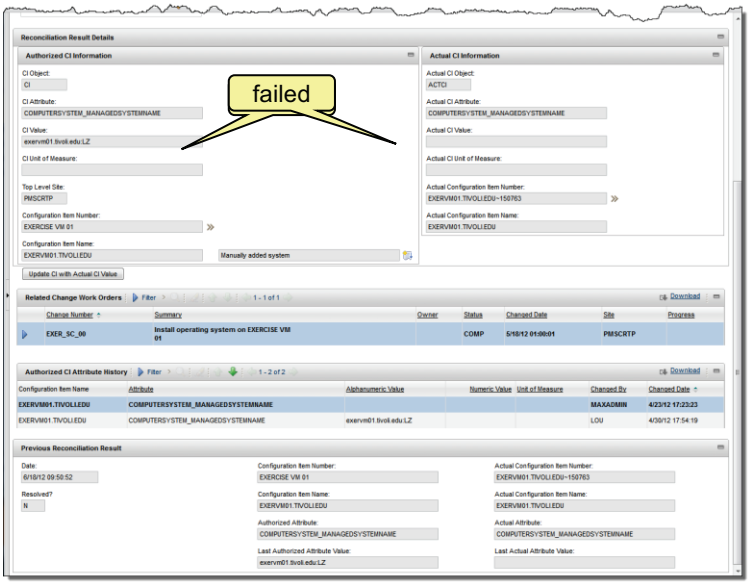


The CI Link Results window

The link results can be access through the IBM SmartCloud Control Desk user interface.

The Reconciliation Result Details window

- Shows the results from the reconciliation task as specified in the task definition.
- Access the results from Go To > Administration > Reconciliation > CI Reconciliation Results.
- Depending on specifications in the task definition, ALL, SUCCESSFUL or FALURE results are shown.
  - ALL, and SUCCESSFUL may generate a lot of data
- You can update the authorized CI with the values in the actual CI by clicking **Update CI with Actual CI value**.

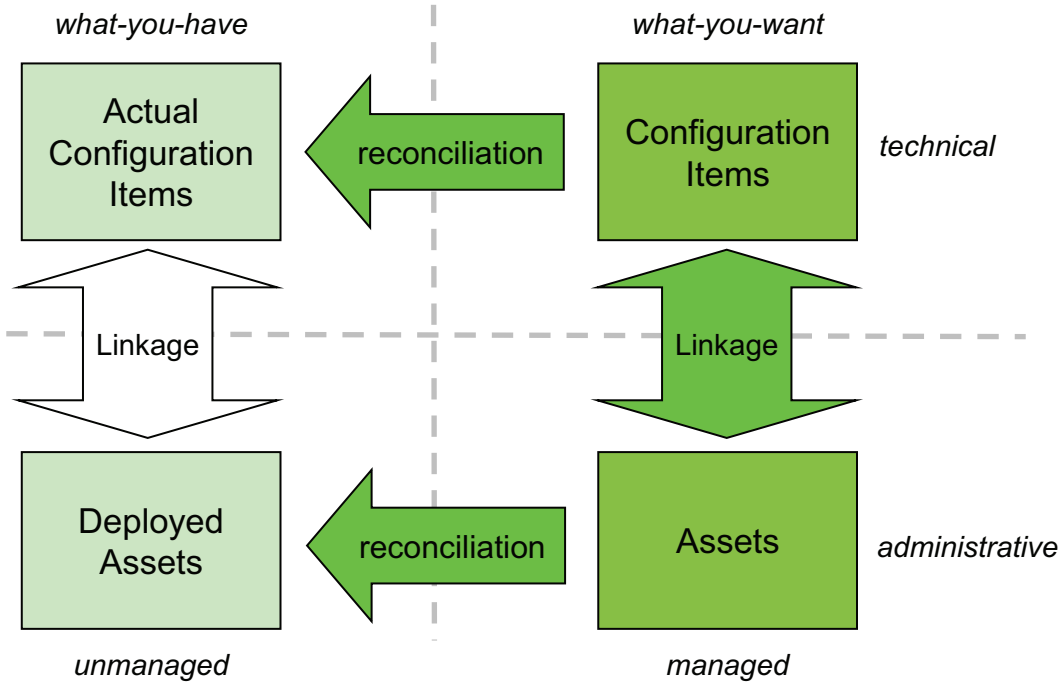


The Reconciliation Result Details window

Notice that the attribute history is shown alongside the result.

Results are stored in the RECONRESULTS table. These can be used by an escalation/action pair to automate processing.

Reconciliation and linkage

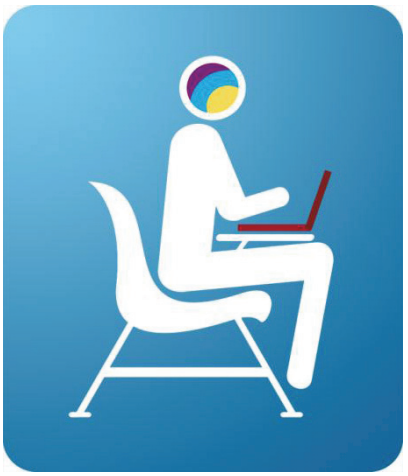


Reconciliation and linkage

Reconciliation tasks provide the mechanics to automate the linkage between authorized CIs and actual CIs, between assets and deployed assets, and between authorized CIs and assets.

These links provide the basics for many functions, for example CI Audit.

Student exercises



Student exercises

Summary

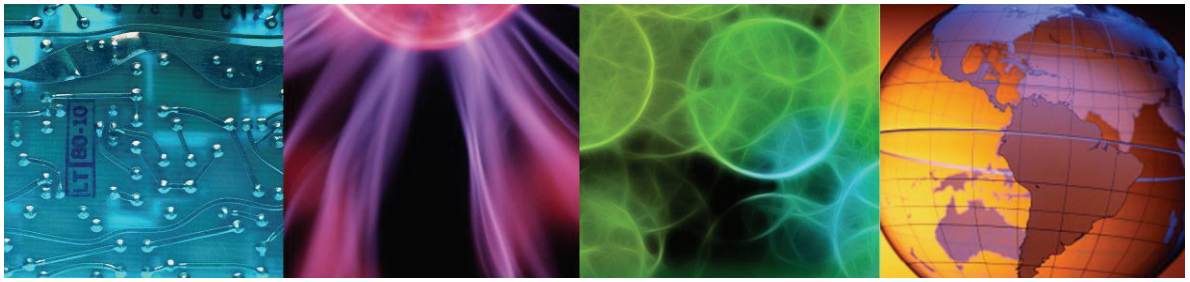
You should now be able to:

- Understand the purpose of the configuration management processes
- Describe the purpose of IBM Tivoli Unified Process and how it relates to the IT Infrastructure Library (ITIL)
- Define common configuration management roles and responsibilities
- Discuss differences and similarities between active and authorized configuration items
- Describe the purpose of naming rules
- Explain promotion, linkage, and synchronization
- Understand the purpose and use of configuration baselines
- Describe the use of configuration lifecycles
- Describe use and configuration of reconciliation tasks

Summary

4 Configuration auditing

Configuration auditing



What this chapter is about

This chapter introduces configuration auditing, a critical component of configuration management, which provides the basic functions for verifying changes and identifying unauthorized changes.

Objectives

After you complete this unit, you will be able to:

- Discuss the purpose and tasks involved in configuration audit
- Explain how CIs and assets may be linked
- Describe the use of the CCILinkAssetsAndCIs reconciliation task

Objectives

Agenda

- Configuration item audit
- The CI update process
- Linking assets and CIs
- Summary

Agenda

Configuration item audit

“Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met. An audit may be carried out by internal or external groups."

Configuration item audit

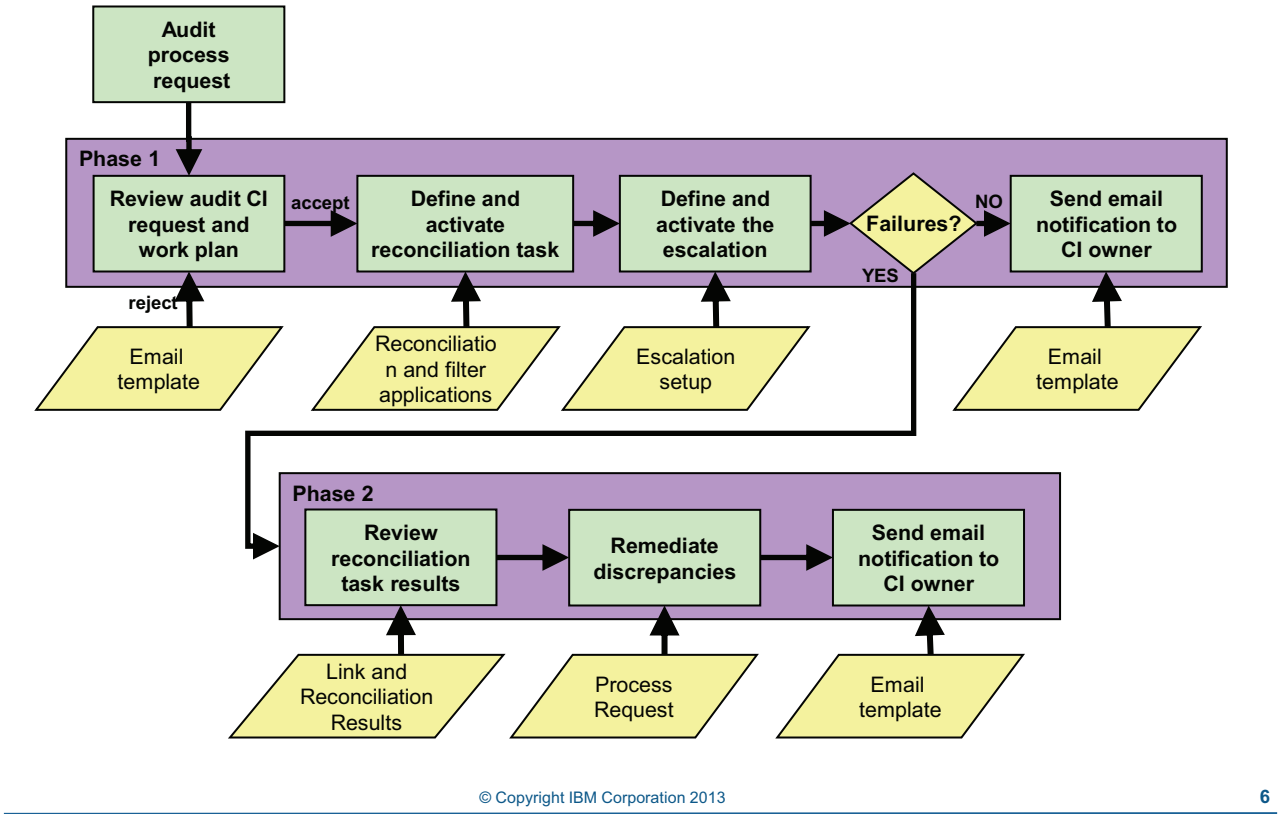
Audit CI process

- The Audit CI process reconciles the value of attributes between the authorized CIs and the actual CIs in the IBM SmartCloud Control Desk CMDB.
- Audits are typically requested through a process request.
- It is often requested to verify correct change implementation.
- Can execute based on schedule, or as a one-off.
- When discrepancies are identified, the configuration auditor is notified.
- The person responsible for managing this process is the configuration auditor
- The audit process relies on reconciliation tasks and escalations.
- The configuration auditor is guided through the definition process in accordance with a response plan

Audit CI process

The CI audit process is used to ensure that the information in the IBM SmartCloud Control Desk is trustworthy.

Both individual CIs and groups of CIs can be audited.



Audit CI process definition

The CI audit process is based on reconciliation tasks and escalations.

It is a two-phased process:

1. Define a reconciliation task that performs the analysis, and an escalation that starts a second process if discrepancies are found.
2. Use the results from the reconciliation task to manually resolve discrepancies.

Phase 1:

- When the configuration auditor receives an audit request, a new reconciliation task is created
- For the reconciliation task, task filter, link rules, and comparison rules must be defined.
  - Change numbers may be used as task filter in order to evaluate the implementation of a specific change.
  - Full CI Comparison is used as the comparison rule when auditing a change, and only comparison Failures are reported.
  - Typically, when verifying a change, the schedule should be set up to only run once.

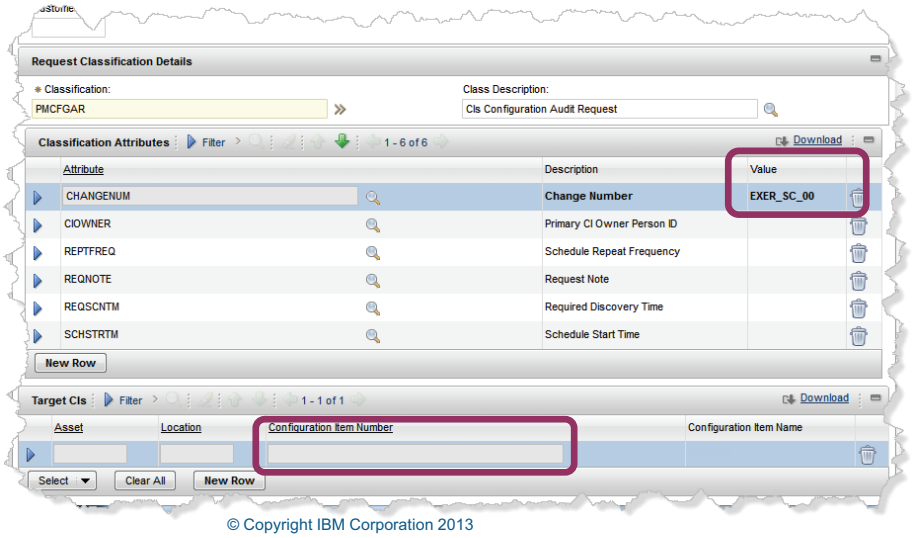
- An escalation is defined to evaluate the results and if Failures are reported, start phase 2.

Phase 2:

- The results are reviewed
- Discrepancies are remediated using promotion, synchronization or manual updates. The auditor needs to work with the CI owner to take the appropriate action.

The audit request

- Submitted by any user with PMREQUESTER authorization
- Classification must be PMCFGAR
- Must include a target CI, or a reference to a change that has a primary target CI defined.
- Classification attributes are used to communicate information related to filtering and execution requirements



The audit request

Audit requests are usually submitted by CI owners or change owners.

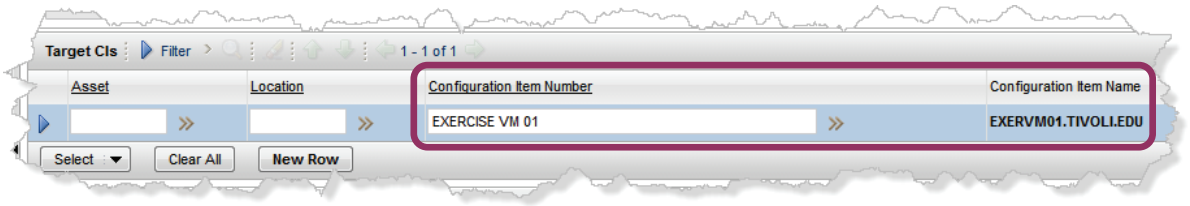
IBM SmartCloud Control Desk uses a special classification (PMCFGAR) for configuration audit requests.

On the request, a specific CI, or a change is used to specify which CIs to audit.

Additional information can be added as attributes of the request to communicate details.

Audit CI process phase 1

- A configuration work order (process) is automatically created when a process request is accepted.
- A set of specification tasks for the process is assigned to the configuration auditor
- All the request definitions are carried over from the process request to the work order.
- Job plan is automatically assigned according to the process classification.
- If the request referenced change, Primary Targets for the change are automatically added as targets to the process.



 8

Audit CI process phase 1

When a request is accepted, the configuration auditor is assigned as the owner of the individual audit tasks.

A response plan is used as a template for the job plan that is used to create the reconciliation task for a specific audit.

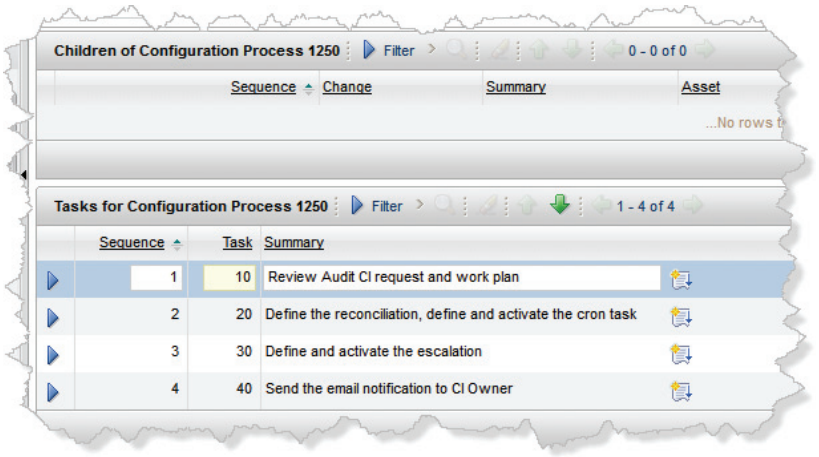
The audit process phase 1 job plan

The default job plan requires the configuration auditor to complete four tasks:

1. Review the plan
2. Define, schedule, and activate a reconciliation task
3. Define an escalation that reacts on the reconciliation task results

   wait for the tasks and escalation to produce results

4. Notify the CI owner



The audit process phase 1 job plan

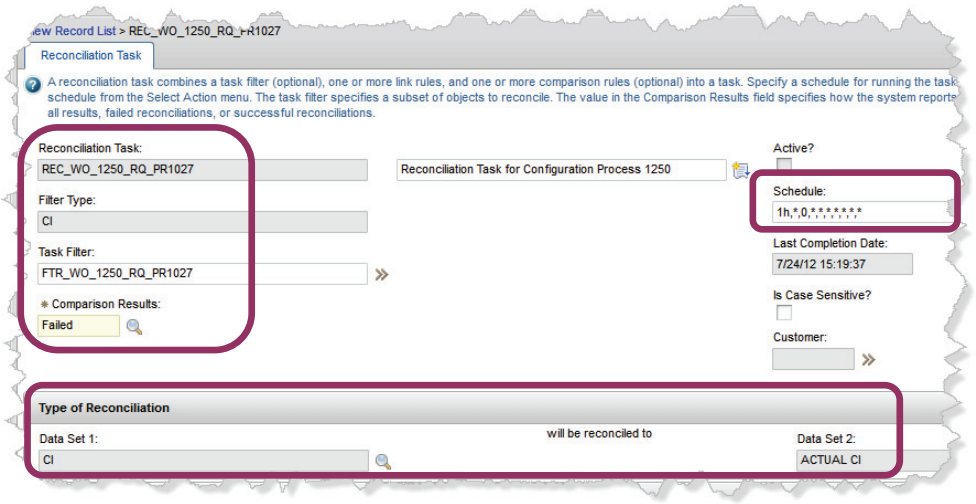
The configuration audit process is based on standard Tpae job plans and tasks. There are no workflows operating behind the scene.

The audit reconciliation task

- Similar to all other reconciliation tasks
- Defines:

  Comparison type: CI > ACTUAL CI
  Filter Type: CI
  Comparison Results: Failed
  Schedule: (once)

- Contains references to:
  - Task filter
  - Link rule
  - Comparison rule



The audit reconciliation task

In the reconciliation task definition, you define the data sets to be reconciled, the type of results you want, and the schedule.

Filters, and rules are also referenced.

