Server Lifecycle Automation (SLA)
Continuous Compliance

Onboarding Guide

Version 48.1 Release 24.5

Server Lifecycle Automation (SLA)
Continuous Compliance

IBM

Onboarding Guide

Version 48.1 Release 24.5

Note
Before using this information and the product it supports, read the information in “Notices” on page 133.

This edition applies to release 24.5 and to all subsequent releases and modifications until otherwise indicated in new editions.

About This Guide

This document serves as functional guide for Account and Server Onboarding Activities for Continuous Compliance (CC) solutions of Server Lifecycle Automation (SLA) Program. This guide is for SLA IOT Deployment Specialists, System Admins and Server On-boarders.

Account onboarding section of this document provides direction to setup basic account related configuration that will govern how users uses CC to organize account endpoints.

Server onboarding section of this document provides direction to onboard a server to CC.

Document Organization

This document is divided into the following chapters.

Chapter 1, “Overview,” on page 1 contains brief explanations on the continuous compliance solution as well as account and server onboarding processes.

Chapter 2, “Assumptions, Constraints and Release Announcements,” on page 3 clearly states the validity of this document, prerequisites for the system and platform supported as well as important announcements for each release including new features.

Chapter 3, “Logging in to SLA Environments using IBMid,” on page 11 explains the use of IBMid to log in to SLA UI as well as how entitlement service works.

Chapter 4, “Roles, Groups and User Administration,” on page 19 explains the role types of the actors in the system and the functions each role type is allowed to perform. Steps to create user groups and user roles can be found under this chapter as well.

Chapter 5, “Change Windows Management,” on page 33 explains how you can setup change windows and associate the managed severs with a different non-default change window using the "Server Change Schedule Management" dashboard.

Chapter 6, “Policy Management,” on page 39 explains what are the compliance profiles that govern the compliance checking and the hierarchy of compliance policy override/customization.

Chapter 7, “Server Onboarding - Legacy,” on page 45 contains the information of server onboarding prerequisites and recounts the steps on how to onboard a server so that you can use continuous compliance solution to manage the server, how to perform inspection on a managed server and how to review the inspection result.

Chapter 8, “Server Onboarding - Message-based SLA Client Install,” on page 91 contains the prerequisites and steps on how to register for messaging services.

Document Control Information

Document Location

This is a snapshot of an online document. Paper copies are valid only on the day they are printed. Refer to the author if you are in any doubt about the currency of this document.

Revision History

Table 1. Document Revision History

Date (MM/DD/YYYY)	Version	Description	Author
07/22/2016	1.0 Release 10.5	Initial version with Sprint 10.5	Sophy Su Yadana Zaw
07/27/2016	2.0 Release 11.1	Updated to Sprint 11.1	Sophy Su Yadana Zaw
08/25/2016	3.0 Release 11.3	Updated to Sprint 11.2 and 11.3	Sophy Su Yadana Zaw
09/30/2016	4.0 Release 11.5	Updated to Sprint 11.4 and 11.5	Sophy Su Yadana Zaw
10/14/2016	4.1 Release 11.5	Removed Change Freeze Updated Supported Platforms Added Virtualization Management Information Added Hypervisor Onboarding Information Added Server Group Management Information Removed a prerequisite step relating to editing docker-compose file from EE from Windows Server Onboarding Prerequisite	Sophy Su Yadana Zaw
10/21/2016	5.0 Release 12.2	Updated to Sprint 12.2	Sophy Su Yadana Zaw
11/09/2016	5.1 Release 12.2	Updated Account Policy Management	Sophy Su Yadana Zaw
11/17/2016	6.0 Release 12.3	Updated to Sprint 12.3	Sophy Su Yadana Zaw
12/6/2016	7.0 Release 12.5	Updated to Sprint 12.5 Updated the Review Server Compliance Check section Updated the Supported Platforms for SRA	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
12/22/2016	8.0 Release 13.1	Updated to Sprint 13.1 Added Supported Browsers Information Added "Note" for empty/invalid attribute values in Compliance Environment and Compliance Update Chapters Added the limitation for server bulk load under Server Onboarding Chapter	Sophy Su Yadana Zaw
01/12/2017	9.0 Release13.3	Updated to Sprint 13.3 Updated the Overview section Updated the Role, Group and User Administration section Updated Management Server Onboarding Steps Added Websphere Onboarding Steps	Sophy Su Yadana Zaw
01/25/2017	10.0 Release13.4	Updated to Sprint 13.4 Updated Server Onboarding Section Updated Review Server Onboarding Section Added Prerequisite Validation Section Under Server Onboarding Steps	Sophy Su Yadana Zaw
02/09/2017	11.0 Release13.5	Updated to Sprint 13.5 Updated Supported Platforms	Sophy Su Yadana Zaw
02/22/2017	12.0 Release 14.1	Updated to Sprint 14.1 Added "Special Notes" section under "Chapter 2: Assumptions and Constraints" Updated the Windows Server Onboarding Prerequisites section	Sophy Su Yadana Zaw
03/01/2017	12.1 Release 14.1	Edited Prerequisites for Windows Server Onboarding Section to include IBM sudo setting requirements and new PowerShell version and hotfix required.	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
03/10/2017	13.0 Release 14.2	Updated to Sprint 14.2 Updated Chapter 2: Assumptions and Constraints Updated Chapter 5: Policy Management Updated Chapter 6: Creating and Updating Compliance Environment Updated Chapter 7: Creating and Updating Compliance Profiles Updated Prerequisites for Onboarding Windows Endpoint section under Chapter 10: Server Onboarding to include limitation on FIPS, steps to add automate user to "ora_dba" group for Oracle Middleware and steps to change the language of the Windows Endpoint to "English". Updated Review Server Compliance Check Section under Chapter 10: Server Onboarding Added Chapter 11: Bulk Override	Sophy Su Yadana Zaw
03/24/2017	14.0 Release 14.3	Updated to Sprint 14.3 Updated Prerequisites for Onboarding Windows Endpoint Section under Chapter 10: Server Onboarding Updated Prerequisites for Onboarding AIX Endpoint Section under Chapter 10: Server Onboarding Updated Server Bulk Load Section under Chapter 10: Server Onboarding Updated Review Server Compliance Check Section under Chapter 10: Server Onboarding	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
04/06/2017	15.0 Release 14.4	Updated to Sprint 14.4 Updated "Prerequisites for Onboarding AIX Endpoint Section under Chapter 10: Server Onboarding" to include a new prerequisite requirement Updated "Prerequisites for Onboarding Linux Endpoint Section under Chapter 10: Server Onboarding" to include a new prerequisite requirement Updated "Server Onboarding Steps under Chapter 10: Server Onboarding" to add new required field "Change Window Schedule" Updated "Server Bulk Load Section under Chapter 10: Server Onboarding" to add new optional field "Change Window Schedule"	Sophy Su Yadana Zaw
04/13/2017	15.1 Release 14.4	Updated "Special Notes" Section to include DBCS Support Announcement as the last bullet point Added supported platforms and middleware for DBCS support under "Supported Platforms" Section under Chapter 2: Assumptions and Constraints	Sophy Su Yadana Zaw
04/21/2017	16.0 Release 14.5	Updated to Sprint 14.5 Updated Chapter 10: Server Onboarding, Prerequisites for Onboarding Windows Endpoint, step 3 to include steps to put "automate" user in the whitelist of password requirements policy Added command to make automate user's password non-expiring as bullet point 3 under Chapter 10: Server Onboarding, Prerequisites for Onboarding AIX Endpoint, step 3	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
05/05/2017	17.0 Release 15.1	Updated to Sprint 15.1 Updated Prerequisites for Onboarding Windows Endpoints Section under Chapter 10: Server Onboarding to include steps to change Windows display language for Windows Server 2008 Updated the "Special Notes" section under Chapter 2: Assumptions and Constraints to add an announcement for the release of new policy version and steps to perform to use it Added the "Policy Versions: Planning and Best Practices" section that describes the recommended the best practices on how to manage policy versions under Chapter 5: Policy Management	Sophy Su Yadana Zaw
05/19/2017	18.0 Release 15.2	Updated to Sprint 15.2 Updated the "Special Notes" section under Chapter 2: Assumptions and Constraints to add an announcement for the release of the new external user interface Added the "Prerequisites for Onboarding Linux Endpoint" section step 3, point number 12 and "Prerequisites for Onboarding AIX Endpoint" section step 3, point number 10 under Chapter 10: Server Onboarding to include step to perform to compliant with ITCS104 password exemption rule C.	Sophy Su Yadana Zaw
05/22/2017	18.1 Release 15.2	Added a point in the note section on top of the "Prerequisite for Onboarding Windows Endpoint" section to inform the users that Windows PowerShell 3.0 requires Microsoft .NET Framework 4.5.	Sophy Su Yadana Zaw
05/29/2017	18.2 Release 15.2	Updated the "Special Notes" section under Chapter 2: Assumptions and Constraints to add RHEL 6.9 and 7.1 as supported platforms for both CC and SRA and add SUSE 11.x as supported platform for SRA	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
06/02/2017	19.0 Release 15.3	Updated to Sprint 15.3 Updated prerequisite sections for Windows/Linux/AIX endpoints to include a note to let users know that they need to submit Service Request to edit EE configuration if they use an endpoint userid other than "automate" Updated "Review Server Compliance Check" section	Sophy Su Yadana Zaw
06/19/2017	20.0 Release 15.4	Updated to Sprint 15.4 Updated RHEL supported platforms user Assumption and Constraints Chapter Revamped Roles, Groups and User Administration Chapter Added Change Windows Management Chapter Removed Account Onboarding Chapter Added Windows Endpoint Password Auto Update for ITCS104 Section under Prerequisite for Onboarding Windows Endpoints Section Added an announcement for migration of old policy profiles to using "Account Policy Customization" under "Special Notes" Section Added the Deviation Override Chapter Added "Bulk Deviation Override (Upload CSV File)" Section under the Deviation Override Chapter	Sophy Su Yadana Zaw
06/20/2017	20.1 Release 15.4	Added point 8 and 9 to update "automate" id's password under "Server Group Management" section under Chapter 10: Server Onboarding Added 2 more prerequisites for Windows Endpoint Password Auto Update feature under Chapter 10: Server Onboarding > Prerequisites to Onboard a Server > Prerequisite for Onboarding Windows Endpoint > Windows Endpoint Password Auto Update	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
07/03/2017	21.0 Release 15.5	Updated to Sprint 15.5 Added the file size limitation for CSV file upload for bulk deviation override under "Bulk Deviation Override (Upload CSV File)" section under "Chapter 11: Deviation Override" Added Security Analyst role and its description under Chapter 3: Roles, Groups and User Administration Added "notes" to the tasks that are accessible only to "Security Analyst" under relevant sections Updated "Prerequisites for Onboarding Linux Endpoint" and "Prerequisites for Onboarding AIX Endpoint" sections to include new prerequisites relating to SSH key	Sophy Su Yadana Zaw
07/10/2017	21.1 Release 15.5	Updated the "Prerequisite for Onboarding Windows Endpoint" section and "Server Group Management" section under "Chapter 10: Server Onboarding" to clarify the prerequisites for Windows workgroup servers and Windows domain servers	Sophy Su Yadana Zaw
07/17/2017	22.0 Release 16.1	Updated to Sprint 16.1 Added CC Server Owner role and its description under Chapter 3: Roles, Groups and User Administration Added "notes" to the tasks that are accessible only to "CC Server Owner" under relevant sections Added the information about "Middleware Discovery" being disabled by default under "Special Notes", "Server Onboarding" and "Server Bulk Load" sections	Sophy Su Yadana Zaw
07/21/2017	22.1 Release 16.1	Edited "Prerequisite for Onboarding Windows / Linux / AIX Endpoint" sections to include the prerequisite checks performed by SLA during onboarding validation	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
07/31/2017	23.0 Release 16.2	Updated to Sprint 16.2 Added the **optional** prerequisite steps to download/copy the chef installer on the endpoint before onboarding to optimize the performance of the overall server onboarding process. See "Prerequisites for Onboarding Windows Endpoint", "Prerequisites for Onboarding Linux Endpoint" and "Prerequisites for Onboarding AIX Endpoint" sections under "Chapter 10: Server Onboarding".	Sophy Su Yadana Zaw
08/14/2017	24.0 Release 16.3	Updated to Sprint 16.3 Added a prerequisite step to reboot server after changing the display language. See "Prerequisites for Onboarding Windows Endpoint" section under "Chapter 10: Server Onboarding" Added the descriptions for the "Release Comparison" tab under Account Policy Customization: Compliance Environment and Compliance Profile chapters Added different download links for different deployment models for the optional prerequisite steps. See "Prerequisites for Onboarding Windows Endpoint", "Prerequisites for Onboarding Linux Endpoint" and "Prerequisites for Onboarding AIX Endpoint" sections under "Chapter 10: Server Onboarding".	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
08/28/2017	25.0 Release 16.4	Updated to Sprint 16.4 Added "Ubuntu" and "SUSE" as supported platforms under the "Supported Endpoint Platforms" section. Added the "automate" user create command for Ubuntu under the "Prerequisites for Onboarding Linux Endpoint" section. Added announcement for GPO support under "Special Notes" section under "Chapter 2: Assumptions and Constraints" Added new section called "Using Microsoft GPO together with CC" under "Chapter 5: Policy Management" to explain how managing a subset of policies using Microsoft GPO together with CC works Added prerequisite step that needs to be performed to use the aforementioned GPO feature under "Prerequisites for Onboarding Windows Endpoint" section under "Chapter 10: Server Onboarding" Added steps to turn on and off the GPO remediation for certain policies under "Creating and Updating Compliance Environments" and "Creating and Updating Compliance Profiles" sections Added new section called "Upgrading the Policy Version of an Existing Environment" under "Chapter 6: Account Policy Customization: Compliance Environment" Updated the screen shots for "Chapter 6: Account Policy Customization: Compliance Environment" Added new section called "Copying and Deleting an Existing Compliance Profile" under "Chapter 7: Account Policy Customization: Compliance Profile"	Sophy Su Yadana Zaw
08/30/2017	25.1 Release 16.4	Added the additional information about the system admin group, system admin role and its responsibilities to "Chapter 3: Roles, Groups and User Administration" section	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
09/07/2017	25.2 Release 16.4	Added information about server validation function being available under "Special Notes" section Added the clarification for platforms supported for the GPO utility under "Supported Endpoint Platforms" section, "Special Notes" section and "Using Microsoft GPO together with CC" section	Sophy Su Yadana Zaw
09/11/2017	26.0 Release 16.5	Updated to Release 16.5	Sophy Su Yadana Zaw
09/28/2017	26.1 Release 16.5	Added clarification to use "Virtual IP 1" address as the server group gateway address while creating server group under "Server Group Management" section under Chapter 10: Server Onboarding	Sophy Su Yadana Zaw
10/02/2017	27.0 Release 17.1	Updated to Release 17.1	Sophy Su Yadana Zaw
10/10/2017	28.0 Release 17.2	Updated to Release 17.2 Added "Appendix C: CC Policies Documentation and Source Code Reference" Added a note linking to aforementioned appendix under the "Policy Versions: Planning and Best Practices" section under "Chapter 5: Policy Management" Added information about new "Process Inspector" access for groups associated to roles of "Support" role type under "Special Notes" section under "Chapter 2: Assumptions and Constraints" Added information about new "Process Inspector" access for groups associated to roles of "Support" role type under "Definition of Role Types within CC and SRA" section under "Chapter 3: Roles, Groups and User Administration" Edited "Account Policy Customization: Compliance Environment" and "Account Policy Customization: Compliance Profile" chapters to include information on enabled and disabled policies	Sophy Su Yadana Zaw
10/23/2017	29.0 Release 17.3	Updated to Release 17.3	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
11/06/2017	30.0 Release 17.4	Updated to Release 17.4 Added note to inform about chef client version upgrade under Chapter 2: Assumptions and Constraints, Special Notes Section Added links to download PowerShell 3.0 Hotfix kb2842230 under Chapter 10: Server Onboarding, Prerequisites for Onboarding Windows Endpoints Section Added links to download new version of the chef client installer for endpoints under Chapter 10: Server Onboarding, Prerequisites for Onboarding Windows Endpoints Section	Sophy Su Yadana Zaw
11/07/2017	30.1 Release 17.4	Updated the port for the Unix servers to reach CHEF server by HOST IP to port 8443/tcp. See Chapter: 10 Server Onboarding, Prerequisite for Onboarding Linux Endpoint Section and Prerequisite for Onboarding AIX Endpoint	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
11/20/2017	31.0 Release 17.5	Updated to Release 17.5 Updated the port for the Unix servers to reach CHEF server by HOST IP to port 443/tcp or 8443/tcp depending on the SLA account creation date. See Chapter: 11 Server Onboarding, Prerequisite for Onboarding Linux Endpoint Section and Prerequisite for Onboarding AIX Endpoint Added notes to inform about usage of IBMid and Single Sign-on support under Chapter 2: Assumptions and Constraints, Special Notes Section Added a chapter for IBMid and Single Sign-on feature. See Chapter 3: Logging in to SLA Environments using IBMid Added notes relating to FIPS support under Chapter 2: Assumptions and Constraints, Special Notes Section Added FIPS related steps under Server Group Management section under Chapter 11: Server Onboarding Updated Chapter 7: Account Policy Customization: Compliance Environment to include information relating to environment rollback version Edited the section relating to the disk space requirement for server onboarding to avoid confusion. See Prerequisites for Onboarding Windows Endpoint/Linux Endpoint/AIX Endpoint sections	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
12/11/2017	32.0 Release 18.1	Updated to Release 18.1 Updated Chapter 2: Assumptions, Constraints and Release Announcements, Supported Endpoint Platforms section to announce Windows 2016 support for Continuous Compliance Updated Chapter 2: Assumptions, Constraints and Release Announcements, Special Notes section to include the announcements for new features available in release 18.1 Added "SLA Entitlement Services" section under Chapter 3: Logging in to SLA Environments using IBMid Edited Using Microsoft GPO together with CC section under Chapter 6: Policy Management to add a note about a known issue	Sophy Su Yadana Zaw
01/15/2018	33.0 Release 18.4	Updated to Release 18.4	Sophy Su Yadana Zaw
02/12/2018	34.0 Release 19.1	Updated to Release 19.1 Updated "Management Server Onboarding Steps" section Updated "Bulk Deviation Override (Upload CSV File)" section	Sophy Su Yadana Zaw
03/05/2018	34.1 Release 19.1	Updated the screenshot of the onboarding key under Chapter 11: Server Onboarding > Prerequisites to Onboard a Server > Prerequisites for Onboarding Linux Endpoint/ Prerequisites for Onboarding AIX Endpoint Added Windows 2016 under OS Version Requirements under Chapter 11: Server Onboarding > Prerequisites to Onboard a Server > Prerequisites for Onboarding Windows Endpoint	

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
03/12/2018	35.0 Release 19.3	Updated to Release 19.3 Added announcements for new terminologies and nomenclature changes under the "Special Notes" section under "Chapter 2: Assumptions, Constraints & Release Announcements" Added RHEL 7.4 as supported platform for CC Made necessary changes, in term of wording and screen-shots, to reflect the nomenclature changes Added "Appendix B: Steps to Import CSV into Excel"	Sophy Su Yadana Zaw
03/12/2018	35.1 Release 19.3	Added sudo requirement for AIX under Chapter 10: Server Onboarding → Prerequisites to Onboard a Server → Prerequisites for Onboarding AIX Endpoint → Functional ID Requirement	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
04/10/2018	36.0 Release 19.5	Updated to Release 19.5 Added the "Known Issues" section under "Chapter 2: Assumptions, Constraints & Release Announcements" to address the known issues relating to onboarding and steady-state password management Added the information relating to the new compliant mode called "Paused Mode" under the "Special Notes" section under "Chapter 2: Assumptions, Constraints & Release Announcements". For detail information relating to Paused Mode, see the CC User's Guide. Edited the "SLA Entitlement Service" section under Chapter 3: Logging in to SLA Environments using IBMid to include information relating to the new LDAP login feature. Added description for Site and Offering under the "Associating User Groups with Roles" section under Chapter 4: Roles, Groups and User Administration Edited the "Using Microsoft GPO together with CC" section under Chapter 6: Policy Management" to update the list of policies supported for GPO Updated the "Server Group Management" section under Chapter 11: Server Onboarding to include a note relating to onboarding password management flow Added a chapter for Server Offboarding Added an appendix for Information on how SLA Manages the Onboarding Password	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
05/15/2018	37.0 Release 20.1	Updated to Release 20.1 Added announcement for supporting offboarding of the decommissioned servers under "Chapter 2: Assumptions, Constraints & Release Announcements". Edited Known Issues section Added the "Sudo Version Requirement" under "Chapter 11: Server Onboarding, Prerequisites to Onboard a Server, Prerequisite for Onboarding AIX Endpoint" to address the sudo version requirement Edited the "Windows Endpoint Password Auto Update to Support Password Expiration Rule" section under "Chapter 11: Server Onboarding, Prerequisites to Onboard a Server, Prerequisite for Onboarding Windows Endpoint" Added the troubleshooting scenario for likely onboarding failures as a subsection called "Troubleshooting Task" under "Chapter 11: Server Onboarding → Server Onboarding Steps"	Sophy Su Yadana Zaw
06/05/2018	38.0 Release 20.3	Updated to Release 20.3 Added a wget version requirement for SUSE Linux under "Chapter 11: Server Onboarding → Prerequisites to Onboard a Server → Prerequisite for Onboarding Linux Endpoint → Software Requirements Topic" Added zLinux as supported platform for CC and SRA under "Chapter 2: Assumptions, Constraints & Release Announcements →Supported Endpoint Platforms" section Added notes about Domain IDs not being supported on Linux and AIX servers under "Chapter 11: Server Onboarding → Prerequisites to Onboard a Server → Prerequisite for Onboarding Linux Endpoint & Prerequisite for Onboarding AIX Endpoint" sections	Sophy Su Yadana Zaw

Table 1. Document Revision History (continued)

Date (MM/DD/ YYYY)	Version	Description	Author
07/02/2018	39.0 Release 20.5	Updated to Release 20.5 Added list of supported middleware under "Chapter 2: Assumptions, Constraints & Release Announcements → Supported Endpoint Platforms" section Updated to clarify that "all_winrm_servers" group is used for all Windows Servers (Windows servers that are using either the local account or the domain account)	Sophy Su Yadana Zaw
07/31/2018	40.0 Release 21.1	Updated to Release 21.1	Sophy Su Yadana Zaw
09/03/2018	41.0 Release 21.3	Updated to Release 21.3 Updated the Server Onboarding steps under “Chapter 11: Server Onboarding” section. Updated with the new field “Onboarding Label” in Enter Server Information screen.	Gifthiya B Mohamed Arif
11/02/2018	42.0 Release 22.1	Updated to Release 22.1 Modified the term "Cablebox" to "JumpHost" in "Chapter 11: Server Onboarding" . Removed "Appendix C- Steps to Import CSV into Excel" and "Notes" from Chapter 12: Bulk Deviation Override (Upload CSV File). Updated the section "Prerequisites to Onboard a Server" in "Chapter 11: Server Onboarding". Updated the section "Using Microsoft GPO together with CC" in "Chapter 6: Policy Management". Updated the section "Known Issues" with the policy information in "Chapter 2: Assumptions, Constraints & Release Announcements".	Gifthiya B Mohamed Arif

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
11/23/2018	43.0 Release 22.3	Updated to Release 22.3 Updated the section "Server Group Management" in "Chapter 11: Server Onboarding". Updated the section "Server Onboarding Steps" in "Chapter 11: Server Onboarding". Updated "Chapter 11: Server Onboarding" with port details. Updated RHEL 7.5 as supported platform in the section "Supported Endpoint Platforms" in "Chapter 2: Assumptions, Constraints & Release Announcements". Renamed Self-Service Delivery (SSD) to Service Request Automation (SRA).	Gifthiya B Mohamed Arif
02/05/2019	44.0 Release 23.3	Updated to Release 23.3 Updated Chapter 2: Assumptions, Constraints & Release Announcements → Supported Endpoint Platforms with the latest OS support version. Updated the section 'Prerequisite to Onboard a Server' in "Chapter 11: Server Onboarding" with windows endpoint software requirement details. Updated the section "Special Notes" in "Chapter 2: Assumptions, Constraints & Release Announcements → Special Notes" with OS display language details.	Gifthiya B Mohamed Arif
02/19/2019	45.0 Release 23.5	Updated to Release 23.5 Updated Chapter 2: Assumptions, Constraints & Release Announcements → Supported Endpoint Platforms with the Oracle products, versions, and supported platforms.	Gifthiya B Mohamed Arif
04/02/2019	46.0 Release 23.5.1	Updated to Release 23.5.1 Added the "Chapter 12: for Messaging Registration Services" with prerequisites and download installer steps. Added a new appendix for 'Valid Timezone Values In Install Configuration File'.	Gifthiya B Mohamed Arif

Table 1. Document Revision History (continued)

Date (MM/DD/YYYY)	Version	Description	Author
04/15/2019	47.0 Release 24.1	Updated to Release 24.1 Removed SSD/SRA specific Features. Updated "Chapter 11: Server Onboarding" and "Chapter 12: Messaging Registration Services" with messaging model details.	Gifthiya B Mohamed Arif
05/28/2019	48.0 Release 24.4	Updated to Release 24.4 Updated the whole document with BPM deprecation of CC functionality. Removed chapters "Environment", "Compliance Profiles", "Reviewing Policy Customizations", "All Potential Overrides", "Deviation Override" and "Server Offboarding". Added a reference for removed chapters in Chapter 6: Policy Management under the section "Using Microsoft GPO together with CC". "Server Onboarding - Legacy" is moved to Chapter 7 and "Server Onboarding - Message-based SLA Client Install" is moved to Chapter 8.	Gifthiya B Mohamed Arif
07/08/2019	48.1 Release 24.5	Updated to Release 24.5 Add more detailed explanations to the required fields in install_config file to reduce confusion. Add limitation “SLA Ehn”	Xiongfei Wei

Approval History

Table 2. Document Revision History

Role	Approver	Approved Version	Approval Date (MM/DD/YYYY)

Contents

Figures

Chapter 1. Overview

Server Lifecycle Automation (SLA) is a Joint Program that provides a complete automation suite in the distributed server space. It provides a shared infrastructure framework for GTS (Global Technology Services) to guarantee client's servers compliance from the moment they are built up to the time when they are in production.

SLA program is comprised of 2 solutions.

1. ASB - Automated Server Build
2. CC - Continuous Compliance

Important: This document is a functional guide for CC solutions. It only covers CC related information. For information on ASB, refer to ASB community page.

Continuous Compliance

CC (Continuous Compliance Solution) is designed to transform many of the Security Processes (for example, Health Check) into a Primary Control Compliance Process. It continuously enforces the security policies that have been agreed by IBM and the customers to the managed servers to maintain them in the compliant state, thus eliminating the need for traditional Security Health Checking. It also provides visibility of the compliance state of a given server to the customers at all time.

Account Onboarding

Account onboarding is a process to setup basic account related configurations that will govern how users use CC to manage endpoints. CC uses role-based access control. During account onboarding, you will add users to different user groups and associate different user groups with user roles. Roles grant users authority to access particular tasks in CC system. You will also perform necessary initial setups such as environment setup and change window setup.

Server Onboarding

Before you can start managing your servers using CC, you must onboard them to the system. Server onboarding section contains information on prerequisites to onboard a server and steps to onboard a server.

Chapter 2. Assumptions, Constraints and Release Announcements

Assumptions

- All necessary servers are built, software is installed, network connectivity and firewall rules have been setup per SAS411 SAS IP Info and Firewall Flow.
- Pre-defined compliance policies that are provided by the CC solution will be supported in this release. The Account Security Focal will be able to modify these based on the requirements of the account being supported.
- An agreed upon set of Health-Check Security Policies already exists and have been approved by the customer and the account team.
- The pre-defined Compliance Policies that are already provided by the CC solution could be used to create a compliance state baseline for a server or a group of servers in the absence of an existing set of agreed policies.
- The Account Deployment Specialist and Deployment Manager have received a note from the SLA Production Deploy team that the SLA system is ready to be used.
- The customer's LDAP has been configured into SLA and the customer users are available to SLA.
- Enhanced UI supports usage only in a single browser window/tab at same time, multiple windows/tabs is not supported.

Known Issues

Known Issues Relating to Password Updates during Onboarding and Offboarding

- While requesting for server onboarding, you must select a server group to which your sever will be onboarded.
- During onboarding, SLA uses the "onboarding password" to authenticate the endpoints and install SLA Client.
- Once SLA Client is installed and configured properly, SLA update the password of automate id in the endpoint from "onboarding password" to "steady-state password". The steady-state password is set to be the same with the password of the server group to which the endpoint is onboarded. The server group's password is set during the server group creation by the user. For more information on server group creation, see “Server Group Management” on page 64.
- When SLA tries to set the password of automate id in the endpoint to steady-state password, the password change can fail due to the following reasons.
  - If the server has a password policy relating to password complexity and the steady-state password does not meet the requirement, the password change will not be successful.
  - If the server has a password history policy which prevent it from reusing the previously used passwords.

    The example scenario would be as follows. A server, Endpoint A, was previously onboarded to a server group, SG1. After Endpoint A was onboarded, its automate id's password was set to the password of the server group SG1. After some time, the user decided to offboard Endpoint A and re-onboard it again to the same server group, SG1. In that case, the onboarding will be successful but the subsequent step of changing the

Endpoint A's password to steady-state password will fail. Thus, any action after onboarding would fail due to authentication issue.For more information on how SLA manages the onboarding and steady-state passwords and the workflow of the process, see Appendix B, “Information on how SLA Manages the Onboarding Password,” on page 119.

Known Issues Relating to IBMid Service

- As of Release 20.1, there is a known issue relating to IBMid Service.
- While launching the CC application, you might face the issue in which the application is not launched and instead a white screen is displayed.
- If you face such issue, clear the browser cache and try relaunching the applications.

Supported Endpoint Platforms

- **OS Platforms supported for Continuous Compliance**
  - AIX: AIX6.1 to 7.2
  - Redhat: RHEL 6.1 to 7.6
  - SUSE: Linux SuSE 11.x and 12.x, SuSE Z390 (zLinux) Support on SuSE 12 and SuSE 11
  - Ubuntu: 14.x and 16.x
  - Windows: Windows 2008 R2, Windows 2012 R2, Windows 2012 Std, Windows 2016 (New, Release 18.1)

    Note: Windows 2016 platform is supported on latest version of SLA client running with the chef client version 12.12.13.
- **Middleware Platforms supported for Continuous Compliance**
  - DB2 version 9.7, 10.1, 10.5, 11.1 on the following Operating Systems:
    - RHEL 6,7
    - Ubuntu 14,16
    - SuSe: 11,12

      Note: DB2 policies are not supported on SuSe s390 platform
    - AIX: 6.1, 7.1

      Note: DB2 version 11.1 is not supported on AIX 6.1
    - Win 2k8 R2, Win 2k12, Win 2k12 R2, Win 2k16
  - Oracle products, versions, and supported platforms are given below:
    - Database 12c Enterprise/Standard Editions
      - RHEL 7 & above
      - SuSe: 12
      - Win 2k8 R2, Win 2k12 R2
    - Database 11g R2 Enterprise/Standard Editions
      - SuSe: 11
      - Win 2k8 R2, Win 2k12 R2
  - WAS V8.5.5, V9.0 (base, Network Deployment) on the following Operating Systems:
    - RHEL 6,7
    - Ubuntu 14.04,16.04

- SuSe: 11,12
- AIX: 6.1, 7.1

Note: IBM WAS V9.0 cannot be installed on AIX 6.1, hence the support for that version is out of scope

- Win 2k8 R2, Win 2k12, Win 2k12 R2, Win 2k16

v **OS Platforms supported by Continuous Compliance for endpoints with DBCS encoding**
  - Redhat: Redhat 7.6
  - Windows: Windows 2008 R2, Windows 2012 R2

v **OS Platforms supported by Continuous Compliance for using Microsoft GPO together with CC to manage certain policies**
  - Windows: Windows 2012 R2, Windows 2012 Std

v **List of Policies that are not supported on RHEL 7.5 and 7.6**
  - policy_linux_motd
  - policy_linux_syslog
  - policy_linux_oracle
  - policy_linux_was
  - policy_linux_mongodb
  - policy_linux_db2

Important: Continuous Compliance Solutions do NOT support 32-bit Operating Systems.

Supported Browsers

List of Web Browsers supported for Continuous Compliance.

v Firefox 38.x.x ESR (Extended Support Release)

v IE (Internet Explorer) 11

Note: As of July, 2015 Firefox 38.x.x ESR (Extended Support Release) is IBM's default browser version.

Special Notes

v The URLs for SLA environments are changed starting from release 13.5.

v You can find the new URL of your SLA environment in the email that is sent to you by SLA Operation team on 21st February 2017 titled "Server Lifecycle Automation (SLA) Production Environment Change Window for IPCenter Accounts SLA 13.5 Deployment, and all accounts with New URL, RCP Web Proxy and OS Update - Completed".

v Alternatively, you can find the new URL of your SLA environment here.

v Starting from Release 14.4, CC & SRA support DBCS. It is important to change your Windows, Linux and AIX endpoint "Display Language" to English before the endpoint is onboarded in order for CC & SRA to support DBCS. The steps to change the Windows Display Language to English can be found under “Prerequisite for Onboarding Windows Endpoint” on page 45.

v Starting from Release 15.1, there will be new policy (cookbook) version for each release. If you want to use the new version of the policy, you must create a new environment with the new version of the policy and move the existing endpoints to the new environment. Steps to move endpoints to new

environments can be found in the CC User Guide under Chapter 11: Server Compliance Management, Reassigning Managed Servers to Different Compliance Profile and Environment section.

