DX Unified Infrastructure Management 23.4.x

Monitoring Configuration Service (MCS)

Customer Adoption Guide

v1.2, May 2024

Disclaimer

Certain information in this document may outline Broadcom's general product direction. This document shall not serve to (i) affect the rights and/or obligations of Broadcom or its licensees under any existing or future license agreement or services agreement relating to any Broadcom software product; or (ii) amend any product documentation or specifications for any Broadcom software product. This presentation is based on current information and resource allocations as of March 2024 and is subject to change or withdrawal by Broadcom at any time without notice. The development, release and timing of any features or functionality described in this presentation remain at Broadcom's sole discretion.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future Broadcom product release referenced in this presentation, Broadcom may make such release available to new licensees in the form of a regularly scheduled major product release. Such release may be made available to licensees of the product who are active subscribers to Broadcom maintenance and support, on a when and if-available basis. The information in this presentation is not deemed to be incorporated into any contract.

Copyright © 2024 Broadcom. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

THIS DOCUMENT IS FOR YOUR INFORMATIONAL PURPOSES ONLY. Broadcom assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Broadcom be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if Broadcom is expressly advised in advance of the possibility of such damages.

Broadcom, the pulse logo, and Connecting everything are among the trademarks of Broadcom and/or its affiliates in the United States, certain other countries, and/or the EU.

Copyright © 2024 by Broadcom. All Rights Reserved.

The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, nor does it convey any license under its patent rights nor the rights of others

Table of Contents

Chapter 1: Traditional Configuration Methodologies 4

Chapter 2: Evolution of Management Configuration Service (MCS) 5

Chapter 3: MCS Improvements in DX UIM 23.4.x Release 7

Improved Scale and Resilience for MCS 7

Reference Architecture of MCS with DX UIM 23.4.x 8

Chapter 4: Summary and Next Steps 9

User Flow 9

Upgrade Guidelines for Existing Customers using Previous Versions of MCS 10

Important Links Related to MCS 10

Troubleshooting Steps**:** Important Callbacks 11

Chapter 1: Traditional Configuration Methodologies

DX Unified infrastructure Management (DX UIM) is a powerful data ingestion platform that spans the collection of monitoring data from various elements across your hybrid enterprise environment. DX UIM employs various probes that modularize the data collection process by focusing on specific infrastructure elements in your environment. This document provides an overview of existing methods of configuration and alarm policy creation and their limitations along with the need to migrate to Monitoring Configuration Service (MCS) and also highlights the upcoming features of MCS in the near future.

In order to collect the data about the infrastructure elements in terms of metrics there are certain methodologies that are currently adopted. For example, when we have computer systems to be monitored and health checks to be analyzed, we define configurations at each computer system. The pre-MCS options are as follows.

- POBC (Bulk Configuration)
- Ability to define the profiles at the probe level (IM GUI)
- Super Packages deployment

POBC (Bulk Configuration) – This is the configuration method available for probes to collect the metrics through the configuration defined in the Admin Console.

The limitations of this approach is that the configuration needs to be applied at each device level. In case there are thousands of devices to be monitored and configuration needs to be applied to thousands of devices simultaneously, it will not be possible. In addition, the configurations would not be handled automatically if the devices were moving in and out of the group.

For more information on Bulk Configuration, please refer to Declaring Inventory, Metrics, and Bulk Configuration.

Ability to define the profiles at the probe level – The metrics to be collected can be defined at probes for a device/computer system where the robot is currently installed. This works well if the number of devices to be monitored is small, however for thousands of devices it is a very cumbersome process to define the configuration at each device level.

Super Packages deployment – To track configuration changes, Super Packages having the specific configurations to be changed, are applied to individual devices through the Super Packages. Configuration can be deployed on the fly, and packages are deployed through the configuration changes in the package contents using directives, and can be used on any probe and not confined to any probe. However, there is no version maintenance of packages and monitoring governance is not possible to determine the configurations that are present at the device level.

Chapter 2: Evolution of Management Configuration Service (MCS)

The traditional methods of configuration management which are currently used without centralized configuration, have the following limitations:

- Difficulty in knowing which configurations are applied on machines; it is not easily possible to get a report on this with a traditional method of configuration without using another way of centralized configuration
- Maintenance of Super Packages is a nightmare if there are many packages installed on different servers; keeping track of packages with versions is very difficult
- Auto reconciliation or reconciliation capabilities are not present when there is any change in the configuration and it does not get auto-corrected
- Difficult to establish monitoring governance to track the configuration changes for monitored devices
- Updates of configuration changes need to be done for each device

With the existing methodologies of configuration having these limitations, the scenario of monitoring thousands of devices is much more cumbersome. There should be a method of configuring the devices based on which configuration changes are pushed to devices more seamlessly. MCS can be used in creating the centralized configuration more seamlessly for monitoring very small (less than 5K devices) to very large (50K devices and above) environments.