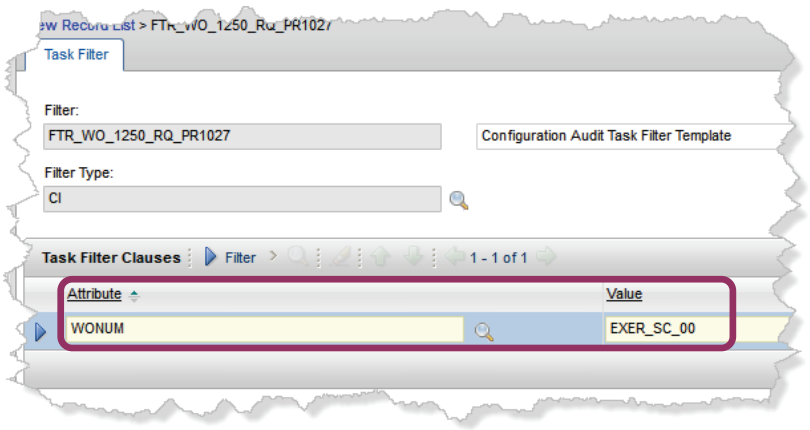
For change verification, you would typically:

- reconcile CIs with actual CIs
- apply filters to the CI records
- report only Failed comparisons
- run the task only once

The audit reconciliation task filter

- Created automatically
- Uses information from the request to define an ‘intelligent’ task filter

- If a change number is specified, this will be used in the task filter to include only CIs that are associated with the particular change work order



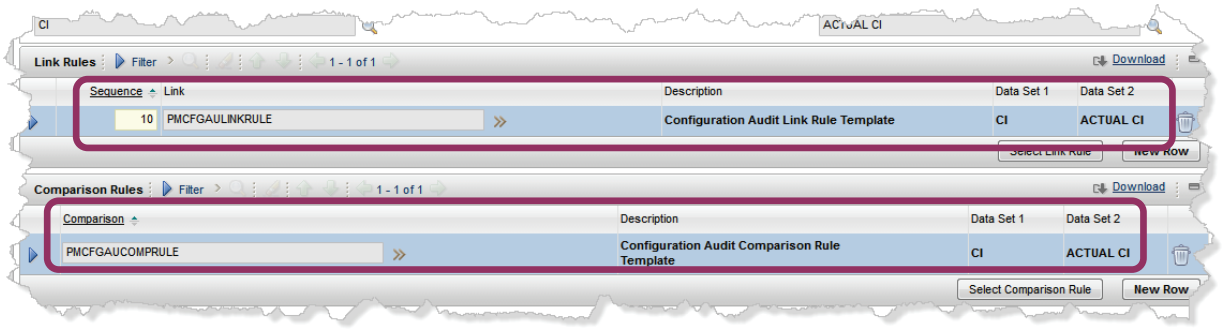
The audit reconciliation task filter

The task filter is created automatically when the audit request is accepted. The change or CI information provided in the request is used to populate the filter.

For change verification, the change number (WONUM attribute) is used to identify the target CIs of the change.

The audit reconciliation link and comparison rules

- Default link rule (PMCFGAULINKRULE) is provided
  - CI.ACTCINUM = AUTHCI.ACTCINUM
- Default comparison rule (PMCFGAUCOMPRULE) is provided
  - Full CI comparison



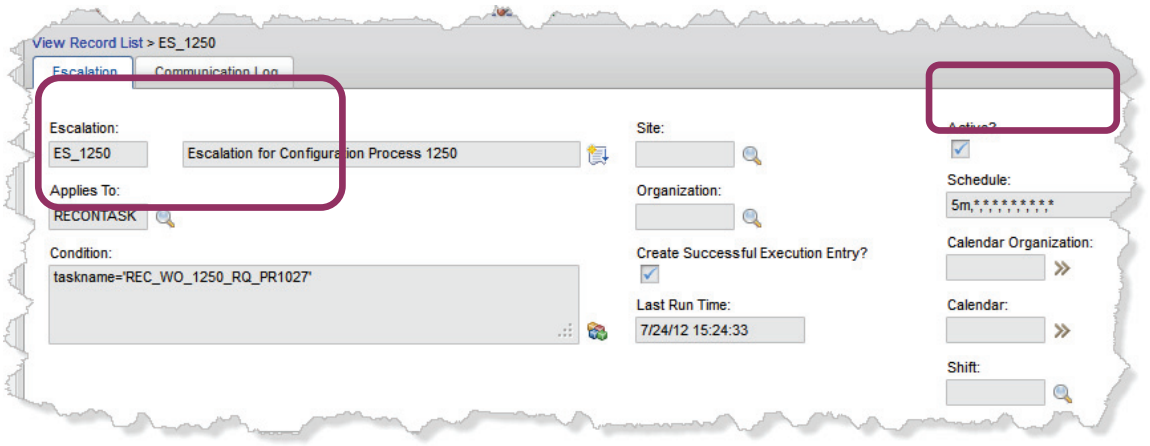
The audit reconciliation link and comparison rules

To audit CIs, the actual CI number (ACTCINUM) is used to identify actual CIs that are linked to authorized CIs

By default, full CI comparison is used to find any discrepancies.

The audit escalation definition and schedule

- The escalation condition tests results in the RECONTASK table for the completion records of the specified reconciliation task
- The escalation should execute more frequently than the reconciliation task



 13

The audit escalation definition and schedule

The escalation that is responsible for initiating phase II, looks at the information in the RECONTASK table to find the results.

In you are using the CI Audit to perform a periodic audit of a group of CIs (for example all AIX systems), you should ensure that the escalation is validated more often that the reconciliation task is executed, This will ensure that all results are evaluated.

The audit escalation audit points and action

- The escalation audit points tests of discrepancies (failed reconciliation results) are identified. If the audit point is true, the action will be invoked.
- The action (PMCFGREMEDIATION) creates an AUDIT 2 task for each discrepancy that has not been resolved.
- The default audit point simply tests if the reconciliation task has completed after the last run of the escalation itself:

```
completiondate >= (select(max(statusdate) from escstatus where escalation =
'<escalation_name>'
```

If you use the default audit point, AUDIT 2 tasks will be generated every time the reconciliation task is executed, even if no new discrepancies were identified.

- To avoid this, redefine the audit point to this:

```
( (select max(datecreated) from reconciresult where
recontaskid=recontask.recontaskid and recontask.taskname =
'<recontask_name>')  >= (select max(statusdate) from escstatus where
escalation = '<escalation_name>') )
or
( (select changedate from escalation where escalation = '<escalation_name>') >
(select max(changedate) from reconciresult where
recontaskid=recontask.recontaskid and recontask.taskname =
'<recontask_name>') )
```


The audit escalation audit points and action

If you use the default audit points for the escalation, AUDIT 2 processes will be generated EVERY time the escalation is evaluated. To avoid this, you can apply conditions in the audit point to ensure that the results that are validated are newer than the last escalation validation.

The revised audit point can be defined like this:

```
( ( select max(datecreated) from reconciresult
   where recontaskid=recontask.recontaskid
   and recontask.taskname = '<recontask_name>') >=
   (select max(statusdate) from escstatus
      where escalation = '<escalation_name>')
)
or
( (select changedate from escalation
   where escalation = '<escalation_name>') >
   (select max(changedate) from reconciresult where
      recontaskid=recontask.recontaskid and
      recontask.taskname = '<recontask_name>'
```

)

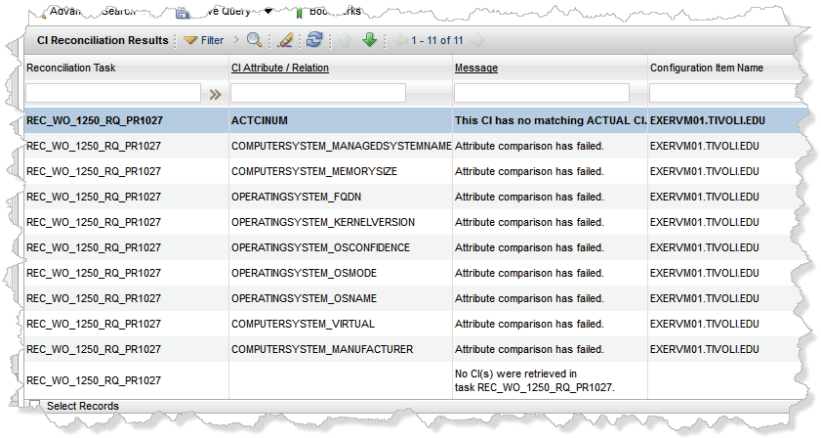
)

Waiting for reconciliation results

- When both the reconciliation task and the escalation have been activated and scheduled, all the configuration auditor needs to do is to wait for the execution of the reconciliation task, and possibly, AUDIT 2 process assignments due to discrepancies.
- To see how the reconciliation rule links CIs and ACTUAL CIs use Go To > Administration > Reconciliation > CI Link Results to view the results for the PMCFGAULINKRULE.

- To see the results, use Go To > Administration > Reconciliation > CI Reconciliation Results.

  Remember that the Comparison Results setting for the task specifies what you might see (SUCCESS, FAILURE, BOTH).
- You can also use the built-in reports to view the results.



For each execution of the reconciliation task with FAILED records, the configuration auditor will receive an AUDIT 2 process assignment.

 15

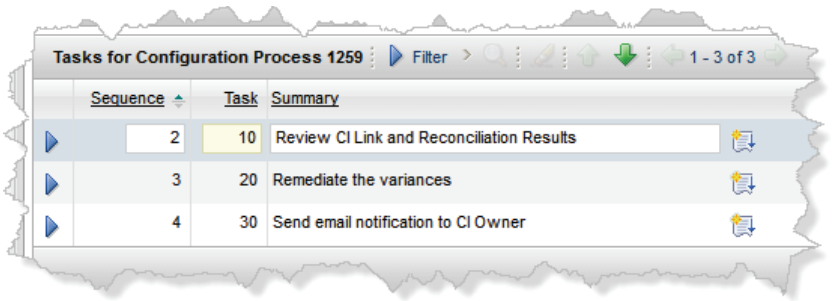
Waiting for reconciliation results

When the reconciliation task has run, link results and reconciliation results will be available.

After the escalation has evaluated the results, the configuration auditor may receive AUDIT 2 assignments.

The AUDIT 2 job plan

- To remediate discrepancies, the configuration auditor is expected to complete three tasks:
  - Review
  - Fix
  - Communicate

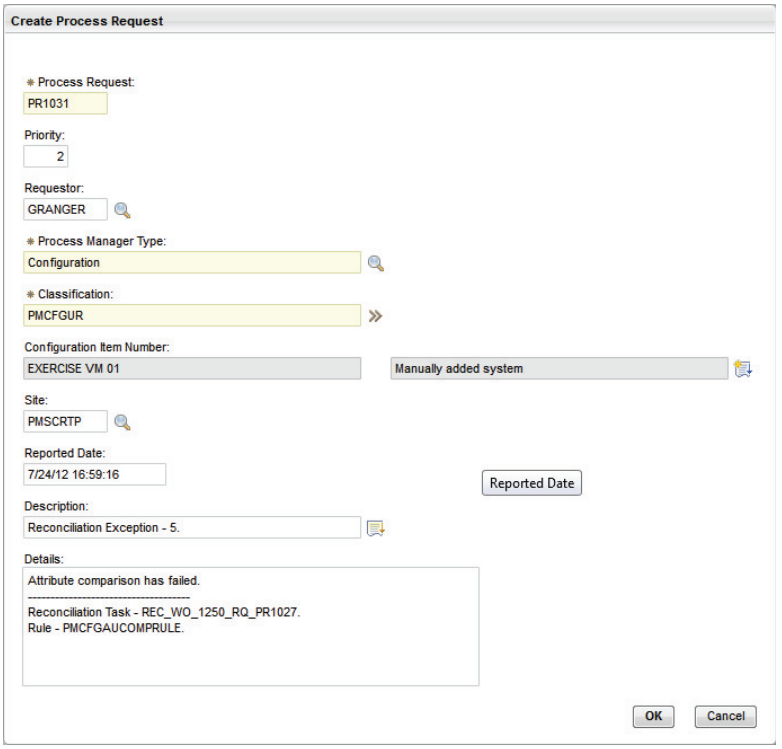


  - To remediate the discrepancies, the configuration auditor can update the Authorized CI attributes manually (for unprotected CIs) or submit a CI Update Process Request

The AUDIT 2 job plan

Remediating audit failures

- The configuration auditor uses the CI Reconciliation Results application to review the results.
- To remediate the discrepancies, the configuration auditor can update the authorized CI attributes manually (for unprotected CIs) or submit a CI update process request.
- When failures have been remediated, the audit records are marked RESOLVED.



Remediating audit failures

Closing the processes

- Configuration processes are treated like ordinary work orders, so before the processes are closed, the configuration auditor should deactivate reconciliation tasks and escalations that do not need to execute on a scheduled basis, for example tasks and escalations created to verify a change.
- Consider modifying the response plan to include steps to do this as part of the AUDIT 1 and AUDIT 2 processes, or create an escalation/action pair that deactivates change-specific resources when the change is closed.

Closing the processes

The CI update process

The purpose of the process is to perform updates to CI configurations or metadata in a controlled, authorized, and well-documented fashion.

The CI update process

The update CI process

- The update CI process is used to perform updates to authorized configuration items. Updating a CI involves one or more of the following items:
  - Attributes
  - Relationships
  - Lifecycle state
  - Baselines
  - Collection membership
  - Change window calendar assignments
  - Or other properties that apply to CIs
- The process is always initiated from a process request.
- Typically, update CI requests are issued as part of the processing of a change or a CI audit.
- The process is mainly used with CIs that are in a protected lifecycle state, or transitioning into one, but can be used with all authorized CIs.

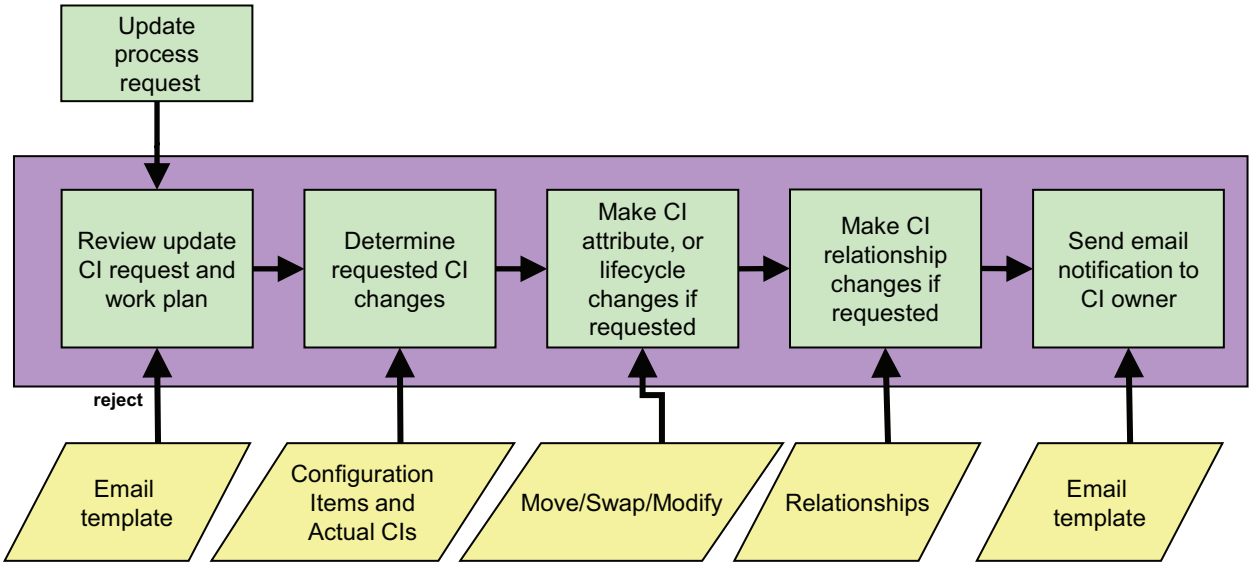
Update CI process

Updates to CIs are primarily performed as the result of the implementation of a change. In the change, the Move/Swap/Modify feature can be used to prepare the updates, save them in a plan, and apply the plan when the implementation tasks complete.

During change preparation, the configuration librarian may be involved to preparing CI updates, based on CI Update requests issued by the change owner.

Some organizations allow the change management team to update CIs without involving the configuration management team.

Update CI process definition



Update CI process definition

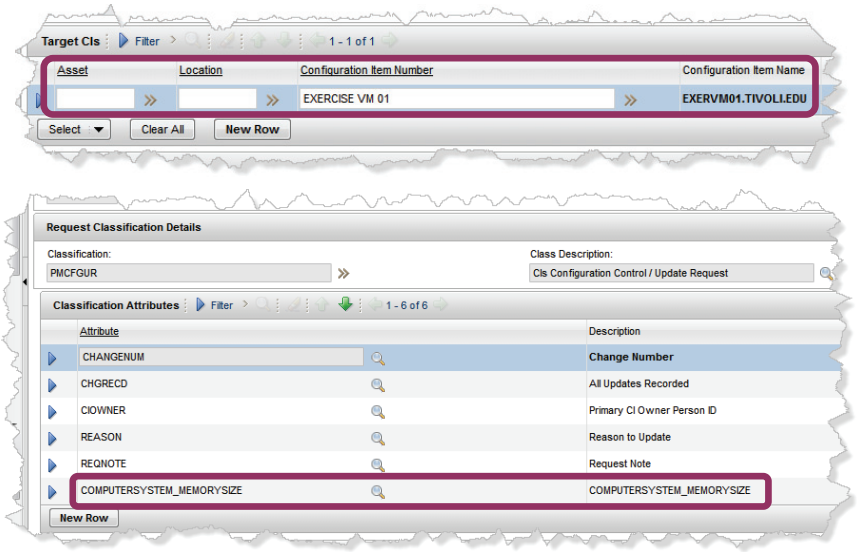
The CI update process is triggered from a request.

When a request has been accepted, the configuration librarian performs these steps to effectuate the update:

1. The review tasks at hand
2. Determine what needs to be changed
3. Use Move/Swap/Modify to create an update plan
4. Modify relationships
5. Notify stakeholders

The update CI request without change reference

- Used to manipulate CIs that are in a *non-protected* lifecycle state
  - Targets CI are specified CIs directly in the request. Requested changes are specified by adding attributes and values that needs to be updated.
  - To request creation/promotion or synchronization no attributes needs to be specified.



The update CI request without change reference

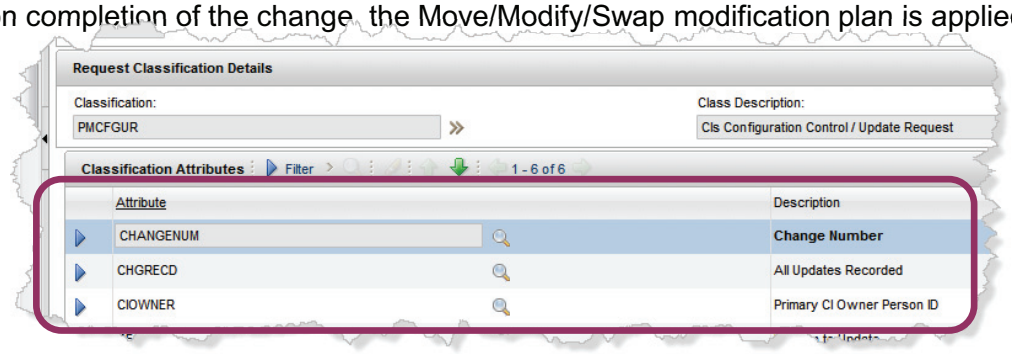
For updates to non-protected CIs, or for update requests that are not related to a change, the request specifies the intended updates, and they are implemented by the configuration librarian.

Depending on the nature of the change, the updates can be applied directly to the CI, or by using the Move/Swap/Modify facility.

The update CI request with change reference

Used to manipulate CIs that are in a *protected* lifecycle state, where state, attribute, or relationship modifications must be approved by the configuration manager.

1. The updates are recorded in the change using Move/Swap/Modify with the *Save to Plan* option.
2. The change job plan includes a task to request approval through an *Update CI Request.*
3. When the request is created, the change number must be recorded in the CHANGENUM attribute and the value of the CHGRFCD attribute must be set to YES.
4. When the update CI request is processed successfully, the change processing can continue to completion.
5. Upon completion of the change, the Move/Modify/Swap modification plan is applied to the CIs.