Note: For best practices on how to manage policy versions, see “Policy Versions: Planning and Best Practices” on page 41.

- Starting from Release 15.2, there will be new and improved user interface (UI). For Release 15.2, the original homepage of your SLA environment will have a new UI. The new homepage UI will include the following links:
  - Service Request Automation (SRA): This link will bring you to the legacy SRA user interface (Process Portal). You can continue to perform all your regular tasks using this original UI.
  - SRA Enhanced UI: This link will bring you to a new user interface for Service Request Automation. The new user interface provides an improved ability to create and review requests. Not all the resource types from the original UI are available in this enhanced UI yet. More resource types will be added to the new UI in the future releases. Approval must still be completed in the original UI for now.
  - Continuous Compliance (CC): This link will bring you to the legacy CC user interface (Process Portal). You can continue to perform all your regular tasks using this original UI.
  - CC Console: This link will bring you to the original Compliance Console user interface.
  - Automated Server Build (ASB): You can access the original user interface of ASB via this link.
  - Risk based Continuous Patch (RCP): You can access the original user interface of RCP via this link.
- Starting from Release 15.4, the CC task used to manage the old policy management profiles such as linux_compliant_server and windows_compliant_server will be sunset. If you are using the old policy management profiles (for example, linux_compliant_server, windows_compliance_server) to manage compliance on servers in CC, you must move to use the new compliance profiles using "Account Policy Customization". See the CC User Guide, Chapter 5: Policy Management, Scenario to Migrate Servers to Account Policy Customization section on migration steps.
- Starting from Release 16.1, middleware discovery is disabled by default to save onboarding and change request execution time. If you want to enable a certain middleware discovery, inform SLA Ops Team to schedule a change window and configure it.
- Starting from Release 16.4, CC supports using Microsoft GPO to manage a subset of Windows related policies. See “Using Microsoft GPO together with CC” on page 41 under "Chapter 5: Policy Management" for the information on how it works. See “Prerequisite for Onboarding Windows Endpoint” on page 45 under "Chapter 10: Server Onboarding" for the prerequisite step that needs to be performed to enable the use of this feature. See Creating and Updating Compliance Environments under "Chapter 6: Account Policy Customization: Compliance Environment" to know how to turn GPO remediation on and off.

  Important: This utility is applicable only to the **Windows 2012 R2** and **Windows 2012 Std** endpoints. This utility is not applicable to the Windows 2008 R2 endpoints and non-Windows endpoints.

- Starting from Release 16.4, the process to re-validate the onboarded servers is available on SRA enhanced UI. See the "Server Revalidation" section under either the CC User's Guide or the SRA User's Guide for the details.
- Starting from Release 17.2, the access to view process instances in the **Process Inspector** is given to the users who are associated to the roles of role type "Support". Process Inspector is used for debugging and monitoring SRA instances, including onboarding.

  Note:

  - This is not retrospective. Users who have access to the Process Inspector will not be able to see the process instances started before they gain the access.
  - Currently, the users who are in the system admin group have the access to the Process Inspector. Their access will remain the same.
  - Some users who are currently in the system admin group might be under the said group due to their access requirement to the Process Inspector. Those users should be migrated to the groups that are associated to the roles of "Support" role type.
  - Anyone who is added to the roles of "Support" role type will gain access to all data in the Process Inspector regardless of the restrictions on access he/she may have inside the SLA application since the Process Inspector access does not follow the CC & SRA role framework.
- Starting from Release 17.4, you can choose to upgrade the chef client of your SLA environment to the newer version, chef client 12.12.13. If you wish to upgrade your chef client, contact the SLA Operation team.
- Starting form Release 17.5, you can log in to SLA environment (BPM UI, SRA Enhanced UI and Compliance Console UI), using IBMid. Single sign-on scenario is also available with the use of IBMid to log in. See Chapter 3, “Logging in to SLA Environments using IBMid,” on page 11 for more details.
- Starting from Release 17.5, FIPS mode is supported. To start managing the servers with FIPS mode turned on, you have to fulfill the following prerequisites.
  - A "Chef Server Upgrade" and "Chef Client Upgrade" must have been performed before you can start enabling FIPS in your endpoints. Chef server upgrade for all SLA environments is scheduled on 27 to 30 November 2017. Please wait for the announcement email from the SLA Operation team for the confirmation of the plan.
  - You must create one or more new "Server Groups" for servers with FIPS turned on. See “Server Group Management” on page 64 for steps on how to create new server groups.
  - The existing server groups that are created prior to FIPS support are **not** editable to support endpoints with FIPS.
  - If you are enabling the FIPS mode in the existing managed servers, you must move them to the new server groups created for FIPS enabled endpoints. There are certain criteria to follow when creating new server groups for existing managed servers.
    - Credential Type and Gateway IP address must be the same in both new and old group for each server.
    - For Unix servers, SSH key in the server will be changed automatically when you move the servers from one server group to another.
    - For Windows servers, every server group has its own password for the "automate" id. When you are moving servers from one server group to another, you can follow either one of the two following scenarios.

1. You can set the password of the new server group to be the same with the password of the old server group, which is the password of the "automate" id of the servers that are under the said server group. To set the password of the new server group to the password of the "automate" id of the servers, you must find out the current password of the "automate" id. Please contact either your deployment specialist or the SLA Operation team.
2. You can set any password for the new server group. However, you must manually change the password of the "automate" id in all the endpoints that are going to be under the new server group before you edit the server groups of each server.

– After creating new server group(s) for FIPS enabled endpoints, you can change the existing servers to be under the new server group via the "Server Details" tab under the "My Servers" page in the "SRA Enhanced UI". See "SRA Enhance UI" chapter of the "SRA User's Guide" for more details.
  - Only the users who are under the system admin group can change the server details, including the server group, of a server.
  - If the change of the server group using "Server Details" page is unsuccessful, you can offboard the server and re-onboard it under the new FIPS enabled server group.

v Starting from Release 18.1, the Entitlement Services can be used together with IBMid. If you are the group owner of entitlement groups, there are actions you should take. See “SLA Entitlement Services” on page 13.

v Starting from Release 18.1, Windows 2016 endpoints are supported for the Continuous Compliance (CC) as long as the endpoint is running with chef client version 12.12.13.

v Starting from Release 18.1, a new compliance status "Issues Found" is introduced in the Continuous Compliance Console. See the CC Console User's Guide for more details.

v Starting from Release 19.3, we will be renaming the following terminologies.

– The **Maintenance Mode** (also known as Compliance Mode) will be renamed as the **Enforcement Mode**.

  It is that point in time within Continuous Compliance where a server/node is being actively managed against governing Security Policy requirements. The Maintenance Mode in UI will be renamed to Enforcement Mode. Auto-remediation to enforce the policy is occurring on a regular interval (24 hours).

  The "Current Mode" of the servers that are already in the maintenance mode before the release 19.3 will **not** be changed to enforcement mode automatically. You can do it manually using the "Manage Enforcement Mode" option. For more information, see "CC User's Guide → Chapter 12. Server Compliance Management → Enforcement Mode".

– The **Compliance Check** (also known as Whyrun) will be renamed as the **Inspection**.

  It is that point in time within Continuous Compliance where a server/node is being compared against governing Security Policy requirements. The Initiate Compliance Check option on the UI will renamed to Initiate Inspection. Report is produced, showing compliance posture as compared to configured policies.

  If you set the mode of a server to "Inspection Mode", a daily inspection in which the server is being compared against governing Security Policy requirements will be run on the server. Unlike the "Initiate Inspection" option,

no report is produced for the daily inspection. Instead, you can see the data from the daily inspection in the Compliance Console.

It is recommended to put servers in either the "Inspection Mode" or "Enforcement Mode". For more information, see "CC User's Guide → Chapter 12. Server Compliance Management → Inspection Mode".

- Starting from Release 19.5, a new compliant mode called the **Paused Mode** is introduced. If a server is in "Paused Mode", no daily inspection or daily remediation will be performed on the server.
- Starting from Release 20.1, SLA supports offboarding of the decommissioned servers (servers that no longer exist in or are disconnected from the system). Previously, this is done by raising the Service Request to the SLA Operations Team and the Operations team helped remove the servers from the system. From Release 20.1 onwards, you can submit server offboarding requests for decommissioned servers using the "Account Management" change category under the "Change Management" option just like any other server. See Server Offboarding for details on how to submit server offboarding requests.

Chapter 3. Logging in to SLA Environments using IBMid

Starting form Release 17.5, you can log in to SLA environment (BPM UI, and Compliance Console UI), using IBMid. Single sign-on scenario is also available with the use of IBMid to log in.

Some prerequisites are to be fulfilled before you can start using the IBMid.

- IBMid SSO (single sign-on) must be enabled in your SLA environment. The enabling and disabling of the IBMid SSO is done during deployment. Contact your deployment specialist or the SLA Operation team if you are unsure whether the IBMid SSO is enabled in your account.
- Request an IBMid if you do not have one. Perform the following step to verify whether you have an IBMid registered with your email.
  1. Visit https://myibm.ibm.com.
  2. You will see the following page. Enter your intranet userid and click the "Continue" button.

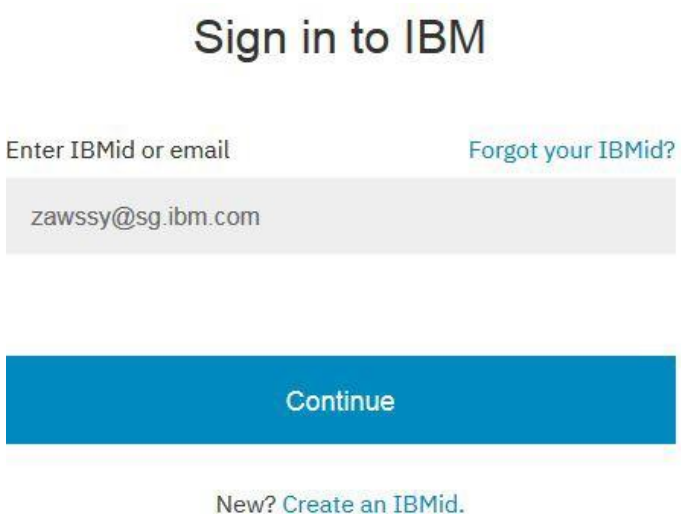


Figure 1. Enter Your Intranet ID

3. If your email is already associated with IBMid, you will see the following message. Click "Sign in to IBM w3id" to start an active single Sign-on session.

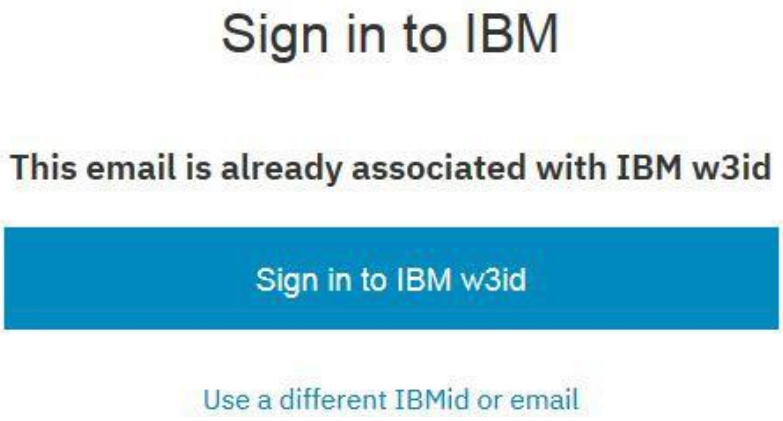


Figure 2. IBMid Exists

4. If you do not see the aforementioned message on screen or if you do not have an IBM intranet id, you must create an IBMid.
5. Click the "Create an IBMid" link to create an IBMid.

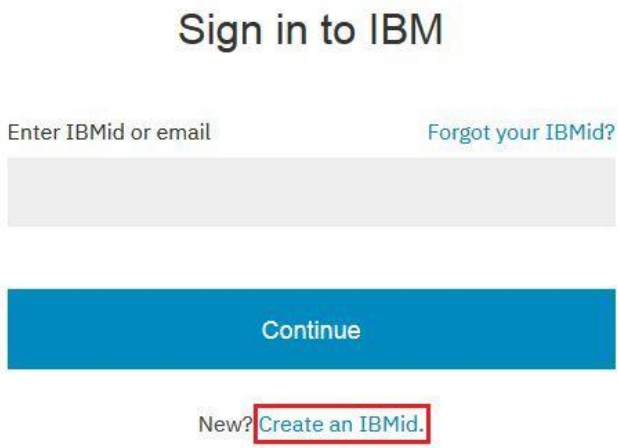


Figure 3. Create IBMid

v You should have proper access right. To be able to login to different applications SLA offers, you should be under corresponding entitlement group. For example, if you want to log in to Compliance Console, you must first be added to the "cc_console_entitlement" group by the group owner (who is either the system admin, also known as the deployment specialist, or any user who is dedicated as group owner of the "cc_console_entitlement" group).

Once all the prerequisites are met, you can start using IBMid SSO to log in to your SLA environment.

IBMid is supported for BPM UI - "Continuous Compliance (CC)" link on your SLA welcome page, and Compliance Console UI - "CC Console" link on your SLA welcome page.

When you click any of the links, you will be automatically logged in if you have a valid single sign-on session, meaning if you have logged in to any IBM domain using IBMid within past two hours. If you do not have a valid single sign-on session, you will be redirected to the IBMid login page.

Note: If "Multi Factor Authentication" is turned on for your IBMid, you will need to enter OTP (one time password) in addition to your user name and password. You will be redirected to the user interface you have selected (BPM UI, or CC Console) after a successful login.
You will be redirected to the user interface you have selected (BPM UI, or CC Console) after a successful login.

- By default, a single sign-on session is valid for two hours.
- Clearing the browser cache will log you out of the session.
- Logging out of any supported SLA UI will only log you out from the UI but not from the single sign-on session.

Please note that you **cannot** use IBMid to log in to WAS (WebSphere Application Server) admin console and BPM admin portal. These applications are to be accessed by limited people with valid access right via deployment admin account.

SLA Entitlement Services

Starting form release 17.5, you can log in to SLA applications, using IBMid with single sign-on capability. Starting from release 18.1, the "entitlement service" is turned on for the IBMid SSO (single sign-on) login.

To utilize the function provided by entitlement service, you need to perform some actions. The SLA entitlement service needs the authenticated user email address to query the entitlements for the user. Thus, if IBMid SSO is enabled in your SLA environment, meaning users log in to your SLA environment using their IBMid, you must make sure that their ids are added to the correct entitlement group. Otherwise, they will not be able to log in to the systems.

SLA solution has a few applications the users can access. These include Continuous Compliance (CC), CC Console, Automated Server Build (ASB) and Risk based Continuous Patch (RCP). The corresponding entitlement groups are as followed.

- cc_entitlement for Continuous Compliance (CC)
- cc_console_entitlement for CC Console
- asb_entitlement for Automated Server Build (ASB)
- rcp_entitlement for Risk based Continuous Patch (RCP)

Important: If you are a system admin (deployment specialist) or the user who is dedicated to be the owner of any "entitlement group" of an existing SLA account, you must add the users who are currently associated to "General User" role under appropriate "entitlement group".

SLA provides an SLA entitlement UI for the user to control the membership of entitlement groups. There are two major authorization methods (Internal and

LDAP) provided by SLA now. Hence there are two ways the user can configure to grant user access to application based on the authorization method chosen. See the respective section.

v "Internal Authorization"

v "LDAP Authorization" on page 16

Internal Authorization

If you have been using the user roles and groups defined in the ProcessPortal, your authorization method is internal. If you are unsure of the authorization method, you can check with SLA Operations team. Perform the following steps to use SLA Entitlement Services.

v Choose a group owner within your organization, normally the system admin or deployment specialist will do the selection.

v Provide the selected group owner's information, including email for IBMid, to the SLA Operations team or Account team so that the owner information can be updated for the above entitlement groups.

v Once the owner information is updated, the owner can log in to the **SLA Entitlement** management portal to add members to each group to grant access to different SLA applications.

v The link for **SLA Entitlements** is on the SLA UI main page.

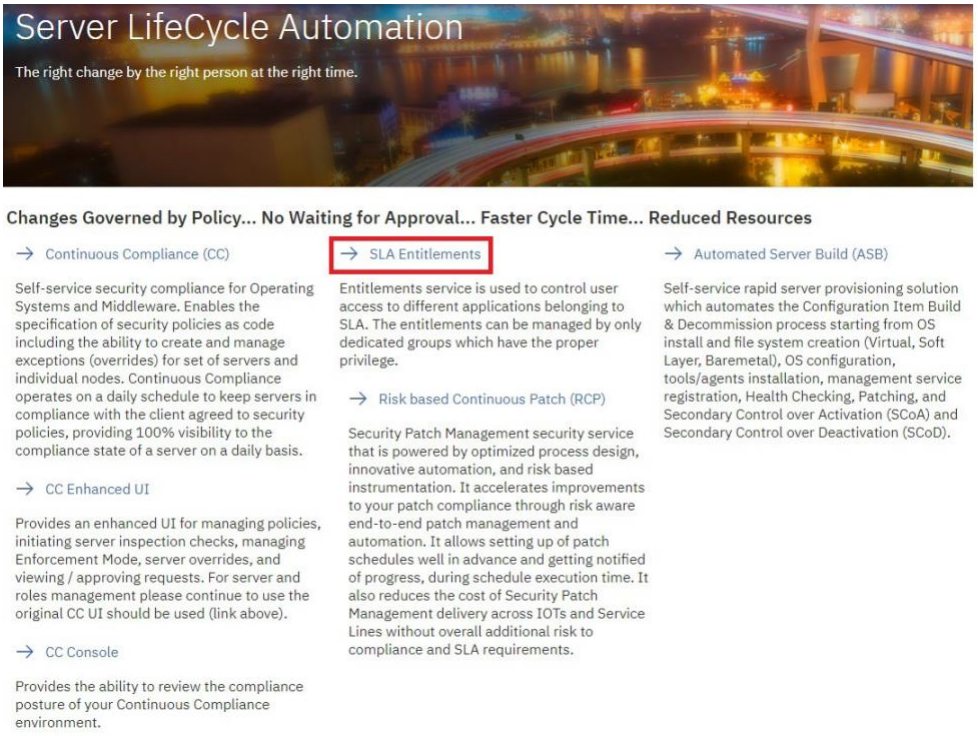


Figure 4. SLA Entitlements Link

v Click the link and log in to the ProcessPortal.

v You will see the groups you manage including the "entitlement groups" that you are made owner of.

v To add a member to a group, click the group name and click the **Members** button.

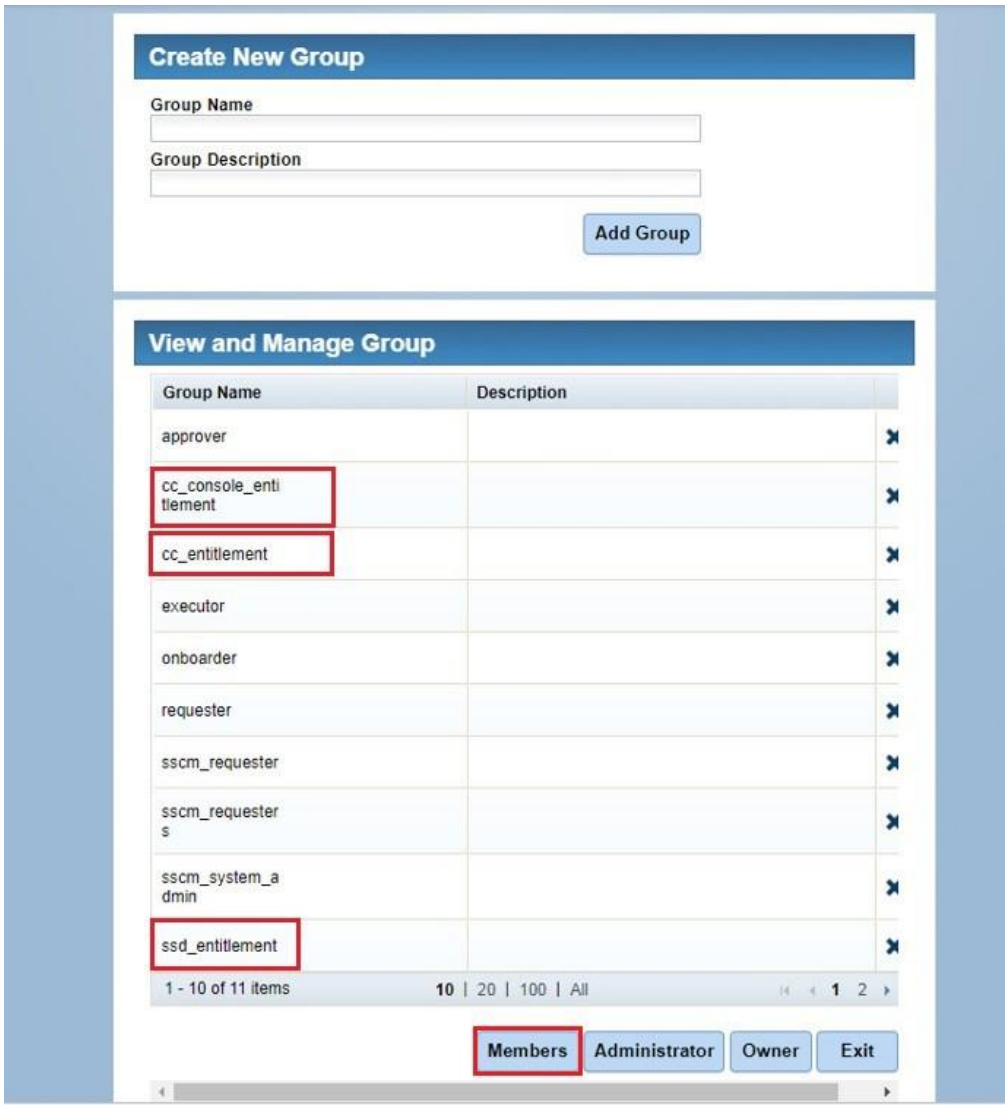


Figure 5. Entitlement Groups

v Enter the email address (associated to the IBMid) of the user in the "Search by Email" field and click "Add".

Figure 6. Add Users to Entitlement Groups

LDAP Authorization

The authorization method is LDAP if the user group information is stored in LDAP server in user's organization. If you are unsure of the authorization method, you can check with SLA Operations team.

In this case, you need to create the LDAP groups corresponding to the entitlement groups listed under "SLA Entitlement Services" main topic in your organization and add the users into the corresponding LDAP groups.

You will see the following message when you click the **SLA Entitlement** link on SLA UI main page.

Figure 7. Configure the LDAP Groups for Entitlement Purpose

Chapter 4. Roles, Groups and User Administration

CC system uses role-based access control. Users of the system come from your company's enterprise directory server (for example, LDAP). Users can be made members of groups that are managed internally within SLA. Groups then get associated to Roles. All members of a group that is associated to a Role can perform the actions designated by that Role. Every Role has a Role Type and there are many different role types in the system. Each role type allows access to do certain things within the system. Roles also have other attributes that can be used to refine (scope) the authority of a user, for example, a role could be associated only with the Test environment or only with servers of a certain Operating System type.

The System Admin Group

The SLA Operations Team will create a system admin group and add one or more users to this group before the SLA environment is handed over to the users. By default, the system admin group is called "sscm_system_admin". However, the name maybe changed for different accounts based on the request from the accounts.

Important: In this document, every mention of "the system admin" group is referring to this group.
Adding the users to the system admin group means assigning them to the role "System Admin". Thus, the users in this group will be the system admins. The initial member of the system admin group is the Deployment Specialist who is designated by the GEO Deployment Program Manager in SLA RTC at the time of deployment.

As a system admin, this initial user (the deployment specialist) is responsible for creating, managing and maintaining the CC related user groups and roles for the account. This user will receive the CC access requests and grant the access requested based on the requester's role within the account. During pre-Go live, the deployment specialists are responsible to obtain the First Line Manager's approval for any new access request. All requests and approval documentation must be retained for audit evidence. Post-Go live, the account team (DPE or delegate) is responsible for obtaining the required approvals and retaining the evidence for access requests.

The system admins must ensure that the separation of duties is maintained. The system admins must also perform the annual re-validation of each CC role and the privileges associated with each role. This includes cleaning out the user ids of the users who have left the company or are no longer part of the team in CC groups.

If you are the initial member or one of the initial members of the system admin group, you should start off by creating

- the "User Roles" based on the business requirement using pre-defined role types, and
- the "User Groups" to be associated with the "User Roles".

All subsequent users who are added to the SLA environment must be added to one of the user groups. Before you start creating the roles, see “Definition of Role Types within CC” on page 20 section to get a better understanding of the

pre-defined role types. See “Creating User Groups” on page 21 and “Associating User Groups with Roles” on page 26 for steps on creating user groups and user roles.

Important: The System Admins are NOT the ONLY ones who can create new user roles/groups. Role Administration can be delegated by creating a role admin group, adding users to the group and associating the group with the role of type "Role Admin". As for Group Administration, any user of any role can create new groups using Group Administration.

Definition of Role Types within CC

Every role you create in SLA system must follow a role type. Role types are predefined in the system. Each role type allows access to do certain things within the system. Users of the system have different role types that allow them to perform various CC related tasks. Roles also have attributes that can be used to refine the authority of a user (scope).

Table 3. SLA Role Types

CC / Common	Roles Type	Description
CC	Account Security Focal	Manages agreed security policies between IBM and Customer at the CSD and Tech Spec doc level while working with SCS and SA teams for implementation Approves/Rejects CC related changes such as compliance environment/profile changes
CC	CC Entitlement	Can log in to the Process Portal
CC	CC Server Owner	Assigns/Reassigns servers into different compliance environments and profiles based on company's security policies Performs sever level compliance policy modifications using "Account Policy Customization" Initiates server inspection Submits overrides and bulk compliance (deviation) overrides Manages servers in enforcement mode
CC	Compliance Console Admin	Can log in to the Compliance Console UI Have access to "Admin" tab and can perform tasks that require admin access in Compliance Console UI
CC	Compliance Console Entitlement	Can log in to the Compliance Console UI
CC	Security Analyst	Sets up compliance environments and profiles based on company's security policies using "Account Policy Customization"
Common	Firewall Admin	Receive tasks for connectivity issues (used for onboarding)
Common	General User	Can log in to the system

Table 3. SLA Role Types (continued)

CC / Common	Roles Type	Description
Common	Onboarder	Users associated with this role are allowed to onboard new servers.
Common	Role Admin	Can define new roles and/or delegate authority to other users.
Common	Support	System support team members that receive tasks related to process errors due to technical issues. The users who are associated to the "Support" role have access to view process instances in the **Process Inspector** for debugging.
Common	Requester	Submits change requests via SRA Change Management. Requester role is for Onboarding & Off-boarding servers in CC.
Not in use	Architect	Decides system requirements (no longer used and planned to be removed)
Not in use	Owner	Manages SLA in production (no longer used and planned to be removed)
Not in use	System Owner	Manages SLA in production (no longer used and planned to be removed)

Creating User Groups

Before creating the user groups, you need to consider who will be members of those groups based upon which roles you will associate those groups to. For more information on Roles and the different types of Roles in SLA, see

v Chapter 4, “Roles, Groups and User Administration,” on page 19

The following are the step to create an onboarder group called "sscm_onboarder". You do not need to use the same group name when you create an onboarder group in your SLA environment. You can create other necessary groups based on your business requirement by following the same steps. See the next section for the steps on how to associate the "sscm_onboarder" group to "Onboarder" role.

1. Go to https://<your_sla_environment>. Click on "Continuous Compliance (CC)" link. User can perform administration tasks such as Server Onboarding, Role Management, Server Inspection etc.

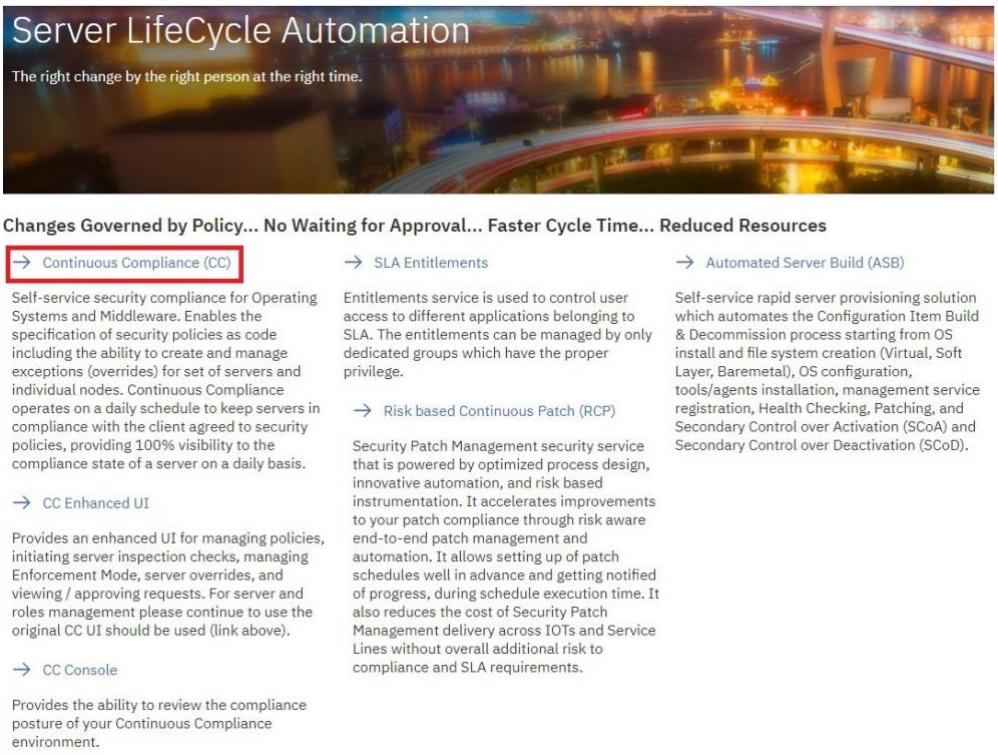


Figure 8. BPM User Interface Link

2. Log in using your LDAP userid or IBMid.

Figure 9. BPM User Interface

3. Click on ' **Organized tabs**' (usually a plus sign in a circle) button from the menu bar on top of the page.

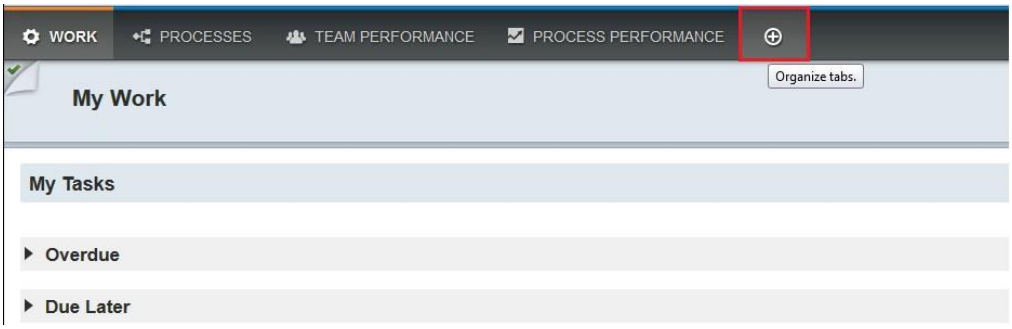


Figure 10. Organize tabs

4. Under '**Hidden tabs**', you will see **Group Administration** and **Role Administration**options.

   Note: SLA supports using LDAP groups as well.