MCS is used to overcome the above difficulties of monitoring. Monitoring becomes more seamless through a zero-touch way of monitoring. MCS does the following in a scenario where several thousands of devices are to be monitored:

- Devices are grouped into individual groups, each having thousands of devices based on group configuration
- Configuration Profiles in MCS are created as a centralized way of defining the configuration and metrics to collect which defines what needs to be monitored; in this way, there is only one process (MCS) that maintains the configuration, and the configuration changes are tracked more effectively
- The profiles once created are applied to thousands of devices in the group and reaches all devices more seamlessly
- Even the updates done at group-level profiles are propagated to devices and configuration updates are easier than traditional configuration methodologies
- Once the device moves in and out of the particular group, the configurations are automatically applied as per configuration profiles present in the groups
- The thresholds on metrics can be configured at centralized locations using ‘alarm policies’ in the Operator Console

MCS provides a method for streamlining the creation and management of monitoring configurations for hundreds of target devices or resources. MCS caters to the centralized monitoring of inventory and devices through templates and profiles. The following table illustrates the differences between the pre-MCS methodologies and MCS.

Infrastructure Manager (IM GUI)	Bulk Configuration (Admin Console GUI)	MCS
Cannot apply the configuration profiles on all devices at one time.	Cannot apply the configuration profiles on all devices at one time.	Can apply the configuration to all devices simultaneously.
Cannot get the governance report on devices and metrics which are configured.	Updates of configuration need to be done on every device.	Devices moving in and out of groups can be handled automatically by removing and adding configurations.
Maintenance of Super Packages is not available.		Centralized policies can be configured based on metrics generated.
		Monitoring governance makes it much easier to get information on the metrics that are collected on the devices.

MCS allows administrators and other authorized users to:

- Create a configuration profile
- Deploy probes automatically to target robots as needed
- Configure probes remotely
- Leverage DX UIM groups to take advantage of policy management
- Create monitoring dashboards to provide a perspective of deployment as per devices and groups

For more information, please refer to the Documentation link on MCS.

Chapter 3: MCS Improvements in DX UIM 23.4.x Release

The following improvements are done as part of MCS with DX UIM 23.4.x which helps to further improve the monitoring bandwidth compared to the DX UIM 20.4 version of MCS.

Improved Scale and Resilience for MCS

With v23.4.x, the zero-touch monitoring configuration that is enabled through MCS has been improved. With its enhanced architecture (see below), MCS now supports monitoring profile deployment for a high-scale inventory in modern data centers. MCS provides a better monitoring template upgrade experience for probes along with stability and supportability compared to previous versions.