Update CI classification is PMCFGUR

The update CI request with change reference

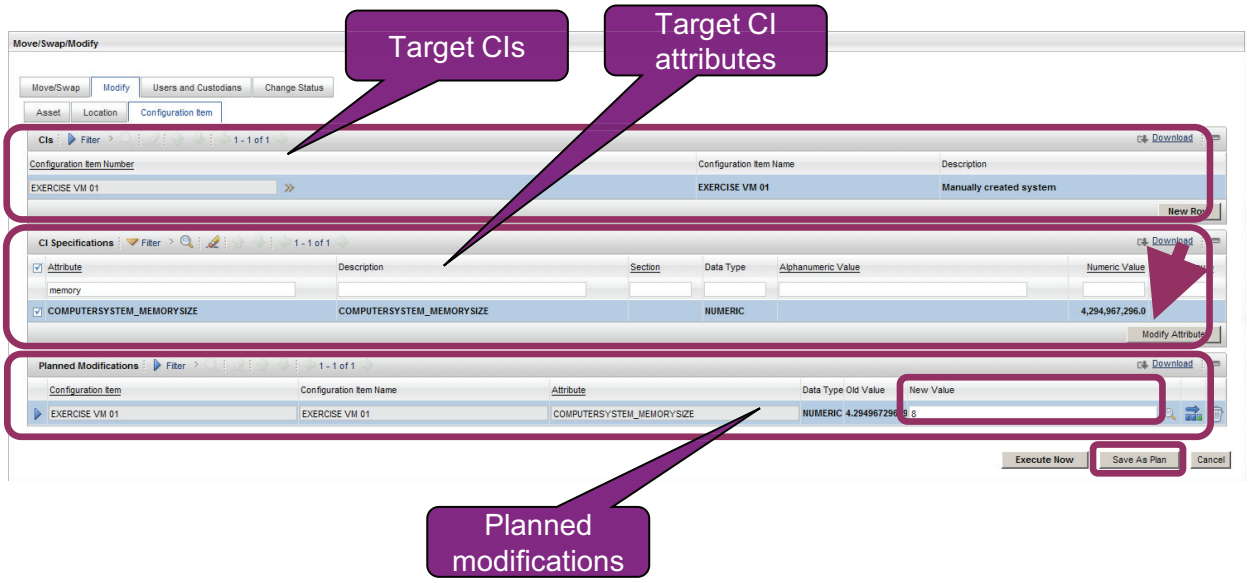
Updates to CIs that are in a protected lifecycle state must be approved.

The change owner uses the Move/Swap/Modify tool to create the plan, which then is reviewed by the configuration management team, and approved.

When the change is implemented, the IBM SmartCloud Control Desk CMDB is updated.

The Move/Swap/Modify application

- Used to change attributes and relationships as part of the change specification
- Use ***Save to Plan*** to hold database updates until the change or process completes
- Can be used by the configuration team or the change team



The Move/Swap/Modify application

The Move/Swap/Modify application is used to modify CIs,

The modifications can be saves as a plan, in which case they will be applied when the change-related implementation tasks complete.

Linking assets and CIs

By linking the asset and CI records for the same resource, you get easy access to both administrative and technical information for the resource. This is useful when performing asset management, or while managing configurations, change and releases.

Linking assets and CIs

Asset-CI linkage

- The same resource can be managed as both an asset and a CI

  Assets contains information of the location, ownership, and financial status of a resource.

  CIs contains detailed configuration and relationship information about the resource, and is the basis for change management activities.

- When enabling the automated synchronization feature, you ensure that common attributes are automatically synchronized ‘on the other side’ when updates are performed.

- The CCILinkAssetsAndCIs reconciliation task is responsible for linkage and creation of generic resources.

- If you want, you can even configure IBM SmartCloud Control Desk to automatically create generic ‘sibling’ resources when new CIs or assets are created.

Asset-CI linkage

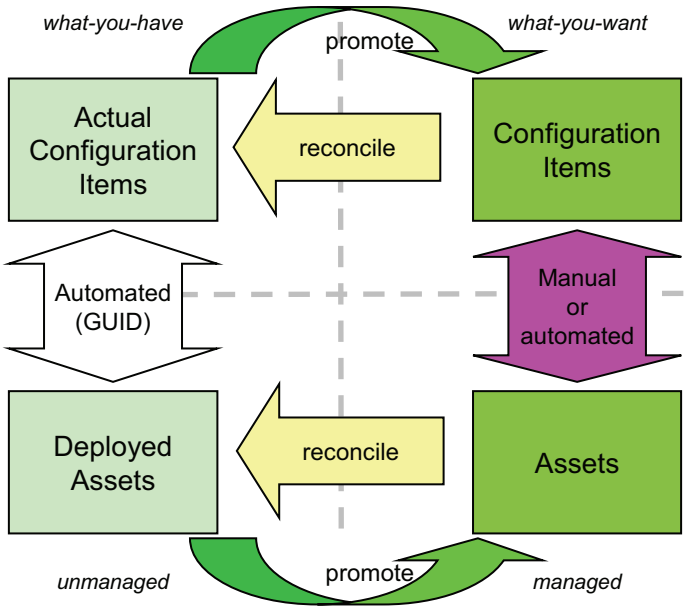
The linkage between assets and CIs can be automated if the actual CIs and deployed assets have the same GUID.

The automation is based on a reconciliation task.

In this case, you can enforce synchronization of key attributes so they are automatically updated, and even automate the creation of generic resources to represent missing siblings.

Linkage and reconciliation tasks

- Managed resources can be linked to their unmanaged siblings through:
  - Manual linkage
  - Promotion of the unmanaged resource
  - Reconciliation based on comparison of common attributes
- Unmanaged resources are linked through the common GUID attributes (NRSGUID/DISGUID)
- Managed resources can be linked:
  - Manually
  - By the CCILinkAssetsAndCIs reconciliation task, which also can create missing managed resources

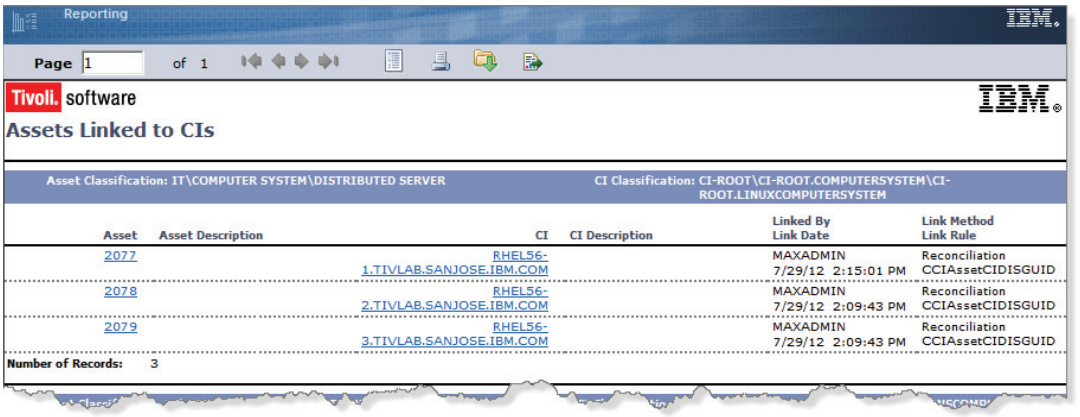


Linkage and reconciliation tasks

The automated linkage of authorized recourses is based authorized > actual > actual > authorized chain of links, or on comparison of common, key (naming) attributes.

The CCILinkAssetsAndCIs reconciliation task

- System provided reconciliation task that links Assets and CIs
- Must be scheduled and activated
- Performs only linkage, so it does not use Comparison rules
- Does not report results in the CI Link Results or Asset Link Results applications
- Identifies resources to be linked in this sequence:
  1. Uses GUID attribute (if it is populated)
  2. Uses standard link rules (attribute comparison). Typically using a common attribute such as serial number.
- Link method and link rule can be viewed in GUI or report



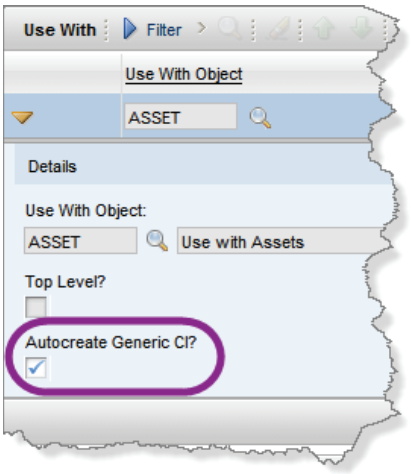
The CCILinkAssetsAndCIs reconciliation task

The CCILinkAssetsAndCIs reconciliation task works like any other reconciliation task.

Notice that results are NOT reported in the Link Results applications. You must use the report to view the link results.

Automated creation of generic assets

- Works only for COMPUTERSYSTEM type resources.
- Must be enabled for the classification of the resource type (classification) for which there is no matching managed sibling
- Requires that the attribute used in the link rule has been populated in the resource that exists
- Resources created by the task are classified as GENERIC (CI or ASSET)
- These common attributes are copied to the generic resource:
  - Serial Number
  - Organization
  - Site
  - Location
  - Customer
  - All common specification attributes (attributes with precisely the same name in both the asset and CI)



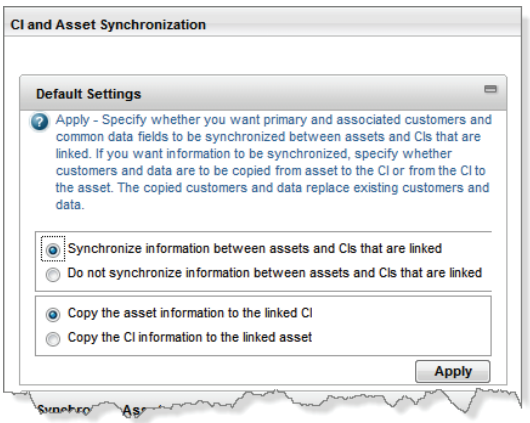
Automated creation of generic assets

You can configure the classification to enable automatic creation of generic resources. If enabled, this will allow IBM SmartCloud Control Desk to create generic resources when missing links are identified.

Automated synchronization

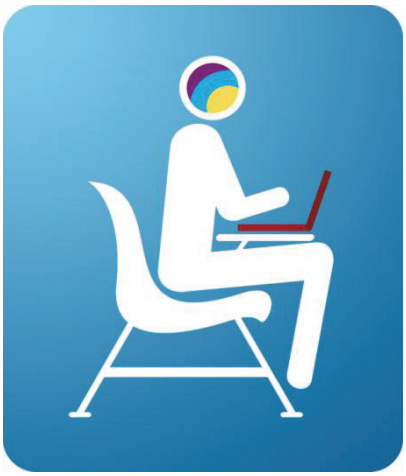
- Must be enabled for your organization
- Synchronizes only in one direction

  CI > Asset or Asset > CI
- Synchronizes these attributes:
  - Serial number
  - Organization
  - Site
  - Location
  - Customer
  - All common specification attributes (attributes with precisely the same name in both the asset and CI)



Automated synchronization

Student exercises



Student exercises

Summary

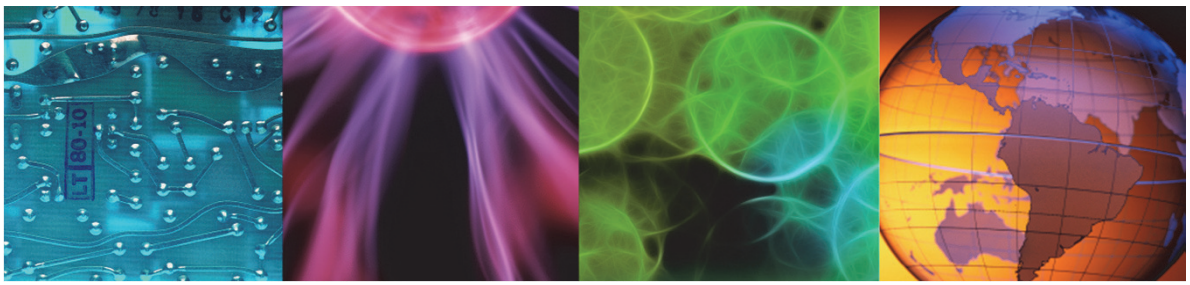
You should now be able to:

- Discuss the purpose and tasks involved in configuration audit
- Explain how CIs and assets may be linked
- Describe the use of the CCILinkAssetsAndCIs reconciliation task

Summary

5 Change management with IBM SmartCloud Control Desk 7.5

Change management with IBM SmartCloud Control Desk 7.5



What this chapter is about

This chapter introduces you to the basics of change management, and takes you through the phases of the three main change processing models supported by IBM SmartCloud Control Desk.

Objectives

Upon completion of this unit, you will be able to:

- Describe the purpose of the change management process manager
- Describe the relationship of process requests to requests for change
- Describe the lifecycle of a process request
- Create and modify process requests
- Apply a job plan to a change
- Manage change windows and detect conflicts
- View the change implementation schedule
- Record and view the impact analysis of a change

 2

Objectives

Introduction to change management

- Change management is the process that is responsible to protect the production environment.
- Its standardized methods and procedures are defined for efficient and prompt handling of all changes. The purpose is to minimize or avoid the impact of change-related incidents on service quality, which would also affect business.

Introduction to change management

Adherence to the change management process is critical to a sound service delivery process. If the updates that are applied to the production systems have not been properly documented, assessed, scheduled, and authorized prior to implementation, unplanned outages can occur, and most likely will.

Outages are costly. Not only the business processes disrupted, but it typically requires many man-hours to troubleshoot, and find the root-cause of the outage. In this process, the documentation of changes provide valuable information, along with other sources of information such as monitoring logs, events, and historical performance and capacity data, to help identify possible root-causes for the outage.

Change management overview

- Change management processes ensure that:
  - Requests for changes are properly registered
  - Proposed changes are adequately documented
  - Changes are assessed for business as well as technical impact
  - Changes are scheduled for implementation at a convenient time
  - Change plans are properly authorized
  - Changes are implemented according to plan

    Change implementation are properly verified
  - The state of the change is properly communicated

Change management overview

Instructor:

The ITIL change management process recommends that changes are initiated from change requests, that document the justification of the change. The ITIL change management process consists of seven phases. Based on change classification, type, and risk some of these phases may be skipped, or automated.

Accept and Classify In this phase the request revived, and the justification is verified. Then the RFC is accepted, the change record is created and classified, and ownership is assigned. Finally the change owner classifies and specifies the change.

Assess Next the change is assessed to verify that it has been specified correctly. In addition, the change is analyzed to identify related resources that may be impacted by the change.

Schedule Then change is then scheduled to find the best time for the implementation.

Authorize	When the change is fully specified, it must be approved (authorized) in order to be allowed to be implemented.
Implement	During implementation updates are applied to the resources in the IT infrastructure.
Verify	After implementation it is verified that the updates had the desired effect and were applied correctly.
Communicate	The results of the change implementation are communicated to the stakeholders.

Main change management processes and roles

Main change management processes

- Create and Record Change Request
- Accept and Categorize
- Assess
- Schedule
- Authorize
- Implement
- Review and communicate
- Close

Key configuration management roles:

Change Manager

The main coordinator and the focal point regarding changes for both the customer and the IT organization

Change Owner

Primary responsible for the overall processing of individual changes.

Change Analyst

Uses deep technical knowledge and subject matter expertise to understand business and technical issues and impacts regarding proposed change.

Change Approver

Has the power to authorize a change. Often member of the Change Advisory Board (CAB)

Change Implementer

Carries out an authorized change

Change Requester

Submits requests to the IT organization.

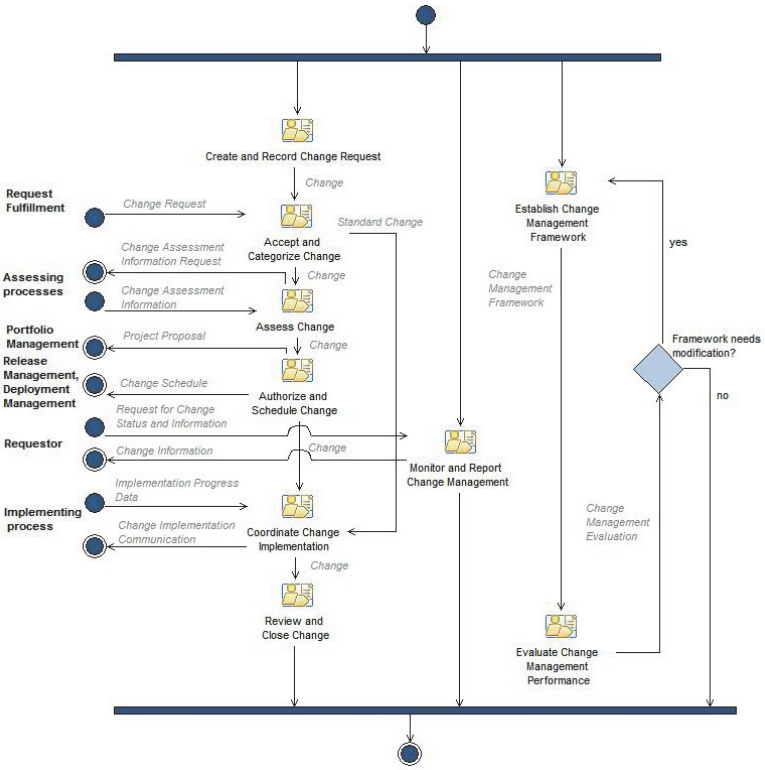
 5

Main change management processes and roles

The change management team consists of members that (typically) are assigned specific roles.

Each role is associated with specific responsibilities. Responsibilities are divided in such a way that members having the same role cannot approve each others work.

The change management process



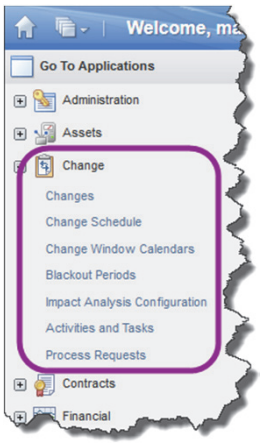
 6

The change management process

In the IBM Tivoli Unified Process documentation you can find this flowchart, and related descriptions and details, of the change management process.

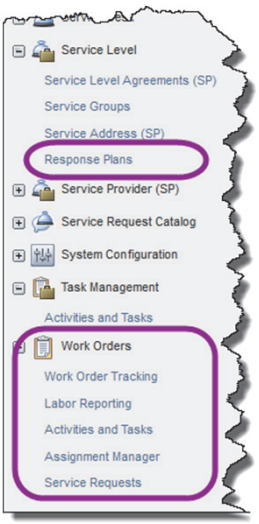
IBM Tivoli Unified Process in a valuable source of information when you want to understand the details of change management, the tasks included in each phase, and the division of responsibilities.

Change management applications and roles



General tools used by most change management users

Role	Security Group	Start Center	Person Group
Change Administrators	PMCHANGEADMIN	Change Administrator (29)	PMCHGADM
Change Analysts	PMCHANGEANALYST	Change Implementer (67)	PMCHGBUS
Change Approvers	PMCHANGEAPPROVER	Change Approval, Analysis and Implementation (31)	PMCHGAPP
Change Implementors	PMCHANGEIMPL	Change Approval, Analysis and Implementation (31)	PMCHGIMP
Change Owners	PMCHANGEOWNER	Change Owner (28)	PMCHGOWN
Change Advisory Board	PMCHGCAB		PMCHGCAB
IT Management Board	PMCHGITM		PMCHGITM
Change Managers	PMCHANGEMGR	Change Manager (30)	PMCHGMA
Business Analyst	PMCHGBUS		PMCHGBUS
Change Requester	REQUESTR		REQUESTR



Administration tools used by the Change Administrator

 7

Change management applications and roles

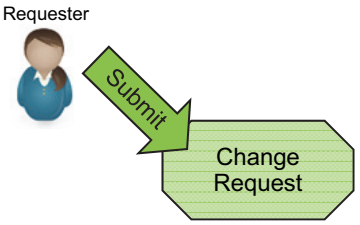
IBM SmartCloud Control Desk uses security groups, and person groups to enforce the roles that are related to change management.

Each member is assigned a start center that provides access to only the functions required to perform the tasks related to the role.

The IBM SmartCloud Control Desk Change, Service Level, and Work Orders application groups contain the applications that are most relevant to change management.

Request for change

- The activities performed by change management are typically based on requests.
- Change requests are submitted by requesters, or automatically as the result of a service request.
- The change request is used to
  - Document and justify the request
  - Identify the requester
  - Assign cost center



- Key Change Process Request information:

* Classification	Determines the type of the change (required)
Description	Descries the nature of the change
Customer	Used in a service provider scenario
Impact	The business impact of implementing the change
Urgency	The speed that is considered appropriate to implement the change
Priority	If not provided, priority is calculated based on impact and urgency
Target(s)	Assets, locations, and/or configuration items
Completion Time	When is the change supposed to be implemented
Attributes	Can be applied to provide control information used by workflows

 8

Request for change

Change requests are typically submitted by change requesters, or automatically generated from service requests.