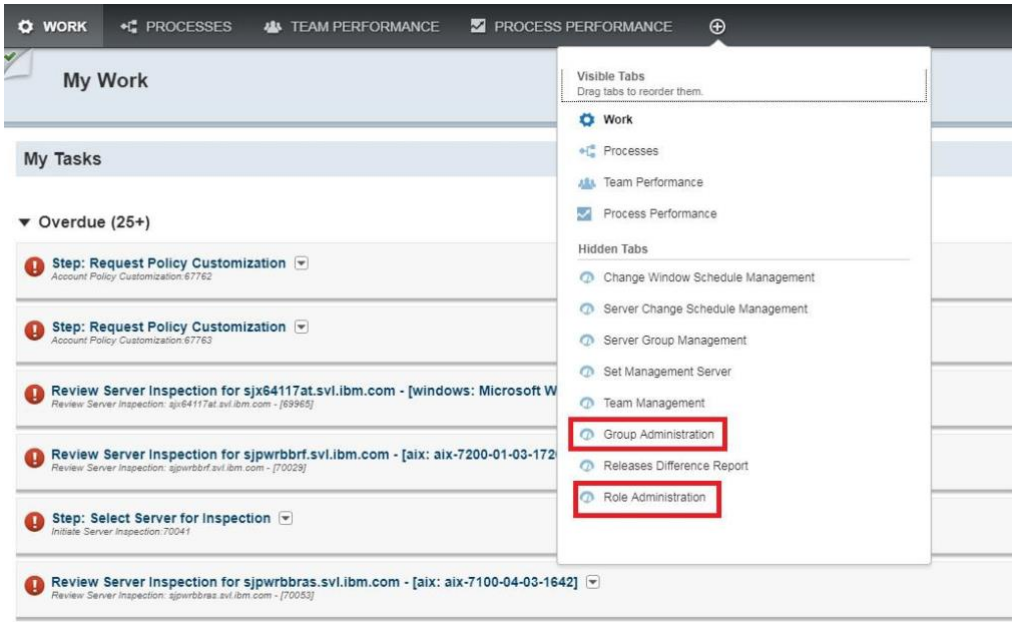


Figure 11. Group Administration & Role Administration under Hidden Tabs

5. Drag the **Group Administration** and **Role Administration** options and drop them under **Visible Tabs**.

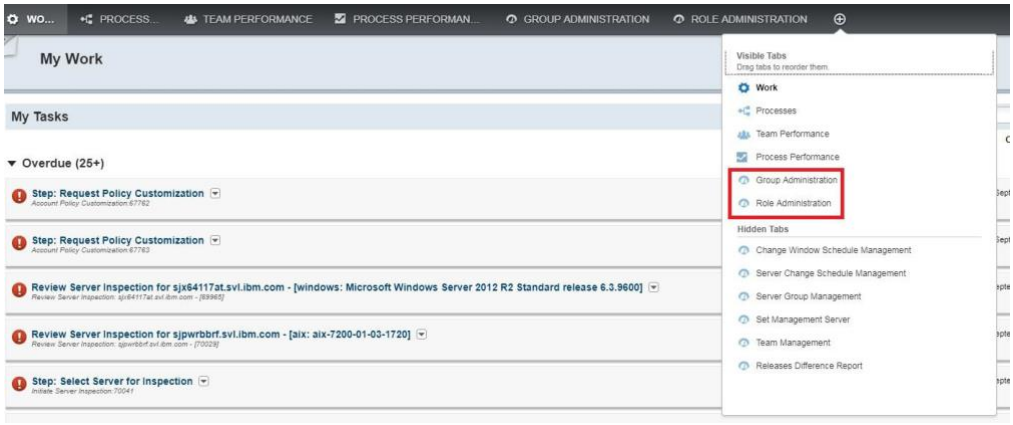


Figure 12. Group Administration & Role Administration under Visible Tabs

6. Using the **Group AdministrationDashboard**, create a group called: '**sscm_onboarder**' .

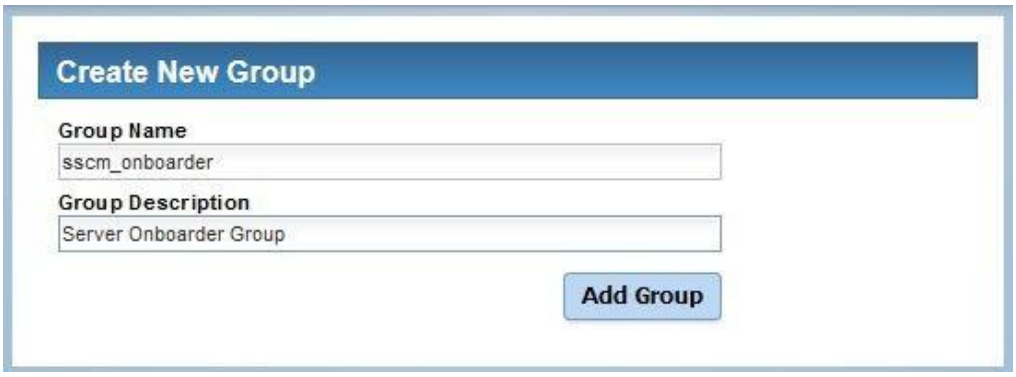


Figure 13. Creating User Group

a. Group Name: **sscm_onboarder**
b. Group Description: <add a brief description>, for example, Server Onboarder Group
c. Once you click '**Add Group**', you will be able to see the group in the table '**View and Manage Group**'. The id that you are logged in is the owner as well as the administrator of the group.

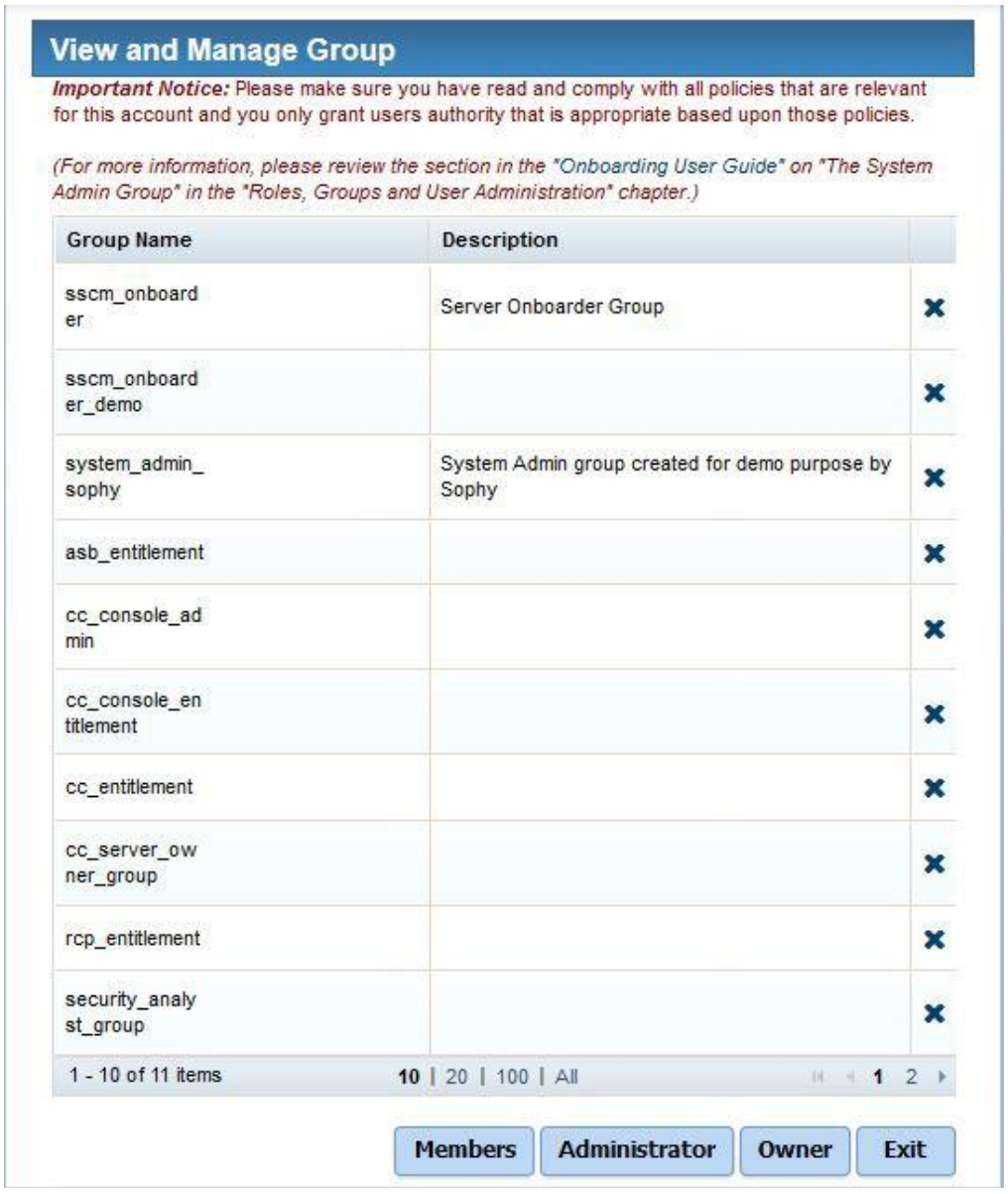


Figure 14. User Group Added

d. Add users who are supposed to perform server onboarding tasks to this group as members.

e. Select the group and click '**Members**'.

f. Enter the email associated to the user who is supposed to be the server onboarder in the '**Search by Email**' field and click '**Add**'. Repeat the same process to add more members.

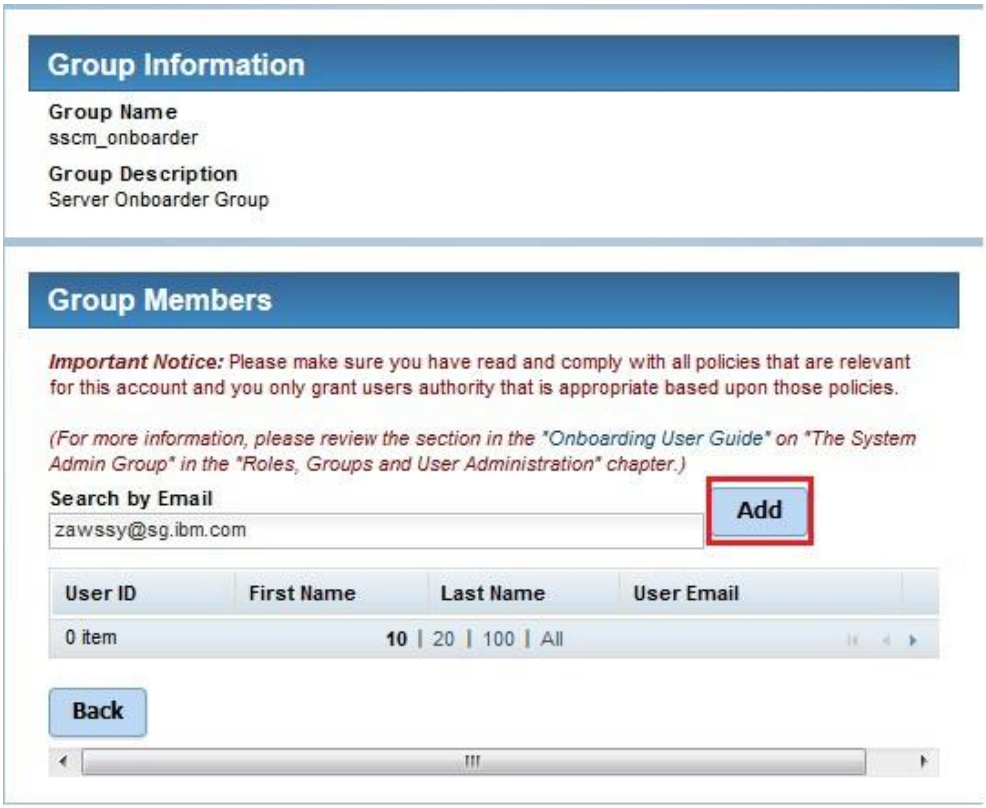


Figure 15. Adding Members in the User Group

g. When you are done, click '**Back**' to go back to '**My Group**' page.

h. If you want to add other users as administrators of this group, click '**Administrator**' and follow the same process as adding members.

i. Unlike members and administrators, there can be only one owner for each group. By default, the user who creates a group is the owner of the group. To change the owner of the group, click '**Owner**'. Enter the email of the user that you want to assign as the owner in the '**Search by Email**' field and click '**Change**'.

   Note: Owner changes can only be performed by the user who is the current owner of the group.

Associating User Groups with Roles

Role administration manages the groups and role types. By associating a group to a role type, users under a group will be able to access CC tasks based on the role type that is bound to the group.

For more information on Roles and the different types of Roles in SLA, see Chapter 4, "Roles, Groups and User Administration," on page 19

1. Launch **Role Administration** from the top menu bar. You will see the **Role Administration** dashboard.
2. **Role Type** drop-down list contains the list of predefined role types.

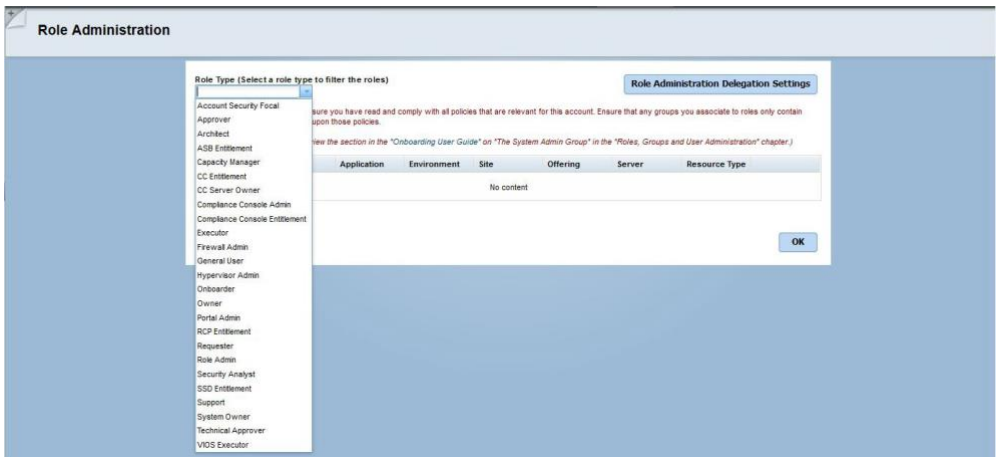


Figure 16. List of Role Types

3. Associate the user groups you have created with appropriate role types. The following example shows the steps to associate the "sscm_onboarder" group you have created in the previous section with "Onboarder" role. By associating the "sscm_onboarder" group with "Onboarder" role, the users that are listed in **sscm_onboarder group** will be able to perform the tasks that are associated to **Onboarder role**.
4. First, create the "Onboarder" role first using predefined role type "Onboarder". Select **Onboarder** from **Role Type** drop-down list and click **Add**.

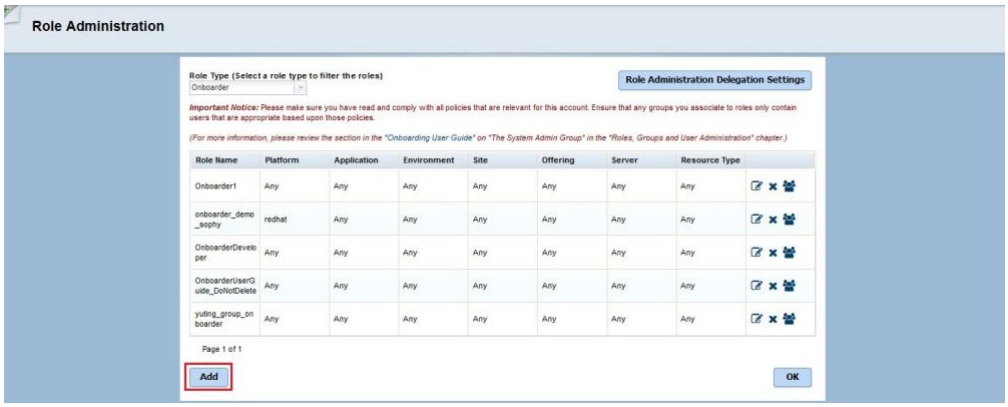


Figure 17. Adding Onboarder Role

5. On the next page, fill in the following:
   a. Admin Scope : The selection for admin scope will vary based on the role authority of the user id you used to log in.
   b. Role Name: Role name can be any unique name which describes role type. In this case, you can name it as **server onboarders**.
   c. User Group: Click **Select** . Search for the user group(s) you have previously created, in this case it should be **sscm_onboarder** group.

      Note: You can associate one role to more than one user group.
   d. Platform: List of platforms that are currently supported in the system. You can limit the access of the users under user selected groups by selecting platform. For example, if you chose Windows, the users under the sscm_onboarder group can only onboard the Windows endpoints. If the two

(or more) user groups you are associating with the user role have different platform access rights, you should associate the user group one by one to the role instead of adding both of them at the same time.

e. Application: List of application that are currently supported in the system.

f. Environment: List of environments that are currently available.

g. Site: Site is equivalent to a Data Center. If you have a specific concept of Site defined, you can use this attribute to provide more information about a server and also to scope role authority.

   Note: Site allows you to associate a server with a data center and then use that to create roles in the system that only allows certain people to manage servers at a certain data center.

h. Offering: Offering is intended to be used for some internal business sub-division as a way for an account to further segregate responsibility of users. If you have a specific concept of Offering defined, you can use this attribute to provide more information about a server and also to scope role authority.

i. Server: List of servers that are currently onboarded.

j. Resource Type: The list of resource type displayed is based on the platform you chose earlier.

k. Click '**OK**'.

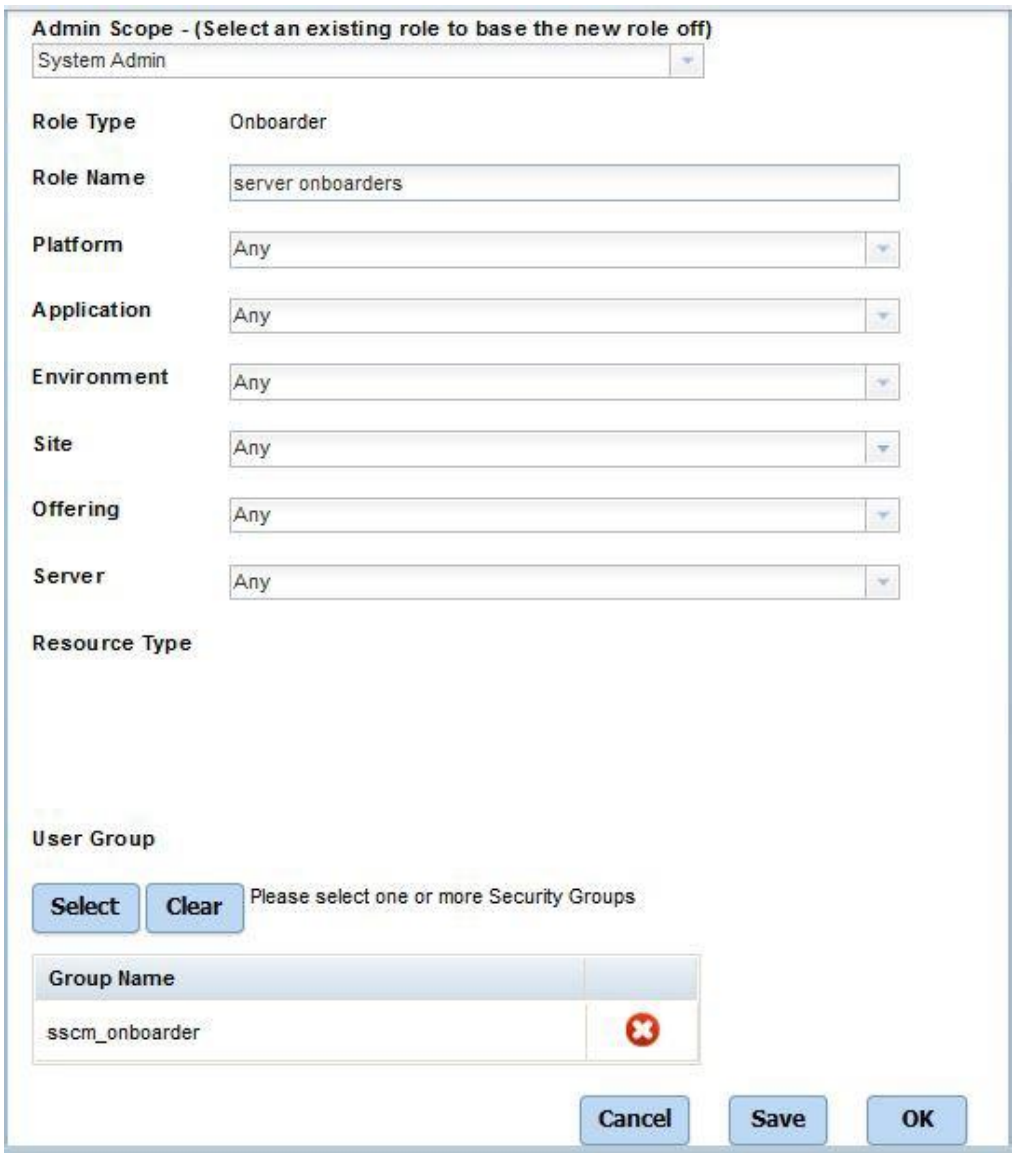


Figure 18. Binding Onboarder Role Type to Onboarder User Group

6. Repeat **Step 4** and **Step 5** to bind the groups you have created to the respective roles.

Team Management

After setting up the groups and roles, you must force refresh the cache by performing the following steps:

1. Click on ' **Organized tabs**' (usually a plus sign in a circle) button from the menu bar on top of the page.

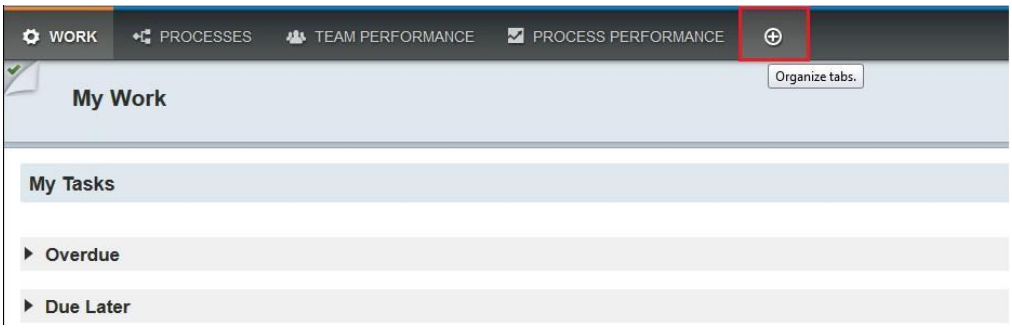


Figure 19. Organize tabs

2. Click on the "Team Management" tab.

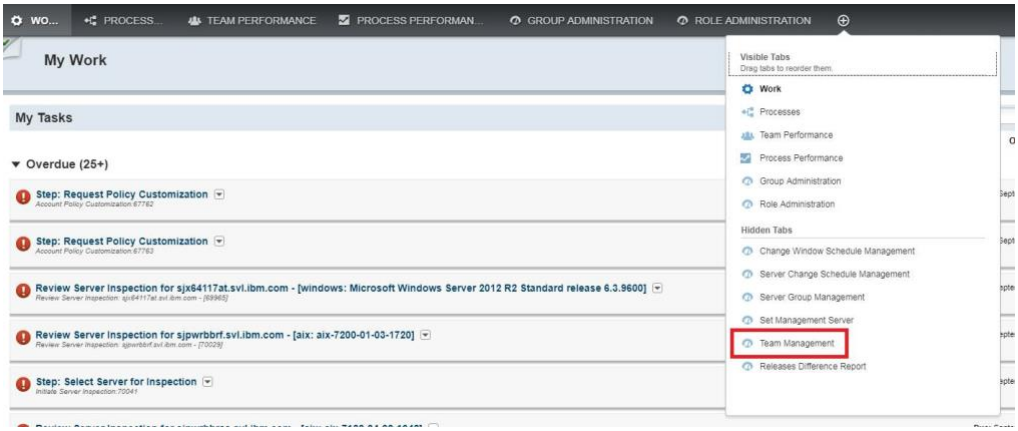


Figure 20. Team Management

3. You will see the list of groups. Click the "Refresh" button beside the groups you have created and associated with the roles.

   Important: Every time a new user is added to a group, you need to perform the aforementioned steps.

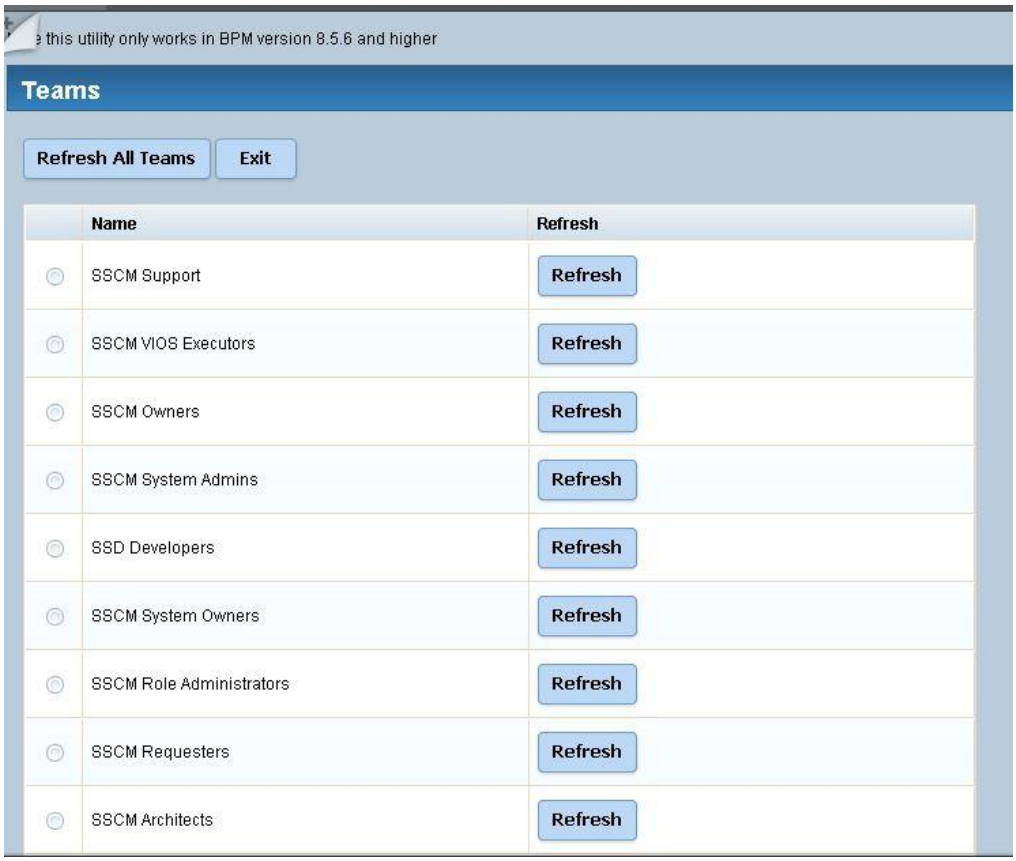


Figure 21. Refresh Groups

Chapter 5. Change Windows Management

Setting up Change Windows

A Change Window is a period during which changes can be made to managed servers in the environment.

Establishing change windows is a key step. CC provides a capability to create new or edit existing change windows and provides functionality to set recurring change windows based on a set of rules in this solution. A default "Eastern" change window is provided with the solution and can be edited by the user.

Important: The system admin group is currently the only group that is able to create, edit or delete change windows in this solution.

1. Click on **'Organize tabs'** (usually a plus sign **+** in a circle) button from the menu bar on top of the page. Clicking on this should provide a drop-down list of options. Choose the "Change Window Schedule Management" option under the "Hidden Tabs" section.

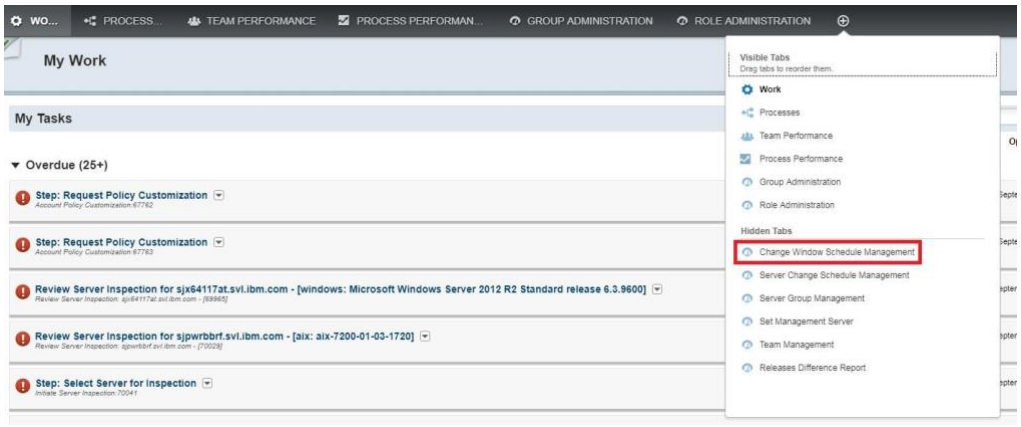


Figure 22. Change Window Schedule Management

2. This will provide you with a screen that shows the default Eastern Schedule, that is, the default change window based on Eastern Time. You will notice that this schedule has been set up to be the default schedule for the solution. In order to add a new schedule, click on the "Add" button.

Figure 23. Add New Change Window

3. Enter the Name of the new time zone and specify the actual timezone that this change window will be scheduled in.

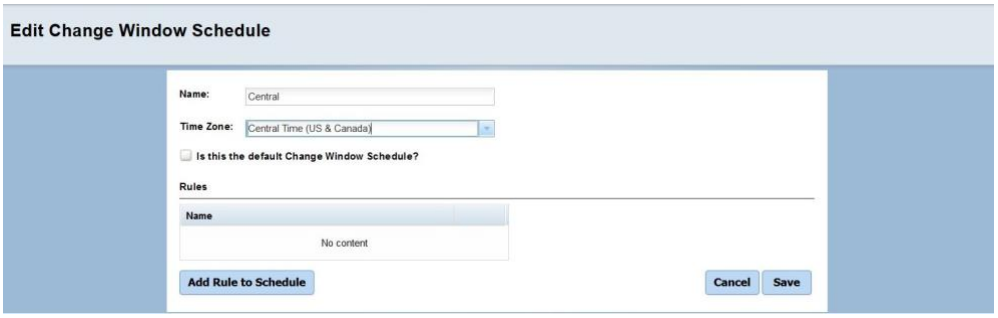


Figure 24. Edit Change Window Schedule

4. If there are no other rules to be added to the schedule, click "Save" to save the Change Window.
5. If you wish to add rules to the schedule, click "Add Rule to Schedule".
6. Enter data into the following fields:
   - Name of the rule
   - How often it repeats. For example, daily, weekly, yearly
   - How often the rule will repeat. **Options are numerical.**
   - Start date and time
   - End date and time. You can define the change window to end on a given date and time, after a set number of occurrences or choose not to end the change window.

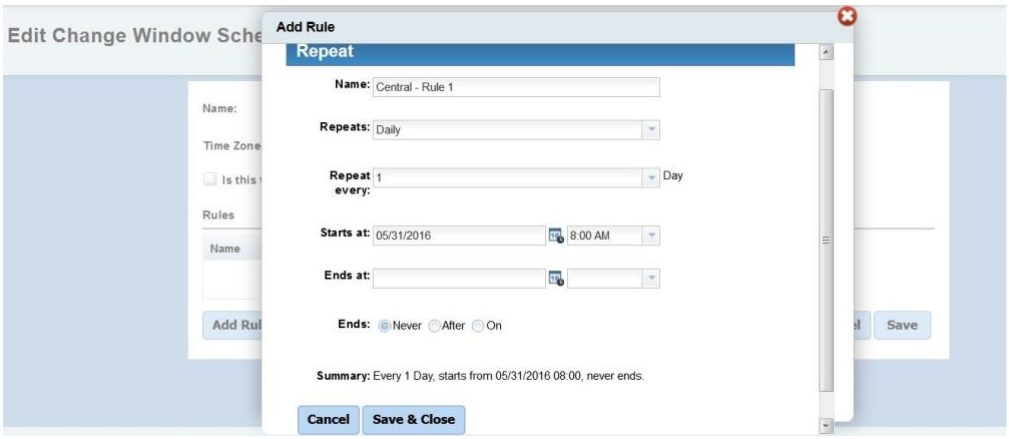


Figure 25. Add Rule to Schedule

7. You will see the summary of rule at the bottom of the pop-up window. Click "Save & Close" to save the rule.
8. Click "Save" to save the Change Window.

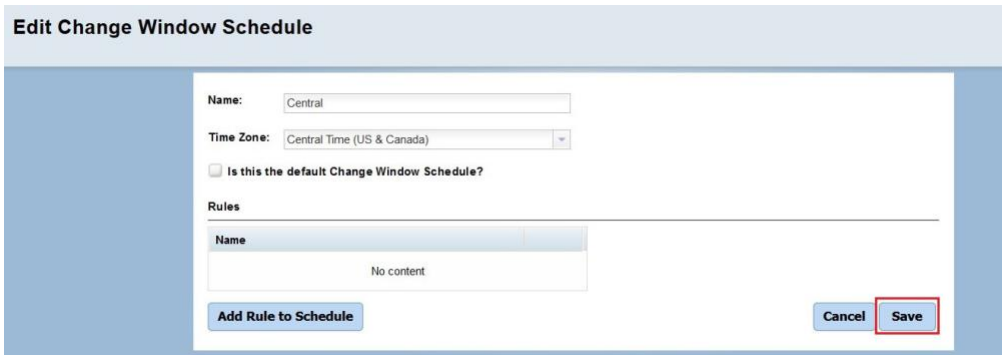


Figure 26. Save the Change Window

9. If you want to edit an existing schedule, click the name of the existing schedule you want to edit and click on the edit button (pencil over square) under "Edit and Delete Buttons" column.

Figure 27. Edit Existing Change Window

10. This will take you to "Edit Change Window Schedule" page where you change the change window name, the timezone and see which servers are associated with the change schedule. You can also control whether this is the default change window and add more rules to the change window as necessary. Once you have edited the change window, click "Save" to save your changes.

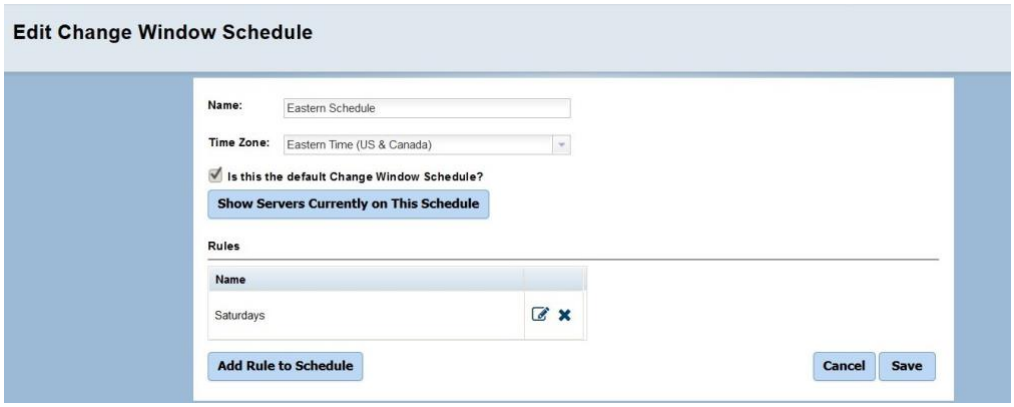


Figure 28. Edit Existing Change Window Schedule

11. If you want to delete an existing change window, click on the delete button (x) under "Edit and Delete Buttons" column.