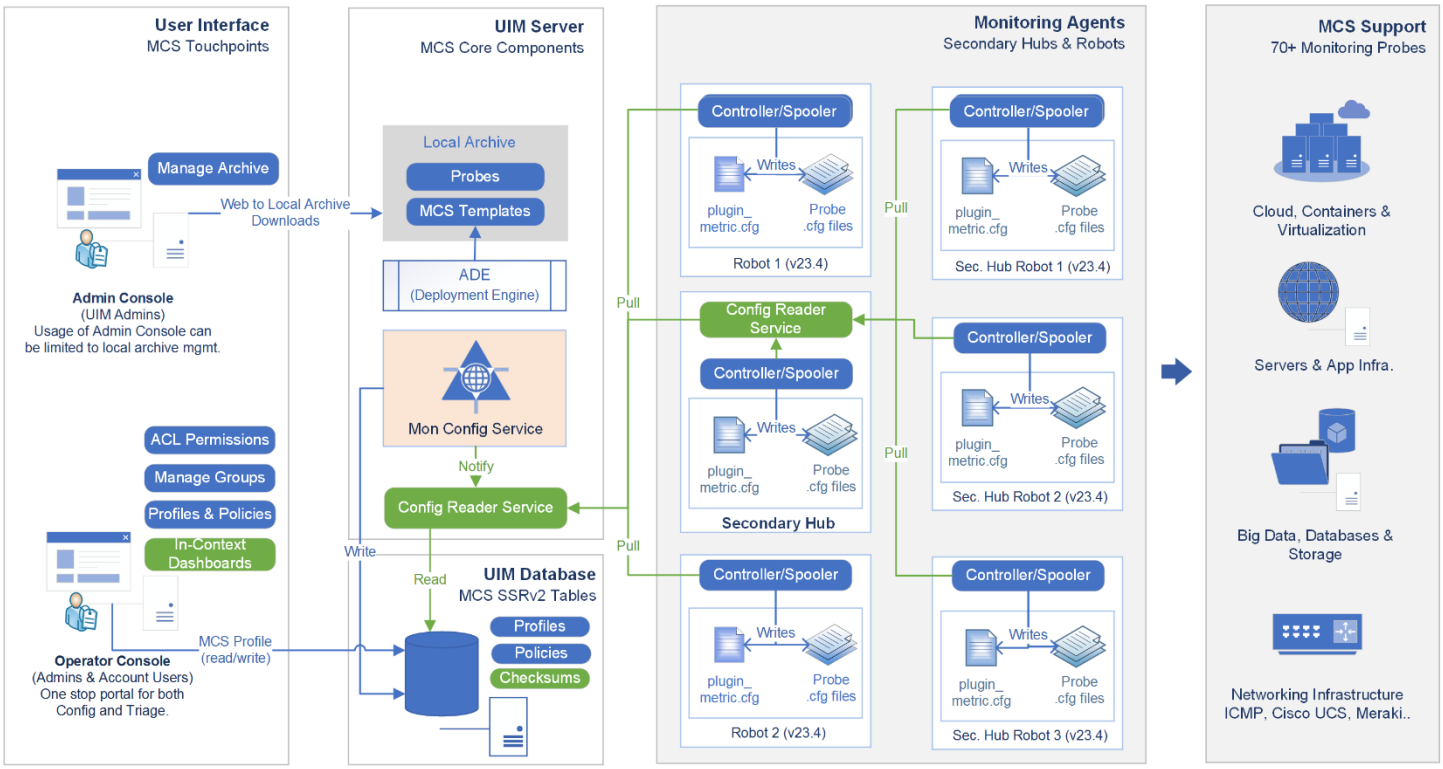
The following enhancements are part of the MCS with DX UIM **23.4.x**:

- MCS is redesigned to leverage the tiered architecture of hubs to provide scalability. Configuration Reader Service is introduced at the hubs. The design also ensures auto-reconciliation of profiles and policies on the robot system. The auto-reconciliation provides resilience and reliability to the monitoring configurations and associated alarm policies.
    - Configuration Reader Service Probe
      The new probe acts as an intermediary caching service between the mon_config_service (running on the primary hub) and all the robots (including robots that are connected to the secondary hub)
    - Redesigned MCS
- Changes to the States of MCS Template Package Migration

An additional set of callbacks is added to recover from an erroneous state of migration and retrigger the migration. For more information, see MCS Template and Profile Migration States.

With these enhancements, MCS offers better resilience and reliability along with higher scalability compared to prior versions.

Reference Architecture of MCS with DX UIM 23.4.x



Chapter 4: Summary and Next Steps

Creating and managing monitoring configurations for hundreds of target devices or resources is time-consuming. You can streamline the manual configuration process by using MCS. MCS allows administrators and other authorized users to create a set of configuration profiles. The profiles are applied concurrently to hundreds of target devices. MCS also automatically deploys probes to target devices as needed. Monitoring happens through the concept of templates and profiles. A template is a 'blueprint' that contains the configuration details for monitoring. For example, to monitor the CPU of a device a CPU Monitor (Enhanced) template is used to create a profile and select the metrics/configurations that need to be monitored.

A new type of MCS profile is included, called an enhanced profile. Enhanced profiles provide a consistent way to configure alarms using MCS. Enhanced profiles enable you to configure metrics, baselines, alarm thresholds, time-over-threshold alarms, and create custom alarm messages, all within a single MCS profile using the Operator Console UI if the policy mode parameter is disabled. If the parameter is enabled, you configure the metrics using the Operator Console and define the thresholds and alarm messages in the Operator Console as part of an alarm policy.