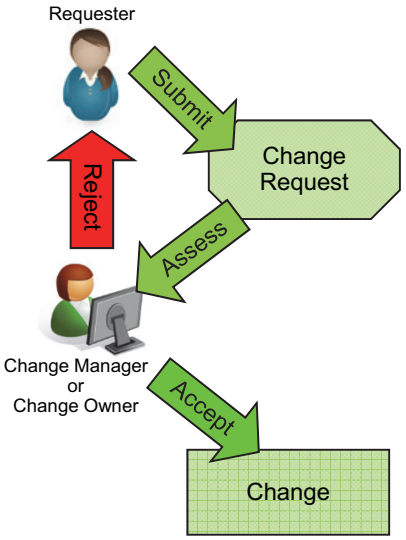
Change requests contains a description of the change, and a classification. The classification is used to specify the kind of change that is requested.

IBM SmartCloud Control Center provides a starter-set of change classifications, but as part of an implementation project, these classifications are tailored to the requirements of a particular organization.

The change requester can augment the RFC with additional information that helps the change management team to properly categorize the change. This additional information may be required to automate the change processing. The Urgency, Priority, and Impact fields are used by IBM SmartCloud Control Desk to calculate the risk, once the change is accepted.

Request for change acceptance

- The change manager or change owner is responsible for accepting or rejecting the request.
- When the change request is accepted, the change is automatically created by the ISMACCEPT workflow.



 9

Request for change acceptance

Change requests are accepted by the change owner, or the change manager, who also assigns ownership of the change to a change owner, or a group of change owners.

Before acceptance, the information is the request is validated. In particular, the following is verified:

- Is the change type appropriate?
- Is the classification correct?
- Is the appropriate target CI specified?
- Are Urgency, Impact, and Importance appropriate?
- Is the requested completion time realistic?

The ISMACCEPT workflow controls the initial change creation process, and can naturally be modified to meet specific requirements, for example for automated processing.

Initialize a change

- The first step in change processing is to properly categorize it.

  By categorization the change, the following attributes are considered/reviewed:

Target(s)	The configuration items that will be subject to change
Urgency	The necessity for the change. How long the implementation can afford to be delayed.
Probability of Failure	The likelihood that the change will not be successful.
Impact	Business impact by not implementing the change.

  Once values are provided for urgency and probability of failure, IBM SmartCloud Control Desk will calculate values for:

Impact	Replaces the original value if the calculated impact is more severe that the originally applied
Priority	Indicates whether this change must be performed before other changes.
Risk	Derived from the overall impact and the probability of failure

- If the change type (standard, normal, emergency) has not been supplied manually, these calculations will be used to determine the change type (for advanced processing)
- An owner, or owner group, is assigned to the
- When the categorization completes, IBM SmartCloud Control Desk will apply a Response Plan, and the response plan will apply the proper job plan.

Initialize a change

The main focus for the change owner in this phase is to:

- Verify the basic change attributes (type, classification, Urgency, target etc.)
- Understand the nature of the request, and apply a change category (major, minor).
- Validate the assigned job plan, and adjust tasks, durations, and targets
- Specify attribute and relationship updates
- Validate and verify requirements for assessment
- Validate and verify requirements for approval

When all of these activities are completed, the change owner routes the change to a workflow. This workflow controls the processing of the change, and uses the specification information to apply a response plan (to assign default job plan, assessment and authorization requirements, and other standard values to the change), and automate preliminary impact analysis, risk calculation, and perform task assignments for the next phase: Acceptance.

Change types

IBM SmartCloud Control Desk supports three different types of changes:

Normal Require that all of the change process steps be completed. These changes require a full range of assessments and authorizations to ensure completeness, accuracy, and the least possible disruption across the data center.

Emergency Must be done immediately. It is of a very high priority. Is typically not performed often. An emergency change contains all of the process steps that are followed for a normal change, but some of the steps might be abbreviated and occur more quickly. For example, you might specify fewer assessments or approvals.

Standard Relatively low-risk and well understood changes. Standard changes are performed frequently. These changes do not have wide-ranging impacts on business-critical CIs, and they are processed so often that they do not need to be assessed, scheduled, approved, or reviewed. A standard change contains only two phases: Accept and Categorize, and Implement. A standard change is closed after implementation is completed.

For all types, you may specify that the change is *Fully Automated*, to avoid human intervention. Automated changes typically use the standard change type, because they do not require assessments, authorization, or scheduling.

Change types

The change type is used to provide an indication of the processing requirements or complexity of the change.

Standard changes are typically automated, and do not require authorization

Normal changes must be properly assessed, scheduled, and authorized.

Emergency changes are treated link normal changes, without authorization in order to expedite the implementation

Change processing methods

When the change initialization completes, the change is routed to a workflow. The selection of workflow determines the change process (phases) to use.

- IBM SmartCloud Control Desk offers two classes of change processes:

Express: Is suited for customers who prefer less automation in favor of a streamlined hands-on approach. Is directed by the PMCHGFIXD1 and PMCHGFLEXD1 workflows.

PMCHGFIXD1 Operates like a wizard, guiding you through a series of steps sequentially to the completion of the process. Ensures that all steps are completed in a certain order.

PMCHGFLEXD1 Completes only the steps for the current phase of the process, updates the status, and exits. The user then clicks the workflow icon again to start the next step in the process. This workflow is more flexible than PMCHGFIXD1.

Advanced: Includes advanced analytics and automation. The advanced process is ideal for customers with a high volume of changes.
Is directed by the PMCHGMAIN1 workflow.

Change processing methods

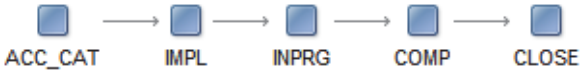
IBM SmartCloud Control Desk implements two different processing modes. The processing mode is determined by the workflow to which the change is routed.

The workflow is responsible for controlling how the change flows through the change process, and for automating tasks that can be performed automatically if all the necessary information is available to the process.

Change phases

- During processing, a change passes through several phases.
- Each phase is responsible for performing specific activities to specify, analyze, access, schedule, approve, implement, review or close the change.

- The phases that applies to a change is determined by the change type.



- Only during the implementation phase, actual work on the target CI(s) is performed. The activities and tasks that are involved are specified in a job plan.

Change phases

The change type (standard, normal, or emergency) is used to determine which change management phases apply to the change. By default, standard changes are the only changes that are candidates for automated processing.

Standard change characteristics

Standard changes:

- Does not require a request for change, but are typically invoked from a service request
- Are pre-approved
- Contain only two phases: Accept and Categorize, and Implement
- Are automatically closed after implementation is completed

Standard change characteristics

The standard change type represent the simplest changes. Typically these are trivial, have minimal impact, and have almost negligible risk.

ITIL defines a standard change as:

> *A pre-approved Change that is low Risk, relatively common and follows a Procedure or Work Instruction. For example password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a Service Request.*

This type of changes make up the bulk of the changes in your environment, and in most instances, investing in automating the processing of these changes will have a huge payoff.

Standard changes

- Standard changes are those that are relatively low-risk and well understood.
- Standard changes are ones that you process frequently, such as resetting passwords, implementing a database, middleware, or server build modification.
- Standard changes do not have wide-ranging impacts on business-critical CIs, and they are processed so often that they do not need to be assessed, approved, or reviewed.
- A standard change contains only two phases:
  - Accept and Categorize,

  and
  - Implement.
- A standard change is closed after implementation is completed.
- Standard changes are often run as *Fully Automated Changes*

Standard changes

Standard changes are changes that are performed routinely, and have low impact, and therefore does not require authorization. These are good candidates for automated processing.

Often standard changes will be requested directly by end-users from the Service Catalog.

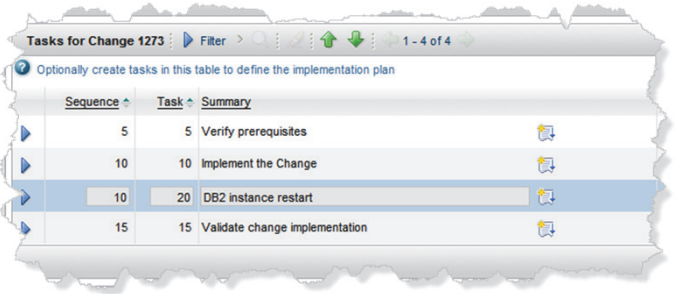
Standard changes include changes such as password reset, deployment and disposal of virtual test systems, installation of middleware or monitoring agents, deployment of antivirus updates and similar routine tasks. However, depending on licensing requirements and policies, some trivial installation tasks may require authorization to authorize the cost of the software license. However, if the installation is requested through the IBM SmartCloud Control Desk Service Request facility, chances are, that the business authorization has already been granted, so the technical authorization is not relevant, and the change can be treated as a standard change.

Specifying a change

To control the implementation of a change, IBM SmartCloud Control Desk uses standard Tivoli process automation engine activities and tasks

- Changes are specified by creating a job plan for the change
- Model job plans can be applied as part of a response plan
- Job plans include tasks that must be completed in order to implement the change
  - Some tasks may be associated with target CIs, others may not.
  - Implementation tasks are used to indicate that the specified target(s) CIs will suffer an outage for the duration of the task.
  - All tasks must have owners, who are responsible for performing the task.
  - Tasks must have a duration
  - In the job plan, the flow of tasks is controlled by assigning predecessors to any task.

When the change owner has specified the standard change and completed the assignments, the workflows moves the change to the next phase.



 16

Specifying a change

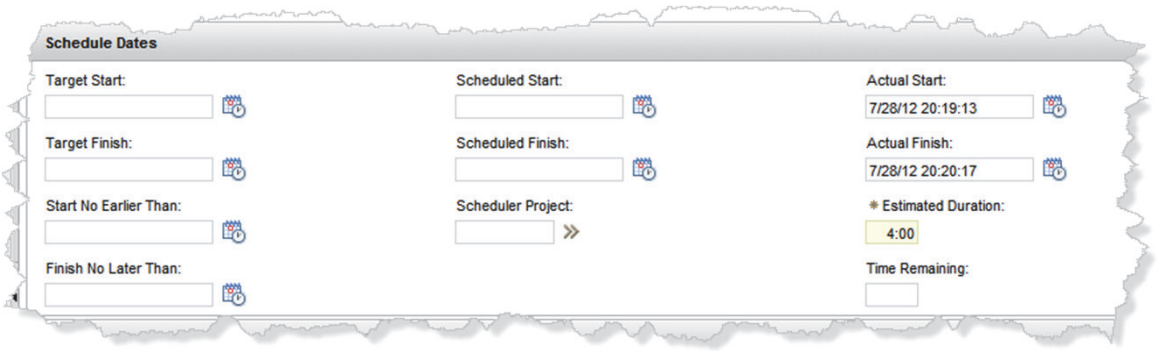
Typically, response plans are developed to such level of detail, that the work for the change owner is reduced to verifying that the change specification is valid. Response plans can be assigned based on very detailed specifications, for example using the combination of change classification, urgency, classification of the target, site, and requestor group. This means, that very specific response plans can be created in order to automate the processing, or minimize the work required by the change owner.

One of the tasks that the change owner may need to perform is scheduling. However, this can also be automated through a workflow.

When the change owner completes the acceptance and categorization phase, the workflow automatically will move the change to implementation.

Change implementation

If the change owner specified a scheduled start date, the change will remain in the Implement state until the start time is reached.



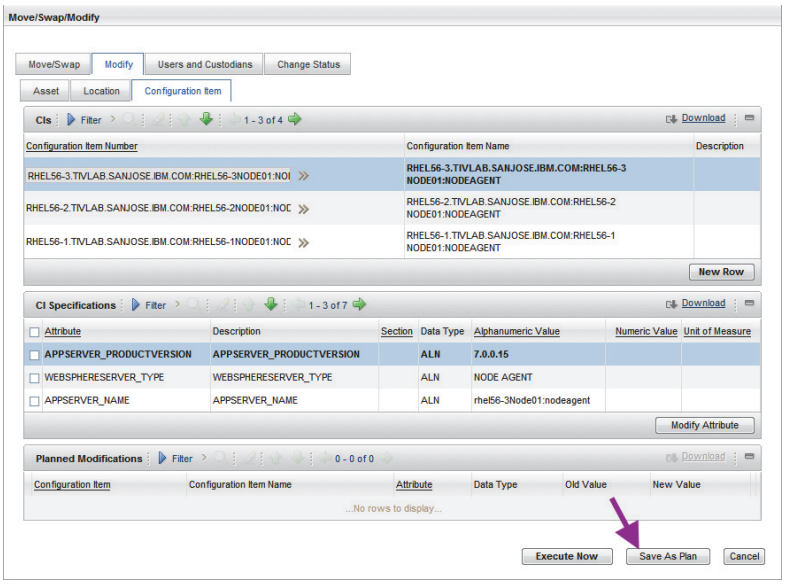
Change implementation

The implementation of the change is performed by the owners of the various implementation tasks in the job plan. Typically these are members of the Change Implementers group.

The change will remain in Implementation status until the schedule time is reached, or the status of the first implementation task is changed from WAPPR to INPROG.

Change in progress

- When the change is *In Progress*, task owners will be assigned tasks as when the predecessor tasks complete.
- For tasks that updates the CMDB, use the Move/Swap/Modify *Save as Plan* option when processing the task. This ensures that the updates are applied to the CMDB when the task completes.



 18

Change In progress

If Scheduled Start was assigned to the task, it will remain in Implementation mode until the scheduled time is reached. At this point in time, the task assignment is issued to the change implementer, and the status is changed to InProgress. If the scheduled start was not specified, the status changes when the change implementer opens the assignment.

After having performed the updates, the change implementer uses the Move/Swap/Modify facility to record updates to the CI. If the Move/Swap/Modify is invoked after all updates have been applied, the change implementer would use the Execute Now option to update the configuration in the CMDB immediately. If multiple updates need to be applied, the change implementer can use the Save As Plan option, in which case the updates are kept on hold until the task completes. As a matter of fact, if your division of responsibilities require that the change owner manages updates to the CMDB, the Move/Swap/Modify updates can be applied by the change owner. In this case the Save As Plan option must be used.

Change closure

- When the last task completes, the status of the standard change is set to Completed and the requester receives a message indicating the result of the processing.

Change closure

Once all implementation tasks have completed, the standard change is automatically moved to the Completed state, and the change owner can review and close the change.

Emergency change characteristics

- Emergency changes:
  - Are characterized by these attributes:
    - Must be done immediately.
    - Have is of a very high priority.
    - Represent the exception
  - Contain all of the process steps that are followed for a normal change, but some of the steps might be abbreviated and occur more quickly. For example, you might specify fewer assessments and approvals, and bypass scheduling.

Emergency change characteristics

Emergency tasks are tasks that require expedited processing.

These tasks may be as simple as updating an expired password for a server component to enable a broken connection between an application server and a database, or as complex as restoring an entire business application across multiple systems in order to reestablish normal operation.

In general, emergency changes are treated like normal changes, with minimal assessment, and authorization, and, depending on the emergency, bypassing normal scheduling.

Emergency changes

- An emergency hange is one that must be done immediately. It has a very high priority.
  - An example of an emergency change might be the installation of new antivirus software during a period of severe viral infestation across the data center.
- Emergency changes are typically not performed on a regular basis.
- An emergency change contains all of the process steps that are followed for a normal change, but some of the steps might be abbreviated and occur more quickly.
  - For example, you might specify fewer assessments or approvals; select not to seek approvals for scheduling conflicts; and so on.
- Emergency changes use the same facilities as the Standard change to categorize, implement and close the change.
- Additional phases, assess, schedule, and authorize, allow for additional assessment, documentation, and control of emergency changes.

Emergency changes

In essence, emergency changes are processed n the same fashion as standard changes, but with additional phases to access, schedule, and authorize the change.

Emergency change acceptance

- Emergency changes are created similar to standard changes:
  - From a request, or manually
- Acceptance and categorization is similar to that of standard changes, but additional considerations related to assessment and approval requirements may apply
- Special response plans may be applied to enforce the use of special job plans, emergency assessment requirements, and minimized approval.
- Content and targets of an emergency changes are specified in the same was as for a standard change.
- When the Accept and Categorize phase completes, the change state is set to *Access*.

Emergency change acceptance

The addition provides better control, more thorough documentation, analysis of the impact of the change, scheduling and optional authorization to ignore change windows, and approval of the change.

All of these phases are injected after change categorization and before implementation.

Change assessment

- Change assessment consists of three activities:
  - Impact analysis
  - Technical assessment
  - Business assessment
- Impacts are calculated automatically by the workflow governing the process
  - Impacts are identified only for implementation tasks
  - The impact analysis is based on CI relationships
- Technical and business assessments are provide a way for SMEs to provide comments based on review of the plan and impacts
  - If implementation notes are added, the change owner is expected to modify the plan

Change assessment

Impact analysis identifies the CIs that rely on the CIs that will suffer performance degradation as result of the change implementation. Most likely, the impacted CIs will be disrupted.

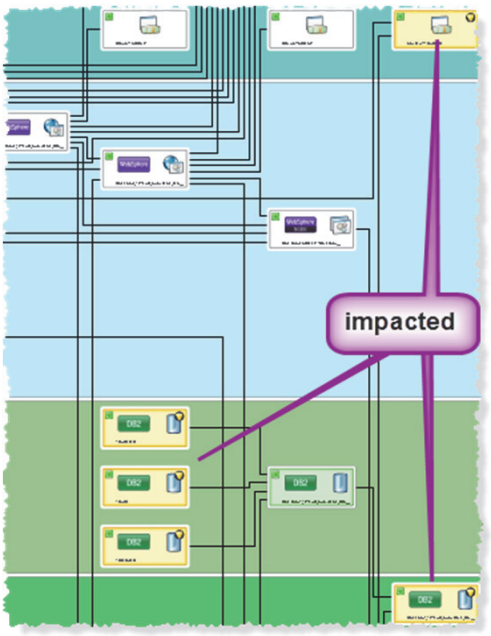
Business assessment evaluates the impact the planned service disruptions will have to the organizations ability to continue to conduct business.

Technical assessment evaluates the technical validity of the implementation plan, and raises any concerns related to the technical correctness and completeness of the change.

Assessment requirements are determined by the change owner when categorizing the change, or by a response plan.

Impact analysis

- The workflow governing the process calculates the impacts of the change before the access phase
  - Only implementation tasks are considered
  - The outage information and relationships between the CIs are used to identify impacts
- The impacts show which related CI will be effected by an outage to the target CIs.
  - For example, a business system will probably be impacted if a database to offlined.
- Impacts are used by the analysts to understand the scope of the change.



 24

Impact analysis

Impact analysis is performed automatically by the change process workflow. However, at any time it can be re-calculated to reflect changes to the change

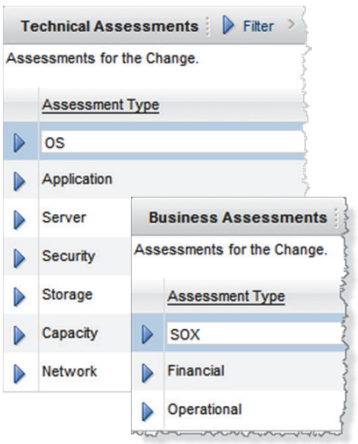
In the detailed information for the impact analysis, you can see exactly which implementation tasks are impacting which CIs, and which relationships caused the impact.

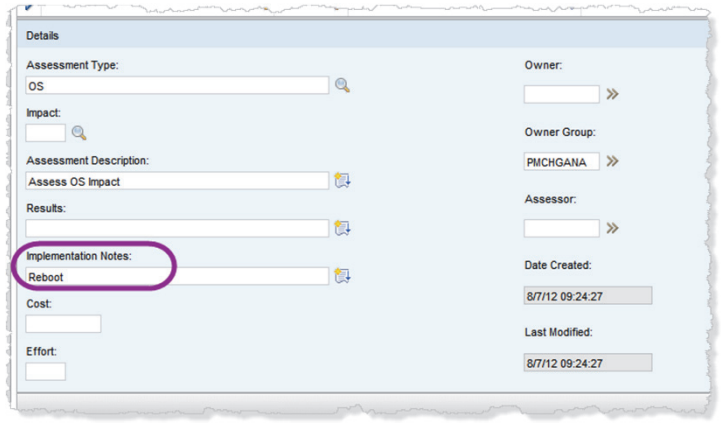
The topology viewer provides an easy-to-use visualization of the impacts.