Figure 29. Exit from Change Window Schedule Management

12. Click "Exit" to exit from "Change Window Schedule Management".

Server Change Schedule Management

During onboarding, you can select the change window to be associated with the servers that are being onboarded. If you want to change the change window of a managed server to a different change window, you can do so using the "Server Change Schedule Management" dashboard after the server is successfully onboarded.

1. Go to https://<your_sla_environment>. Click on "Continuous Compliance (CC)" link. Log in using your LDAP userid or IBMid.

Figure 30. BPM User Interface

2. Click the ' **Organized tabs**' (usually a plus sign in a circle) button from the menu bar on top of the page.

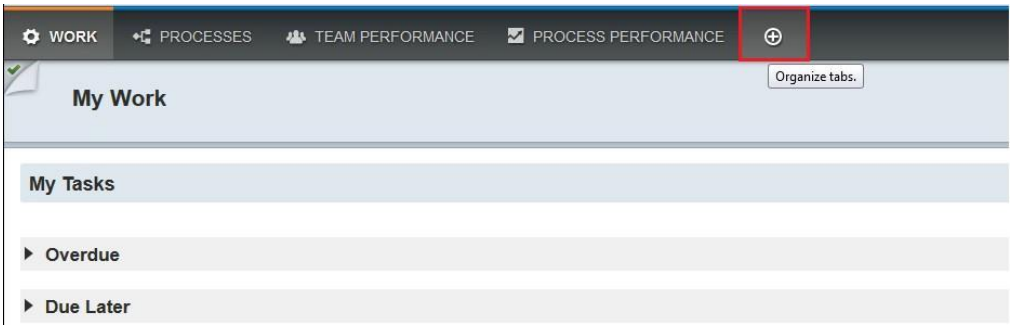


Figure 31. Organize tabs

3. Click the "Server Change Schedule Management" tab.

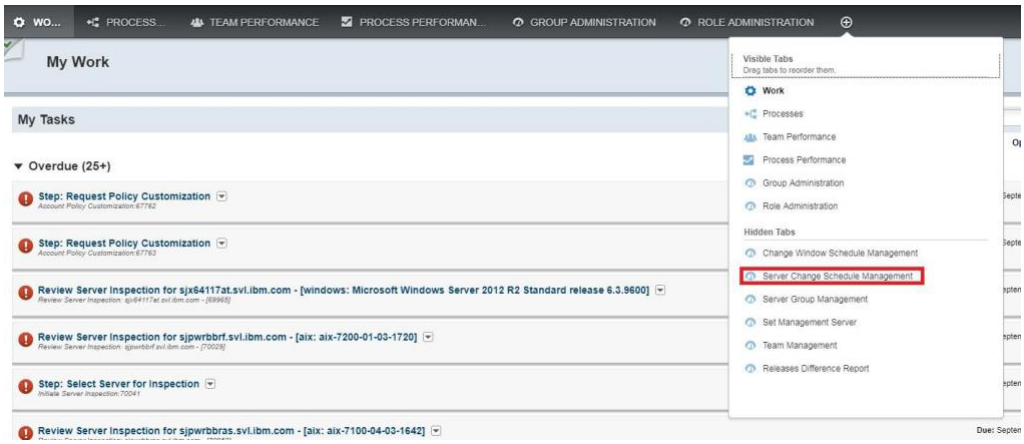


Figure 32. Server Change Schedule Management

4. You will see the list of managed servers and the change schedule associated with them.

Figure 33. Managed Servers and Associated Change Schedules

5. Click the edit button for the managed server for which you want to change the schedule. A pop-up window will appear and you can select a different change schedule that is currently available in the system.

   Note: You cannot create a new change schedule using this dashboard. You can only select from the schedules that are currently available. If you want to create new change window, see "Setting up Change Windows" on page 33

Figure 34. Select New Change Schedule

6. Select the schedule you want and click "Save".
7. Click "Exit" to exit from the task.

Chapter 6. Policy Management

- **An environment** is comprised of a group of managed servers that have the same or similar compliance requirements.
- **A compliance profile** is a named set of compliance policies.
- **A compliance policy** is a specific policy that is enforced on a "managed server" managed by Continuous Compliance.

Continuous Compliance now provides the ability to create an environment that can be associated with a managed server during the onboarding process. The environment contains a set of policies that are used to keep managed systems compliant. Those policies can be customized (overridden) by changing values of attributes that the policies use during enforcement. An example of these attributes would be the password length on a password length policy. The default value may be 8 and an account may have a more stringent requirement to make sure password rules specify that the password length needs to be minimum of 10. The password length attribute could be “overridden” to be 10 instead of 8.

Policies that are defined at the environment level will be part of a defined baseline set of compliance policies. This will allow the Account Security Focal to customize a set compliance policies that will executed across a broad number of servers that have similar compliance requirements. A default environment being provided with the solution, will provide a set of customized policies that comply with IBM's internal ITCS104 security standards. During the onboarding process, managed servers can now be associated with an environment. The policies that are enabled in an environment and that are applicable to a managed server will be evaluated against that managed server's configuration during its inspection.

Important: If an override is submitted containing an invalid attribute value such as an empty required field or an incorrect data type, the submission of the override will write the invalid attribute value to the policy.

Policy Customization Hierarchy

Continuous Compliance provides 3 levels at which attributes can be customized/overridden:

- For a group of servers via Environment level (baseline)
- For a group of servers via Compliance Profile level (custom), and
- For a given server via Managed Server (Node) level.

This hierarchy should be considered as you plan how to onboard your servers and customize the compliance policies within the compliance profiles and environments. Properly configured policies at the environment level will greatly minimize the number of individual server policy customizations that will need to be made and violations that will need to be resolved at the server level. Overrides set at the server level will be executed after those run at the compliance profile and then at the environment level. Overrides set at the compliance profile level will be run after those policies enforced at the environment level.

Environment Level Customization

Continuous Compliance now provides the ability to create and customize Environments via the Policy Management process. New environments are created and customized during the first stages of the onboarding process. During server onboarding, a managed server will be associated with the appropriate environment and a compliance profile. Authorized users can customize policy attributes that are associated to the environment. Any servers associated to that environment will use the attributes specified at the environment level. It is highly recommended that operating system compliance policies be defined at the environment level.

Note: Environment level customization is done by users associated with "Security Analyst" role.

Compliance Profile Level Customization

Continuous Compliance will contain a new compliance profile, the **cc_policy_enforcer profile**, which should be customized if the account has a need to use a unique recipe to enforce compliance. This should be chosen as the default compliance profile during the server onboarding of any managed server added to the solution. For more information on this profile, please refer to Appendix C, “CC_Policy_Enforcer Compliance Profile,” on page 121

Note: Compliance Profile level customization is done by users associated with "Security Analyst" role.

Managed Server (Node) Level Customization

When an inspection is run against a managed server, a task is created for an authorized user to review the policy violations. For each violation, the authorized user can choose to have the violation fixed (that is, bring it into compliance) or create an override based upon the current value. Overrides specified at this level will take precedence over any customization/override specified on the compliance profile associated to this server.

Note: Server level customization is done by users associated with "CC Server Owner" role. The customization steps are similar to "Environment" and "Profile" level policy customizations.

Policy Overrides: Planning and Best Practices

- Try to identify overrides that apply to an environment as a whole so that you can avoid or minimize the need to make overrides at managed server level
- Try to group servers that are similar to each other from a compliance perspective. When running continuous compliance, choose one or two servers that are representative of the group of servers and review the compliance results. Adjust policies or establish a set of overrides based on the inspection results, which can then be applied to the rest of the servers in the group. Process the rest of the servers in the group in the same manner.
- It is recommended that operating system compliance policies should be customized at an environment level
- Start by using the default environment profile that is provided with the solution to evaluate the initial set of managed nodes. This profile is set up to comply with IBM internal ITCS104 security guidelines.

- A Compliance profile should only be customized if there is a new release, if customization will be required at the account level or if there are unique, customized policies that are required by the account.

Policy Versions: Planning and Best Practices

Starting from Release 15.1, there will be a new policy (cookbook) version for each release. As the number of policy versions grows, maintaining the policies in the production environment without disrupting any applications or services running in production will become more crucial. These are the recommended the best practices on how to manage policies.

- Create a pre-production compliance environment along with each production environment so that new policies can be tested in systems in the pre-production environments before moving to production.
- Onboard a set of preproduction endpoints under a pre-production compliance environment.
- When the new policy versions are released, evaluate the changes and decide if you want to upgrade to the new versions of the policy.
- If you want to upgrade to the new versions of the policy, you can upgrade the policy versions in the pre-production environments and perform the initial server inspection (whyrun) on different endpoints in the pre-production environment first.
- If the whyrun results are acceptable, you can run the systems in the pre-production for a certain period to make sure there are no issues and/or you can upgrade the production compliance environments to the new policy versions.

A read-only version of CC policies documentation and source code is available for the user's reference. See Appendix A, “CC Policies Documentation and Source Code Reference,” on page 117 for further information.

Using Microsoft GPO together with CC

Continuous Compliance allows you to manage the Windows systems that are using Active Directory using GPO and CC together. You will have flexibility to switch between CC and GPO for certain policies.

Important:

- This utility is applicable only to the Windows 2012 R2, Windows 2012 Std and Windows 2016 endpoints.
- This utility is not applicable to the Windows 2008 R2 endpoints and non-Windows endpoints.
- This item is only required in release 21.3 or earlier version. Since release 21.3.1, this item is no longer required.

  Manually login to the endpoint at least once using the "automate" user ID before you start using this utility. This is to create the user profile files on the endpoint. Otherwise, this utility may not work properly on the endpoint. This is a known issue.

  The user will need interactive logon only for allowing the creation of the profile folder. A tool to automate the logon to multiple endpoints is made available here https://ibm.biz/BdYSJG from where you find reference to the autoRdp_v3_for_customer.zip tool.

It is further recommended to perform the logon using the automate user on your operating system image source, so you will not need to do this step on every spawned server as it is already contained in your source image.

To be able to use GPO together with CC, you must update the "automate" user id to have Active Directory Privileges. Configure domain controller by running the following on your Windows endpoint using PowerShell.

```
Enable-WSManCredSSP server
```

Note: The "automate" user must be a domain user.
You will see the output similar to the sample output below.

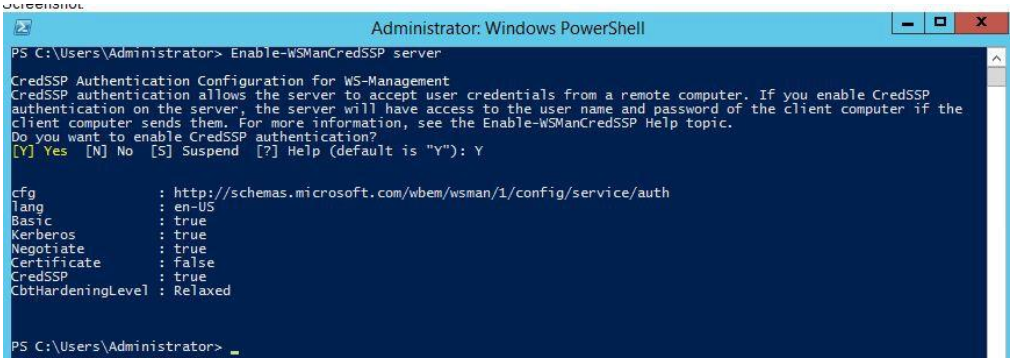


Figure 35. Enabling CredSSP Authentication

For now, there are five policies that can be manage using both GPO and CC. See the list below.

1. policy_windows_audit_logging_requirements
2. policy_windows_log_retention
3. policy_windows_password_policy
4. policy_windows_osr (partial support for Windows 2016 as of release 18.1)
5. policy_windows_event_log_guest_access
6. policy_windows_user_access_control
7. policy_windows_defender
8. policy_windows_admin_account

For the policies that can be managed by GPO, you will have the option to allow GPO remediation.

Note:

v If the GPO remediation is enabled, CC will make sure the GPO settings are compliant. CC will govern the policies and attribute values and check and remediate GPO where it drifts.

v If the GPO remediation is enabled but the endpoint is not configured into the domain, CC will manage the security settings at the local level.

v If the GPO remediation is enabled but CC is unable to read the GPO settings, CC will not update any local or GPO setting.

v If you do not allow CC to manage GPO policies, CC will indicate that there is a compliance deviation that cannot be remediated.

v GPO settings will not be honored at the Server Level Customization.

For more details on Environment and Policy Override, refer CC Enhanced UI User Guide.

Chapter 7. Server Onboarding - Legacy

Important:

Starting from release 23.5.1, a new SLA Client with a message-based communication model is available and would be enabled on a pre-request basis. This new model would provide better security, stability and maintainability of the solution, and recommended model to adopt. Plans should be made on all accounts to eventually move to that model. Please refer to Chapter 8, "Server Onboarding - Message-based SLA Client Install," on page 91for more details.

Before you can start managing a server, you must onboard the server that you want to manage. You can submit a server onboarding request to onboard a server.

Important: Prior to the onboarding request submission, you must fulfill the prerequisites. Go through the sections under "Prerequisites to Onboard a Server" and perform the prerequisite steps that are applicable to your endpoints.

Prerequisites to Onboard a Server

- Before you can onboard a server, you must have an endpoint id set up for the server (endpoint) you want to onboard.

  Important: From sprint 11.5 onwards, if your environment has been integrated to IP Center, you can skip the ID set up step. However, you must provide SLA Operation Team with the hostname and IP address of the endpoint you want to onboard prior to onboarding. SLA Operation Team will add the information in configuration so that you can successfully onboard the endpoint.
- The server should be configured to use an NTP time servers.

Prerequisite for Onboarding Windows Endpoint

Check whether your endpoint meets the following requirements.

Connectivity Requirements

- The hostname of the endpoint must be resolvable from the Execution Engine Server.
- The port 5985/tcp on endpoint must be reachable from the Execution Engine Server.
- For the endpoints using domain account, the port 5985 on domain controllers and domain members should be opened since WinRM uses port 5985.
- The endpoint must be able to reach the Execution Engine by HOST IP on port 3333.
- The endpoint must be able to reach CHEF Server by HOST IP on port 443/tcp for SLA environments created by 20 July 2017.
- The endpoint must be able to reach CHEF Server by HOST IP on port 8443/tcp for SLA environments created after 20 July 2017.

Disk Space Requirements

- The endpoint must have at least 5 GB available for CHEF client binaries located in C:\IBM\cobalt folder.

v The C:\IBM\cobalt folder may be placed as a mount point to a separate file system to contain the space consumed by CHEF

OS Settings Requirements

v The endpoint clock must be synchronized within 15 minutes of the chef server.

OS Version Requirements

v Windows 2008 R2

v Windows 2012 R2

v Windows 2012 Std

v Windows 2016

Memory Requirements

v The recommended amount of RAM available for CHEF client to run is 512MB.

Software Requirements

v All Windows Servers must meet prerequisites which is to have PowerShell 3.0 (or higher) with 512 MB memory (or higher) configured.

Note: Windows Server 2016 uses PowerShell 5.1. No hotfix installation is needed.

v In addition, hotfix **kb2842230** needs to be deployed for PowerShell 3.0.
  - For Windows Server 2008 R2, deploy Windows Hotfix KB2842230 for Win2008 R2.
  - For Windows Server 2012, deploy Windows Hotfix KB2842230 for Win2012.
  - Download and install the hotfix.
  - Restart the endpoint after the successful hotfix installation.

v Microsoft .NET Framework 4.5 is required to install PowerShell v3.0. Windows Server 2012 and 2012 R2 include the .NET Framework 4.5. Windows Server 2008 R2 only includes .NET Framework 3.5.1. If your endpoint OS is Windows Server 2008 R2 you MUST manually put .NET Framework 4.5 in place in your endpoint.

v Starting from Release 17.5, FIPS mode is supported. However, a chef server upgrade must have been performed before you can start turning on the FIPS in your endpoints. Chef server upgrade for all SLA environments is scheduled on 27 to 30 November 2017. Please wait for the announcement email from the SLA Operation team for confirmed plan. For FIPS enabled endpoints, you must create a separate server group. See “Server Group Management” on page 64 for steps on how to create server groups with FIPS enabled.

Functional ID Requirements

Perform the following prerequisite steps on the Windows endpoint you want to onboard to meet the functional id requirement.

Important: The prerequisite steps must be completed on a server using a language with DBCS characters in order for information to display properly on the console.

1. Add a Windows userid named **automate** on each target server endpoint.

   Note: It is not mandatory to name the user "automate". You can have a different name if you want to. The description is only for standardization purpose. However, the userid must be the same for all Windows workgroup

servers. Likewise, the userid must be the same for all Windows domain member servers. If you use a different userid from "automate", the userid you use will be added to the server group "all_winrm_servers" which is the default server group for Windows servers. See “Server Group Management” on page 64 for more information on "Server Groups".

In this section below, "automate" user is referred to be the exact userid "automate". Please replace "automate" with the correct userid if a different userid is used. **If your account is using a different userid name other than "automate", file a Service Request to SLA Ops Team in the SCCD system to update SLA EE configuration before onboarding any CCI.**

2. Add **automate** user to administrators.
   a. Login using Window RDP Application as the **Administrator** user to the Window Endpoint.
   b. Launch the **Control Panel** in the Window Endpoint.
   c. Open the **User Accounts** settings.
   d. Click the **Manage another account** link.
   e. Click the **Add a user account** link.
   f. Enter **automate** in the **User name** field.
   g. Click **Next** to create the automate user.
   h. Click **Finish** to return to Manage User account screen.
   i. Select the automate user in the users list page.
   j. Click the **Change the account type** link.
   k. Add the "automate" user to the Administrator group. Select **Administrator** under the account type selection page, then click the **Change Account Type** button.
3. Set a password for **automate** user. Set to known password (The password for Windows endpoint that is sent to you by SLA Operation Team in the **Confidential email** when your environment is ready to use.)

   Note:

   - Based on your account policy, you can choose to make the password of the **automate** user non-expiring. See **Step 4**.
   - However, some compliance rules, for example ITCS104, specify that systems cannot have user ids with non-expiring passwords. For windows in particular, they have to be changed every 90 days. There are two ways to change the endpoint password every 90 days:
     a. You can manually change the password before it expires in the endpoint and update the password in SLA UI using "Server Group Management" task. See **step 8 and 9** of the Server Group Management section.
     b. Alternatively, you can submit a service request to configure SLA to automatically change the "automate" id's password on regular basis and schedule a change window to enable the auto update. See “Windows Endpoint Password Auto Update to Support Password Expiration Rule” on page 52 for more details.
4. If you want the password of the automate user to never expire, the password must be set as "never expires" and the **automate** user must be added to the whitelist for password max age policy. Replace "automate" with the correct userid if a different userid is used. Perform the following steps.

   To set automate user's password as non-expiring:

a. Login using Window RDP Application with your administrator account to the Window Endpoint.
b. Go to **Server Manager → Dashboard**.
c. On the top-right corner, click on the **Tools** option and select **Computer Management**.
d. The **Computer Management** window will pop up.
e. On the left side of the window, expand the **Local Users and Groups** option.
f. Open **Users** folder under "Local Users and Groups".
g. You will see the **automate** user. Double click on the automate user.
h. The **automate Properties** window will pop up to display the properties of the automate user.
i. Check the check-box beside **Password never expires** if it is not checked.
j. Click **Apply** and then click **OK**.
k. Logout of the endpoint.

To add automate user into the whitelist for password requirements policy:

a. Log in to your SLA environment.
b. Select **Account Policy Customization.**
c. Under **Environments** tab, select the environment under which you want to onboard your window endpoint.
d. Look for **policy_windows_password_requirements** policy.
e. Click the **Customize Policy** link associated to the policy_windows_password_requirements.
f. The attributes of the policy will be displayed in the right-hand pane on the screen.
g. Click the **plus sign inside the green circle** next to the title **Exempted users**.
h. A new text field will appear under "Exempted users" section.
i. Add **automate** as userid in the text field.
j. Click **Save** and then click **Submit for Review**.
k. This policy customization requires the approval from the "Account Security Focal".
l. After the "Account Security Focal" has approved the customization, the password for automate user will be non-expiring.

5. If the **automate** user's display language is currently not set to "English (United Sates)", change the "Windows display language" to English. The display language for "automate" user must always be "English". This is a crucial step for CC to support DBCS. Perform the following steps to set the display language to English.

   Note: If English US is not installed on server initially and the server cannot connect to internet, server admin need to prepare En-US language pack for offline installation.

   v The language installation file is available at download centers for OEMs and System Builders. Download the language installation file.

   Microsoft OEM site: https://www.microsoftoem.com/Login.aspx

   OEM Partner Center: https://dpcenter.microsoft.com

   v Use "Run" from the start menu and then run the "lpksetup.exe" by entering lpksetup.exe and clicking "OK".

   v Select "Install display languages" option in the next pop-up.

- Browse for the "En-US" language pack you have previously downloaded in the first and click "Next".
- Wait for the installation to be completed and click “Finish”.

Here is a video to install windows language CAB file https://www.youtube.com/watch?v=kzfuX_e_6iY

Steps to change the display language of Windows Server 2008:

a. Login using Window RDP Application as the **automate** user to the Window Endpoint.
b. Launch the **Control Panel** in the Window Endpoint.
c. Open the **Clock, Language, and Region** settings.
d. Click the **Change display language** link.
e. The **Region and Language** window will appear.
f. Go to **Keyboards and Languages** tab.
g. Select **English** under **Choose a display language** drop-down under "Display Language" section.
h. Click **Apply**.
i. In the same **Keyboard and Languages** tab, under "Keyboard and other input languages" section, click the **Change keyboards...** button.
j. Under **General** tab, change default input language to **English (United States) -US**.
k. Use **Move Up** button to make sure "English" is the first language.
l. Click the **Apply** and **OK** buttons.
m. Reboot the endpoint and re-login with **automate** to ensure "English" language is taking effect.

Steps to change the display language of Windows Server 2012 or later:

a. Login using Window RDP Application as the **automate** user to the Window Endpoint.
b. Launch the **Control Panel** in the Window Endpoint.
c. Open the **Clock, Language, and Region** settings.
d. Click the **Language** link.
e. Click the **Add a language** link.
f. The list of languages will be displayed.
g. Scroll down to **"E"**. Double click **English**.
h. Select **English (United States)**.
i. Click **Add**.
j. Use **Move Up** button to make sure "English" is the first language.
k. Click the **Options** for English language.
l. Check if **Windows display language** is **Enabled**.
m. Set **English (United States)** as Windows display language by clicking **Change override** and selecting English (United States) as display language.
n. Reboot the endpoint and re-login with **automate** to ensure "English" language is taking effect.

6. If **Oracle** middleware is installed on your endpoint, perform the following steps to add the **automate** user to the group with privileges to run Oracle commands.
   a. Login using Window RDP Application as the **Administrator** user to the Window Endpoint.

b. Launch the **Control Panel** in the Window Endpoint.
c. Open the **System and Security** settings.
d. Click the **Administrative Tools** link.
e. Open **Computer Management** under Administrative Tools.
f. The Computer Management window will be displayed. You will see the menu on the left side of the window. Click the **Local Users and Groups** option.
g. You will see two folders under the "Local Users and Groups". Open the **Groups** folder.
h. You will see a group named **ora_dba** with the description "Oracle DBA Group".
i. This group is automatically added when the Oracle is installed on your endpoint. It is the group that has privilege to run Oracle commands.
j. Double-click on the "ora_dba" group to open.
k. Click the **Add** button.
l. Enter **automate** in the "Enter the object names to select (examples):" field and click the "Check Names" button.
m. Click **OK**.
n. You will now be able to see the "automate" user added under "Members:" list of "ora_dba" group.
o. Click **Apply** and then click **OK**.

All the Windows endpoints should use **either** the local account **or** the domain account. Not both.

If the account you are using is a domain account, see “Prerequisites for Windows Server Onboarding with Domain Account” on page 53.

If the account you are using is a local account, see “Prerequisites for Windows Server Onboarding with Local Account” on page 54.

Prerequisites to use GPO to manage a subset of Security Policies

Continuous Compliance allows you to manage the Windows systems that are using Active Directory using GPO and CC together. You will have flexibility to switch between CC and GPO for certain policies. To be able to use GPO together with CC, you must update the "automate" user id to have Active Directory Privileges. Configure domain controller by running the following on your Windows endpoint using PowerShell.

```
Enable-WSManCredSSP server
```

Note: The "automate" user must be a domain user.
You will see the output similar to the sample output below.

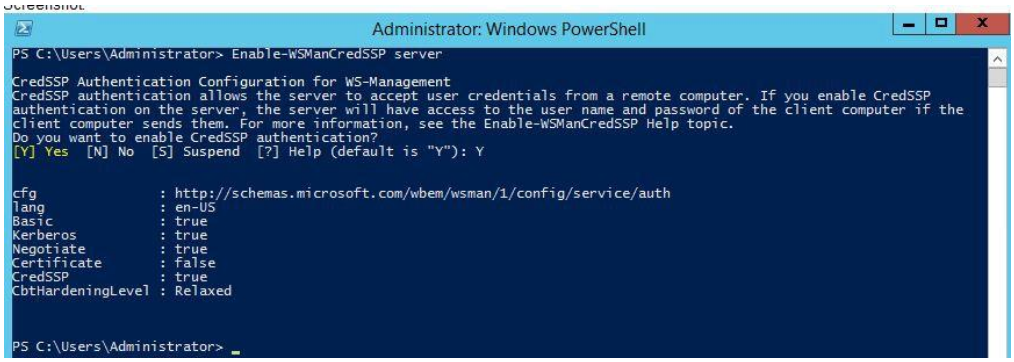


Figure 36. Enabling CredSSP Authentication

Optional Requirements

Note: Performing the following steps may result in the faster onboarding process and the lesser onboarding failure. However, they are not mandatory and not performing them will not deter you from successful endpoint onboarding.
Some installer files that are downloaded on the endpoints during onboarding are large files. It takes a long time for the endpoints to download the installers. This may lead to the onboarding failure especially when there is a network bandwidth limitation in the environment. To optimize the onboarding process, SLA allows you to download the necessary installers to the endpoints before onboarding. Downloading the installers to the endpoint before you start onboarding it will improve the performance of the overall onboarding process. Perform the following steps to download the installer files to the endpoint you want to onboard.

1. Download the installer from the following links based on the deployment model of your account.

   If your account is using JumpHost, download from the following link.

   v For environments using chef client 12.4.1

   https://<JumpHost_ip_address>:3333/shared/chef-client-cobalt-12.4.1-win.zip

   v For environments using chef client 12.12.13

   https://<JumpHost_ip_address>:3333/shared/chef-client-cobalt-12.12.13-win.zip

   If your account is using IPCenter, download from the following link.

   v For environments using chef client 12.4.1

   https://<IPCenter_JumpHost_ip_address>:3333/shared/chef-client-cobalt-12.4.1-win.zip

   v For environments using chef client 12.12.13

   https://<IPCenter_JumpHost_ip_address>:3333/shared/chef-client-cobalt-12.12.13-win.zip

   If your account is an on-premise account, download from the following link.

   v For environments using chef client 12.4.1

   https://<your_sla_ee_server_hostname>:3333/shared/chef-client-cobalt-12.4.1-win.zip

   v For environments using chef client 12.12.13

   https://<your_sla_ee_server_hostname>:3333/shared/chef-client-cobalt-12.12.13-win.zip

2. Copy the installer, either **chef-client-cobalt-12.4.1-win.zip** or **chef-client-cobalt-12.12.13-win.zip** depending on the chef client version your environment is using, to the directory **C:\temp\chef**

Windows Endpoint Password Auto Update to Support Password Expiration Rule

Compliance rules specify that systems cannot have user ids with non-expiring passwords. For example, compliance rules may dictate that passwords have to be changed every 90 days. There are two ways to change the endpoint password every 90 days:

1. You can manually change the password before it expires on the endpoint and update the password in SLA UI using "Server Group Management" task. See **step 8 and 9** of the Server Group Management section.
2. Alternatively, you can submit a service request to configure SLA to automatically change the "automate" userid's password on regular basis and schedule a change window to enable the auto update.

This section is for option 2. Once you have enabled the password auto update, the password of the automate userid will be changed automatically before it is expired. You can customize the number of days in the password reset interval for your SLA environment. For example, if you specify the interval to be 3 days and the password is expiring within 3 days, SLA will change the password of the endpoints. You can also define the minimum password length and character groups. Defining allowed character group means defining which type of characters are allowed in the password. For example, you can specify that password can contain only the alphanumeric characters and no special character. Endpoints that are using Windows local accounts as well as endpoints that are using Windows domain accounts can be configured for password auto update.

The following are the prerequisites to use this password auto update feature.

- The onboarding password is required for "Windows local account". When setting up the userid to onboard a new server, you do not need to know the current password that is managed by SLA. Instead, the onboarding password is used to setup the userid before onboarding the server into SLA. Once the server is onboarded, SLA will change the server password to the SLA managed password. Once the password is about to expire, SLA will change the password of the automate userid on all onboarded Windows servers. If an endpoint using "Windows local account" is offboarded, SLA will change its automate userid's password back to the onboarding password.
- The automate userid password change is not applicable for accounts managed using the IPCenter deployment model.
- Your SLA environment must have the "Support" role created, a "User Group" associated to that role, and users added to the "support user group". See Chapter 4, “Roles, Groups and User Administration,” on page 19 for information on how to create user groups and roles.
- At least one server must be put into either the Enforcement Mode (previously known as Maintenance Mode or Continuous Compliance Mode) or the Inspection Mode for the expiring password to be auto updated.
- For Windows domain accounts, make sure RAST-AD-Powershell is installed by using the following powershell commands (run in the powershell command window as administrator)

```
Import-Module ServerManager
Add-WindowsFeature RSAT-AD-PowerShell
```

- If this feature is enabled for Windows domain account, do not use the 'automate' id to logon to Windows domain account. The password can be out of sync between the server and domain controller if there is a logon session.
- At least one server is put to Maintenance Mode (Continuous Compliance Mode) as the feature event is triggered from server side.
- Add members to Support role so that they will get email notifications and tasks if there is failure that requires manual fix.
- IPCenter accounts are not supported.

In case of password auto update failure, the users associated with the "Support" role will receive a task called "Manual Fix and Provide Temporary Password" in their workspace and an email notifying about the task in their inbox. The email will contain the list of servers for which the password auto update failed.

Important: If you do not have the "Support" role and group in place with users in the group, no one will be able to see the "Manual Fix" task when the password auto update fails.

If you are a support team member, perform the following steps.

1. Check if the servers are up.
2. Set the same temporary password to all the servers for which the password auto update failed. You can see the server list in the email.
3. Log in to SLA UI and claim the "Manual Fix and Provide Temporary Password" task.
4. Enter the temporary password set in the servers in the "Password" filed and click "Retry".

Figure 37. Enter Temporary Password in case of Password Auto Update Failure

Prerequisites for Windows Server Onboarding with Domain Account

1. If the account is a **domain account**, then it must be a member of the local administrators group (due to UAC, User Account Control).
2. Log in to your Windows endpoint as a user with Administrator privileges.
3. Setup winrm.

   Note:

- Always use only **one** type of command line tool throughout the setup since commands work differently for different command line tools
- For newly provisioned Win2012 R2 Std and Win2012 Std endpoints, the first command line that creates winrm (winrm create winrm/config/listener?Address=*+Transport=HTTP) can be omitted. Only run the second line.

If you are using **PowerShell**, run the following commands:

```
winrm create winrm/config/listener?Address=*+Transport=HTTP
winrm set winrm/config/Winrs '@{MaxMemoryPerShellMB="512"}'
```

If you are using **Command Prompt (cmd)**, run the following commands:

```
winrm create winrm/config/listener?Address=*+Transport=HTTP
winrm set winrm/config/Winrs @{MaxMemoryPerShellMB="512"}
```

4. Restart the winrm server by running these 2 commands:

```
net stop winrm
net start winrm
```

5. Reboot the Windows Endpoint if the hotfix upgrade returns with required reboot.

Prerequisites for Windows Server Onboarding with Local Account

1. If the account is a **local account**, then it must be a member of the Administrator group.
   - UAC does not allow local accounts to access to the WinRM service. To access a remote WinRM service in a workgroup, UAC filtering for local accounts must be disabled by creating the following **DWORD registry entry** and setting its value to 1:

     Set the value of this key: `[HKEY_Local_Machine\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] LocalAccountTokenFilterPolicy` to **1**.

   Note: Use "Run" from the start menu and then run the "regedit" to create the registry entry.
2. Log in to your Windows endpoint as a user with Administrator privileges.
3. Setup winrm.

   Note:
   - Always use only **one** type of command line tool throughout the setup since commands work differently for different command line tools
   - For newly provisioned Win2012 R2 Std and Win2012 Std endpoints, the first command line that creates winrm (winrm create winrm/config/listener?Address=*+Transport=HTTP) can be omitted. Only run the second line.