Hence, with centralized configuration, we can effectively manage configurations on individual devices and MCS is strongly suggested for the same. For the existing methodologies being used for configuration management, e.g., Super Packages, the transition to MCS is planned in the near future. This will seamlessly migrate the Super Packages configurations to MCS Configuration Profiles. New features that will be available in the near future are listed below:

- Utility to transition existing Super Packages (non-MCS) to MCS configuration seamlessly without the need to recreate the configuration profiles; after transition, the systems are monitored through centralized MCS
- Generation of a monitoring governance report based on the device details and metrics being monitored
- Visualization of alarm policies to effectively visualize the policies configured at the individual device or group level

User Flow

a) The templates which are the base for creating the monitoring configurations are present in the form of template packages
b) User imports the package from Admin Console and deploys them
    i) For example for the cdm probe, the package name is cdm_mcs_templates which contains all the configuration parameters for the cdm probe
    ii) Once the package is deployed, the templates are shown in the UI and it is always recommended to use the <u>enhanced</u> templates for monitoring purposes
    iii) In this case, to monitor the CPU of a device, use the CPU Monitor (Enhanced) template
    iv) Once the metrics are selected in the UI, the profile is created and monitoring commences
    v) Policies can be defined in the UI, based on when the threshold breach occurs and alarms are raised

Upgrade Guidelines for Existing Customers using Previous Versions of MCS

Migration of profiles is needed for an administrator if the latest version of the template is available in the archive. In this case, the administrator imports the latest version of the probe template package and deploys it to the Primary hub. Note that the callback *activate_probe_templates_package* is used to migrate the profiles of prior template versions to the upgraded template version.

For more information, please refer to MCS Templates Workflow for an Administrator.

If you are using the DX UIM 20.4 version of MCS, the following features are not applicable as they are automatically handled in DX UIM 23.4.x:

- **plugin_metric_correction** – This callback is not applicable after DX UIM 23.4.x as the latest version of MCS is not responsible for pushing the configuration
- **mcs_recon** – The functionality of mcs_recon is not applicable in DX UIM 23.4.x and reconciliation happens automatically
- **Transform the existing profiles using the cli** – The latest version of MCS with DX UIM 23.4.x utilizes the concept of checksums to determine the integrity of profile data. The checksum information is stored in the database and to compute the checksum of previously created profiles of 20.4 version the mcs-cli utility is used. Please refer to the Monitoring Configuration Service section titled *"Leverage the Redesigned MCS v23.4.x"* that describes the steps to transform the profiles in the 20.4 version to the 23.4.x version or above.

Important Links Related to MCS

Once the MCS Adoption prerequisites have been met, please review the guidelines for MCS adoption. The following guidelines are to be considered before the adoption of MCS once your environment is upgraded to DX UIM 23.4.x or above.

Sizing Recommendation – Ensure that the DX UIM sizing recommendations are reviewed and implemented
Documentation of MCS – It is recommended to review the MCS documentation for a smoother MCS adoption process.
Review Upgrade Checklist – Please refer to the DX UIM Upgrade Guide and Pre-Planning Checklist for 23.4 and review and leverage the full planning guide as well.

Troubleshooting Steps: Important Callbacks

The callbacks listed below have been added as part of the DX UIM 23.4 release for better troubleshooting to assist in analyzing the checksum mismatch of data:

- **get_Profile_plugin_checksum_Data** – The callback is used for getting the data based on which the checksum is generated related to the plugin_metric section given **profileId** as input
- **get_Profile_probe_checksum_Data** – The callback is used for getting the data based on which the checksum is generated related to the probe section given **profileId** as input
- **get_Policy_plugin_checksum_Data** – The callback is used for getting the data based on which the checksum is generated related to the probe section given **policyId, csId** as input
- **get_Policy_PDS** – Gets the PDS for PolicyId that is written to plugin_metric.cfg
- **get_Profile_PDS** – Gets the PDS for profileId that is written to plugin_metric.cfg, probe.cfg

For more information on MCS troubleshooting, refer to Troubleshooting Monitoring Configuration Service (MCS).

configuration_reader_service plays an important role in storing the profile information in a cache and communicating with robots. For failures related to profile deployments, please refer to the troubleshooting steps of configuration_reader_service that are helpful. Please refer to: Configuration Reader Service Troubleshooting for more details.

Note: Collect the following logs listed below if any problems are related to MCS

1. mon_config_service logs (nimsoft/probes/service/mon_config_service) of the primary hub
2. configuration_reader_service logs of primary/secondary hub (nimsoft/probes/service/configuration_reader_service)
3. controller logs (/nimsoft/robot) of robot
4. spooler logs (/nimsoft/robot) of robot
5. mcsuiapp logs (/nimsoft/probes/service/wasp)