In this example, you do not see the target CI, because the type of the CI that is the target of the change (Db2InstanceConfigValue) is not included in the business view.

Technical and business assessments

- The need for assessments is determined by the change owner during the specification of the change.
- Technical assessments are performed by change analysts
- Business assessments are performed by business analysts.





- If implementation notes are applied to an assessment, the change owner is encouraged to modify the job plan to accommodate the comment.

25

Technical and business assessments

IBM SmartCloud Control Desk is delivered with three types of business assessments. These can be expanded as needed:

- Financial
- Operational
- Legislative (SOX)

Similarly, a starter-set of technical assessment categories is provided:

- Application
- Capacity
- OS
- Network
- Security
- Server
- Storage

For each assessment category the assessors apply an impact. This will be used to calculate the overall assessed impact, and re-calculate the risk for the change.

If the assessors add implementation notes to the change, the change owner is expected to modify change accordingly.

Emergency change scheduling and authorization

- Typically, because of the urgency, emergency changes are implemented without thorough scheduling and with expedited authorization.

Emergency change scheduling and authorization

The workflows governing the change process has no special processing for emergency changes, so the change owner is required to complete these phases. This ensures that it is documented that the phases have been bypassed if this happens to be the case.

Often, especially if the change impact and risk are high, the change owner will seek authorization from a change approver who is authorized to make that decision, and can provide a fast answer. Your organizations policies and procedures determine how emergency changes should be treated, and the workflows can be instrumented to support the process.

The same is true for scheduling. It may not be required to schedule the emergency change, but if it is scheduled for implementation outside a change window, or inside a blackout period, IBM SmartCloud Control Desk will normally require special authorization to update CIs during production. This authorization is typically bypassed for emergency changes.

Emergency change implementation

- The implementation of the emergency change is similar to that of standard changes.
- During this phase, the documented modifications are applied to the target CI by a owner of the change implementation tasks.

Emergency change implementation

The workflows governing the change process does not provide any special processing for implementation of emergency changes. However, you can apply SLAs to ensure that emergency changes are escalate faster that other types of changes.

Emergency change review

- When the change completes, the change owner must review the results to determine if:
  - The change has had the desired effect and met its objectives.
  - Stakeholders are content with the results; if they are not, they can identify the shortcomings.
  - The change has led to no undesirable side-effects to functionality, service levels, security, costs, and so on.
- If the emergency change was initiated without a corresponding change request, the change owner can create a request retrospectively to complete the documentation of the history of change.
- When the review is done, the change can be closed.

 28

Emergency change review

To complete an emergency change, the change implementation should be reviewed, and stakeholders should be informed about the new status of the CIs.

Most emergency changes are issued against CIs in protected lifecycle states, production CIs, so during the review, Operations should be consulted to verify that the operation of the impacted CIs is normal, of if the monitoring tools indicate any unusual situations that can be attributed to the change.

Normal change characteristics

- Normal changes:
  - Are characterized by these attributes:
    - Require that all of the change process steps be completed
  - Require the full range of assessments, scheduling, and authorizations to ensure completeness, accuracy, and the least possible disruption across the data center.

Normal change characteristics

Normal changes are changes that require the full assessment, scheduling, and authorization.

They are more complex and have higher impact and risk than standard changes, and are as critical as emergency changes.

Normal changes

- Normal changes require that all of the advanced change process steps be completed.
- These changes require a full range of assessments and authorizations to ensure completeness, accuracy, and the least possible disruption across the data center.
- In addition, these changes must be scheduled to ensure that blackout periods are not violated, that CI modifications occur during defined change windows, that change owners are available to perform the needed tasks, and so on.
- The normal type is used when a change will produce impacts on business-critical applications and other critical CIs.
- Normal changes might have a high risk, as determined by their impacts and probability of failure.
- Examples of normal changes might include an enterprise-wide Microsoft Windows operating system update or an email system upgrade.

Normal changes

Processing of normal changes with all the assessments, impact analysis, scheduling and authorization is only supported using the advanced change procession workflows.

The normal change goes through a series of phases in which the understanding of the change and its impact gradually increases,

The process is somewhat iterative, since the change owner may need to modify the job plan based on input from the assessors, and this may change the job plan, targets, impacts, and estimated times. When these attributes change, the impact must be recalculated, and this may lead to yet more modifications.

When the change is fully understood, it is approved by one or more approvers, before it can be implemented.

Upon implementation, the change owner must verify that the expected results were achieved, and communicate to new status to the stakeholders.

Normal change processing

- Normal changes are processed following the same processing phases as the emergency changes, however, there is most likely much more focus on:
  - Assessments
  - Scheduling
  - Authorizations

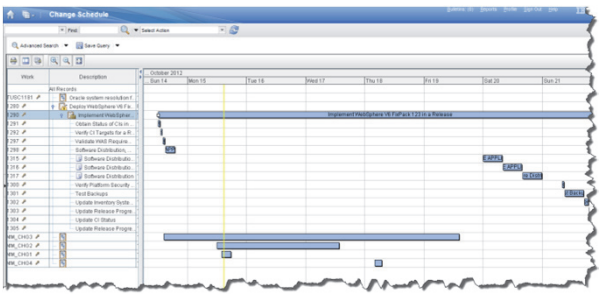
Normal change processing

In essence, normal changes are processed like emergency changes but with the full assessment, scheduling, and authorization.

These features are only supported by the advanced change processing workflows that are provides as part of IBM SmartCloud Control Desk. The advanced change processing workflows can easily be integrated with custom workflows to implement processes that meet the special requirements of your organization.

Change scheduling

- Change scheduling focuses on finding appropriate time slots in which to perform implementation tasks
- The following factors are taken into account:
  - CI outage (none, degraded, or offline) for both target and impacted CIs
  - CI change windows for both target and impacted CIs
  - Blackout periods
  - Resource availability (if you are using calendars for the task owners)
  - Task dependencies
- When the implementation tasks have been scheduled, the remaining tasks are scheduled using calendars and task dependencies



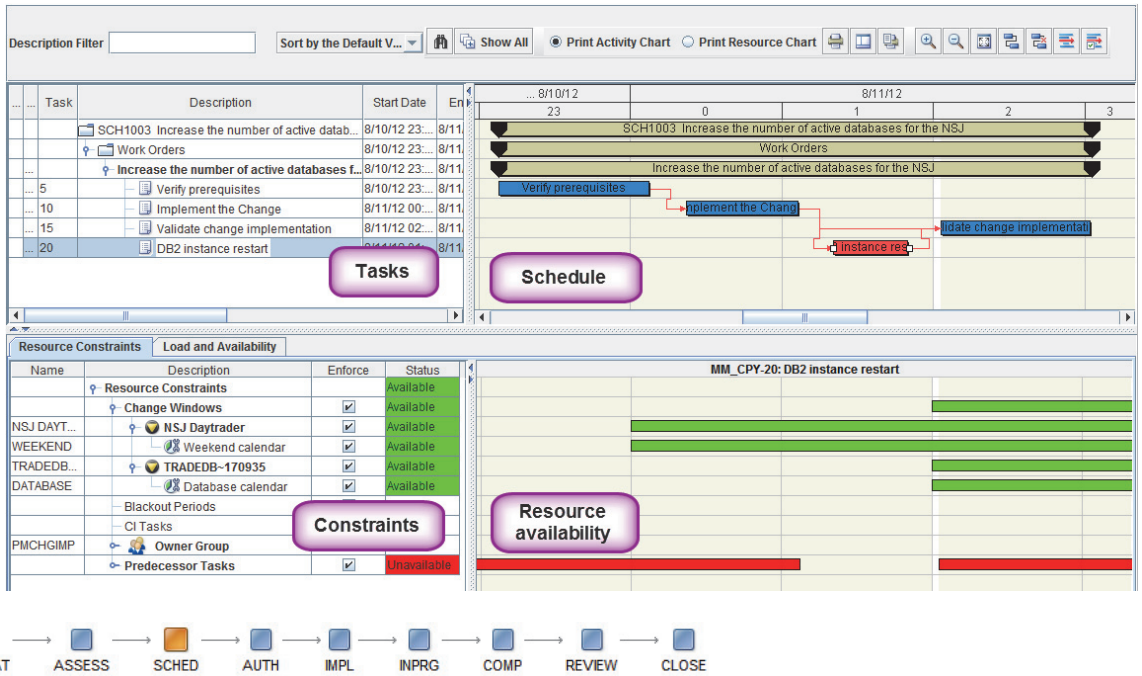
Change scheduling

When scheduling a change, the change owner tries to find the most convenient time to implement the change. Convenience is determined by when service disruptions are allowed to the CI or any impacted CIs, the availability and utilization of the implementation resources, and the availability of the CI.

IBM SmartCloud does not allow for implementation of multiple changes in the same timeframe on the same CI. The Change schedule provides an overview of all scheduled changes.

IBM SmartCloud Control Desk scheduler

- The Scheduler provides an interactive Gantt chart in which you can visualize and modify the planned schedule, alongside resource availability and constraints.



IBM SmartCloud Control Desk scheduler

When scheduling changes, the Gantt-view based Scheduler application (located in Planning and Scheduling application group) provides a very easy-to-use interface to schedule complex changes.

The Scheduler visualized task, task dates, task dependencies, and task status.

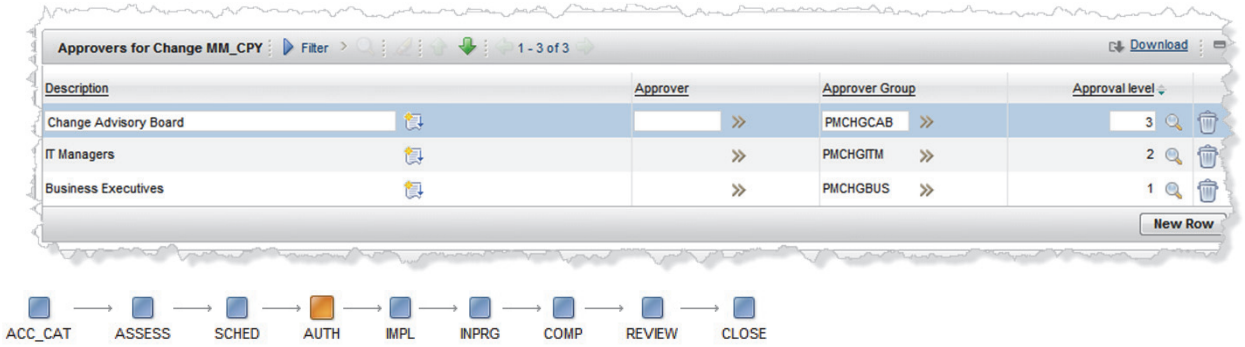
You can use drag-and-drop to re-schedule tasks.

In addition, you see the constraints that may prevent you from scheduling a change task for a specific period in time.The constraints that are considered are:

- Task dependencies
- CI availability (a CI cannot be included in more than one change at any point in time)
- Change windows for the CI and any impacted CIs
- Blackout periods
- Availability of implementation resources

Authorizing changes

- During the authorization phase of the change processing, you obtain the approval from one or more approvers.
- Typically the change advisory board is the primary authorization authority, but for high-impact, or high-risk changes you may also need the approval from IT or Business executives.
- The change owner specifies the level of authorization, and whether or not to obtain approval from a single or all the specified approvers.
- During authorization, the approvers use IBM SmartCloud Control Desk to access all the information, plan, schedule, impacts, assessment, related to the change in order to make an informed decision.



Authorizing changes

When the change has been categorized, assessed, and scheduled it is ready to be authorized.

IBM SmartCloud Control Desk automatically assigns approval tasks to the change approvers that are specified in the change.

Authorization can be granted from individual approvers, or members of an approval group (the CAP). In addition you can specify several levels of approval, and prioritize them

If multiple approvers are specified, you can configure the approval workflows to receive approval in a multiple ways ranging from one member from one group at any level to all members of all groups at all levels. The approval workflows will automatically assign approval task, as needed.

Normal change implementation and completion

- After approval has been obtained, normal changes progress in a fashion similar to emergency changes.
- For all types of changes you can apply automated tasks that for example create CI audit requests that are submitted to the configuration management team during the Review phase. The benefits of this are:
  - It is verified that the modifications were implemented as described in the change.
  - An audit track exists to document the results of your work.

  However, the drawbacks are:
  - Handing of the verification to configuration management may increase the turnaround time for the change.
  - The change process may become

Normal change implementation and completion

Upon approval, the normal change is implemented, reviewed, and closed in a similar fashion to emergency changes.

For normal changes, consider submitting a CI audit request to have the configuration management team verify that the modifications have been applied correctly.

If a Business Application Mapping tool like TADDM is implemented, the information that it discovers provide the current CI configurations and relationships, and this is used in the CI Audit process to reconcile authorized and actual CIs. In theory, only changes, for which all the included CIs pass an audit, should be closed successfully.

Student exercises

Student exercises

Summary

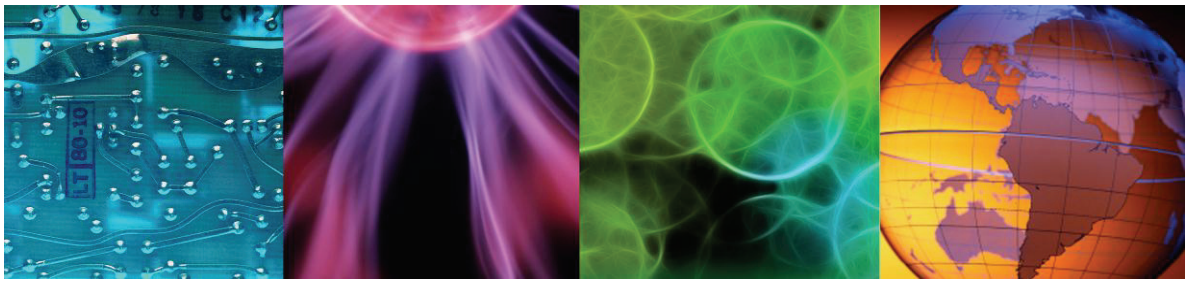
By now you should be able to:

- Describe the purpose of the change management process manager
- Describe the relationship of process requests to requests for change
- Describe the lifecycle of a process request
- Create and modify process requests
- Apply a job plan to a change
- Manage change windows and detect conflicts
- View the change implementation schedule
- Record and view the impact analysis of a change

Summary

6 Release management with IBM SmartCloud Control Desk 7.5

Release management with IBM SmartCloud Control Desk 7.5



What this chapter is about

This chapter focuses on how the release management features in IBM SmartCloud Control Desk can help you manage the implementation complex changes, such as composite changes that need to be coordinated across a number of CIs, or mass roll-out of software updates. These types of changes are commonly referred to as *releases*.

Objectives

- After you complete this unit, you will be able to:
- Articulate the main purposes of the release management discipline.
- Identify the IBM SmartCloud Control Desk applications used for release management.
- Understand the roles and responsibilities related to release management
- Describe the main phases of a generic release plan.
- Explain the use of the definitive media library

Objectives

Release management overview

- Release management:
  - is the controlled deployment of approved changes within the IT infrastructure
  - is integrated with change management
  - is used to manage complex changes to both hardware and software resources
    - Changes to multiple CIs that need to be coordinated (application rollout)
    - Changes that involve software deployment to a large number of CIs (mass updates)
  - can leverage operational management products (OMPs) such as IBM Tivoli Provisioning Manager, and Tivoli Application Dependency Discovery Manager.

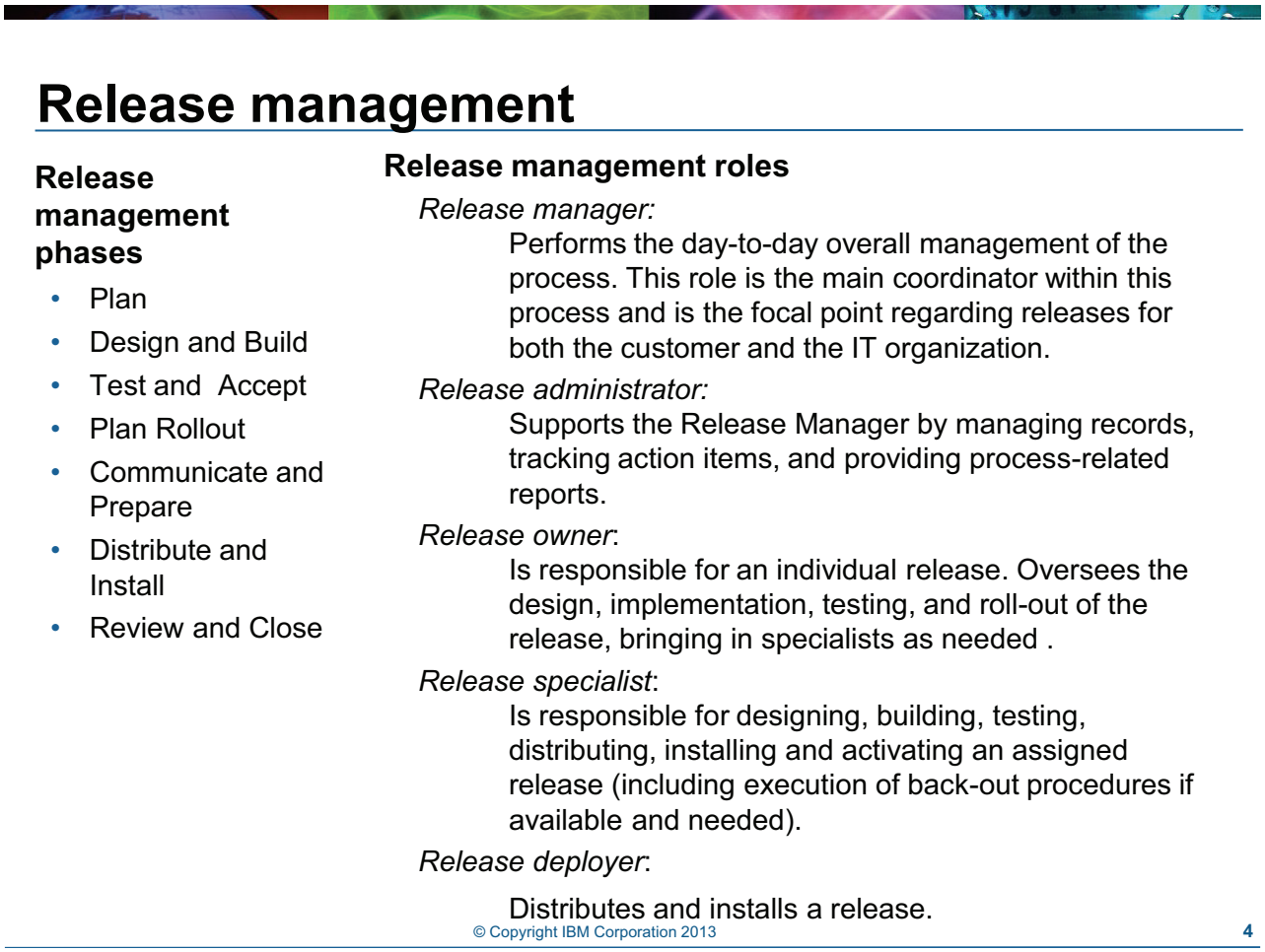
Release management overview

The overall objective for release management is to implement changes to IT services taking a holistic (people, process, technology) view which considers all aspects of a change including planning, designing, building, testing, training, communications and deployment activities. You can think of release management as an extension to change management that allows you to manage complex changes that include many individual changes and/or many target CIs.

Releases are used to deploy major update bundles to the infrastructure on a regular basis, for example every 3 months. Over time, changes of general, non-critical nature, for example fix packs and antivirus signature updates, are accumulated and added to a release. Once the time for the deployment of the release comes, the release owner plans the sequence in which the individual changes will be applied, and how to optimize the utilization of the implementation resources while minimizing downtime.

Releases are also used to manage mass-deployment of the same change, for example a Windows FixPack, to multiple servers.

In addition to managing releases and their related changes, releases management also involves management of the definitive media library, and interaction with deployment tools such as tivoli provisioning manager.



Release management

Because releases contain multiple target CIs and/or multiple changes, the management of releases is more complex than that of changes. In principle, each release is a project in its own right, and in the Plan phase the release owner basically defines the major milestones in the project, and plans the activities and tasks needed to reach the milestones. The release owner also includes people resources to ensure that there are no bottlenecks related to availability of staff. For regular, periodic releases changes have been added to the release, so the primary task is to analyze the changes, and create a deployment plan that minimizes outage and optimizes resource utilization.