   If you are using **PowerShell**, run the following commands:

   ```
   winrm create winrm/config/listener?Address=*+Transport=HTTP
   winrm set winrm/config/Winrs '@{MaxMemoryPerShellMB="512"}'
   ```

   If you are using **Command Prompt (cmd)**, run the following commands:

   ```
   winrm create winrm/config/listener?Address=*+Transport=HTTP
   winrm set winrm/config/Winrs @{MaxMemoryPerShellMB="512"}
   ```

4. Restart the winrm server by running these 2 commands:

   ```
   net stop winrm
   ```

```
net start winrm
```

5. Reboot the Windows Endpoint if the hotfix upgrade returns with required reboot..

Prerequisite for Onboarding Linux Endpoint

Check whether your endpoint meets the following requirements.

Connectivity Requirements

- The hostname of the endpoint must be resolvable from the Execution Engine Server.
- The port 22/tcp on endpoint must be reachable from the Execution Engine Server.
- The Execution Engine Server must be able to access endpoint by ssh with the "automate" user using public key authentication.
- The endpoint must be able to reach the Execution Engine by HOST IP on port 3333.
- The endpoint must be able to reach CHEF Server by HOST IP on port 443/tcp for SLA environments created by 20 July 2017.
- The endpoint must be able to reach CHEF Server by HOST IP on port 8443/tcp for SLA environments created after 20 July 2017.

  Note: If you are unsure of the creation date of your SLA environment, check with your account's deployment specialist or SLA Operation team.

Disk Space Requirements

- The endpoint must have at least 5 GB available on /opt/IBM/cobalt for CHEF client binaries.
- The /opt/IBM/cobalt folder may be placed as a mount point to a separate file system to contain the space consumed by CHEF

OS Settings Requirements

- The endpoint clock must be synchronized within 15 minutes of the chef server.

OS Version Requirements

- Redhat 6.1 to 7.4
- SUSE 11.x and 12.x
- Ubuntu 14.x and 16.x

Memory Requirements

- The recommended amount of RAM available for CHEF client to run is 512MB.

Software Requirements

- The current wget version, **wget-1.11.4-1.32.1**, which is shipped with SUSE Linux does not support TLS v1.2.

  Your wget version must support TLS v1.2 or else wget command will fail to establish SSL connection with the chef-server.

  You can either manually download a wget version that supports TLS v1.2 or you can use the following command to add TLS v1.2 to wget command.

  ```
  wget --secure-protocol=tlsv1_2 --no-check-certificate https://
  <JumpHost_ip_address>:3333/shared/cobalt-chef-12.12.13-sles11.tar.gz
  ```

Functional ID Requirements

Perform the following prerequisite steps on the Linux endpoint you want to onboard to meet the functional id requirement.

1. Request a local group called **automate** on each server (endpoint).

   Note: Domain ID are not supported for Linux servers.

2. Create one privileged ID named **automate** on each target server endpoint and make it a member of the automate group.

   Note: It is not mandatory to name the user "automate". You can have a different name if you want to. The description is only for standardization purpose. However, the userid must be the same for all endpoints. In this section below, "automate" user is referred to be the exact user id "automate". Please replace "automate" with the correct user id if a different user id is used. **If your account is using a different userid name other than "automate", file a Service Request to SLA Ops Team in the SCCD system to update SLA EE configuration before onboarding any CCI.**

   - The ID must have system administrator authority
   - The ID is the same as login enabled “service/application/functional” (per Account policy), not shared.
   - At the end of the setup, the ID will be non-expiring, with no valid password and will only be accessible using SSH keys.

3. Follow the steps to create **automate** user.
   - Login to **Linux Endpoint Terminal** console as **root** user
   - Create the user by running the following commands based on the operating system of your endpoint.

     For Redhat Endpoint and SUSE Endpoint, run the following command.

     ```
     useradd -m automate
     ```

     For Ubuntu Endpoint, run the following command.

     ```
     useradd -m automate -s /bin/bash
     ```

   - Update the automate user account with non-expiring password option by running this command:

     ```
     chage -I -1 -m 0 -M 99999 -E -1 automate
     ```

   - Switch to the automate user account by running this command:

     ```
     su automate
     ```

   - Create the .ssh directory under the user home directory by running this command:

     ```
     mkdir /home/automate/.ssh
     ```

   - Update the permission of the .ssh directory to 700 by running this command:

     ```
     chmod 700 /home/automate/.ssh
     ```

   - Create the authorized_keys folder under the .ssh directory by running this command:

     ```
     touch /home/automate/.ssh/authorized_keys
     ```

   - Update the permission of the authorized_keys file to 600 by running this command:

     ```
     chmod 600 /home/automate/.ssh/authorized_keys
     ```

   - Place the SLA onboarding public key you received from SLA deployment specialist in the authorized keys file for the “automate” user, **/home/<automate id>/.ssh/authorized_keys**.

Note:

- Some compliance rules require that the ssh public keys deployed to customer servers to be compliant. A compliance key has certain format to follow. See an example server onboarding public key used by SLA below.

```
from="10.120.22.50,10.120.22.53,10.91.118.222",command="~/.ssh/sshd_cmd_logge
r 897:F:*SLAAUT:automation" ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDC9g85rCZvOfrdOLR+dpBRlqrSMr8y6cikgY6MiRoQCJV9f
19mPTo0+W5smQPtD5bz165DgSlm9UOz2GcJ+zAJDUaKKa7SUku/U9F2c0a0Ofz/ByWWEa7wBdoM5H
Bh5IGYPzOBCGEDcPx/8+b9AVgwH08RvjEIQsraAWyRP7S/HFt7yEbpiOxm500vb7i6TIh8zIsZm4O
d11ajDFtwRqE1hnbSatIz9d93VtdSRv6rTqC2bJoBYM8jufL7bf4lzjNtXe5t7ogaYJgsyn03KbsX
2l+mOh/tbiKxyG67mUoEYrV3Qfhi1oeSiEA/LhBW9vWB7TmFIjbWVTawg+v7Fk1D
SLA Onboarding !!897/F/*SLAAUT/IBM/Compliance As Code onboarding!!
```

Figure 38. Sample SSH Key

- As a part of the same requirement, the file **~/.ssh/sshd_cmd_logger** must exist on the endpoint and must be executable. It must create logs in **/var/log/hist/.<target_userid>.sh_history/**
- SLA will add the **"from="** clause and **"command="** clause to the public keys so that they will follow the required format. Default argument to command logger is **'897:F:*SLAAUT:automation'**. Default ssh public key comment is: **'!!897/F/*SLAAUT/IBM/Compliance As Code onboarding!!'**.
- If you do not want to use the default settings, inform SLA Ops team to change the configurations of your account.

v Copy the command logger script 'sshd_cmd_logger' to the endpoint. Perform the following steps.

Note: If you used a custom command logger script, replace the filename in the commands with the filename that you are using.

a. Download the "sshd_cmd_logger" file from here.
b. Copy the downloaded file to **/home/<automate id>/.ssh**.
c. Change the ownership of the file. The file must be owned by the "automate" userid. Run the following command. If you are using a different userid instead of the "automate", replace automate with the userid you are using.

   chown automate:automate /home/automate/.ssh/sshd_cmd_logger

d. Change permission of the 'sshd_cmd_logger' file to 750. Run the following command.

   chmod 750 /home/<automate id>/.ssh/sshd_cmd_logger

v Create a directory **/var/log/hist** with permissions 'drwxrwxrwt' (1777). Run the following commands.

mkdir -p /var/log/hist

chmod 1777 /var/log/hist

v Exit back to root user by running this command:

exit

v Grant the automate user sudo access. Using “visudo” command, add the following entry to /etc/sudoers file

%automate ALL=(ALL) NOPASSWD: ALL

v Once the ssh key has been verified, change the “automate” id to have no useable password by setting 'password=*' in /etc/shadow for the automate user. Go to /etc/shadow and run the following command.

```
echo "automate:*" | chpasswd -e
```

Note: For IBM GTS sudo setting must be applied through globally approved template 141_CMAE_GLB_V1.1.0.txt, unless locally approved template supersedes

Optional Requirements

Note: Performing the following steps will result in the faster onboarding process and the lesser onboarding failure. However, they are not mandatory and not performing them will not deter you from successful endpoint onboarding.
Some installer files that are copied to the endpoints during onboarding are large files. It takes a long time for SLA to copy the installers to the endpoints. This may lead to the onboarding failure especially when there is a network bandwidth limitation in the environment. To optimize the onboarding process, SLA allows you to copy the necessary installers to the endpoints before onboarding. Copying the installers to the endpoint before you start onboarding it will improve the performance of the overall onboarding process. Perform the following steps to copy the installer files to the endpoint you want to onboard.

v For Redhat Server

1. Download the installer from the following links based on the deployment model of your account.

   If your account is using JumpHost, download from the following link.

   - For environments using chef client 12.4.1

     https://<JumpHost_ip_address>:3333/shared/cobalt-chef-12.4.1-rhel6.tar.gz

   - For environments using chef client 12.12.13

     https://<JumpHost_ip_address>:3333/shared/cobalt-chef-12.12.13-rhel6.tar.gz

   If your account is using IPCenter, download from the following link.

   - For environments using chef client 12.4.1

     https://<IPCenter_JumpHost_ip_address>:3333/shared/cobalt-chef-12.4.1-rhel6.tar.gz

   - For environments using chef client 12.12.13

     https://<IPCenter_JumpHost_ip_address>:3333/shared/cobalt-chef-12.12.13-rhel6.tar.gz

   If your account is an on-premise account, download from the following link.

   - For environments using chef client 12.4.1

     https://<your_sla_ee_server_hostname>:3333/shared/cobalt-chef-12.4.1-rhel6.tar.gz

   - For environments using chef client 12.12.13

     https://<your_sla_ee_server_hostname>:3333/shared/cobalt-chef-12.12.13-rhel6.tar.gz

2. Copy the installer, either **'cobalt-chef-12.4.1-rhel6.tar.gz'** or **'cobalt-chef-12.12.13-rhel6.tar.gz'** depending on the chef client version your environment is using, to the directory **/tmp/chef/**.

   Note: You must be able to use the "automate" user to copy file into the /tmp folder using 'scp' command.

3. If this directory does not exist in endpoint, create the directory using the following command.

   mkdir -p /tmp/chef/

4. Change ownership of the chef directory in tmp folder using the following command.

   chown -R <automate id> /tmp/chef

v For Suse Server

1. Download the installer from the following links based on the deployment model of your account.

   If your account is using JumpHost, download from the following link.

   - For environments using chef client 12.4.1

     https://<JumpHost_ip_address>:3333/shared/cobalt-chef-12.4.1-sles11.tar.gz

   - For environments using chef client 12.12.13

     https://<JumpHost_ip_address>:3333/shared/cobalt-chef-12.12.13-sles11.tar.gz

   If your account is using IPCenter, download from the following link.

   - For environments using chef client 12.4.1

     https://<IPCenter_JumpHost_ip_address>:3333/shared/cobalt-chef-12.4.1-sles11.tar.gz

   - For environments using chef client 12.12.13

     https://<IPCenter_JumpHost_ip_address>:3333/shared/cobalt-chef-12.12.13-sles11.tar.gz

   If your account is an on-premise account, download from the following link.

   - For environments using chef client 12.4.1

     https://<your_sla_ee_server_hostname>:3333/shared/cobalt-chef-12.4.1-sles11.tar.gz

   - For environments using chef client 12.12.13

     https://<your_sla_ee_server_hostname>:3333/shared/cobalt-chef-12.12.13-sles11.tar.gz

2. Copy the installer, either **'cobalt-chef-12.4.1-sles11.tar.gz'** or **'cobalt-chef-12.12.13-sles11.tar.gz'** depending on the chef client version your environment is using, to the directory **/tmp/chef/**.

   Note: You must be able to use the "automate" user to copy file into the /tmp folder using 'scp' command.

3. If this directory does not exist in endpoint, create the directory using the following command.

   mkdir -p /tmp/chef/

4. Change ownership of the chef directory in tmp folder using the following command.

   chown -R <automate id> /tmp/chef

v For Suse s390x Server

1. Download the installer from the following links based on the deployment model of your account.

   If your account is using JumpHost, download from the following link.

   - For environments using chef client 12.4.1

     https://<JumpHost_ip_address>:3333/shared/cobalt-chef-12.4.1-sles11-s390x.tar.gz

   - For environments using chef client 12.12.13

https://<JumpHost_ip_address>:3333/shared/cobalt-chef-12.12.13-sles11-s390x.tar.gz

If your account is using IPCenter, download from the following link.

- For environments using chef client 12.4.1

  https://<IPCenter_JumpHost_ip_address>:3333/shared/cobalt-chef-12.4.1-sles11-s390x.tar.gz

- For environments using chef client 12.12.13

  https://<IPCenter_JumpHost_ip_address>:3333/shared/cobalt-chef-12.12.13-sles11-s390x.tar.gz

If your account is an on-premise account, download from the following link.

- For environments using chef client 12.4.1

  https://<your_sla_ee_server_hostname>:3333/shared/cobalt-chef-12.4.1-sles11-s390x.tar.gz

- For environments using chef client 12.12.13

  https://<your_sla_ee_server_hostname>:3333/shared/cobalt-chef-12.12.13-sles11-s390x.tar.gz

2. Copy the installer, either **'cobalt-chef-12.4.1-sles11-s390x.tar.gz'** or **'cobalt-chef-12.12.13-sles11-s390x.tar.gz'** depending on the chef client version your environment is using, to the directory **/tmp/chef/**.

   Note: You must be able to use the "automate" user to copy file into the /tmp folder using 'scp' command.

3. If this directory does not exist in endpoint, create the directory using the following command.

   mkdir -p /tmp/chef/

4. Change ownership of the chef directory in tmp folder using the following command.

   chown -R <automate id> /tmp/chef

Prerequisite for Onboarding AIX Endpoint

Check whether your endpoint meets the following requirements.

Connectivity Requirements

- The hostname of the endpoint must be resolvable from the Execution Engine Server.
- The port 22/tcp on endpoint must be reachable from the Execution Engine Server.
- The Execution Engine Server must be able to access endpoint by ssh with the "automate" user using public key authentication.
- The endpoint must be able to reach the Execution Engine by HOST IP on port 3333.
- The endpoint must be able to reach CHEF Server by HOST IP on port 443/tcp for SLA environments created by 20 July 2017.
- The endpoint must be able to reach CHEF Server by HOST IP on port 8443/tcp for SLA environments created after 20 July 2017.

  Note: If you are unsure of the creation date of your SLA environment, check with your account's deployment specialist or SLA Operation team.

- The Execution Engine Server must be able to reach the port 22/tcp on the endpoint's HMCs if you are using the virtualization management feature.

Disk Space Requirements

v The endpoint must have at least 5 GB available on /opt/IBM/cobalt for CHEF client binaries. This could be a separately mounted file system.

OS Settings Requirements

v The endpoint clock must be synchronized within 15 minutes of the chef server.

OS Version Requirements

v AIX Version 6.1 TL 9 (or higher)

v AIX Version 7.1 TL 3 (or higher)

v AIX Version 7.2

Memory Requirements

v The recommended amount of RAM available for CHEF client to run is 512MB.

Software Requirements

v The endpoint must have the library zlib v1.2.2.1 or higher available to execute Ruby.

Sudo Version Requirements

v The endpoint must have sudo version 1.7.0 and above.

v The server validation will fail if the endpoint is using the version lower than 1.7.0

Functional ID Requirements

Perform the following prerequisite steps on the AIX endpoint you want to onboard to meet the functional id requirement.

1. Request a local group called **automate** on each server (endpoint).

   Note: Domain ID are not supported for AIX servers.

2. Create one privileged ID named **automate** on each target server endpoint and make it a member of the automate group.

   Note: It is not mandatory to name the user "automate". You can have a different name if you want to. The description is only for standardization purpose. However, the userid must be the same for all endpoints. In this section below, "automate" user is referred to be the exact user id "automate". Please replace "automate" with the correct user id if a different user id is used. **If your account is using a different userid name other than "automate", file a Service Request to SLA Ops Team in the SCCD system to update SLA EE configuration before onboarding any CCI.**

   v The ID must have system administrator authority

   v The ID is the same as login enabled “service/application/functional” (per Account policy), not shared.

   v At the end of the setup, the ID will be non-expiring, with no valid password and will only be accessible using SSH keys.

3. Log in to your AIX endpoint as a user with Administrator/root privilege.

   v Create the "automate" group by running this command:

   ```
   if [ "`lsgroup -a automate`" != "automate" ]; then mkgroup "automate";
   fi
   ```

- Create the "automate" user by running this command.

  ```
  if [ "`lsuser -a automate`" != "automate" ]; then useradd -m -g
  "automate" "automate"; fi
  ```

- Update the automate user account with non-expiring password option by running this command:

  ```
  chuser maxage=0 automate
  ```

- Create the .ssh directory by running this command:

  ```
  mkdir -p /home/automate/.ssh
  ```

- Change the owner of the .ssh directory to "automate" user:

  ```
  chown automate:automate /home/automate/.ssh
  ```

- Update the permission of the .ssh directory to 700 by running this command:

  ```
  chmod 700 /home/automate/.ssh
  ```

- Change the owner of the .ssh/authorized_keys directory to "automate" user:

  ```
  chown automate:automate /home/automate/.ssh/authorized_keys
  ```

- Update the permission of the .ssh/authorized_keys directory to 600 by running this command:

  ```
  chmod 0600 /home/automate/.ssh/authorized_keys
  ```

- Place the SLA onboarding public key you received from SLA deployment specialist in the authorized keys file ".ssh/authorized_keys" for the "automate" user.

  ```
  echo '<SLA_onboarding_public_key>' >> /home/automate/.ssh/
  authorized_keys
  ```

  Note:

  - Some compliance rules require that the ssh public keys deployed to customer servers to be compliant. A compliance key has certain format to follow. See an example server onboarding public key used by SLA below.

```
from="10.120.22.50,10.120.22.53,10.91.118.222",command="~/.ssh/sshd_cmd_logge
r 897:F:*SLAAUT:automation" ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDC9g85rCZvOfrdOLR+dpBRlqrSMr8y6cikgY6MiRoQCJV9f
19mPTo0+W5smQPtD5bz165DgSlm9UOz2GcJ+zAJDUaKKa7SUku/U9F2c0a0Ofz/ByWWEa7wBdoM5H
Bh5IGYPzOBCGEDcPx/8+b9AVgwH08RvjEIQsraAWyRP7S/HFt7yEbpiOxm500vb7i6TIh8zIsZm4O
d11ajDFtwRqE1hnbSatIz9d93VtdSRv6rTqC2bJoBYM8jufL7bf4lzjNtXe5t7ogaYJgsyn03KbsX
2l+mOh/tbiKxyG67mUoEYrV3Qfhi1oeSiEA/LhBW9vWB7TmFIjbWVTawg+v7Fk1D
SLA_Onboarding !!897/F/*SLAAUT/IBM/Compliance As Code onboarding!!
```

Figure 39. Sample SSH Key

  - As a part of the same requirement, the file **~/.ssh/sshd_cmd_logger** must exist on the endpoint and must be executable. It must create logs in **/var/log/hist/.<target_userid>.sh_history/**
  - SLA will add the **"from="** clause and **"command="** clause to the public keys so that they will follow the required format. Default argument to command logger is **'897:F:*SLAAUT:automation'**. Default ssh public key comment is: **'!!897/F/*SLAAUT/IBM/Compliance As Code onboarding!!'**.
  - If you do not want to use the default settings, inform SLA Ops team to change the configurations of your account.

- Copy the command logger script 'sshd_cmd_logger' to the endpoint. Perform the following steps.

Note: If you used a custom command logger script, replace the filename in the commands with the filename that you are using.

a. Download the "sshd_cmd_logger" file from here.

b. Copy the downloaded file to **/home/<automate id>/.ssh**.

c. Change the ownership of the file. The file must be owned by the "automate" userid. Run the following command. If you are using a different userid instead of the "automate", replace automate with the userid you are using.

```
chown automate:automate /home/automate/.ssh/sshd_cmd_logger
```

d. Change permission of the 'sshd_cmd_logger' file to 750. Run the following command.

```
chmod 750 /home/<automate id>/.ssh/sshd_cmd_logger
```

- Create a directory **/var/log/hist** with permissions 'drwxrwxrwt' (1777). Run the following commands.

```
mkdir -p /var/log/hist
chmod 1777 /var/log/hist
```

- Grant the automate user sudo access. Using "visudo" command, add the following entry to /etc/sudoers file

```
echo "automate ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers
```

- Once the ssh key has been verified, change the "automate" id to have no useable password by setting 'password=*' in /etc/security/passwd for automate user. Go to /etc/security/passwd and run the following command.

```
echo "automate:*" | chpasswd -c -e
```

- Increase shell limit for "max resident set size":

```
chsec -f /etc/security/limits -s root -a "rss=-1"
```

- Increase shell limit for "Maximum number of processes available to a single use" :

```
chsec -f /etc/security/limits -s root -a "nofiles=50000"
```

Optional Requirements

Note: Performing the following steps will result in the faster onboarding process and the lesser onboarding failure. However, they are not mandatory and not performing them will not deter you from successful endpoint onboarding. Some installer files that are copied to the endpoints during onboarding are large files. It takes a long time for SLA to copy the installers to the endpoints. This may lead to the onboarding failure especially when there is a network bandwidth limitation in the environment. To optimize the onboarding process, SLA allows you to copy the necessary installers to the endpoints before onboarding. Copying the installers to the endpoint before you start onboarding it will improve the performance of the overall onboarding process. Perform the following steps to copy the installer files to the endpoint you want to onboard.

1. Download the installer from the following links based on the deployment model of your account.

   If your account is using JumpHost, download from the following link.

   - For environments using chef client 12.4.1

     ```
     https://<JumpHost_ip_address>:3333/shared/cobalt-chef-12.4.1-aix71.tar
     ```

   - For environments using chef client 12.12.13

     ```
     https://<JumpHost_ip_address>:3333/shared/cobalt-chef-12.12.13-
     aix71.tar
     ```

If your account is using IPCenter, download from the following link.

v For environments using chef client 12.4.1

```
https://<IPCenter_JumpHost_ip_address>:3333/shared/cobalt-chef-12.4.1-aix71.tar
```

v For environments using chef client 12.12.13

```
https://<IPCenter_JumpHost_ip_address>:3333/shared/cobalt-chef-12.12.13-aix71.tar
```

If your account is an on-premise account, download from the following link.

v For environments using chef client 12.4.1

```
https://<your_sla_ee_server_hostname>:3333/shared/cobalt-chef-12.4.1-aix71.tar
```

v For environments using chef client 12.12.13

```
https://<your_sla_ee_server_hostname>:3333/shared/cobalt-chef-12.12.13-aix71.tar
```

2. Copy the installer, either **'cobalt-chef-12.4.1-aix71.tar'** or **'cobalt-chef-12.12.13-aix71.tar'** depending on the chef client version your environment is using, to the directory **/tmp/chef/**.

   Note: You must be able to use the "automate" user to copy file into the /tmp folder using 'scp' command.

3. If this directory does not exist in endpoint, create the directory using the following command.

   ```
   mkdir -p /tmp/chef/
   ```

4. Change ownership of the chef directory in tmp folder using the following command.

   ```
   chown -R <automate id> /tmp/chef
   ```

Server Group Management

In a standard installation of CC, access to and from the customer network segment is protected by a SAS gateway (SASg). The following scenarios are currently supported by the system:

v No SASg

v Single SASg

v N SASg - any number of gateways

v Mixed environment in which some groups of servers are behind SASgs and others are not

Note: In all cases, a server can only be behind a single SASg at a time or behind none.

The way in which servers are associated to a SASg is by the **"Server Group"** that they are associated to during onboarding. Each Server Group has a Gateway Address that can be specified. This address is the IP address of the SASg and is how the customer endpoints can communicate back into the IBM Management Segment. Server Groups also are bound to a 'credential type'. Because Unix / Linux use a different protocol for communications and authentication, they cannot be defined in the same Server Group as Windows servers. However, any number of server groups can be defined to share the same Gateway Address.

Server groups can be managed using **"Server Group Management"** function. By default, there are two server groups defined in the system:

- all_ssh_servers, and
- all_winrm_servers

The default server groups cannot be deleted or renamed. Unix / Linux servers use the "all_ssh_servers" group by default and Windows servers will use the "all_winrm_servers" group. The gateway address associated to these default groups will be the **"Virtual IP 1"** address of your JumpHost.

If you have endpoints in multiple networks, you will need multiple SAS gateways so that SLA can manage servers in those disconnected environments. You must setup additional server groups before onboarding servers using "Server Group Management" function.

If you have servers behind an additional SASg, you should define at least one additional "Server Group" per "Credential Type", that is, one for Windows and one for non-Windows. Each group should specify the appropriate gateway address. Once defined, the server groups will be available for selection during "Sever Onboarding". It is important to select the appropriate "Server Group" during onboarding. If the wrong group is selected during onboarding, the server will fail the validation and you will not be able to onboard the sever. If this happens, you can add the server into a different onboarding batch and select the correct "Server Group".

Important:

- Starting from Release 17.5, FIPS mode is supported. To start managing the servers with FIPS mode turned on, you must create one or more new "Server Groups" for servers with FIPS turned on.
- The existing server groups that are created prior to FIPS support are **not** editable to support endpoints with FIPS.
- If you are enabling the FIPS mode in the existing managed servers, you must move them to the new server groups created for FIPS enabled endpoints. There are certain criteria to follow when creating new server groups for existing managed servers.
  - Credential Type and Gateway IP address must be the same in both new and old group for each server.
  - For Unix servers, SSH key in the server will be changed automatically when you move the servers from one server group to another.
  - For Windows servers, every server group has its own password for the "automate" id. When you are moving servers from one server group to another, you can follow either one of the two following scenarios.
    1. You can set the password of the new server group to be the same with the password of the old server group, which is the password of the "automate" id of the servers that are under the said server group. To set the password of the new server group to the password of the "automate" id of the servers, you must find out the current password of the "automate" id. Please contact either your deployment specialist or the SLA Operation team.
    2. You can set any password for the new server group. However, you must manually change the password of the "automate" id in all the endpoints that are going to be under the new server group before you edit the server groups of each server.

v After creating new server group(s) for FIPS enabled endpoints, you can change the existing servers to be under the new server group via the "Server Details" tab under the "My Servers" page in the "CC Enhanced UI".
  - Only the users who are under the system admin group can change the server details, including the server group, of a server.
  - If the change of the server group using "Server Details" page is unsuccessful, you can offboard the server and re-onboard it under the new FIPS enabled server group.

v There is currently no way to delete a server group via the user interface.

1. Go to https://<your_sla_environment>. Click on either the "Continuous Compliance (CC)" link. Log in using your LDAP userid or IBMid.

Figure 40. BPM User Interface

2. Click on ' **Organized tabs**' (usually a plus sign in a circle) button from the menu bar on top of the page.

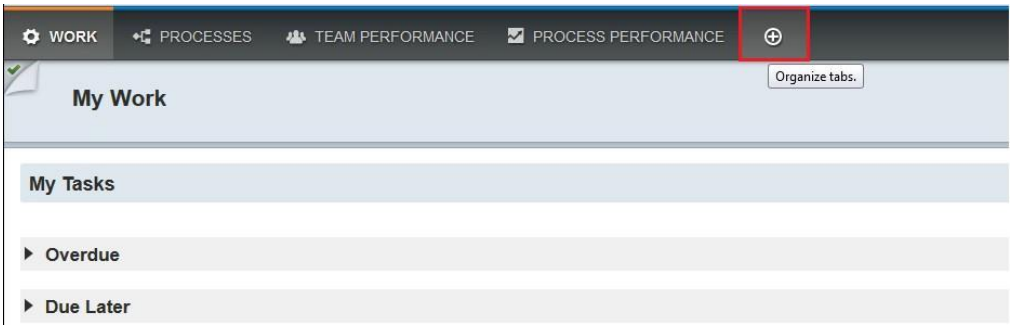


Figure 41. Organize tabs

3. Under '**Hidden tabs**', you will see **Server Group Management** options.

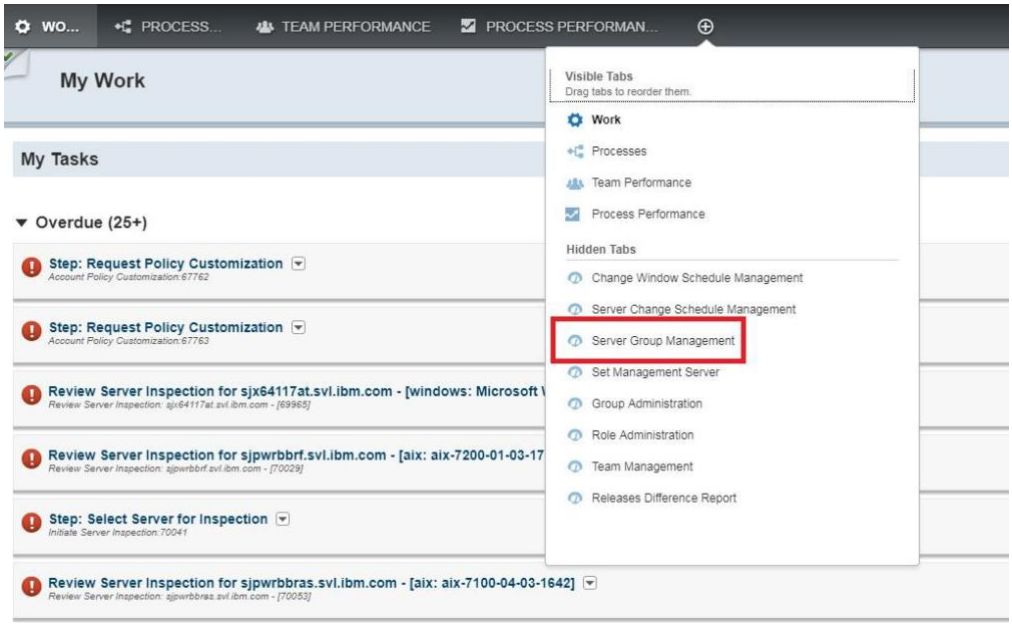


Figure 42. Server Group Management under Hidden Tabs

4. Drag the option and drop them under **Visible Tabs**.

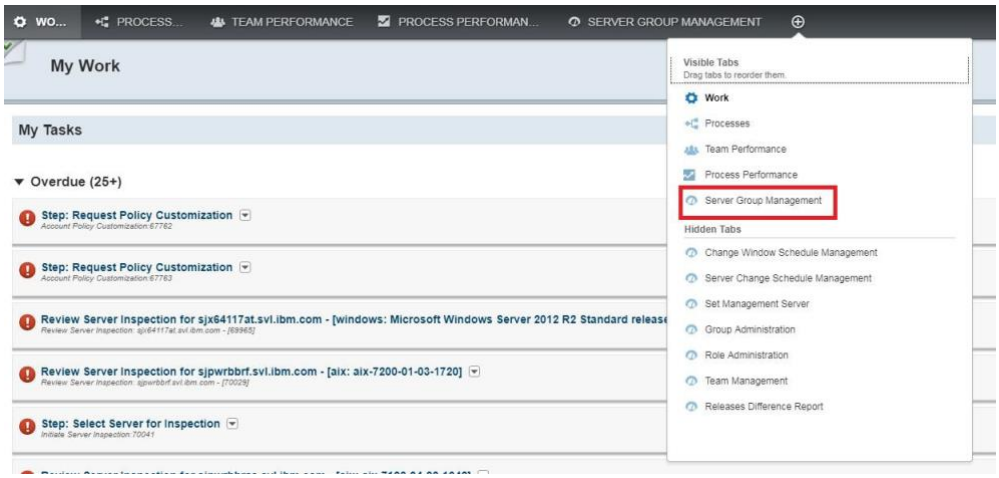


Figure 43. Server Group Management under Visible Tabs

5. Click on the "Server Group Management" tab. There are two default managed server groups provided by the system. The group "all_winrm_servers" is for Windows systems. The "all_ssh_servers" group is for Linux and AIX systems that are using ssh credential type.

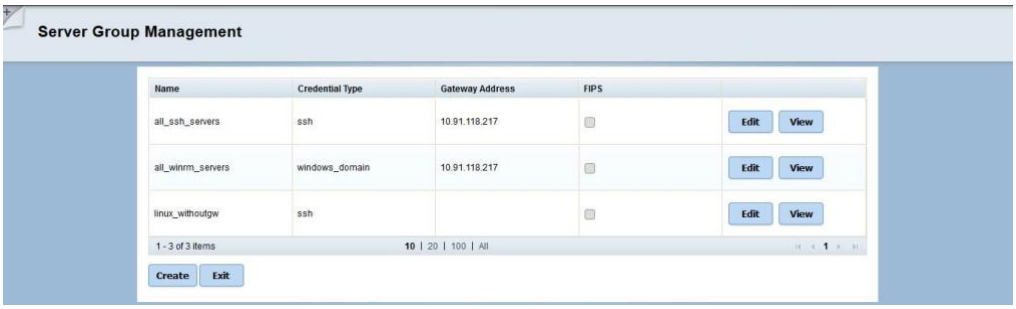


Figure 44. Server Group Management

6. **To create a new managed server group**, click "Create".

Figure 45. Click Create to Create a New Server Group

7. You will be redirected to the page where you need to fill in the detailed information for the server group. There are three credential types;

   v ssh

   v windows_local, and

   v windows_domain.

   The credential type specified on the Managed Server Group will be used to control which types of servers can be assigned to the group. For example, Windows servers can only be associated to Managed Server Groups with a credential type of 'windows_local' or 'windows_domain' and *nix servers can only be associated to servers with a credential type of 'ssh'. Based on the credential type of the server group you are creating, the information required is different.

   a. For "ssh" credential type, choose "ssh" from "Credential Type" drop-down list and fill in the following information.

      v Group Name: A specific group name.

      v Gateway Address: The inbound address to be used by the endpoint when talking to SLA system, previously known as "JumpHost Address".