The Design and Build phase is primarily used when new software needs to be deployed. In this phase, the new software is tested, deployment scripts are being developed, documentation updated.

Next, the deployment package is tested. Once it has passed test and verification, it is approved, and is now registered with the Definitive Media Library (DML). This ensures that the software package is under strict change control, and that it is properly backed up.

At this point the release owner knows what it takes to implement the changes in the release. In this phase there is no difference between periodic and mass deployment releases. The goal for the

release owner is to develop a deployment plan that meets the needs of the organization reaches the milestones in accordance with the original plan. In this deployment plan, the release owner must include tasks such as documentation updates, training, and communication to stakeholders about the upcoming changes. Naturally there is also an authorization step to ensure that the plan is reviewed and approved by the proper authorities.

When the plan is approved, it is time for the release owner to start interacting with the change management team in order to coordinate the implementation of the changes in the release. Most changes have already been approved before they are included in a release, so the new schedule needs to be communicated, and optionally re-approved.

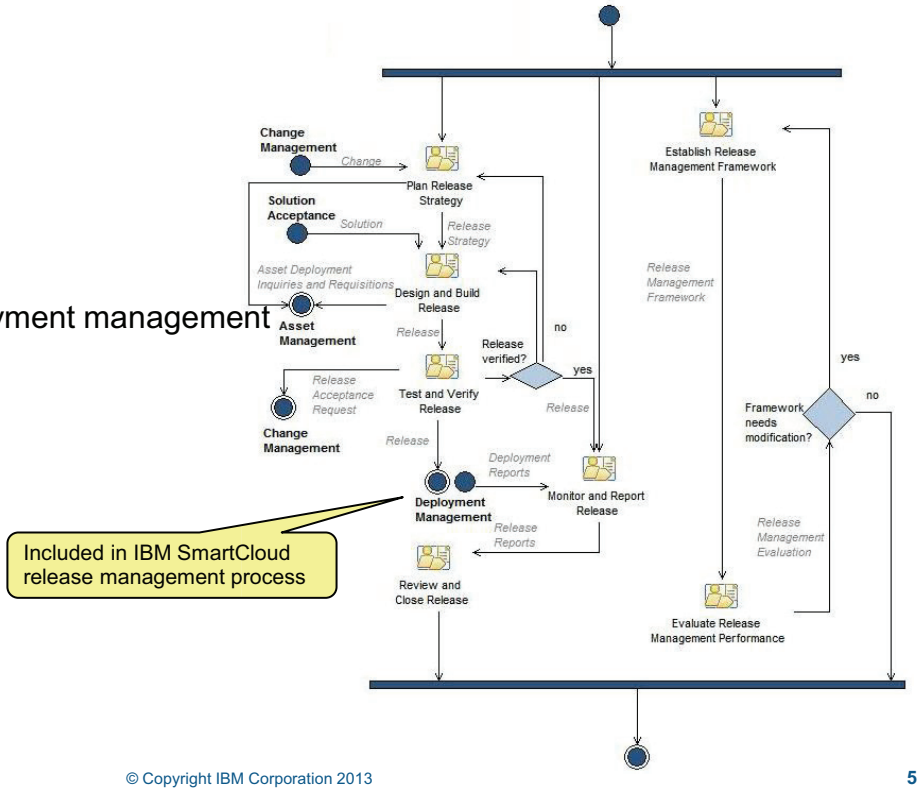
To implement the plan, the individual changes it contains are implemented in the sequence determined by the release manager.

Similarly to change processing, the release ends with a verification, communication and closure phase in which the release owner verifies that the expected results were achieved, and that the stakeholders are content.

The ITIL release management process

Main phases:

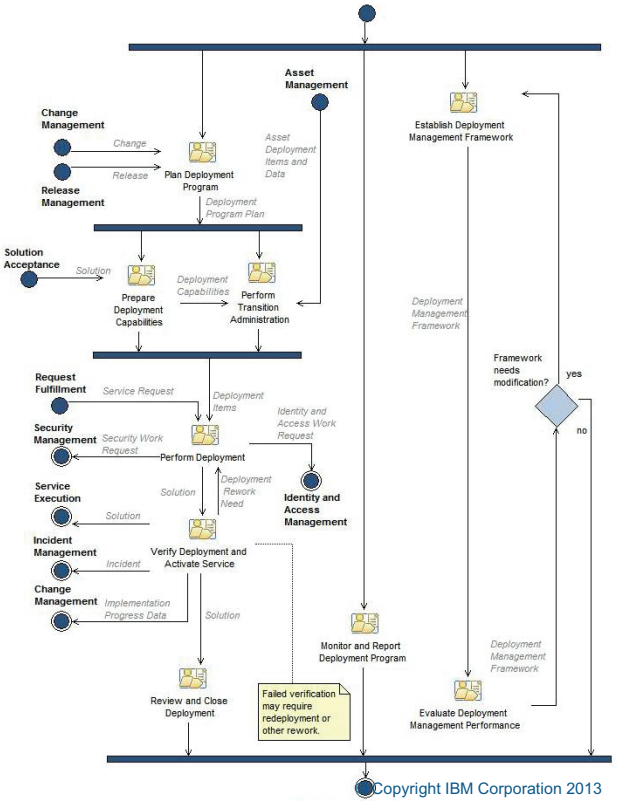
- Plan
- Design and build
- Test and verify
- Plan rollout
- Communicate
- Hand off to deployment management
- Review and close



The ITIL release management process

The high-level phases of a release processing as defined by ITIL is similar to those defined in IBM SmartCloud Control Desk. The main difference is, that the tasks performed by the deployment management team are included in the IBM SmartCloud Control Desk release processing workflows.

The deployment management process



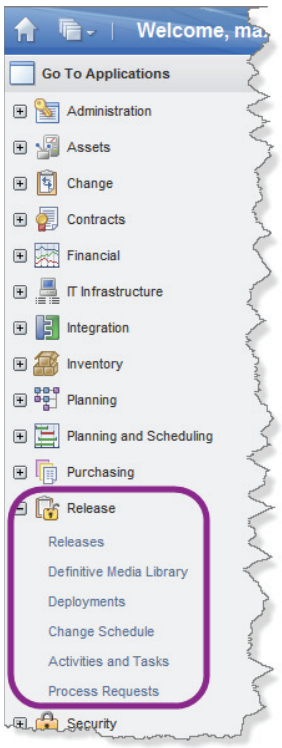
Main phases:

- Plan Deployment
- Prepare
- Perform Deployment
- Verify

The deployment management process

As you can see, the ITIL deployment management activities are included in IBM SmartCloud Control Desk release management process in the early Design, Build and Test, Accept phases, as well as in the actual deployment.

Release management applications and roles



Role	Security Group	Start Center	Person Group
Release Manager	PMRELEASE MANAGER	Release Manager (3)	PMRELMGR
Release Administrator	PMRELEASE ADMIN	Release Administrator (2)	PMRELADM
Release Owner	PMRELEASE OWNER	Release Owner (4)	PMRELOWN
Release Specialist	PMRELEASE SPECIALIST	Release Specialist (5)	PMRELSPC
Release Deployer	PMRELEASE DEPLOYER	Release Deployer (6)	PMRELDEP

General tools used by most Release Management users

Release management applications and roles

Like the other ITIL-based management disciplines, release management is also associated with a specific set of roles, which are assigned certain responsibilities.

In IBM SmartCloud Control Desk, each role is associated with a start center. Start centers are identified by a number which are shown in parentheses.

In the navigation bar, all IBM SmartCloud Control Desk applications are available from the Release application group.

Release management implementation

- In IBM SmartCloud Control Desk, the release management implementation is characterized by:
  - The release management process is driven by standard job plans and task automation used by Tivoli's process automation engine, rather than workflows.
  - Sample job plans are provided, but not response plans.
  - Approved changes can be imported into a change to reference CIs. (There is no linkage in the implementation phase).
  - Uses the Scheduler to schedule releases. Results are added to the Change Schedule.
  - Registers software images in the definitive media library
  - Can leverage OMPs for automated software deployment or backup/restore

Release management implementation

Contrary to the change management processes, the release management processes are driven by job plans, and automated tasks rather than workflows. If you are used to the dynamic nature of the change management processes, it may take a while to become used to working with release management.

Release management supports the use of response plans that are automatically applied when a release request is accepted, but IBM SmartCloud Control Desk does not provide any templates. If you want to use this facility, you must create your won response plans, and populate them with the content that matches your requirements. This is of course not dependent o whether or not templates are provided.

When changes are added to a release, only the target CIs defined for the change are included in the change. If the change contains specific CIs as targets of any implementation tasks, these are not automatically added to the release.

Release specification (plan)

- When specifying releases the release owner manually:
  - Create your own job plans (templates are provided) that specify what needs to be done.
  - Define dependencies between tasks
  - Classify your tasks and apply flow actions and assisted workflows
  - Assign ownership for each task.

- During this phase you consider:
  - What is the nature of the release (hw, sw, site, documentation)?
  - Which CIs are involved, do you need to create any?
  - Who are the stakeholders?
  - Are any changes involved in the release?

Release specification (plan)

Tivoli's process automation engineThe first phase of a release is the Plan phase. In this phase, the release owner defines the major milestones and outlines the high-level activities of for the release. To complete this task, the release owner used standard facilities in Tivoli's process automation engine to create a job plan that contains activities and tasks which may of may not depend on one another.IBM SmartCloud Control Desk does provide sample job plans that can be leveraged.

One important aspect that may be new to people with a change management background is the classification of tasks. Release management uses specific task classifications to assist certain functions, for example definition of software packages. The release owner may also apply automated tasks to the job plan to automate certain tasks, for example notifications.

Naturally each release is unique, so the release owner needs to consider the requirements for training, documentation, communication, staffing, authorization, scheduling, and more for each and every release.

Release management job plans

- Seven release activity job plans are provided with the product:
  - PMRELEASE Generic ITIL V3 aligned job plan
  - PMRELDB Database installation
  - PMRELMW Middleware installation
  - PMRELSB Server build
  - PMRELBLDTE Build and test a release package
  - PMRELDPY Plan, prepare, and deploy a release package
  - PMRELSEDPY Build, test, verify, plan, and deploy a release package
- A single change job plan is provided
  - PMRELCHG Forces the change to wait for the release to complete
- No sample response plans are provided with IBM SmartCloud Control Desk

Release management job plans

IBM SmartCloud Control Desk provides a set of template activity job plans for release management. These cover most cases for which you would consider creating and implementing a release.

In addition, a special job plan, which should be assigned to changes that are included in releases, is provided. This job plan should replace the implementation tasks in the change, and the only activity it performs is to wait for the change to complete, and then close the change.

Task classifications

You can use the following task classifications to apply specific importance to selected tasks:

PMRELCPR **Change Progress**
Use this classification for tasks that change the progress value of a release.

PMRELIMP **Implementation**
Use this classification for an implementation task. An implementation task is any task that makes modifications to a configuration item (CI).

RELDEFSW **Define/Refine software**
Use this classification if the task instructs the task owner to define or refine a software package.

RELIMPSW **Import software**
Use this classification for tasks that involve importing software image CIs into a DML repository.

REQADCTR **Request to add Change to a Release**
Use this classification for tasks that involve importing changes into a release.

REQRMCFR **Request to remove Change from a Release**
Use this classification for tasks that involve importing changes into a release.

SWDIST **Software Distribution**
Use this classification for tasks that distribute software.

 11

Task classifications

When defining the release plan, the release owner can use special task classifications to apply special processing for selected tasks.

IBM SmartCloud Control Desk provides a set of pre-defined task classifications. Naturally, this can be extended to cover additional use cases.

Assisted workflows

Among the provided assisted workflows are:

PMRELACCEP	Determine whether a release is accepted.
PMRELDSTSW	Start a deployment using an Integration Module.
PMRELGETST	Get the status of a deployment.
PMRELPLN	Provide assistance for planning a release.
PMRELROLL	Approve a rollout plan.
PMRELSCHED	Release schedule approval.
PMRELSCOPE	Release scope approval.
PMRELSWDST	Launch to the Deployments application from a task.

These workflows can be associated with certain process tasks in order to help the task owner complete the task.

Assisted workflows

In addition to the special classifications, the release owner can apply assisted workflows, which allow the task owner to easily complete the task.

Release packaging (build)

- When building a release package the release specialist:
  - Identifies and documents HW requirements.
  - Identifies SW installation images, and registers them in the CMDB.
  - Creates installation and customization instructions.
  - Creates automation scripts for SW installation, customization, integration.
  - Creates and documents back-out procedures.
  - Creates/updates training material and operational procedures.
  - Creates a release package that contains all the deliverables.
- During this phase you consider:
  - What is the nature of the release (hw, sw, site)?
  - Which types of resources are involved, do you need to create any?
  - Is SW included?
  - How are the resources being deployed?

 13

Release packaging (Build)

In the release contains deployment of software components or updates, it is more than likely that the release plan will include the Design and Build, and Test and Accept phases. However, these phases are also used to plan for major hardware or building changes.

Design and Build is the responsibility of the release specialist, and basically consists of developing and documenting the necessary procedures, scripts, and definitions in the tools used for deployment, needed to deploy the software in question.

If new hardware or modifications to the physical infrastructure, for example installation of a new air-conditioning system, The Design and Build phase may include planning for the installation, ensuring access, verification of power demand, and so on.

Release verification (test)

- When testing and verifying the release package the release deployer:
  - Tests the release package, and documents the results.
  - Upon successful testing (acceptance) the software package is registered in the definitive media library
- During this phase you consider:
  - Is a dedicated test environment required?
  - Is the change properly documented?

Release verification (test)

The release deployer is responsible for testing and verifying the deployment packages built by the release specialist.

Definitive media libraries

ITIL definition:

One or more locations in which the definitive and approved versions of all software configuration items are securely stored. The definitive media library may also contain associated configuration items such as licenses and documentation. It is a single logical storage area even if there are multiple locations. The definitive media library is controlled by service asset and configuration management and is recorded in the configuration management system.

In IBM SmartCloud Control Desk, only CIs that are in an operational state can be added to the definitive media library. Also, only software from the definitive media library is acceptable for use in a release.

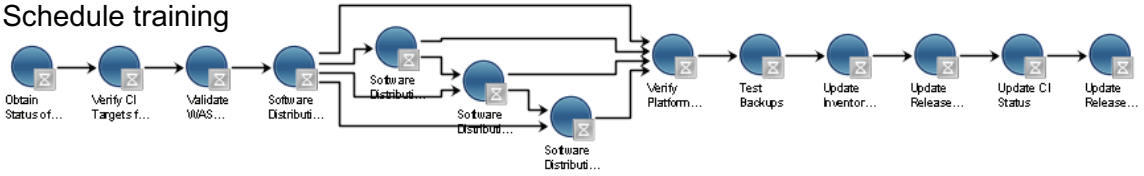
Definitive media libraries

When a software deployment package has been accepted, it is registered in the Definitive Media Library. This library is under change control, so the configuration librarian needs to be involved.

The Definitive media Library is associated with tasks that ensure that the information is backed up, that restoration can be performed, and that copies for disaster recovery exist.

Release planning (plan rollout)

- When planning the rollout of the release, the release owner and release deployer:
  - Create detailed plans with dates and deliverables for the rollout to each site.
- Schedule delivery of any new (HW) CIs to each site.
  - Schedule the release implementation
  - Schedule training



- During this phase you consider:
  - Who perform the implementation, when, and how?
  - What is the planned duration of each implementation task?
  - What are the targets of the release implementation?
  - Are any particular prerequisites needed?
  - Is training required?

 16

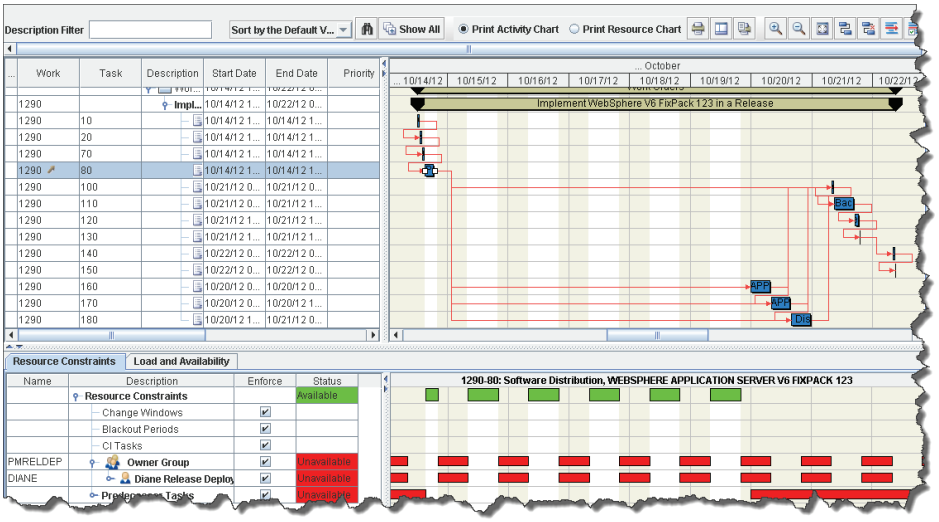
Release planning (plan rollout)

When all the procedures for deployment and implementation of the changes in the release have been defined and approved, all that is left is for the release owner to create an implementation plan. This may sound as an easy task, but because of the complexity of the release, and the dependencies of the changes it contains, it can be a complex, and time consuming task.

During development of the deployment plan the release owner may find the Workplan Map a convenient tool to visualize the plan and access the task details.

Release scheduling

- The Scheduler is a valuable tool for the release owner when scheduling the rollout plan.
- To create a scheduler project, reference the work order number for the activity in the release that represents the implementation phase

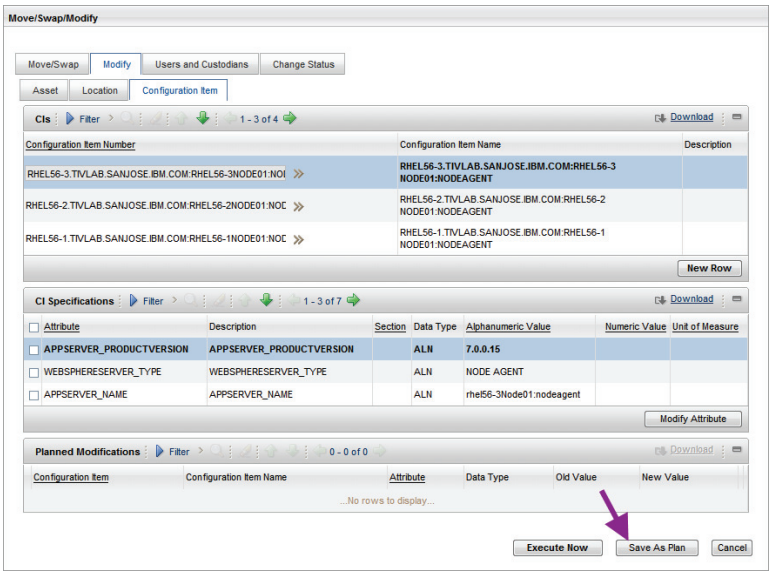


Release scheduling

The Scheduler application allows you to create a release implementation schedule using a graphical interface that shows the schedule alongside the resource utilization, change windows, and blackout periods. This helps you ensure that you schedule the implementation tasks at the optimal times.

Move/Swap/Modify

- When working with implementation tasks, use the *Save As Plan* option of the Move/Swap/Modify tool to record anticipated updates to the target CIs.



- Once the task completes, the CI attributes are updated according to the plan.

Move/Swap/Modify

The changes that are included in a release are either approved changes that have been subject to the full change processing before being added to the release, or changes that are created during release processing. For mass-deployment of software, it is not uncommon, that the release management team initiate changes themselves. Either way, to ensure that the changes to the CIs are not updated in the IBM SmartCloud Control Desk CMDB before the change has been implemented, you should use the Save As Plan option of the Move/Swap/Modify tool, when you plan the individual changes. This ensures that the information in the IBM SmartCloud Control Desk is updated only after successful completion of the implementation tasks in the change.

Release synchronization (communicate)

- When communicating the release implementation schedule, the release owner:
  - Informs stakeholders, users, and support personnel about the upcoming event(s)
  - Schedule site-specific testing, system shutdowns, reminders about the release, and so on.

- During this phase you consider:
  - Who are affected by the release?
  - Will the users experience outages?
  - Are any particular prerequisites needed?
  - Is training required?

Release synchronization (communicate)

When the rollout plan is completed and approved, the release owner must ensure that the organization is informed about the upcoming changes.

Releases typically have a greater impact than changes. Outages caused by releases may affect many users and several parts of the business, so it is important that the communication about the changes that are about to happen is proactive, timely, and concise. This will allow the lines of business to plan in accordance with the rollout plan.

It is especially important that the implementation activities are synchronized with the operations team to make sure that they are aware of changes to the infrastructure that may affect operations. If CIs are added or removed, operations need to modify their procedures (this should already be in the release plan), to begin managing the new resources or stop managing resources that are removed.

Release rollout (implementation)

- When implementing the release, the following activities takes place:
  - Distribution and installation of hardware and software, ensuring appropriate data is provided for asset and configuration updates
  - Customization, where needed, of:
    - CIs to reflect their specific usage context
    - Identity and access records (by initiating updates using the Identity and access management process)
    - Security mechanisms (also using update requests, to the security management process)
  - Removal of redundant services and assets, (processes, procedures and tools).
  - Introduction of new or changed processes to the service provider teams responsible for service management activities.
- The release owner:
  - Oversees that the implementation tasks progress as expected

 20

Release rollout (implementation)

The success of the release implementation is naturally dependent upon the amount of work and attention to details that were put into creating and specifying the plan.

During implementation, the individual changes are implemented in the sequence specified in the plan.

The release owner can check the progress of the implementation, and communicates with the configuration management team to verify that the changes are implemented as expected.

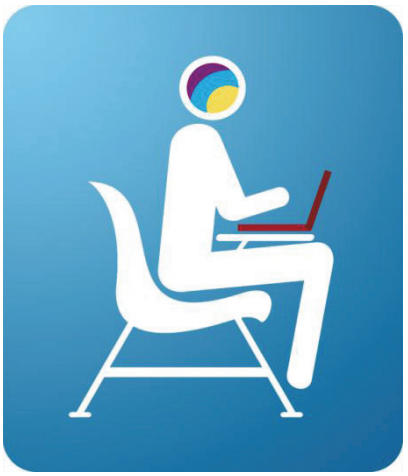
Release review (complete)

- When reviewing the release, the release owner:
  - examines the information relating to the usage of a release
  - identifies what has worked well and what has not
  - identify improvements in any aspect of the release
- During this phase you consider:
  - Success rates from deploying the release
  - Efficiency, in both people and technical resource, in deploying the release
  - User feedback on missing and erroneous documentation and usage guidance

Release review (complete)

As for most other projects, the final review assesses the effectiveness of the release, and tries to extract and document the successes as well as failures of the release. This information will provide valuable input for the next release in terms of what to-do, and what-not-to-do.

Student exercises



Student exercises

Summary

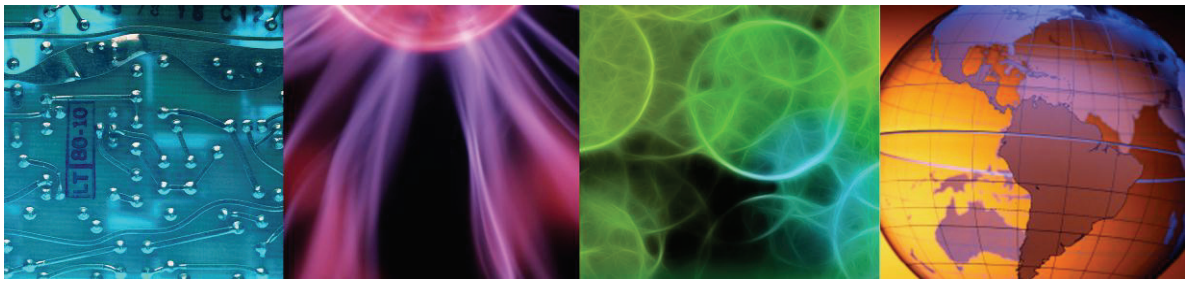
By now, you are able to:

- Articulate the main purposes of the release management discipline.
- Identify the IBM SmartCloud Control Desk applications used for release management.
- Understand the roles and responsibilities related to release management
- Describe the main phases of a generic release plan.
- Explain the use of the definitive media library

Summary

7 IBM SmartCloud Control Desk 7.5 summary

IBM SmartCloud Control Desk Summary



What this chapter is about

This chapter summarizes the benefits of using IBM SmartCloud Control Desk to establish a CMDB, and manage your configurations, changes, and releases using its advanced facilities.

Objectives

Upon completion of this unit, you will be able to:

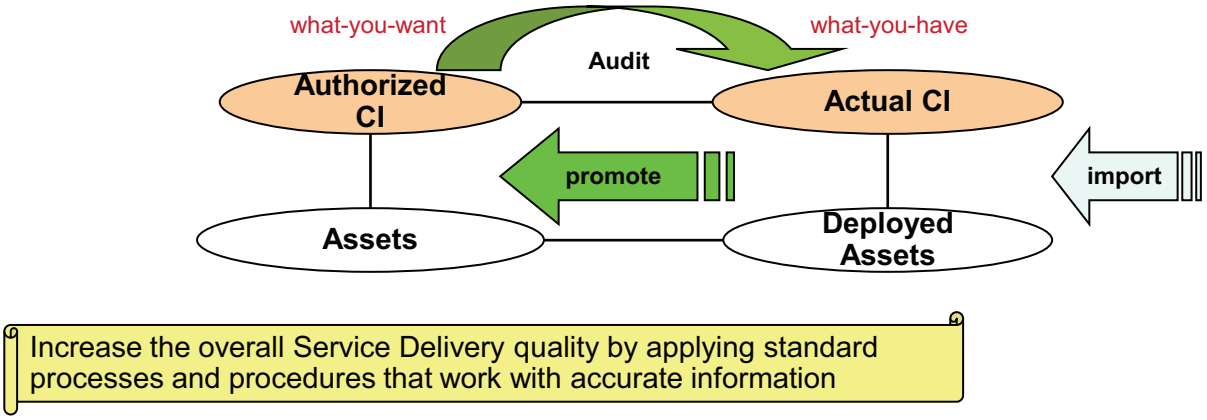
- Describe the key facilities in IBM SmartCloud Desk that facilitates ITIL-based processes for:
  - Configuration management
  - Change management
  - Release management
- Explain how the CMDB is organized
- Articulate the use and benefits of:
  - Configuration Item audit
  - Baselining
  - Impact analysis
  - Scheduling
  - Adaptive workflows

Objectives

Configuration, change, and release management

Manages the technical aspects of the IT infrastructure

- Ensure a trustworthy CMDB
- Reduce impact of changes by defining standard, workflow-driven change procedures
- Ensure integrity of existing infrastructure during release of new hardware or software



Configuration, change, and release management

IBM SmartCloud Control Desk

- uses two representations for your resources: assets and configuration items
- stores the actual and authorized configurations of both assets and CIs in its CMDB

Authorized (managed) resources can be created manually, or by promoting actual (unmanaged) resources

By comparing the actual and authorized resources you can verify that the actual configurations adhere to your plan.

Basing IT management on standardized processes, automation, and especially accurate information helps the IT department improve the Service Delivery quality, avoid mistakes and un-expected outages, and lower the man-power resources needed support the IT based systems that are needed to conduct the business.

Configuration , change, and release management benefits

Feature	Benefits
CI Auditing and remediation	▪ Immediately remediate an audit variance by • updating an Authorized CI to reflect the Actual value • creating a Change or Service Request • Sending an email to the CI owner ▪ View approved Changes for a CI when viewing an audit variance to help determine if there was an approved change that caused the variance. ▪ View CI attribute history while viewing an audit variance. ▪ View the last audit results for the same CI.
Compliance Policy enforcement	▪ Track and record changes across the organization ▪ Manage desired states of CIs, application and service configurations to validate compliance with internal and external policies
Calendaring capability	▪ Schedule changes to minimize impact - change windows, resource scheduling can help identify exposures to planned changes, thus protecting critical business services
Blackout period identification	▪ Blackout periods identify critical business periods when outages would be expensive. ▪ Automated Change scheduling can help avoid blackout periods ▪ Can apply to all CI's or to selected CI's ▪ Blackout period approvers can be specified
Business Impact Analysis	▪ Complete technical and Business impact analysis capabilities ▪ Based on thorough relationships, analysis can be performed to spot direct relationship impact as well as associated impacts to outages due to changes.
Change and Release authorization	▪ Prevent unauthorized changes by verifying authorization access based on roles
Deployment of approved images	▪ Save on support costs by deploying approved images from the Definitive Media Library ▪ Supports a number of media libraries; Also integrates with IBM Rational Asset Manager

Configuration, change, and release management benefits

Adopting ITIL based processes to manage the configuration of your infrastructure provides many benefits. The most obvious are:

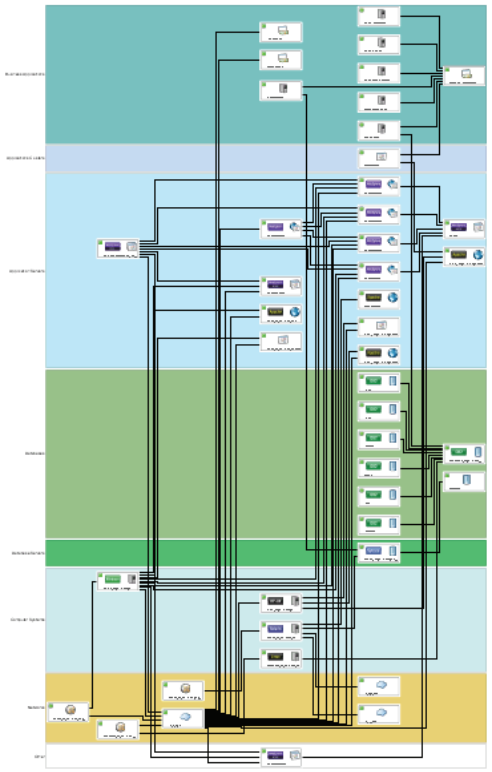
- Improve the quality of your service delivery by minimizing unplanned outages
- Reduce costs by avoiding problems, managing SW licenses better, optimize resource utilization and reduce energy consumption and CO2 footprint
- Understand complex application infrastructures

Visualizes topologies

Helps incident, problem management understand complex relationships

- Business and Detail views
- Filtering, and search capabilities
- Shows status, changes, and impacts

Quickly identify dependencies and relationships to increase the quality and speed in evaluating incidents, working with problems, and assessing change impacts.



Visualizes topologies

The topology views provided in IBM SmartCloud Control Desk allows you to easily identify dependencies, and identify resources that are impacted by a change.

Swim lanes provide a convenient grouping of similar resources.

Providing a facility to easily understand dependencies and relationships helps increasing the responsiveness and quality of:

Incident Management:
Determine impacts and relationships to focus the initial investigation and better classify and categorize the incidents.

Problem Management:
Focus problem determination and troubleshooting to decrease failure-time-to-resolution.

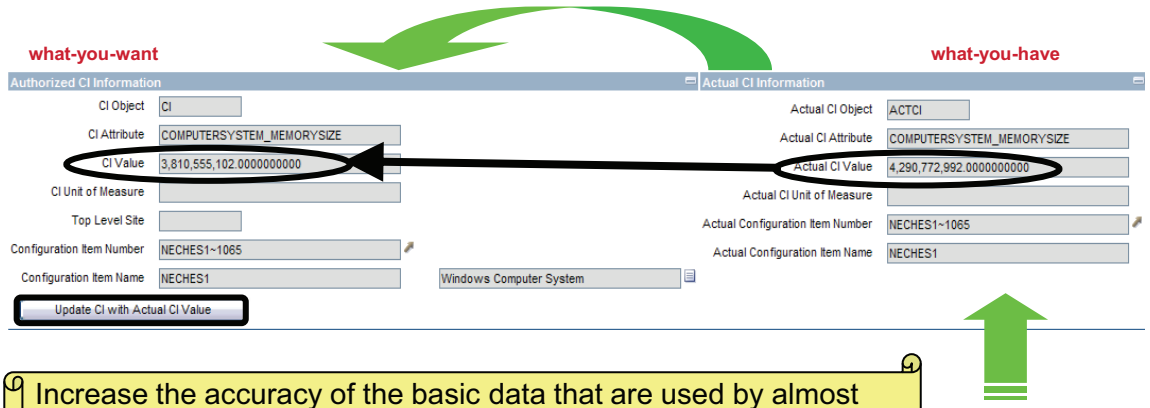
Configuration Management:
Visualize business service and application configurations including OSI layers 2-7 to document and verify compliance.

Change Management:

Provide visual impact analysis to identify all components that are affected by a change.

CI auditing: Ensuring a trustworthy CMDB

- Ensure accurate Authorized CIs to allow business processes to run successfully and efficiently
  - Immediately remediate an audit variance by updating authorized with actual value
  - Create a Change, Incident or Problem to remediate an audit variance.
  - Browse approved Changes, attribute history, and audit results for a CI
- Identify unauthorized Changes before they cause problems



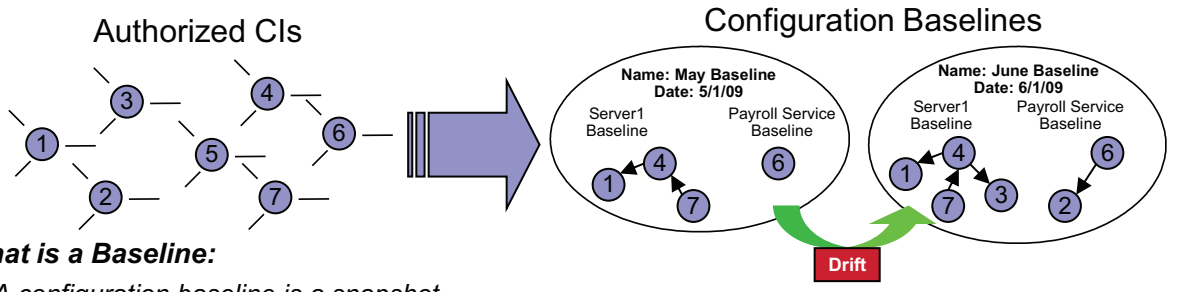
Increase the accuracy of the basic data that are used by almost any IT management process for visualization, control, and automation.

CI auditing: Ensuring a trustworthy CMDB

The configuration item audit function is key to ensuring that the CMDB is trustworthy, and to identify unauthorized changes.

This helps the business increase the accuracy of the data that are used by most IT management processes for visualization, control, and automation.

CI baselines

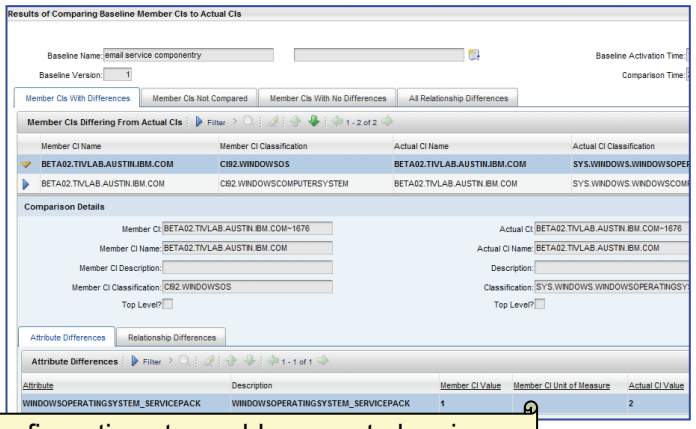


What is a Baseline:

"*A configuration baseline is a snapshot that represents an approved configuration at a particular time that people can reference, compare to, and apply changes to in a manner that is understandable.*"

Business Value:

- Provide IT standardization by easily taking a snapshot of CIs, at any time, to produce an approved configuration.
- Ability to quickly detect changes to those approved configurations.



Maintain approved business system configurations to enable correct planning, accounting, and resource allocation to ensure service delivery.

 7

CI baselines

Baselines allow you to identify application drift.

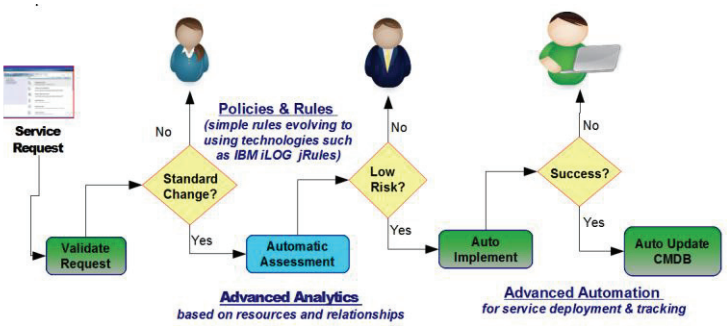
This information:

- Helps you track the business application compositions.
- Enables ensuring that staffing, accounting, and other related topics matches the actual implementation.
- Enables automated processes to react to dynamics in the business application configurations.

Change management: automate and standardize changes

- Organizations need to “standardize” and “automate” changes to save on labor cost
- User roles evolve more towards determining policies, managing risk and reviewing / validating tool recommendations.

  Example:
  - Standard / pre-authorized changes” can be fully automated, with full change records, as long as the conditions are met.
  - Else, queued for human assessment / review / approval / implementation / corrective action.



- Standardize and pre-authorize low risk changes to process them quickly, or in an automated fashion.
- Automated Risk, Impact and Priority calculation that drive the Change process flow to ensure the Changes get processed quickly, accurately and there is minimal impact to the business.

 8

Change management: automate and standardize changes

Virtualization and Cloud increases the rate and pace of change – Customers are asking for ways to automate routine changes without requiring human touch.

- Allow customers to easily standardize and pre-authorize routine (low risk) changes to process them quickly, therefore allowing them to focus on their high risk Changes
- Automated Risk, Impact and Priority calculation that drive the Change process flow to ensure the Changes get processed quickly, accurately and there is minimal impact to the Business.

Automated calculation of key process drivers

Risk: Based on impact & probability of failure

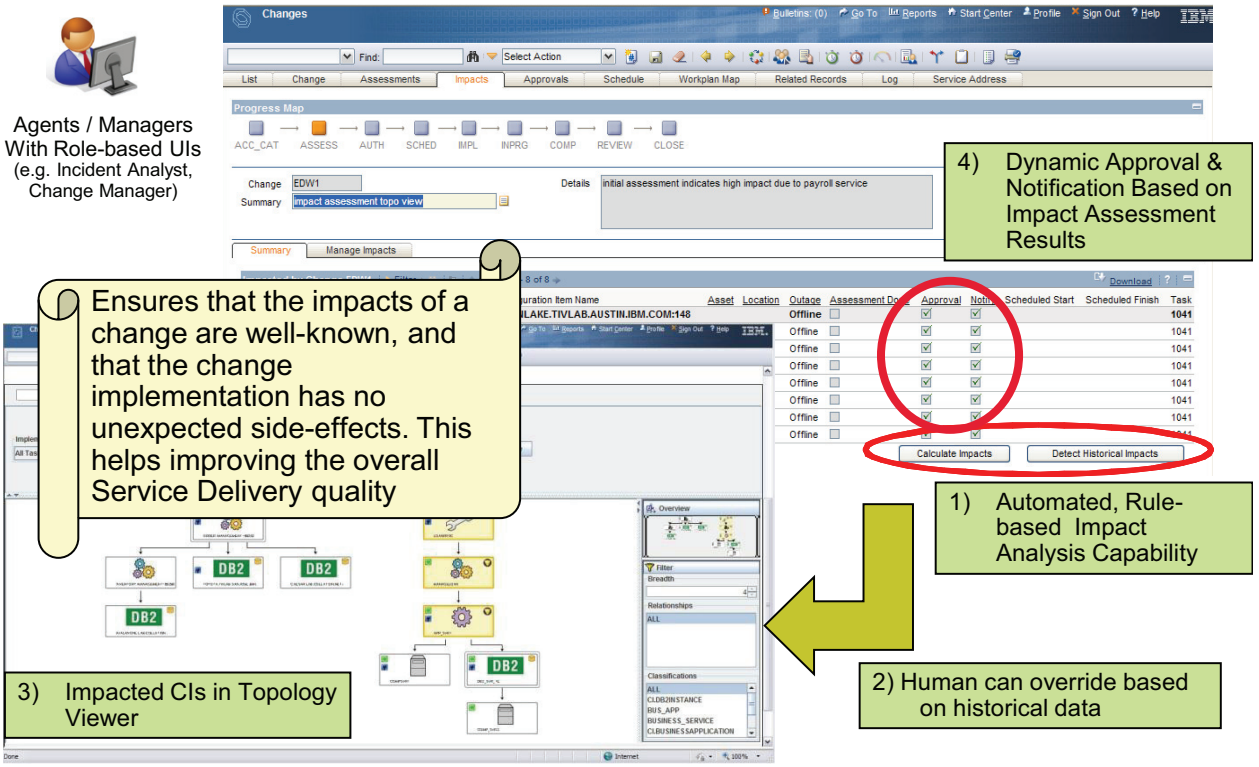
Impact: Based on outage impact & maximum assessed impact

Priority: Based on impact and urgency

Automatic process adjustment based on these calculated values

- Standard Change
- Emergency Change
- Normal Change

Change management – business impact analysis



 9

Change Management - business impact analysis

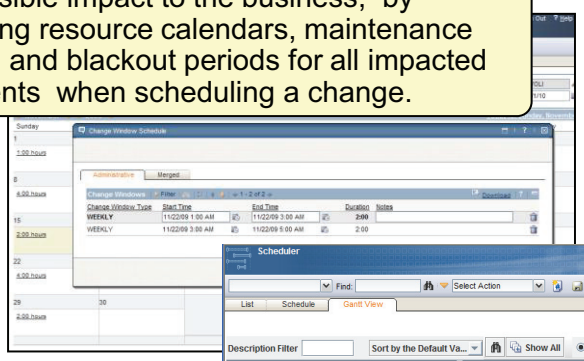
The automated impact analysis that is built into the IBM SmartCloud Control Desk change management feature identifies the resources that will be impacted by a change.