        Important: Use the **Virtual IP 1** address of your JumpHost as the gateway address.

      v FIPS: Turn on or off the FIPS support of the server group by checking or unchecking the FIPS check-box.

      v Server Name Resolution: Support DNS Settings per server group level.

        For "Server Name Resolution" type, choose any of the type from the drop-down. The options available in the drop-down are "Account Level

Settings", "No DNS", "Use DNS" and "DNS and No DNS". If you select "Use DNS", or "DNS and No DNS", "DNS Servers" field appears. Enter the DNS Server details.

- Click "Save" once the required selection is done.

Figure 46. Creating new Managed Server Group for ssh Credential Type

b. For "windows_local" credential type, choose "windows_local" from "Credential Type" drop-down list and fill in the following information.

- Group Name
- Gateway Address: the inbound address to be used by the endpoint when talking to SLA system, previously known as "JumpHost Address"

  Important: Use the **Virtual IP 1** address of your JumpHost as the gateway address.
- Login user: by default, it is the "automate" user
- Password
- FIPS: Turn on or off the FIPS support of the server group by checking or unchecking the FIPS check-box.
- Server Name Resolution: Support DNS Settings per server group level.

  For "Server Name Resolution" type, choose any of the type from the drop-down. The options available in drop-down are "Account Level Settings", "No DNS", "Use DNS" and "DNS and No DNS". If you select "Use DNS", or "DNS and No DNS", "DNS Servers" field appears. Enter the DNS Server details.
- Click "Save" once the required selection is done.

Figure 47. Creating new Managed Server Group for windows_local Credential Type

c. For "windows_domain" credential type, choose "windows_domain" from "Credential Type" drop-down list and fill in the following information.

- Group Name
- Gateway Address: the inbound address to be used by the endpoint when talking to SLA system, previously known as "JumpHost Address"

  Important: Use the **Virtual IP 1** address of your JumpHost as the gateway address.
- Login user: by default, it is the "automate" user
- Password
- Domain name where the user account resides. This is the domain short name, not the FQDN.
- FIPS: Turn on or off the FIPS support of the server group by checking or unchecking the FIPS check-box.
- Server Name Resolution: Support DNS Settings per server group level.

  For "Server Name Resolution" type, choose any of the type from the drop-down. The options available in drop-down are "Account Level Settings", "No DNS", "Use DNS" and "DNS and No DNS". If you select "Use DNS", or "DNS and No DNS", "DNS Servers" field appears. Enter the DNS Server details.
- Click "Save" once the required selection is done.

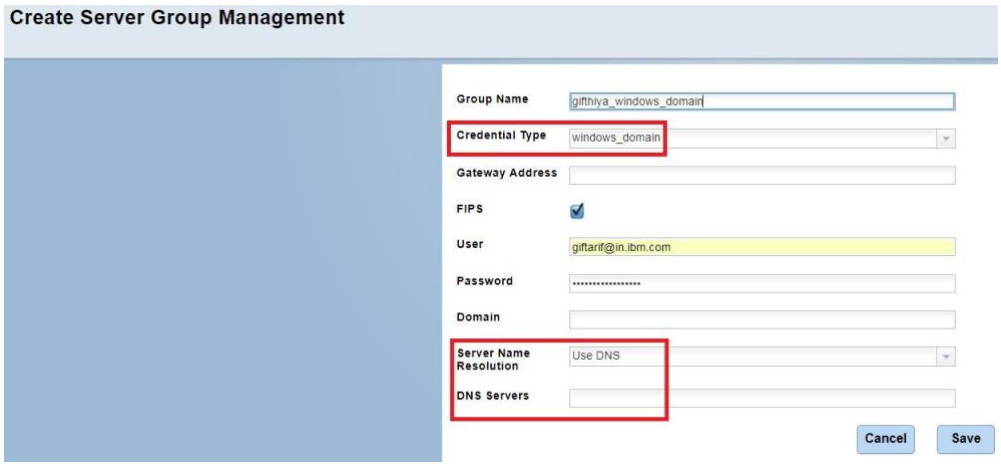


Figure 48. Creating new Managed Server Group for windows_domain Credential Type

8. Once you click the "Save" button, you should see the new managed server group you have created in the server group table.

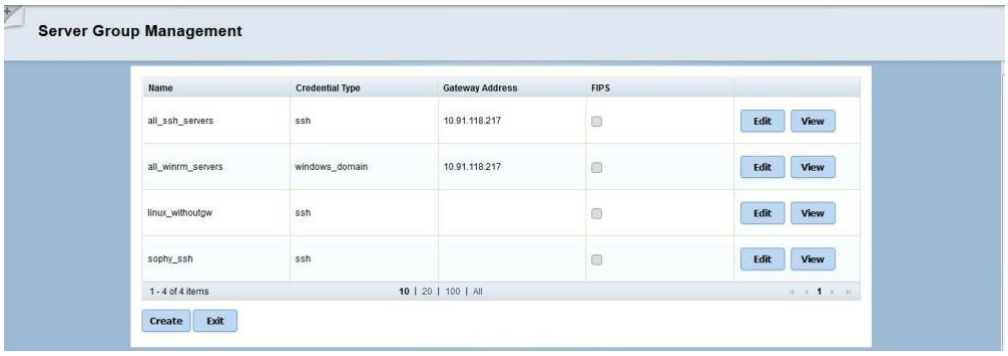


Figure 49. New Managed Server Group Added to the Table

9. **To update the password for the "automate" id of your Windows endpoints**, click the "Edit" button corresponded to the server group that your endpoint is using.

   Note: Server Group Name, Credential Type, Gateway Address and FIPS mode are not updatable via UI after the Server Group is initially created. Only the password for the "automate" user is editable.

Figure 50. Click the "Edit" Button to Update the Password for "automate" id

10. Enter the password you have set for the "automate" id in your endpoint and click the "Save" button.

    Important: Changing the password of a server group in the "Server Group Management" only changes the password stored by CC. It does not sync the new password to the servers under the server group. You must make sure password of all the servers under the same server group are updated to the new value by making necessary manual password updates in each endpoint.

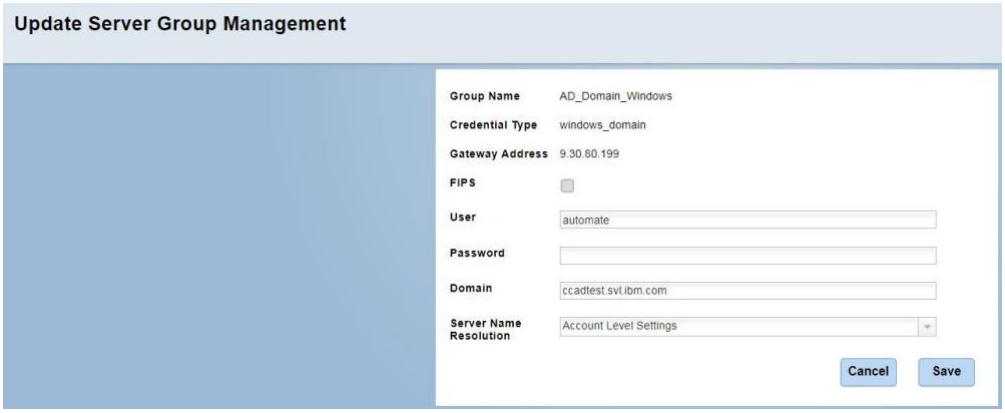


Figure 51. Enter the Password for "automate" id and Click Save

Server Onboarding Steps

CC provide two ways to manage hostname and IP address. By default, your SLA environment is configured to use a DNS server. If your SLA environment is configured NOT to use a DNS server upon your request, it will use custom hostname resolver file to manage hostname and IP address.

If your SLA environment uses a DNS server, you need to enter only the server FQDN (the hostname) of the server you are onboarding. The DNS server will resolve the hostname and get the IP address of server you entered based on the hostname.

If your SLA environment does not have a DNS server, you need to enter both the server FQDN (the hostname) and the IP address of the server you are onboarding. SLA will store the hostname / IP address pair in a custom file for future reference.

1. When the prerequisites are fulfilled, you can create and submit a server onboarding request. Go to https://<your_sla_environment>. Click on either the "Continuous Compliance (CC)" link. Log in using your LDAP userid or IBMid.
2. Click on the **Server Onboarding** function on the right side of the page.

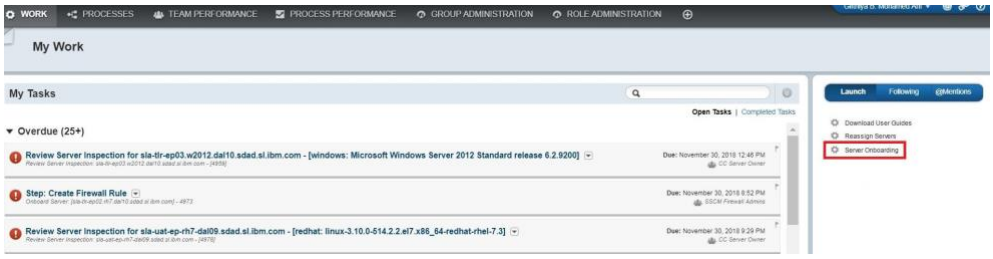


Figure 52. Server Onboarding

3. Once you click on **Server Onboarding** option, the system redirects you to the server onboarding page.

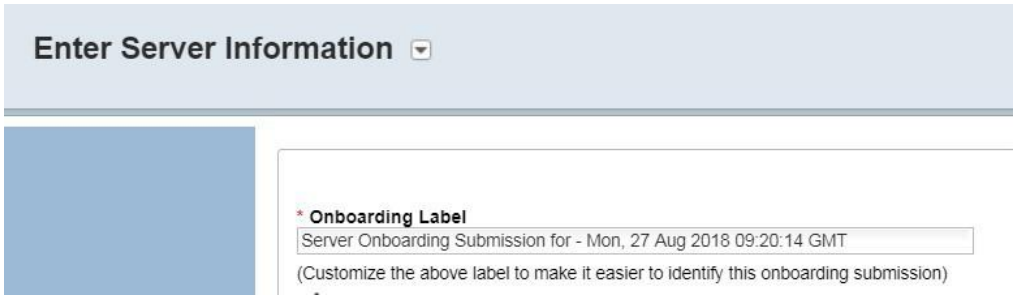


Figure 53. Enter Server Info

Note: If messaging services is enabled, you will see the below page.

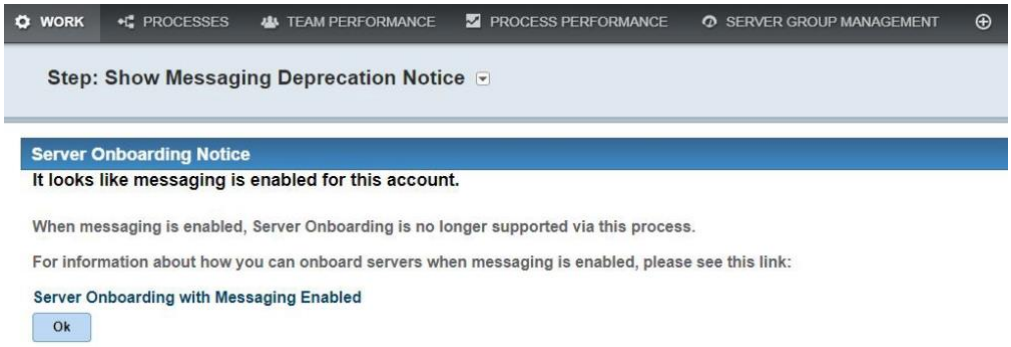


Figure 54. Enter Server Info

4. The “Onboarding Label” field displays the server onboarding information which includes a description with day and time of submission. This field is customizable for the user to easily identify the onboarding submission.
5. The "No Change Window" check-box decides whether the onboarding of the current server or batch of servers will happen immediately or follow a change window. If you check the "No Change Window" check-box, the onboarding of the current batch of servers will not follow a change window, and thus, they will be onboarded immediately.
6. Otherwise, uncheck the "No Change Window" check box and select a change window under the "Change Window" drop-down list. The list of change windows comes from the default change window associated with the account. If you want to associate the current onboarding sever with a different

non-default change window, you can do so using the "Server Change Schedule Management" dashboard after the onboarding.

7. If you wish to import the server information from file instead of manually entering the server information, select "Import from file" option and see “Server Bulk Load” on page 80
8. Otherwise, enter the server information below. The following images are the screen example of "Enter Server Info" page for SLA environments that are using DNS servers and No DNS servers.
9. Enter the information of the server you want to onboard. The mandatory fields are denoted with a red asterisk (*)
   - Server FQDN: The full hostname of the server you want to onboard (for example, cc-test7-endpt1-dal.sdad.sl.dst.ibm.com)
   - Select Platform: The server operating system/platform (e.g., red hat, windows, AIX)
   - Select Server Group: If you have endpoints in multiple networks, you may need multiple SAS gateways so that SLA can manage servers in those disconnected environments. Servers are grouped based on gateways using "Server Group Management" function. Select the server group to define the gateway the server you want to onboard will be using.

     Note: There are two default managed server groups provided by the system. The group "all_winrm_servers" is for Windows systems. The "all_ssh_servers" group is for Linux and AIX systems that are using ssh credential type.

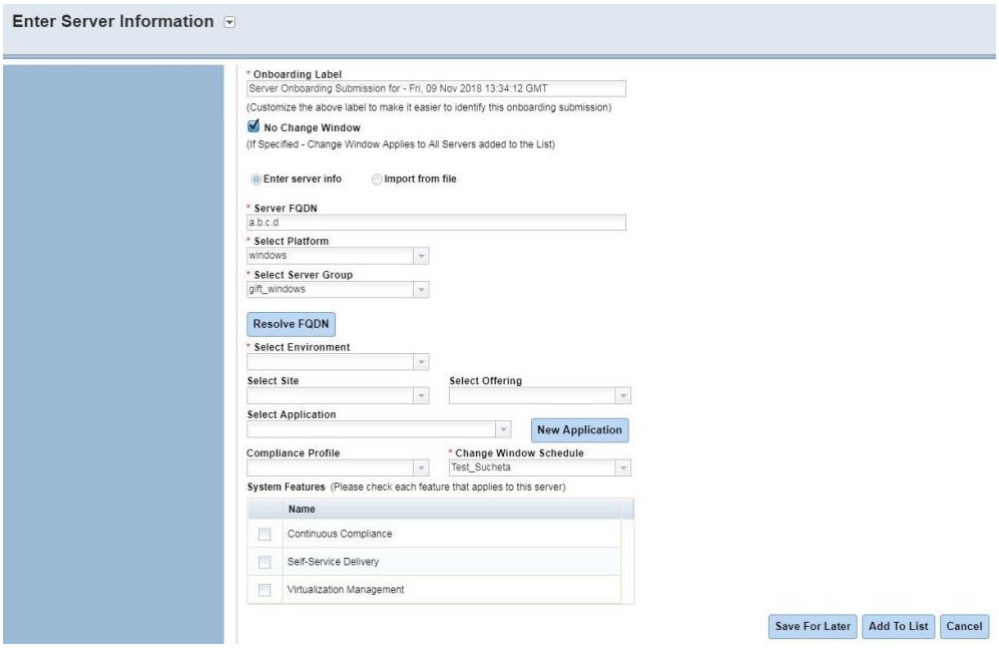


Figure 55. Enter Server Info Screen for SLA Environments Using DNS Server

10. When you select No DNS server group from "Select Server Group" drop-down and click on "Resolve FQDN", the below message appears requesting to enter the IP address. IP address is only for SLA Environments that are not using DNS server.

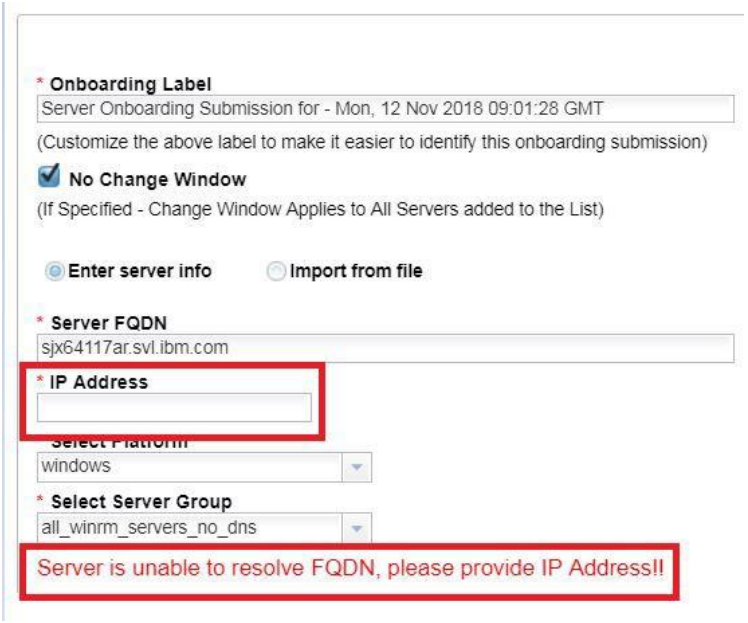


Figure 56. Enter Server Info Screen for SLA Environments that are NOT Using DNS Server

11. Enter the IP address of the server you want to onboard and enter the other fields to proceed with the server onboarding.
12. If server is able to resolve, IP Address appears in read only mode.

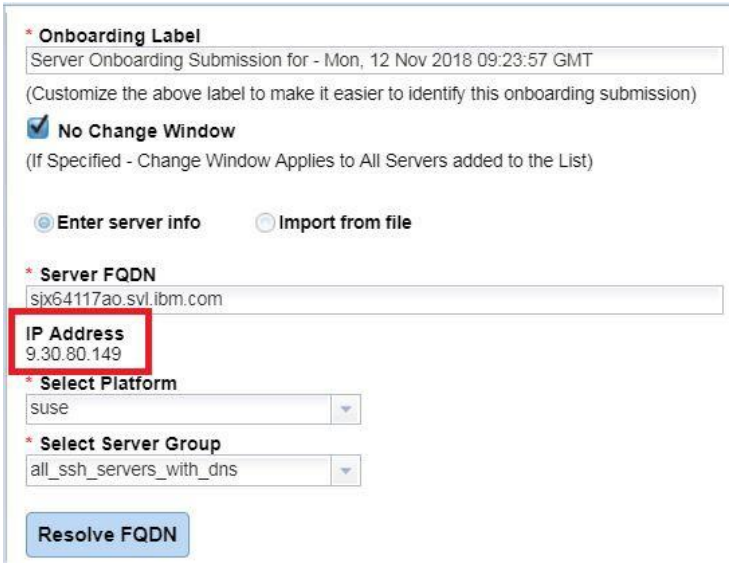


Figure 57. IP Address in read only mode for NO DNS Server Group

13. When you select 'DNS and No DNS' server group from "Select Server Group" drop-down and click on "Resolve FQDN", IP Address appears in read only mode if the server is able to resolve.

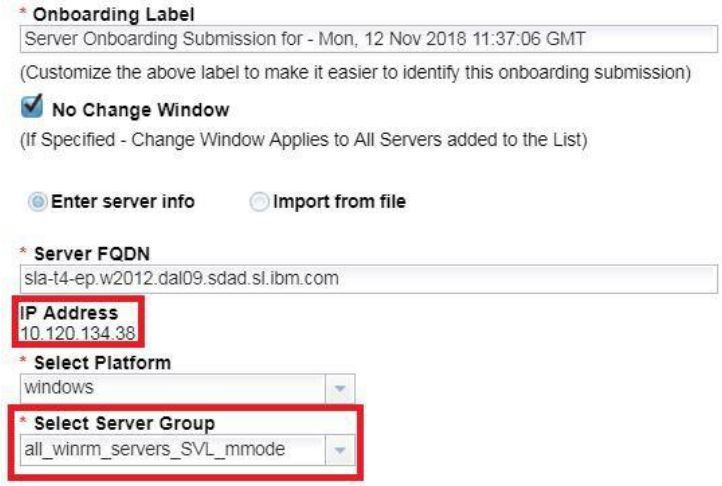


Figure 58. IP Address in read only mode for DNS and NO DNS Server Group

14. If the server is not able to resolve, the below error is displayed and an IP address field appears in editable mode. Enter the IP address and the other fields to proceed the server onboarding.

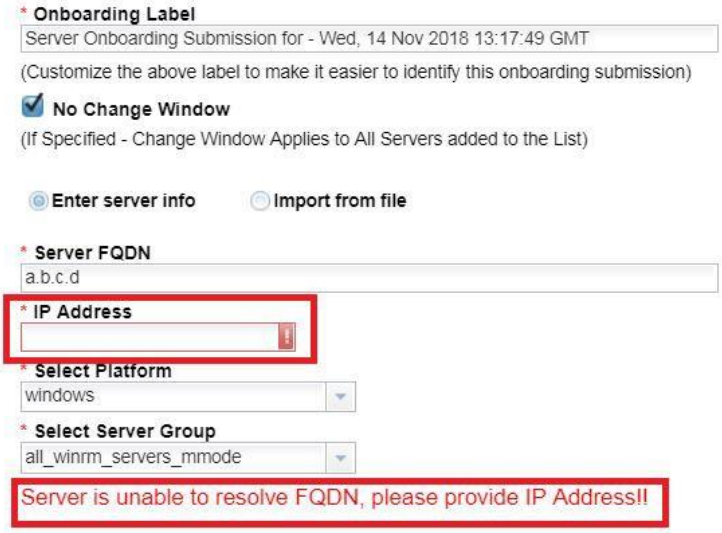


Figure 59. IP Address in editable mode for DNS and NO DNS Server Group

15. When you select DNS server group from "Select Server Group" drop-down and click on "Resolve FQDN", the below message appears if the provided inputs are incorrect.

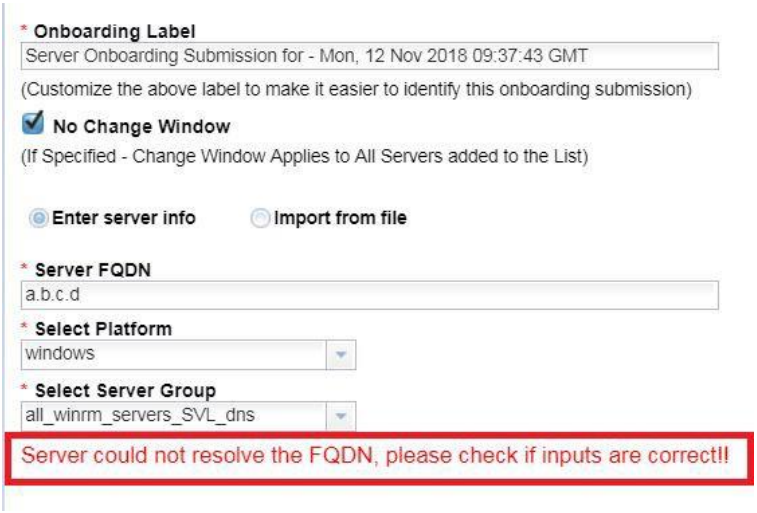


Figure 60. Error Message to Enter Correct Inputs

16. Enter the information of the server you want to onboard. The mandatory fields are denoted with a red asterisk (*)
    - v Select Environment: The default compliance environment that has been reviewed and customized in the Environments
    - v Select Site (optional): Site is equivalent to a Data Center.

      Note: Site allows you to associate a server with a data center and then use that to create roles in the system that only allows certain people to manage servers at a certain data center.
    - v Select Offering (optional): Offering is intended to be used for some internal business sub-division as a way for an account to further segregate responsibility of users.

      Note: Similar to "Site", "Offering" allows you to use offerings in role definition to limit authority.
    - v Select Application (optional): Application or middleware installed on the server. If you cannot find the application your server is using in the **Select Application** drop-down list, you can create new application by clicking **New Application**.

      Note: Middleware discovery is disabled by default to save onboarding and change request execution time. If you want to enable a certain middleware discovery, inform SLA Ops Team to schedule a change window and configure it.
    - v Compliance Profile (optional): If you are using "Continuous Compliance" system feature, you must select the compliance profile. The **cc_policy_enforcer** compliance profile should specified for each managed server being onboarded. This is done by clicking on the down arrow next to the Compliance Profile field and choosing the cc_policy_enforcer profile.

      Note: Associating the managed server to an environment and a compliance profile enables the Account Security Focal to control the correct compliance policies that will be run against a given managed server or set of managed servers. This will make the process of customizing the compliance policies that are applicable across a large number of servers more efficient.

- Change Window Schedule: A Change Window is a period during which changes can be made to managed servers in the environment. Select the change window to be associated with the servers that are being onboarded. If you want to change the change window of a managed server to a different change window after the server is successfully onboarded, you can do so using the "Server Change Schedule Management". See "Server Change Schedule Management" on page 36 for more details.
- System Features: the system feature(s) that applies to this server. Select all the features that apply.
- Click **Save For Later** if you want to complete the information and submit the request later.
- Click **Add To List** to add the server to the "Server List" table. This function allows you to submit an onboarding request that contains more than one server.
- Click **Cancel** to cancel the task.

Figure 61. Add Servers to the List

17. Once you have added the server to the list, the server information will appear under "Server List" table.
18. You will be able to see an additional button called **Validate**. You must pass the validation before you can submit the servers for onboarding. The validation step will check whether all the prerequisites for onboarding have been met. Go to "Prerequisite Validation" on page 84 and perform the steps listed there.

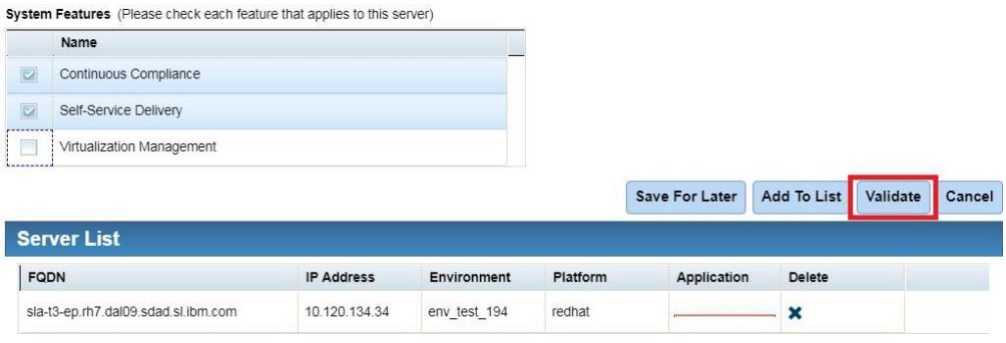


Figure 62. The Server is Added to the Server List and Validate Button Appear

19. If there is any issue with the connectivity between the chef-server and the endpoint you are trying to onboard, you can manually test the connection and grant connection access to the endpoint. See “Grant Connection Access to Endpoint” on page 86.
20. If you have selected **"Continuous Compliance"** feature during onboarding, a compliance inspection (whyrun) will be run on the servers when they are successfully onboarded. This inspection will check the server against the policies under the selected environment and profile. Once the inspection is complete, you will see a task called "Review Server Inspection for <your_selected_endpoint_hostname>" in your workspace. This task allows you to review the inspection results of each of the policies that were enforced. See “Review Server Inspection” on page 87 for more details.
21. On successful submission of the server, check the server log in “My Task” page from the Continuous Compliance portal.

    Note: If the server validation fails, user must check the entered server details and try again to onboard.

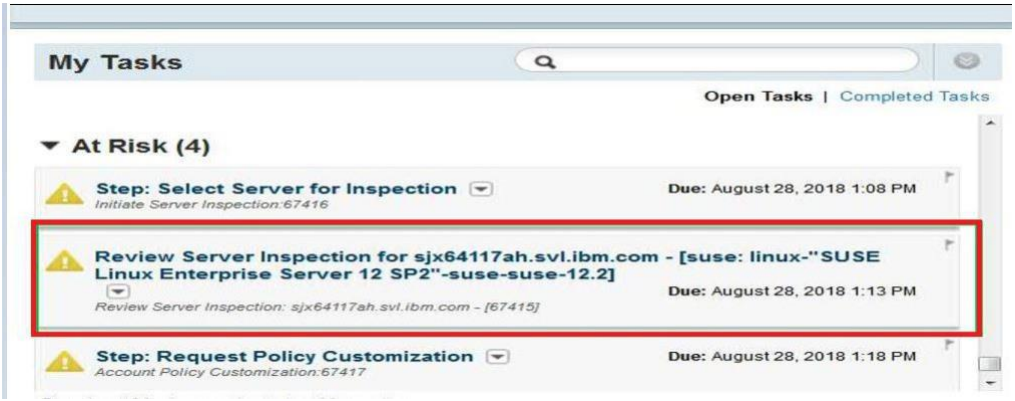


Figure 63. Server Log in My Task

22. The onboarded server detail is listed in “Initiate Server Inspection” page.

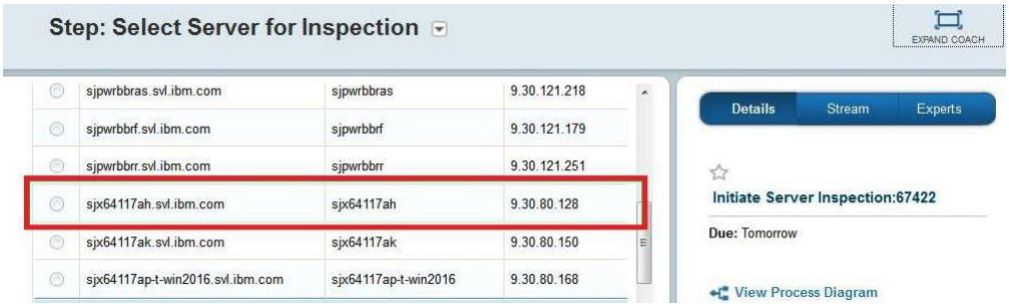


Figure 64. The Server details listed in Initiate Server Inspection page

23. “My Bulk Request” page in CC Enhance UI portal shows the Onboarding label description which is easy to identify the user request.

Figure 65. Onboarding request details in My Bulk Requests page

Server Bulk Load

1. If you wish onboard servers in bulk, you can do so by importing the server information from file instead of manually entering the server information.
2. Select "Import from file" option for "Server Onboarding".
3. You will be presented with a screen where you can download the template for the file.

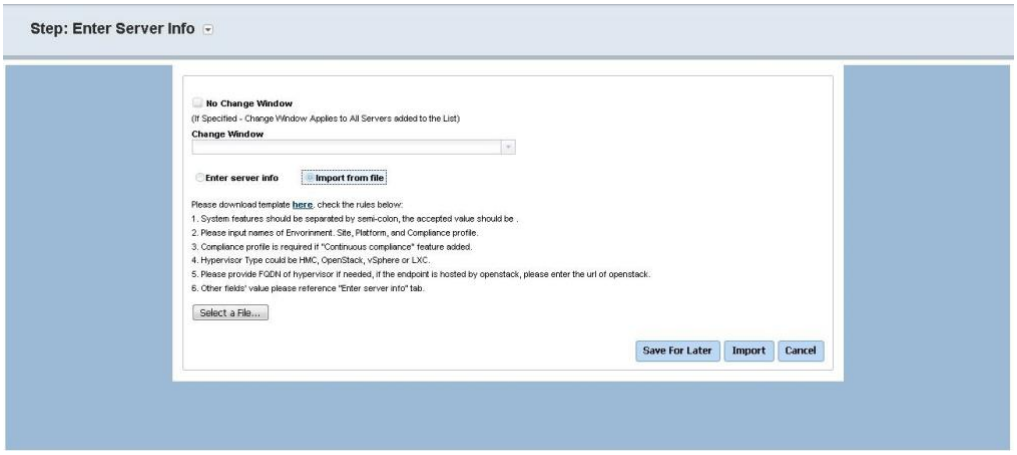


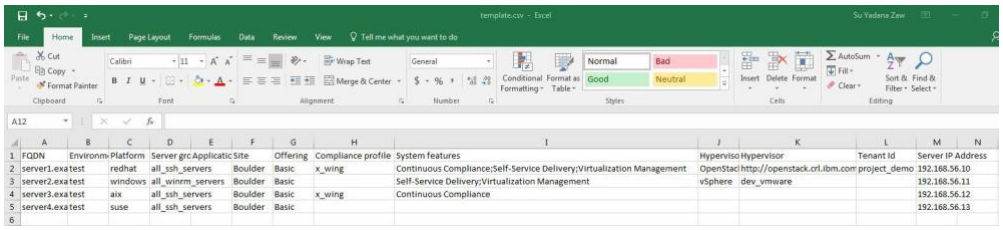
Figure 66. Import Server Info from file

4. Download the template file and read the rules presented on the page.
5. Create the file that contain the information of the server you want to onboard based on the template and the rules. An example of CSV file is shown below.

```
FQDN,Environment,Platform,Server group,Application,Site,Offering,Compliance
profile,System features,Hypervisor type,Hypervisor,Tenant Id

rhel66.crl.ibm.com,test,redhat,all_ssh_servers,,Boulder,Basic,x_wing,Continuous
Compliance,OpenStack,http://openstack.crl.ibm.com:5000/v2.0/tokens,project_d
emo

cobalt-vm-
win3.pok.ibm.com,test,windows,all_winrm_servers,,Boulder,Basic,,,vSphere,dev_
vmware

dwin003.dub.usoh.ibm.com,test,aix,all_ssh_servers,,Boulder,Basic,,,,

cobalt-suse.cr.ibm.com,test,suse,all_ssh_servers,,Boulder,Basic,,,,
```

Figure 67. Example CSV File

Note: If your SLA environment does not have a DNS server, you need to create a field for the IP address of the server you are onboarding at the end of the file. You can see the example below.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	FQDN	Environm	Platform	Server grc	Applicatic	Site	Offering	Compliance profile	System features	Hypervisc	Hypervisor	Tenant Id	Server IP Address	
2	server1.exa	test	redhat	all_ssh_servers		Boulder	Basic	x_wing	Continuous Compliance;Self-Service Delivery;Virtualization Management	OpenStac	http://openstack.crl.ibm.com	project_demo	192.168.56.10	
3	server2.exa	test	windows	all_winrm_servers		Boulder	Basic		Self-Service Delivery;Virtualization Management	vSphere	dev_vmware		192.168.56.11	
4	server3.exa	test	aix	all_ssh_servers		Boulder	Basic	x_wing	Continuous Compliance				192.168.56.12	
5	server4.exa	test	suse	all_ssh_servers		Boulder	Basic						192.168.56.13	
6														

Figure 68. Example CSV File 2

When creating the CSV file, you can refer to “Enter server info” below. You can go back to "Enter Server Info" page if you need more reference. You can refer to “Server Onboarding Steps” on page 72 of this guide as well.