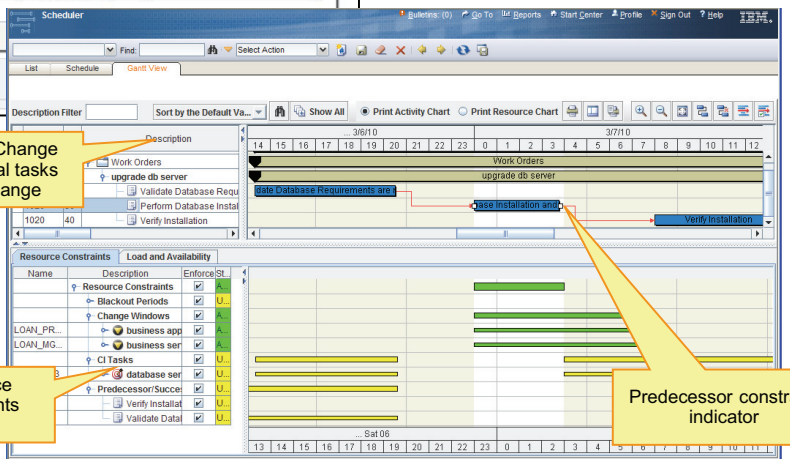
By combining this information with information related to change windows, blackout periods, and implementation resource availability changes can be automatically scheduled.

Change scheduling – subject to multiple constraints

Ensures that change implementation has the least possible impact to the business, by considering resource calendars, maintenance windows, and blackout periods for all impacted components when scheduling a change.

- Schedule based on:
  - Change Windows
  - Black out periods
  - Change Implementation Schedule
- Automated Change Scheduling
  - Tasks, People, CI windows
- Schedule Conflict Detection
- Schedule Visualization



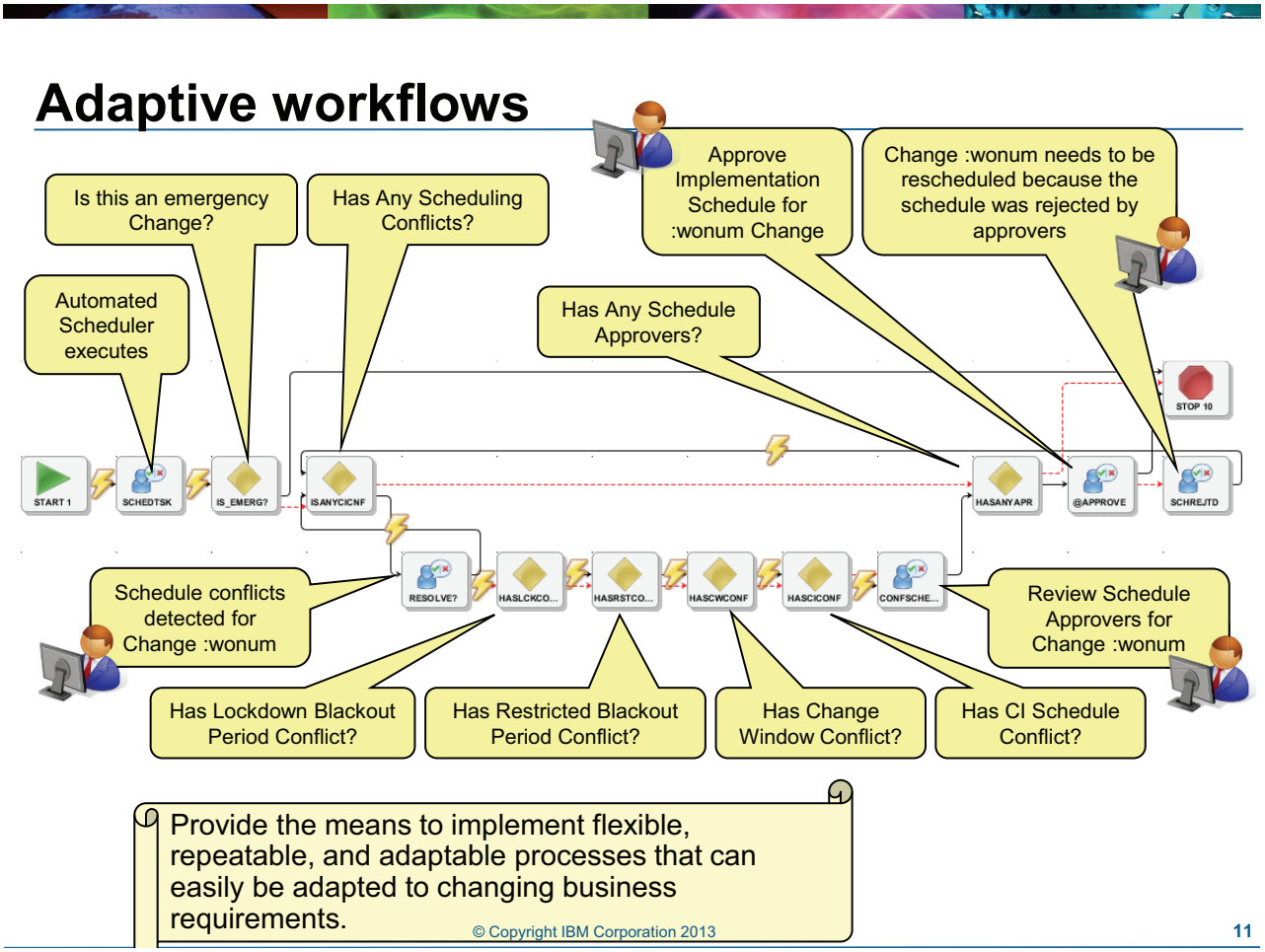


Agents / Managers
With Role-based UIs
(e.g. Incident Analyst, Change Manager)

Change Scheduling - subject to multiple constraints

The Gantt chart based scheduler is a valuable tool to visualize schedules, and to identify constraints that prevent scheduling at specific times.

The scheduling facility includes information about maintenance windows and blackout periods for all impacted Cis as well as the calendars for the implementation resources. This ensures that changes are implemented when they disturb normal business operations the least.



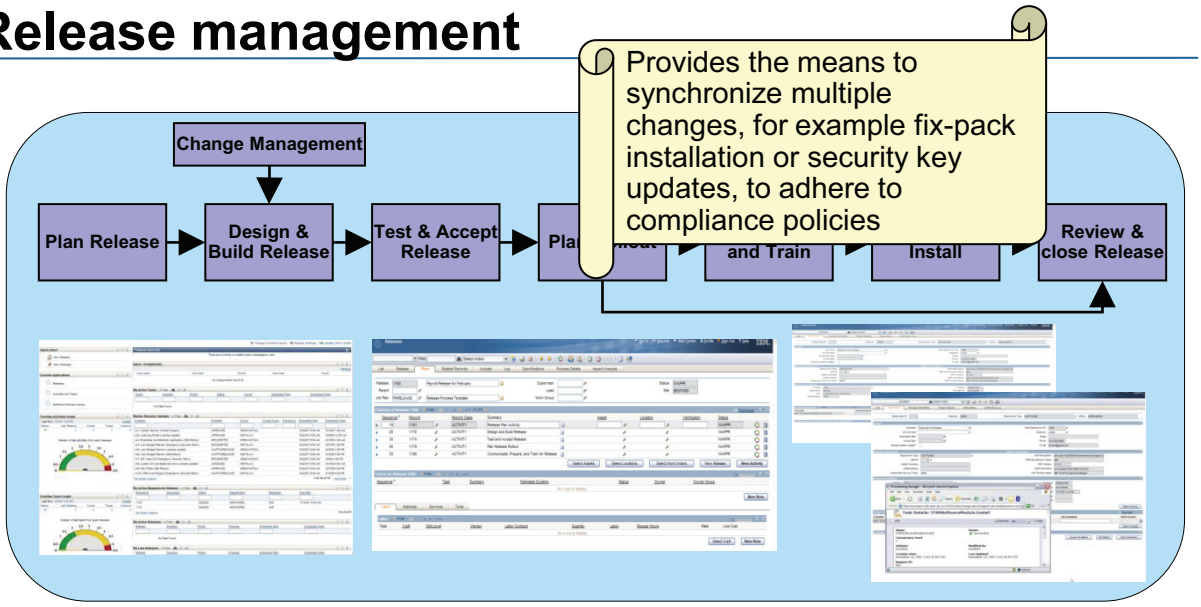
Adaptive workflows

IBM SmartCloud Control Desk uses workflows to control the change processing. Within the workflows, the change can be routed trough different paths based on information in the change.

Workflows are used in conjunction to automated tasks, to automate the change processing, including implementations.

IBM SmartCloud Control Desk provides several ITIL compliant workflows, which can be modified to meet specific needs.

Release management



- Ability to plan and oversee the successful roll-out of new and changed software and associated hardware, including documentation and training.
- Role-based start centers, workflows, scheduling and analytics
- Integration with deployment tools like Tivoli Provisioning Manager and Tivoli Application Dependency Discovery Manager, and to software repositories like the Rational Asset Manager

Release management

Powerful release manage function enable management of complex changes that require coordination of updates to multiple resources or mass deployment of software.

Such multi-change implementations are often required to orchestrate installation of fix-packs, or password/security key updates.

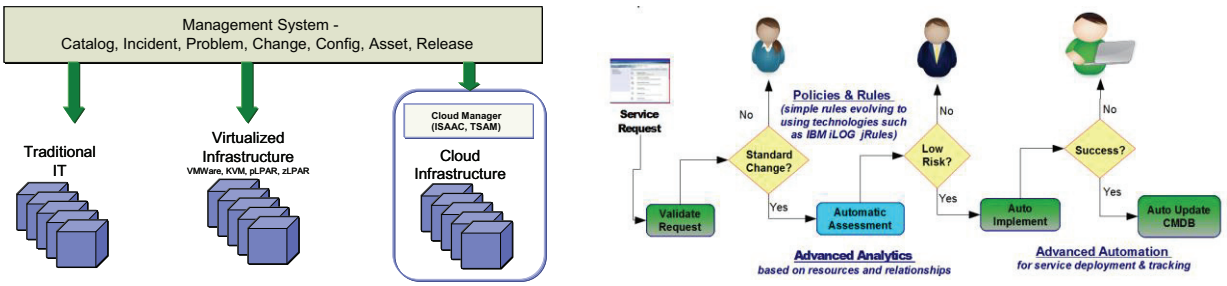
Controlling and documenting these updates helps the business demonstrate and prove compliance with current legislation and adherence with internal policies.

Cloud-ready service management

Challenge: The very things that make Cloud-like infrastructures so beneficial to organizations – they are dynamic, responsive, flexible – can quickly bring down a datacenter if it is not managed correctly. Cloud encourages quicker changes – which also result in an increasing volume of changes. Traditional change management products are not ideal for managing such an environment and customers can quickly find themselves unable to keep up with their own technology.

Solution: A unified approach to service management with analysis and policy-based automation to reduce labor costs and improve responsiveness.

Combine ITIL-based process controls with solution-oriented run-book automation in a way that ensures flexibility and extensibility while maintaining adherence to governance principles.



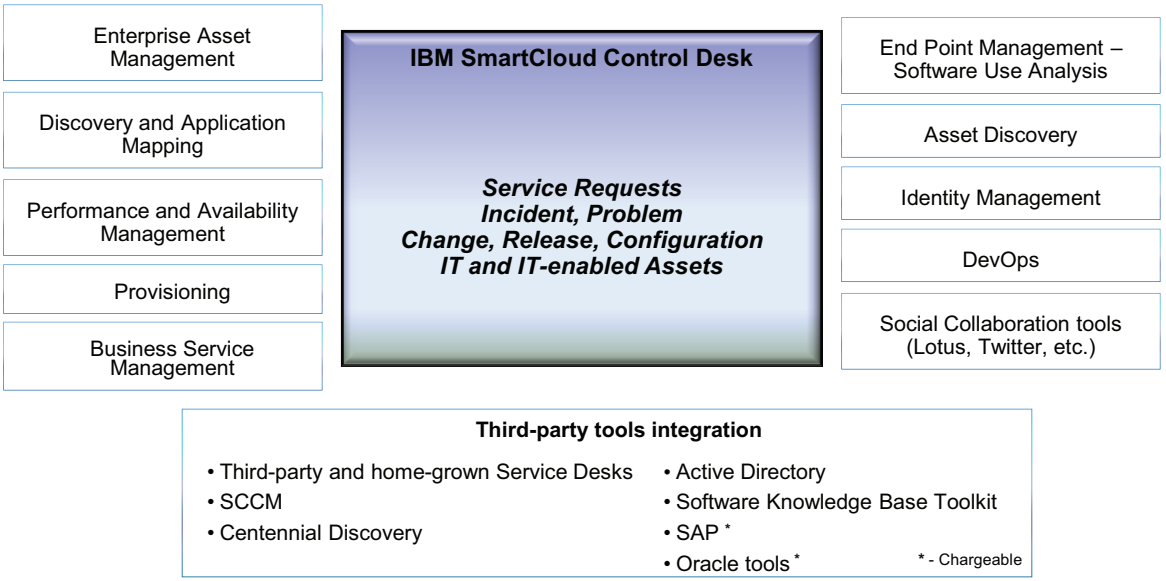
 13

Cloud-ready service management

IBM SmartCloud Control Desk provides the basic platform data, and automation capabilities that enable you to keep up with the dynamics of cloud environments.

Integration for end-to-end service management

IBM SmartCloud Control Desk integrates with other IBM and third-party solutions to provide an end to end service management solution



Integration for end-to-end service management

Service desk and service catalog are the face of operations to the end user

Third-party tools integration

Improve efficiency by integrating with existing service desks, Computer Telephony Integration systems, create your own integration

Business Service Management

Provide a business dashboard with customizable views that detail service performance levels

Discovery and Application Mapping

Discover infrastructure to be managed and populate into the CMDB

Asset Discovery

Maintain an up-to-date inventory of software, hardware and software use data

End Point Management

Meet compliance requirements and manage vulnerabilities through effective patch and configuration management of servers and endpoints

DevOps

Bridge the gap between Development and Operations by integrating with Rational Team Concert and Rational Asset Manager

Identity Management

Manage user access to services and requests such as password reset based on requester's authorization

Performance and Availability management

Reduce MTTR, operation costs and outages by monitoring infrastructure events to uncover the root cause of problems

Provisioning

Increase quality of service delivery by reducing time taken to provision new services

Cloud Services

Service catalog Provisioning of cloud

Adding business value with IBM SmartCloud Control Desk

IBM SmartCloud Control Desk can transform the value your organization brings to the business by:

Bridging organizational silos

- ✓ Unifying asset, change and service management processes under a single platform, single GUI, single license for assets across the enterprise

Enabling change at cloud speed

- ✓ Providing ready-to-use policy-based analysis and automation to enable “zero-touch” automation of ITIL change management across traditional and cloud infrastructures
- ✓ Dramatically enhancing process mean time to repair and service quality

Increasing your staff productivity, empowering your customers

- ✓ Raising service staff profiles – L1 becomes L2
- ✓ Enabling self service to your customer’s organization

Lowering software asset costs and mitigating license compliance risks

- ✓ Managing entire asset lifecycle, improving procurement and disposal processes
- ✓ Mitigating audit risks and costs
- ✓ Reclaiming unused software assets

Adding business value with IBM SmartCloud Control Desk

Summary

By now, you can:

- Describe the main components and functions of IBM SmartCloud Desk that facilitates ITIL based processes for:
  - Configuration Management
  - Change Management
  - Release Management
- Explain how the CMDB is organized
- Articulate the use and benefits of:
  - Configuration Item audit
  - Baselining
  - Impact analysis
  - Scheduling
  - Adaptive workflows

Summary

More about Cloud & Smarter Infrastructure

You can find the latest information about IBM Cloud & Smarter Infrastructure education offerings online at the following location:

www.ibm.com/software/tivoli/education/

Also, if you have any questions about education offerings, send an email to the appropriate alias for your region:

- Americas: tivamedu@us.ibm.com
- Asia Pacific: tivtrainingap@au1.ibm.com
- EMEA: tived@uk.ibm.com

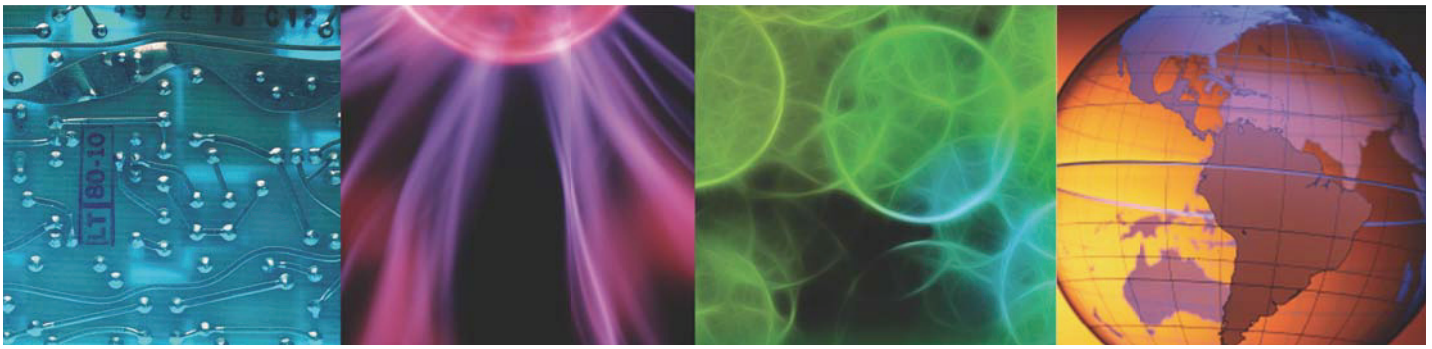
Cloud & Smarter Infrastructure user groups

You can get even more out of Cloud & Smarter Infrastructure software by participating in one of the 91 independently run Cloud & Smarter Infrastructure user groups around the world. Learn about online and in-person user group opportunities near you at www.tivoli-ug.org.

Certification

All IBM certifications are based on job roles. They focus on a job a person must do with a product, not just the product's features and functions. Online certification paths are available to guide you through the process for achieving certification in many IBM Cloud & Smarter Infrastructure areas. See ibm.com/tivoli/education for more information about certification.

Special offer for having taken this course: *Now through 31 December 2013*: For completing this course, you are entitled to a 15% discount on your next examination at any Thomson Prometric testing center worldwide. Use this special promotion code when registering online or by telephone to receive the discount: **15CSWR**. (This offer might be withdrawn. Check with the testing center.)



ibm.com/training

Authorized IBM Training

Printed in Ireland

CT6UGEN