Note: First line should be the header, please keep it. Fill in all the mandatory fields. Optional fields that are not relevant to the servers can be left empty. For example, if the server is going to use "Virtualization Management" feature, the hypervisor related information (Hypervisor type, Hypervisor, Tenant Id) must be filled in the relevant fields. Please check with your Hypervisor Admin for the required information. Otherwise, those fields can be left empty.

a. FQDN (mandatory): The fully qualified domain name of the server
b. Environment (mandatory): The environment the server belongs to. Please check “Enter server info” section to get the available environments.
c. Platform (mandatory): The platform of the server. Please check “Enter server info” section to get the available platforms.
d. Server group (mandatory): If you have endpoints in multiple networks, you may need multiple SAS gateways so that SLA can manage servers in those disconnected environments. Servers are grouped based on gateways using "Server Group Management" function. Select the server group to define the gateway the server you want to onboard will be using.

Note: There are two default managed server groups provided by the system. The group "all_winrm_servers" is for Windows systems. The "all_ssh_servers" group is for Linux and AIX systems that are using ssh credential type.

e. Application (optional): Application or middleware installed on the server. Please check “Enter server info” section for available values.

   Note: Middleware discovery is disabled by default to save onboarding and change request execution time. If you want to enable a certain middleware discovery, inform SLA Ops Team to schedule a change window and configure it.

f. Site (optional): Site of the server. Please check “Enter server info” section for available values.

g. Offering (optional): Offering of the server. Please check “Enter server info” section for available values.

h. Compliance profile (mandatory if ‘Continuous Compliance’ system feature is set): For available profiles, please check the selections in “Enter server info”.

i. System features (optional): These are the features of the server, you find the available features in “Enter Server info”. As this field is multiple selected, please separate the values by semi-colon.

j. Hypervisor Type (mandatory if ‘Virtualization Management’ system feature is set): To indicate what kind of hypervisor environment this is server is hosted on. Available values are HMC, OpenStack, vSphere and LXC now.

k. Hypervisor (mandatory if ‘Virtualization Management’ system feature is set): The FQDN or URL of the hypervisor

l. Tenant Id (mandatory if ‘Virtualization Management’ system feature is set and the hypervisor is OpenStack): If the hypervisor is OpenStack, tenant id is required.

m. Server IP Address(mandatory for SLA Environments that are not using DNS server): The IP address of the server you want to onboard

n. Change Window Schedule (optional): A Change Window is a period during which changes can be made to managed servers in the environment. If you want to associate the servers you are onboarding with a specific change window, you can *add a new column at the end of the template file* for "Change Window Schedule". If you do not define any change window, the servers will be associated with the default change window. If you want to change the change window of a managed server to a different change window after the server is successfully onboarded, you can do so using the "Server Change Schedule Management". See “Server Change Schedule Management” on page 36 for more details.

6. Click on the "Select a File" button after you have created the file.
7. Select the file to upload and click "Import".

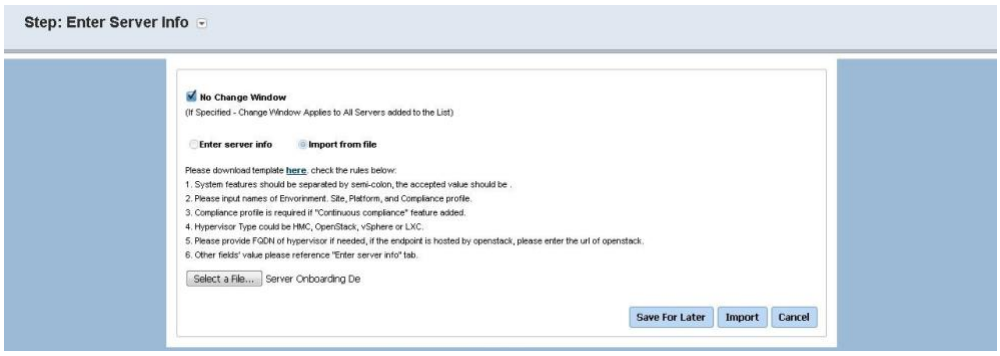


Figure 69. Import the CSV File

8. Once you clicked "Import", you will see the following screen while the system is processing the import. You can wait or you can click "Check Later". The system will continue importing the server data either way.

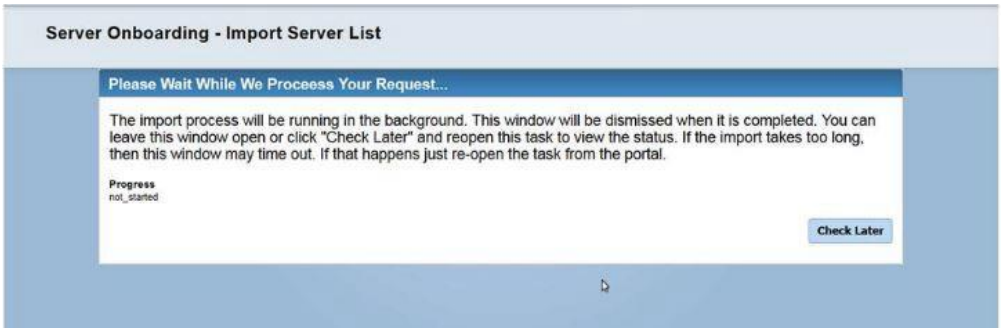


Figure 70. Server Onboarding - Import Server List Loading Page

9. If you click "Check Later", you will be able to go back to the same page later via the "Server Onboarding - Import Server List" task created on your workspace.
10. Once the data is fully imported, the server information will appear under "Server List" table.

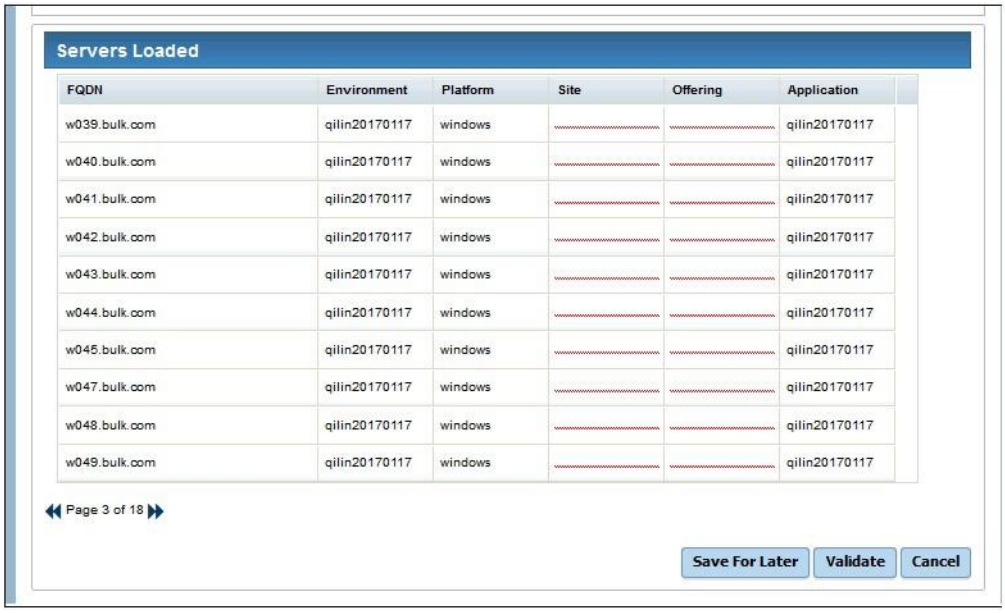


Figure 71. Servers are Added to the Server List Table

11. You must pass the validation before you can submit the servers for onboarding. The validation step will check whether all the prerequisites for onboarding have been met. Go to "Prerequisite Validation" and perform the steps listed there.

Prerequisite Validation

v Once you click **Validate** on the "Enter Server Info" page, you will see the following screen while the system is performing validation. You can wait while the validation is performed or you can click "Check Later". The system will continue with the validation either way.

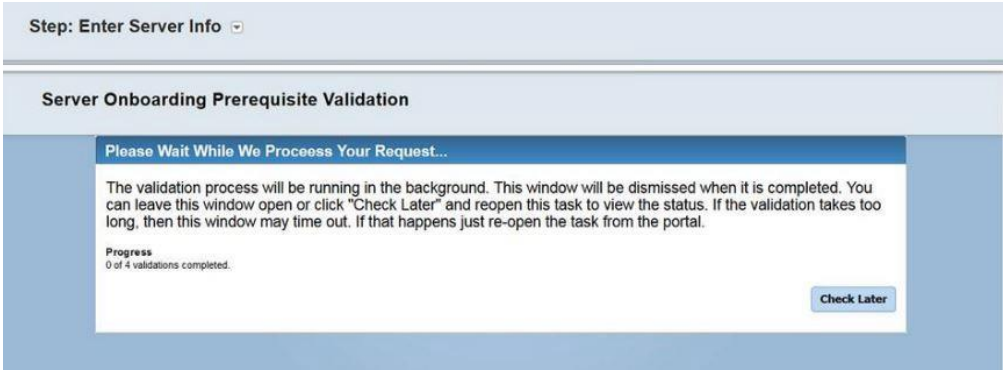


Figure 72. Server Onboarding Prerequisite Validation Loading Page

v If you click "Check Later", you will be able to go back to the same page later via the "Server Onboarding Prerequisite Validation" task created on your workspace.

v Once the validation is done, you will be automatically redirected to the "Prerequisite Validation Results" page. Only the servers that passed validation can be submitted for onboarding.

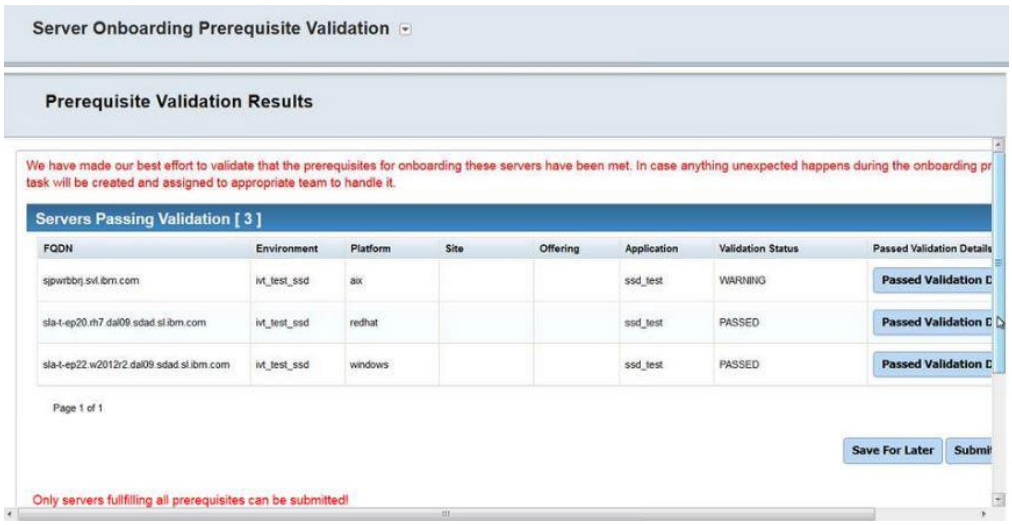


Figure 73. Prerequisite Validation Results

v You can check the validation details by clicking the "Passed Validation Details".

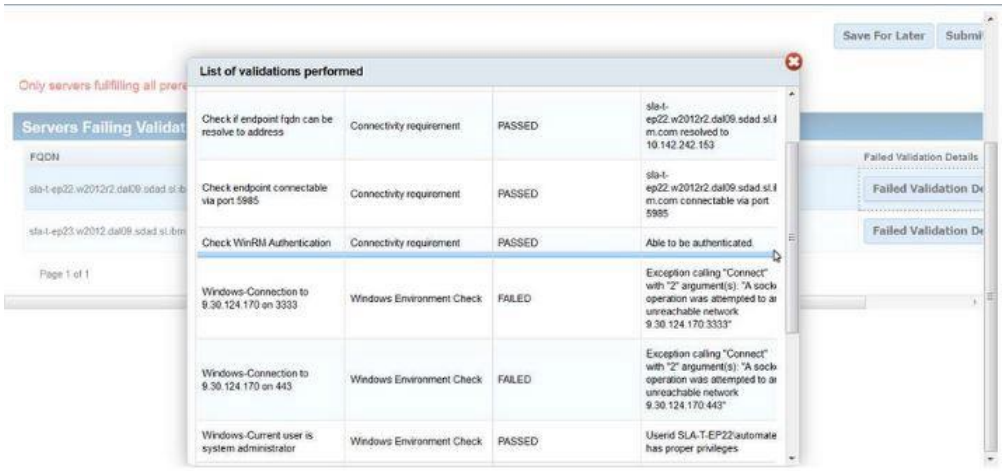


Figure 74. Validation Details

v Click the "Submit" button to submit the servers that passed the validation for server onboarding.

Figure 75. Submit Servers for Onboarding

Note:

v If you are onboarding servers to Continuous Compliance solution, the server(s) will be processed and an initial inspection (whyrun) will be run when the server has been added to the system fully. This process may take up to 20 minutes per server. Note that multiple servers can be processed in parallel. For large lists of servers, this process may take a while. The compliance whyrun will compare the server's configuration against the security policies that were set up in Compliance Profiles. This is a check only, no changes are made to the server(s) at this point in time.

v Once the check is completed, a new task called "Review Server Inspection for <your_selected_endpoint_hostname>" will appear on your workspace. Follow the steps under "Review Server Inspection" on page 87 of this guide and perform server inspection review.

Grant Connection Access to Endpoint

1. Login as system admin or account security focal or sscm executor.
2. If there are any issue with the connectivity between the endpoint and the chef-server, it will create a task "Step: Manually Test Connection".
3. Open the task "Step: Manually Test Connection" and click "Verified" and this should proceed with the server onboarding.
4. There should be a task created called "Grant Access to Endpoint".
5. Open the task "Grant Access to Endpoint" and Accept it.

Troubleshooting Task

When onboarding a server, there are two possible outcomes.

1. Onboarding is successful and no further action is needed.
2. Onboarding fails and a troubleshooting task is created on your workspace.

   Note: You must have a "Support" role access to be able to see this task.

   When the troubleshooting task is created, click the task to claim it. Once you are on the troubleshooting task page, you must take either one of two actions.

   a. Retry. This will reattempt the onboarding again. If it fails again, another troubleshooting task will be created. In such cases, you may need to seek assistance from the SLA Operations team.

b. Abort Onboarding. Once you abort onboarding, the status of the server in the DB will be changed to "Onboarding Aborted". In this state, you will be able to onboard the server again in the future.

Important: If you do not take action on the troubleshooting task, the server will stay in the "Onboarding" state indefinitely. You will not be able to re-onboard the server or offboard the server. Make sure you take one of the two actions under the troubleshooting task.

Review Server Inspection

This task allows you to review the inspection (whyrun) results of each of the policies that were enforced. You will be presented with the list of deviations.

1. Click the "Review Server Inspection for <your_selected_endpoint_hostname>" task and claim it to see the results of the execution of the "Compliance Profile" policies in inspection mode.

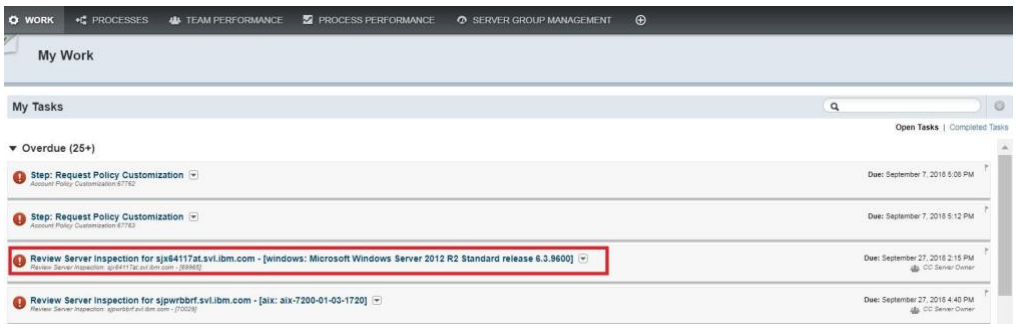


Figure 76. Review Server Inspection

2. Review the results of each one of the policies that were enforced. You will notice that there will be deviations that are allowed to be overridden and deviations that cannot be overridden. Review and determine if you would like to perform an override by checking the "Override" check box and providing a justification for the override.

   Note: The deviations that are not being overridden will be remediated. However, the remediation will occur only when the server is put into the "Enforcement Mode (formerly known as Maintenance Mode or Continuous Compliance Mode)". See "CC User Guide, **Chapter 11: Server Compliance Management > Enforcement Mode" for more information on the Enforcement Mode**.

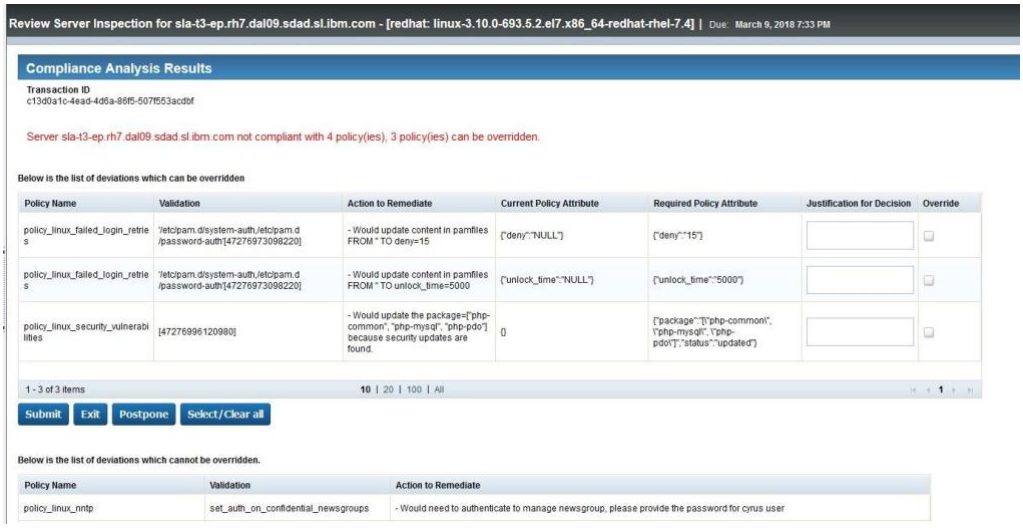


Figure 77. Server Inspection Result

3. Once you have specified overrides for all of the policies in question you may click "Submit".

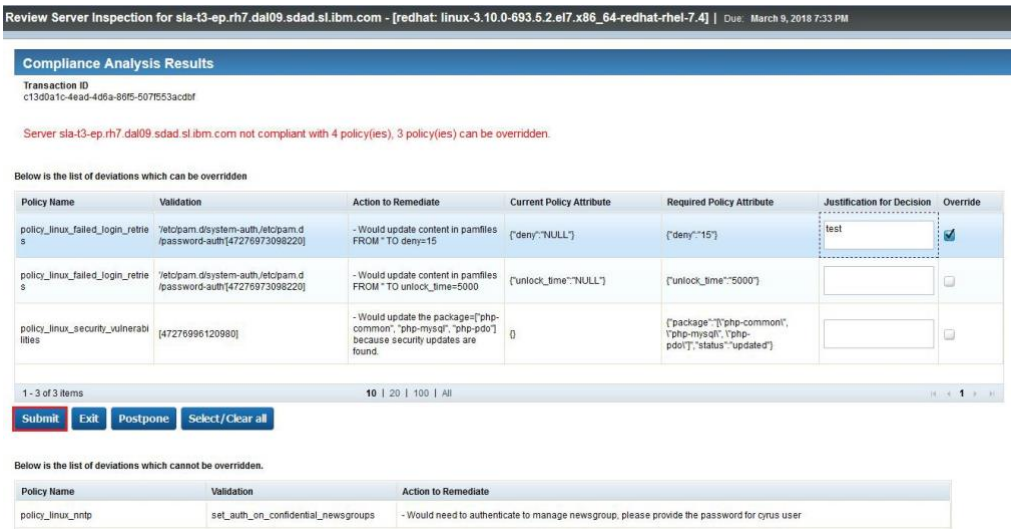


Figure 78. Submit Override for Server Compliance

4. If you want to postpone the action and review the inspection results again at a later time, click the "Postpone" button. You will still be able to see the task in your workspace and will still be able to access the task later.
5. If you want to close the review task without submitting any override, click the "Exit" button. The task will disappear from your work space.
6. If you click "Submit" without selecting any policy deviation to be overridden, you will receive a pop up window saying you did not choose any policy to override. Click on the "Exit" button. The review task will disappear from your workspace.

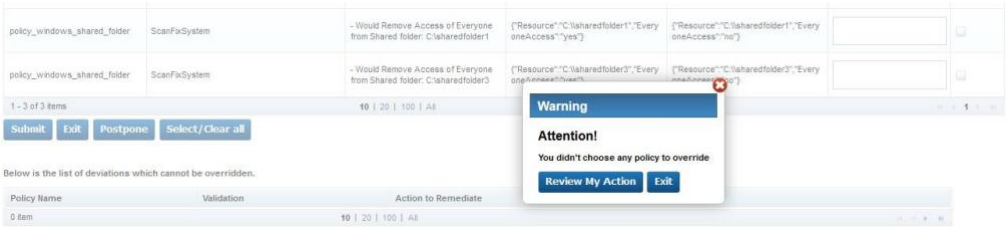


Figure 79. Exit the Task without Override

Note:

Once the compliance policy violations and overrides are reviewed and submitted, there are several scenarios that might be true:

1. The user submitted no overrides and exited the task. The processing is completed. The deviations that are not being overridden will be remediated when the server is put into the enforcement mode.
2. The user specifies several overrides and submits the request for approval. Once the approver approves the overrides, the override requests are sent to CC and the overrides and default policies are added to the run list during the change window that is associated to the server. The results are provided via a "Step: Inspection Result" task on the workspace.
3. The user specifies several overrides and submits the request for approval. The approver rejects all overrides. The results are provided via a "Step: Inspection Result" task on the workspace and all processing is ended. The user should review the reasons for the rejection of the overrides. The user may then choose to run the process "Initiate Server Inspection" for each server.
4. The user specifies several overrides and submits the request for approval. The approver approves only some of the overrides and rejects the rest. The results are provided via a "Step: Inspection Result" task on the workspace. The override requests for approved overrides are sent to CC. The approved overrides and policies are added to the run list within the change window that is associated to the server. The user may also review the reasons for the rejection for the rejected overrides. Then, run the "Initiate Server Inspection" process.

Chapter 8. Server Onboarding - Message-based SLA Client Install

Before you can start managing a server, you must onboard the server that you want to manage.

Starting from release 23.5.1, a new SLA Client with a message-based communication model is available and would be enabled on a pre-request basis. This new model would provide better security, stability and maintainability of the solution, and is our recommended model to adopt. Plans should be made on all accounts to eventually move to that model.

The Message-based SLA Client fundamentally changes how the application interacts with an endpoint. Instead of connecting directly to the endpoint using protocols like SSH or WinRM, the new SLA Client uses messaging to accomplish the same thing.

Below are the high-level steps to perform SLA Client installation:

1. Complete prerequisite for server
2. Define the server to SLA
3. Download the SLA Client Installer, copy to server and prepare the Config file
4. Validate the endpoint and config file before onboarding
5. Setup the File Caching Server or pre-stage the Chef Client to reduce network traffic and speed up the installation (Optional)
6. Install SLA Client
7. Verify the installation

To add new servers, see "Defining Servers to SLA" on page 95. Prior to the messaging service request submission, you must fulfill the prerequisites. Go through the sections under "Prerequisites for SLA Client Install" and perform the steps that are applicable to your endpoints to onboard.

Prerequisites for SLA Client Install

For accounts existing before Mar 2019, the Message-based SLA Client will not be enabled for you by default. In order to experience the full benefits of the new model, raise a Service Request to the SLA Operation team by following instruction in the below link. Messaging Model Enablement Request Process.

Prerequisite for Onboarding Windows Endpoint

Check whether your endpoint meets the following requirements.

Connectivity Requirements

- If the account is configured to use 'DNS-only' to resolve endpoint ip, the hostname of the endpoint must be resolvable from the Execution Engine Server. Refer to Chapter 7, "Server Onboarding - Legacy," on page 45 for more details on DNS and no-DNS.
- The endpoint must be able to reach the Execution Engine by HOST IP on port 3333/tcp.

- The endpoint must be able to reach the Execution Engine by HOST IP on port 9093/tcp.
- The endpoint must be able to reach the CHEF Server by HOST IP on port 8443/tcp.

Disk Space Requirements

- The endpoint must have at least 5 GB available for CHEF client binaries located in C:\IBM\cobalt folder.
- The C:\IBM\cobalt folder may be placed as a mount point to a separate file system to contain the space consumed by CHEF

OS Settings Requirements

- The endpoint clock must be synchronized within 15 minutes of the chef server.

OS Version Requirements

- Windows 2008 R2
- Windows 2012 R2
- Windows 2012 Std
- Windows 2016

Memory Requirements

- The recommended amount of RAM available for CHEF client to run is 512MB.

Software Requirements

- All Windows Servers must meet prerequisites which is to have PowerShell 3.0 (or higher) with 512 MB memory (or higher) configured.

  Note: Windows Server 2016 uses PowerShell 5.1. No hotfix installation is needed.
- In addition, hotfix **kb2842230** needs to be deployed for PowerShell 3.0.
  - For Windows Server 2008 R2, deploy Windows Hotfix KB2842230 for Win2008 R2.
  - For Windows Server 2012, deploy Windows Hotfix KB2842230 for Win2012.
  - Download and install the hotfix.
  - Restart the endpoint after the successful hotfix installation.
- Microsoft .NET Framework 4.5 is required to install PowerShell v3.0. Windows Server 2012 and 2012 R2 include the .NET Framework 4.5. Windows Server 2008 R2 only includes .NET Framework 3.5.1. If your endpoint OS is Windows Server 2008 R2, you MUST manually put .NET Framework 4.5 in place in your endpoint.
- Starting from Release 17.5, FIPS mode is supported. However, a chef server upgrade must have been performed before you can start turning on the FIPS in your endpoints. For FIPS enabled endpoints, you must create a separate server group. See “Server Group Management” on page 64 for steps on how to create server groups with FIPS enabled.

Functional ID Requirements

- Under the message-based SLA Client, not required to setup any dedicated functional ID for Windows endpoints.
- The SLA Client will be running as a Windows Service under the Local SYSTEM account, thus there should not be any settings/policies which would block that.

- During the installation process, the setup script must be run with Local Administrator privilege.

Prerequisite for Onboarding Linux Endpoint

Check whether your endpoint meets the following requirements.

Connectivity Requirements

- If the account is configured to use 'DNS-only' to resolve endpoint ip, the hostname of the endpoint must be resolvable from the Execution Engine Server. Refer to Chapter 7, "Server Onboarding - Legacy," on page 45 for more details on DNS and no-DNS.
- The endpoint must be able to reach the Execution Engine by HOST IP on port 3333/tcp.
- The endpoint must be able to reach the Execution Engine by HOST IP on port 9093/tcp.
- The endpoint must be able to reach the CHEF Server by HOST IP on port 8443/tcp.

Disk Space Requirements

- The endpoint must have at least 5 GB available on /opt/IBM/cobalt for CHEF client binaries.
- The /opt/IBM/cobalt folder may be placed as a mount point to a separate file system to contain the space consumed by CHEF

OS Settings Requirements

- The endpoint clock must be synchronized within 15 minutes of the chef server.

OS Version Requirements

- Redhat 6.1 to 7.6
- SUSE 11.x and 12.x
- Ubuntu 14.x and 16.x

Memory Requirements

- The recommended amount of RAM available for CHEF client to run is 512MB.

Functional ID Requirements

- Under the message-based SLA Client, the application will be running as a daemon process in backend owned by a user and group.
- The owner user account should not be able to login to the box.
- The owner user account should be able to run command with root privileges via sudo or other means without being prompt for password.

  Note: For the Redhat released before 2014, there is a default setting of 'requiretty' in /etc/sudoers that will violate this requirement. If not to change the default value, disable the setting for the sla owner ID using "Defaults:<sla owner> !requiretty".
- During the installation process, the setup script must be run with root privileges via sudo or other means.

Prerequisite for Onboarding AIX Endpoint

Check whether your endpoint meets the following requirements.

Connectivity Requirements

- If the account is configured to use 'DNS-only' to resolve endpoint ip, the hostname of the endpoint must be resolvable from the Execution Engine Server. Refer to Chapter 7, "Server Onboarding - Legacy," on page 45 for more details on DNS and no-DNS.
- The endpoint must be able to reach the Execution Engine by HOST IP on port 3333/tcp.
- The endpoint must be able to reach the Execution Engine by HOST IP on port 9093/tcp.
- The endpoint must be able to reach the CHEF Server by HOST IP on port 8443/tcp.

Disk Space Requirements

- The endpoint must have at least 5 GB available on /opt/IBM/cobalt for CHEF client binaries.
- The /opt/IBM/cobalt folder may be placed as a mount point to a separate file system to contain the space consumed by CHEF.

OS Settings Requirements

- The endpoint clock must be synchronized within 15 minutes of the chef server.

OS Version Requirements

- AIX Version 6.1 TL 9 (or higher)
- AIX Version 7.1 TL 3 (or higher)
- AIX Version 7.2

Memory Requirements

- The recommended amount of RAM available for CHEF client to run is 512MB.

Software Requirements

- The endpoint must have the library zlib v1.2.2.1 or higher available to execute Ruby.
- The endpoint must have library libffi available available to execute Ruby.
- The endpoint must have library gmp available available to execute Ruby.

Functional ID Requirements

- Under the message-based SLA Client, the application will be running as a daemon process in backend owned by a user and group.
- The owner user account should not be able to login to the box.
- The owner user account should be able to run command with root privileges via sudo or other means without being prompted for password.
- In order for the application to run correctly, the "max resident set size" need to be increased by below command:

  ```
  chsec -f /etc/security/limits -s root -a "rss=-1"
  ```

- In order for the application to run correctly, the "Maximum number of processes available to a single user" need to be increased by below command:

  ```
  chsec -f /etc/security/limits -s root -a "nofiles=50000"
  ```

v During the installation process, the setup script must be run with root privileges via sudo or other means.

Defining Servers to SLA

To prevent arbitrary servers from being added into the tool, an authorized user who has onboarder or system admin role must first let SLA know about the sever.

When you define a new server into SLA, it will be added to a whitelist in the registration service and becomes eligible to have the SLA Client installed on it. If you attempt to install the SLA Client on an endpoint that is not in the whitelist, it will be blocked when it attempts to register and an error message will be displayed in the output console in which the setup script is being run.

You do not need to onboard a server via ProcessPortal and go through the entire server onboarding process for said servers. Perform the following steps.

1. Navigate to SLA landing page and login to SLA Enhanced UI with a user that has either Onboarder or System Admin or both roles.
2. Click on 'My Servers' available in the left pane below the 'Dashboard' option.

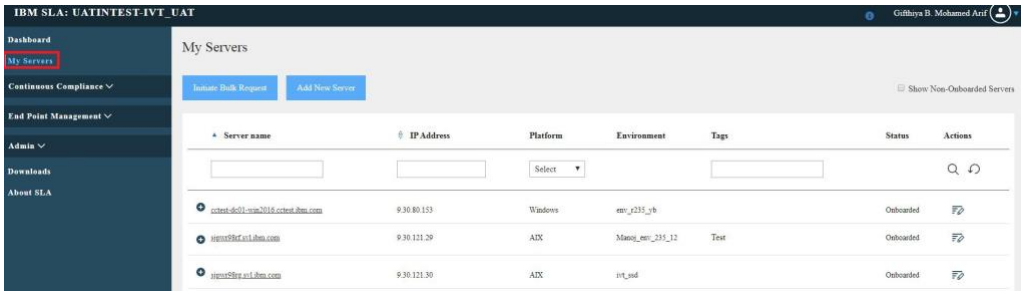


Figure 80. My Servers

3. Click the "Add New Server" button.

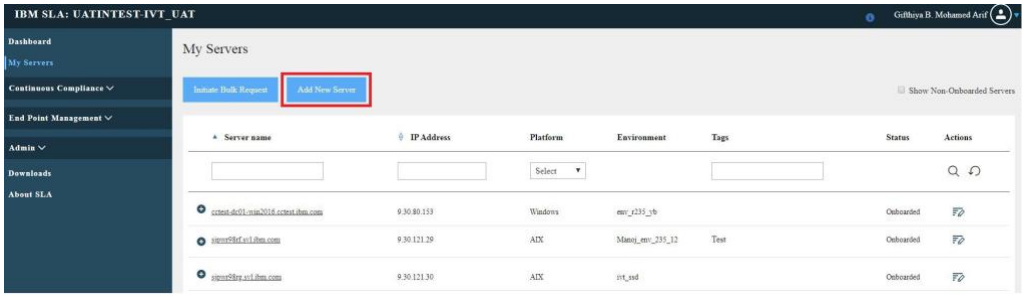


Figure 81. Click Add New Server

Note: This link is visible only to user with Onboarder or System Admin roles. If you are not sure about the role you have, you could click the arrow icon next to your name in the upper right corner, expand the 'Groups & Role Types' section and verify as shown in the below screenshot.

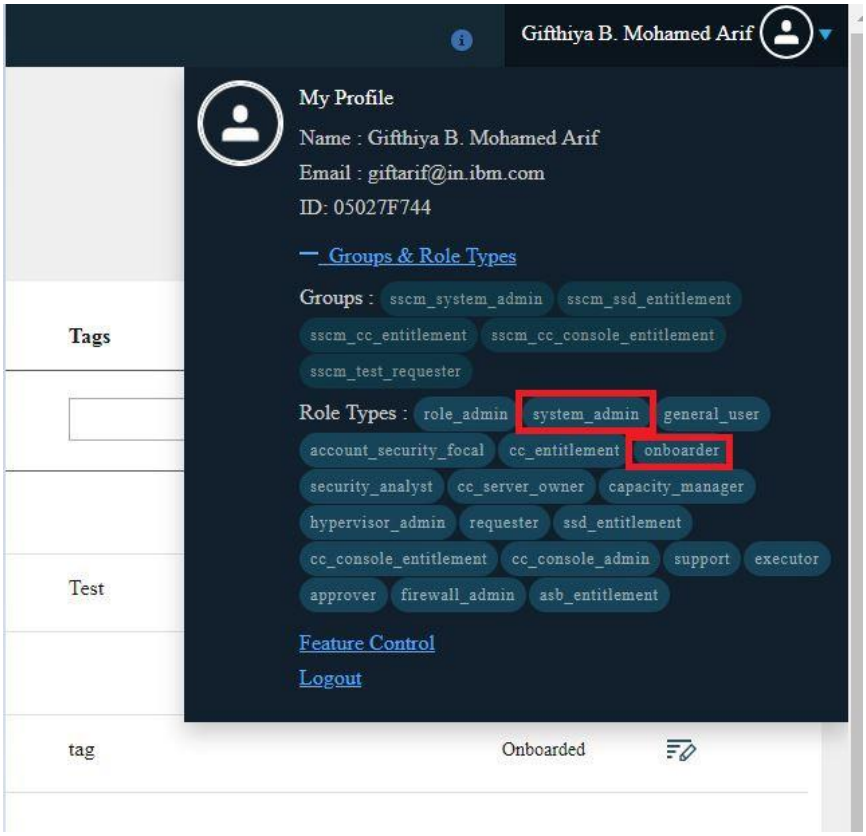


Figure 82. Group & Role Types

4. Enter the server details in the fields. There are two (2) approaches to enter server details and they are explained below:

   a. Add individual servers manually

   1) Enter 'Server Name', 'Platform' and 'Server Group' information and click 'Resolve FQDN' button under the 'Actions' column. The IP Address will be automatically populated, if the FQDN/IP Address pair is resolvable.

   2) If the name resolution failed and the account is configured to use 'no-DNS' or 'both DNS and no-DNS', user will be prompted to enter the IP Address Manually. If the name resolution failed and the account is configured to use 'DNS only', an error will be displayed, and you would need to verify the DNS server is configured correctly and the endpoint is registered in the DNS server. Refer to Chapter 7, "Server Onboarding - Legacy," on page 45 for more details on DNS and no-DNS.

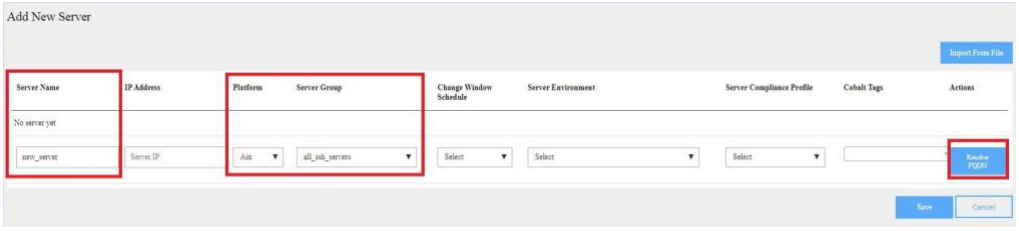


Figure 83. Add Individual Servers Manually

3) Select the 'Change Window Schedule': A Change Window is a period during which changes can be made to managed servers in the environment. Select the change window to be associated with the servers that are being onboarded. If you want to change the change window of a managed server to a different change window after successful server onboarding, you can perform that action using the "Server Change Schedule Management". Refer “Server Change Schedule Management” on page 36.
4) Select the 'Server Environment': The default compliance environment that has been reviewed and customized in the Environments.
5) Select the ‘Server Compliance Profile’: The default compliance environment that has been reviewed and customized in the Compliance Profiles

   Note: Associating the managed server to an environment and a compliance profile enables the Account Security Focal to control the correct compliance policies that will be run against a given managed server or set of managed servers. This will make the process of customizing the compliance policies that are applicable across a large number of servers more efficient.
6) Select the ‘Cobalt Tags’ (Optional): You could associate none or one or multiple tags to a server. A Cobalt Tag is an arbitrary identifier that could be used to group a set or related servers and could be used to filter servers quickly in the ‘My Servers’ page.
7) Click the ‘+’ icon under the ‘Actions’ section to add server to pending list.

   Note: You will get an error message if you try to save the server without clicking the plus sign first.

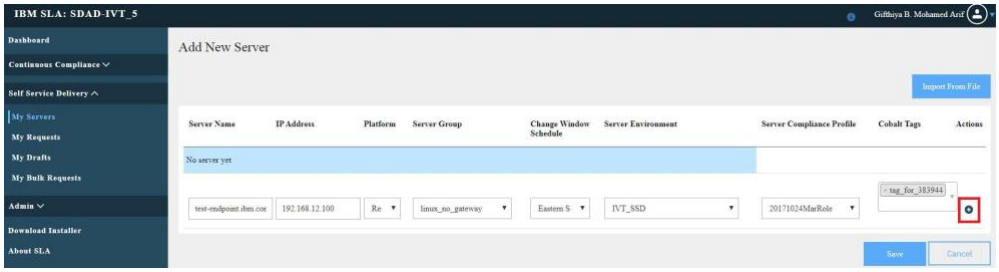


Figure 84. Click the "+" Icon

b. Add multiple servers through import a CSV file

1) To enter the server details manually, import a CSV file. Click ‘Import From File’ button.

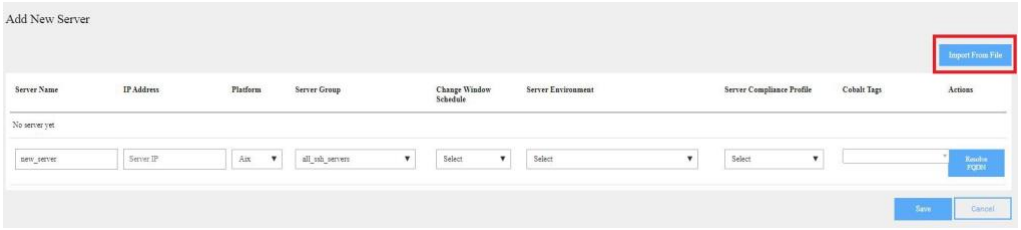


Figure 85. Import From File

2) Download the CSV file template from the prompt.

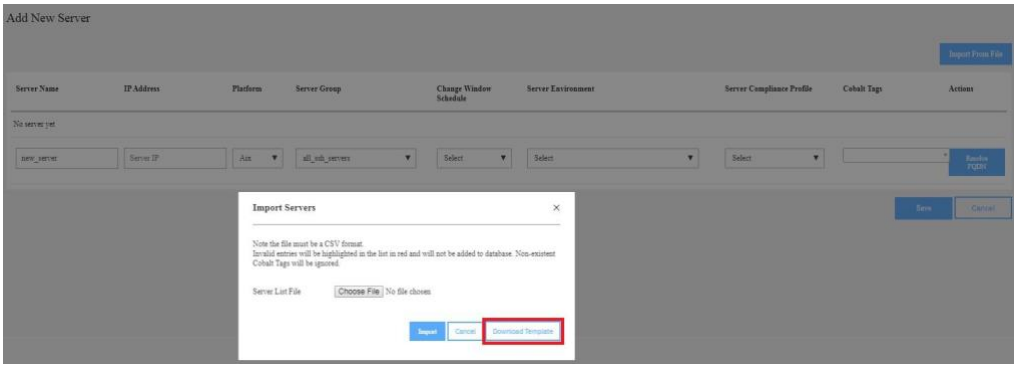
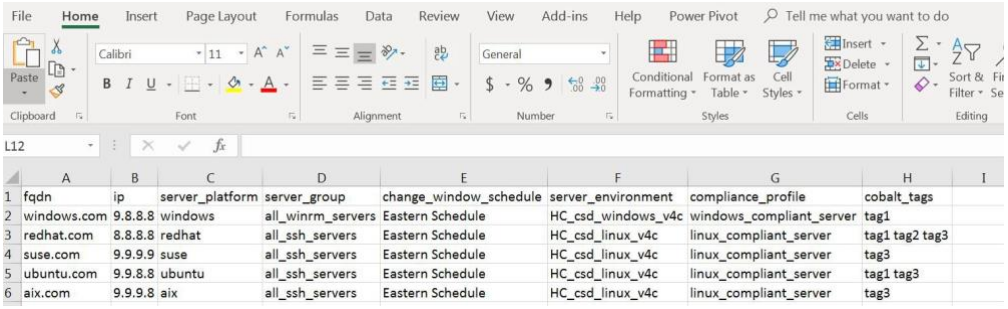


Figure 86. Download Template

3) Add server details to the CSV template and save the excel file in your system. The details of each field could be find in section "Add individual server manually" mentioned above.



	A	B	C	D	E	F	G	H
1	fqdn	ip	server_platform	server_group	change_window_schedule	server_environment	compliance_profile	cobalt_tags
2	windows.com	9.8.8.8	windows	all_winrm_servers	Eastern Schedule	HC_csd_windows_v4c	windows_compliant_server	tag1
3	redhat.com	8.8.8.8	redhat	all_ssh_servers	Eastern Schedule	HC_csd_linux_v4c	linux_compliant_server	tag1 tag2 tag3
4	suse.com	9.9.9.9	suse	all_ssh_servers	Eastern Schedule	HC_csd_linux_v4c	linux_compliant_server	tag3
5	ubuntu.com	9.9.8.8	ubuntu	all_ssh_servers	Eastern Schedule	HC_csd_linux_v4c	linux_compliant_server	tag1 tag3
6	aix.com	9.9.9.8	aix	all_ssh_servers	Eastern Schedule	HC_csd_linux_v4c	linux_compliant_server	tag3

Figure 87. Add Servers in CSV File

4) Select the prepared CSV file from your system and click "Import". Entries from the CSV file will be processed and validated.

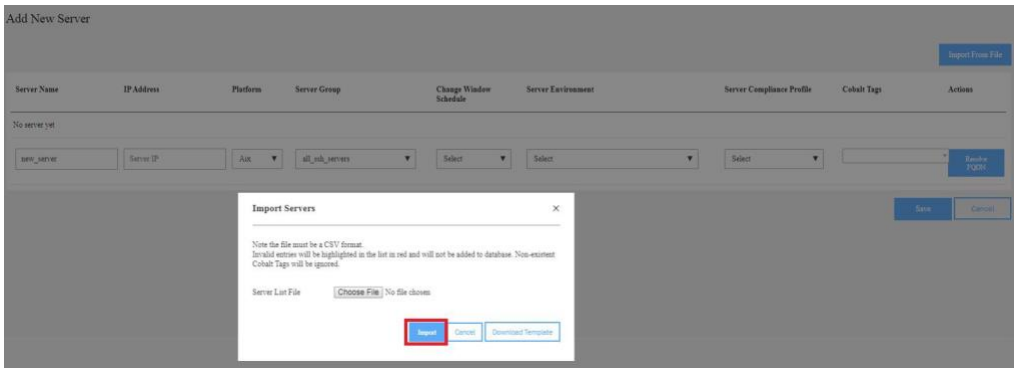


Figure 88. Click the "Import" Button

5) Servers that passed the validation will be added to the 'pending' list and if the validation is failed, those servers will be highlighted with red background and will be ignored in later steps.

   Note: Additional validation will be performed in later steps, thus it is possible for servers that passed this validation stage to be shown as 'invalid' in later validations.

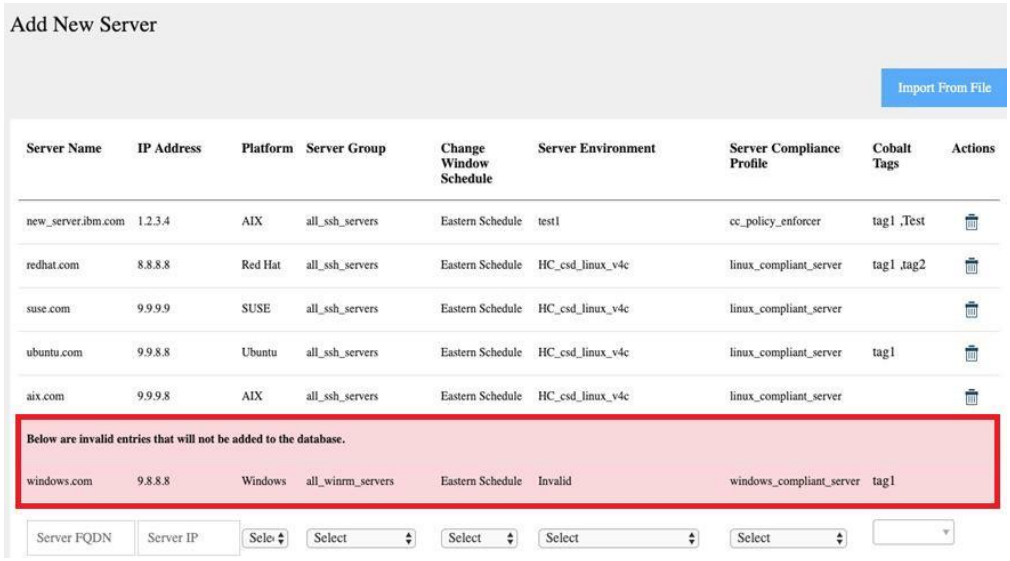


Figure 89. Validation Failed Servers

6) Click 'Save' to add the server record(s) to the tool, which would add them to the whitelist of the registration service as well.

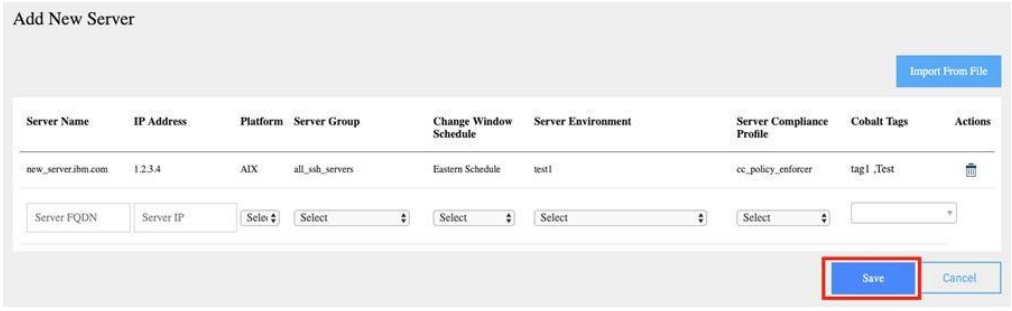


Figure 90. Click the "Save" Button

7) The result of the 'save' action will be displayed in a prompt. Additional validation will be performed at this stage, and the reason for any failure will be displayed.

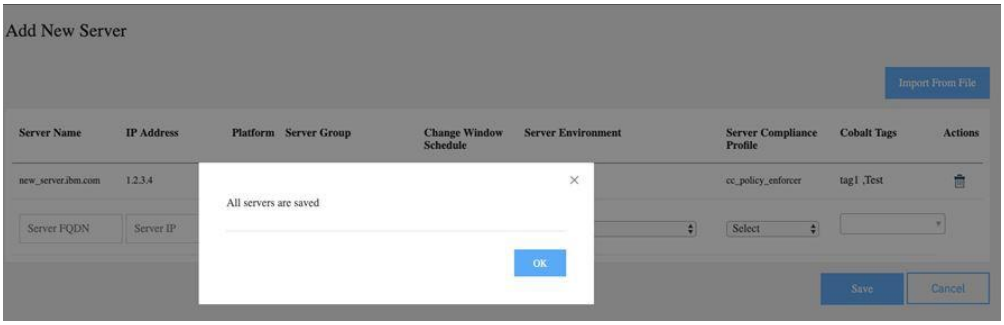


Figure 91. Servers Saved Prompt

Below is the screenshot when there is a validation failure.

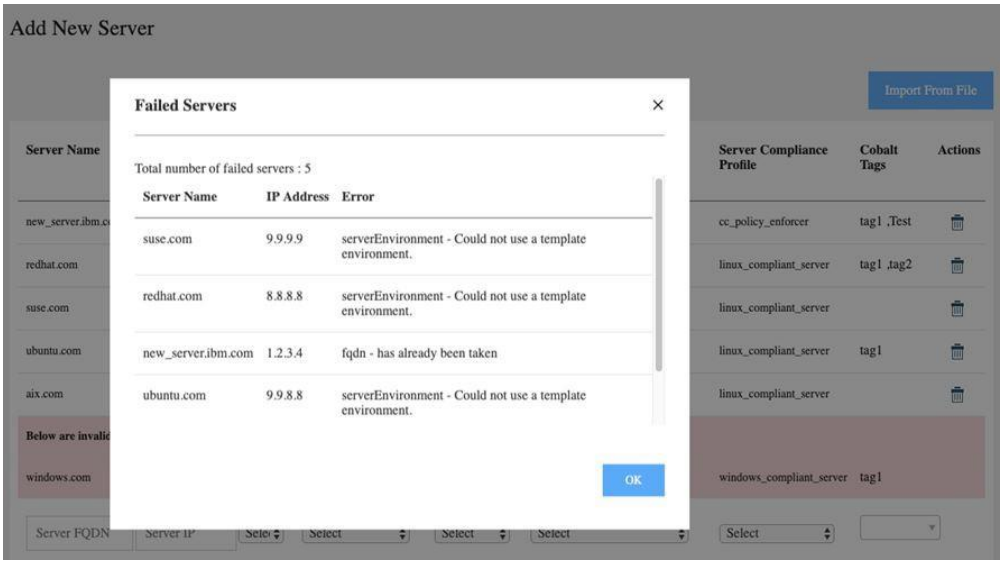


Figure 92. Failed servers Details

5. You can delete the newly added server using the delete icon available in the same row.

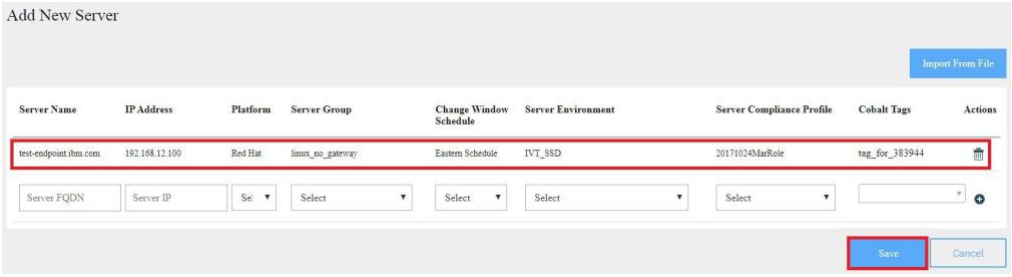


Figure 93. Delete Servers

6. You can keep adding more servers by entering the server details.
7. You will see the servers you added under "My Servers" page. Their status will be **"Offboarded"**.

   Note: Make sure the "Show Non-Onboarded Servers" check-box is checked. Otherwise, you will not be able to see the list of servers in the offboarded state.

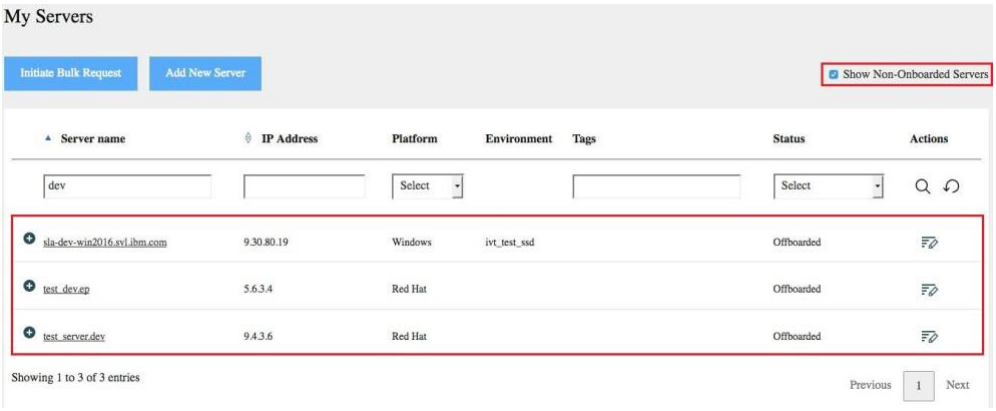


Figure 94. Servers that are Added (in Offboarded state)

Download the SLA Client Installer

1. When the prerequisites are fulfilled, login to SLA UI as SSCM. Click on the " CC Enhanced UI" link and log in using your LDAP userid or IBMid.
2. Click on **Downloads** and you can see three (3) tabs.
   a. Download SLA Installers
   b. Download Chef Installers
   c. Download Validation Script

   Downloads SLA Installers page appears by default on clicking Downloads option.

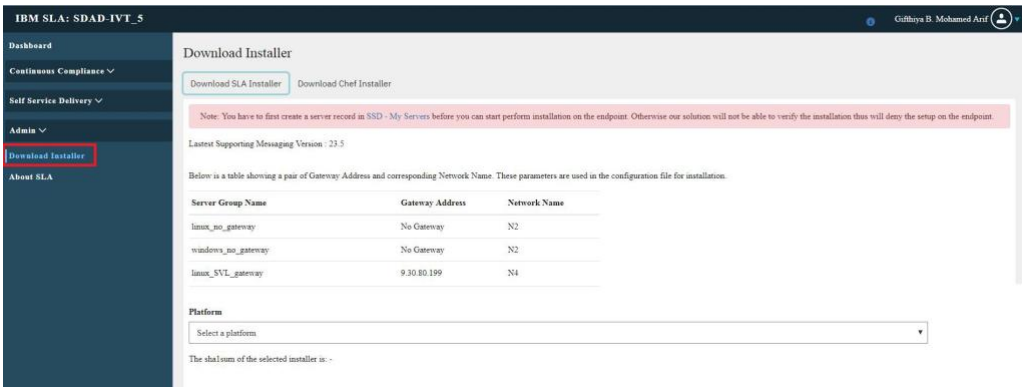


Figure 95. SLA UI → CC Enhance UI → Download Installer

3. Select the platform on which the Installer will be used at, and click ‘Download’. Below is an example of 'Redhat' platform.
4. Select 'Redhat' option from 'Platform" drop-down menu and click on 'Download'.

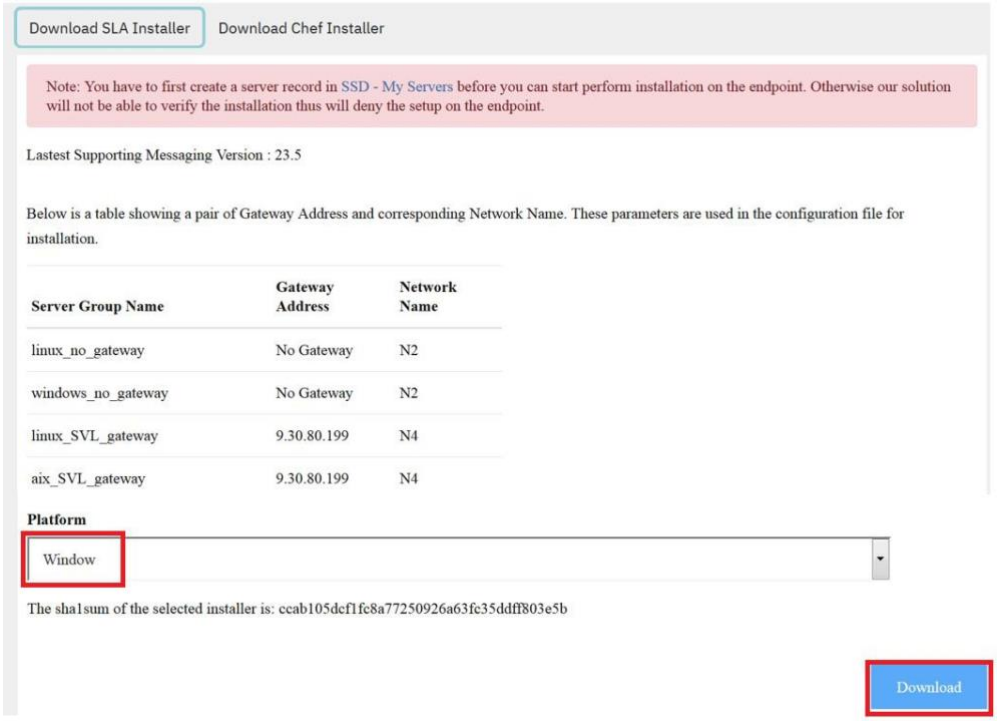


Figure 96. Select Platform and Download

5. The sha1sum of the installer will be displayed on the UI, which could be used to verify the integrity of the downloaded file.

Figure 97. Sha1sum of the Selected Installer

6. Download will be initiated. Once the download is complete, copy the downloaded installer to the target endpoint and extract the installer to any directory.
7. Double-click on setup file to extract the zipped folder.

   Any additional automation tool could be utilized to facilitate this step.

   a. On Windows endpoints, the installer could be unzipped with the GUI.
   b. On Linux/AIX endpoints, the installer could be untarred with command:

      `tar xf <path to installer> -C <path to the target untar directory>`

   The extracted directory appears as below.
8. When extracting the installer package, you can see a 'sample_install_config' file generated' for reference.

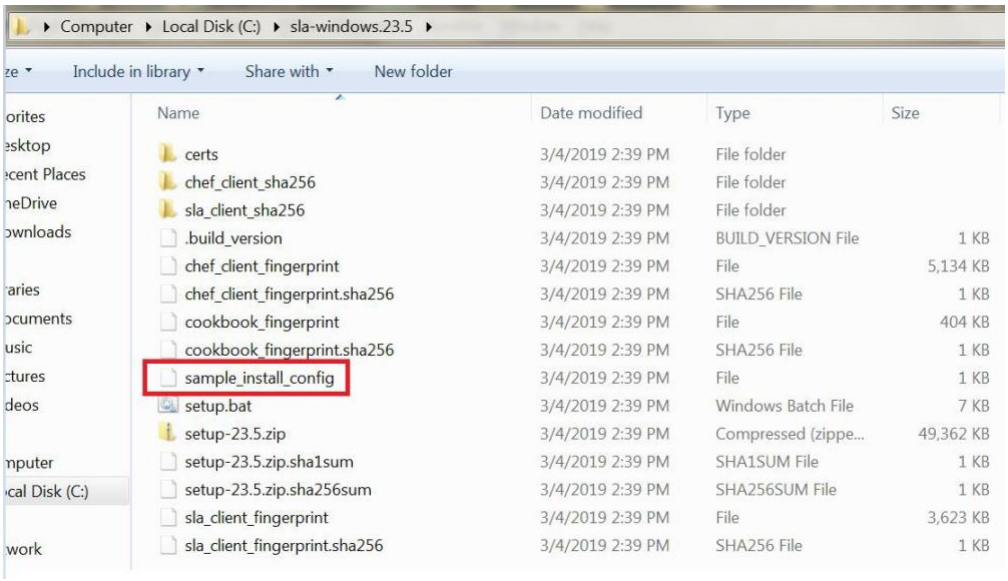


Figure 98. Sample Install Config File

9. Open the sample file to view the required values and create the configuration file. Below are the applicable fields in the file and explanation on each field:

   v fqdn: server's fqdn. The value is case and leading/trailing space sensitive, thus need to be exact match the entry created in 'My Servers' page of SLA UI

   v platform: server's platform name. valid entries are: aix, redhat, suse, ubuntu, windows

- network_name: network name the server belongs to. You could get the value from the 'Download Installer' page by looking up server's group name.
- ipaddress: server's IP address. If server has multiple ip, this should be the one which will route your traffic through the network tunnel
- account_gcsc: account short code for the current account; this value is case-sensitive and must match EE record
- kafka_url: kafka server's URL with port number. Unless otherwise configured, this value should be set to 9093. kafka url must be the SDS name of the EE server e.g. sla-p-emea999-ee.sdad.sl.ibm.com:9093 even though this is not resolvable in the local DNS
- kafka_ip: kafka server's IP address. In the presents of SASG, the SASG VIP1 should be used, if Direct VPN the routable address of the SASFW e.g. 158.87.34.3. The kafka_url and the kafka_ip are used to generate an entry in the local custom_hosts resolver file for identifying how to reach the kafka server
- timezone: Time zone in the format of TZ database, e.g. America/New_York, Europe/Paris. If you are not sure about whether the timezone you provided is valid, refer to Appendix D, "Valid Timezone Values In Install Configuration File," on page 123
- owner: For Windows, this could be either SYSTEM or a MSA account user(only required if you need to modify GPO object) name;

  For Linux or AIX, the user will be the owner of the files and service.

  The owner needs to meet the requirements stated in the "Prerequisites for SLA Client Install" on page 91. The ID need to meet all IBM functional ID standards(for EU account, refer to this link) and privilege file template(unless otherwise agreed, sudo template 141 should be used).
- group: Linux & AIX only: Group that owns the file. If not set, default value is 'root'
- account_type: Windows only: Valid values include: SYSTEM, MSA
- batch: Optional, group installation request with same batch in one bulk request. If not provided, installation date (yyyy-mm-dd format) will be used

10. Create a new config text file in the same format. Below is an example of windows platform.

```
fqdn=mywindowsserver.example.com
platform=windows
ipaddress=1.1.1.1
network_name= n1
account_gcsc=example
kafka_url=something.sdad.sl.ibm.com:9093
kafka_ip= 1.1.1.200
timezone=America/New_York
owner=SYSTEM
account_type=SYSTEM
batch=install_batch_1
```

Figure 99. Example Values for Windows Platform

11. Below is an example of Redhat platform.

```
fqdn=myredhatserver.example.com
platform=redhat
ipaddress=1.1.1.2
network_name= n1
account_gcsc=example
kafka_url=something.sdad.sl.ibm.com:9093
kafka_ip= 1.1.1.200
timezone=America/New_York
owner=automate
group=automate
batch=install_batch_2
```

Figure 100. Example Values for Redhat Platform

12. If the library libgmp and libffi is not available on the endpoint, the server onboarding for AIX fails with the below error.

```
Copying cert files to /opt/IBM/cobalt/setup.23.5/resource
Copying fingerprint files to /opt/IBM/cobalt/setup.23.5/resource/fingerprint
Copying entrypoint shasum files to /opt/IBM/cobalt/setup.23.5/resource/chef_client_sha256
Copying entrypoint shasum files to /opt/IBM/cobalt/setup.23.5/resource/sla_client_sha256
exec(): 0509-036 Cannot load program /opt/IBM/cobalt/rubies/ruby-2.4.5/bin/ruby because of the following errors:
0509-150 Dependent module libgmp.a(libgmp.so.10) could not be loaded.
0509-022 Cannot load module libgmp.a(libgmp.so.10).
0509-026 System error: A file or directory in the path name does not exist.
```

Figure 101. Example Values for AIX Platform

13. Navigate to the extracted folder and start installation by running command. Enter the config file name in command screen and run the script to start the installation.

```
root@sjx64117ab:/tmp/sla-redhat.23.5 ×
[root@sjx64117ab sla-redhat.23.5]# pwd
/tmp/sla-redhat.23.5
[root@sjx64117ab sla-redhat.23.5]# ls -l
total 221272
drwxrwxr-x. 2  499  499       199 Mar  3 08:50 certs
-rw-r--r--. 1  499  499   1826450 Mar  3 08:50 chef_client_fingerprint
-rw-r--r--. 1  499  499       256 Mar  3 08:50 chef_client_fingerprint.sha256
drwxrwxr-x. 2  499  499        24 Mar  1 22:49 chef_client_sha256
-rw-rw-rw-. 1 root root      3147 Mar  4 03:43 citScanOutput.xml
-rw-r--r--. 1  499  499    387203 Mar  3 08:47 cookbook_fingerprint
-rw-r--r--. 1  499  499       256 Mar  3 08:47 cookbook_fingerprint.sha256
-rw-r--r--. 1 root root         0 Mar  4 03:43 dsmerror.log
-rw-r--r--. 1 root root       241 Mar  4 03:39 install_config
-rw-r--r--. 1  499  499      1019 Mar  3 08:50 sample_install_config
-rw-r--r--. 1  499  499 106547200 Mar  3 08:47 setup-23.5.tar
-rw-r--r--. 1  499  499        57 Mar  3 08:47 setup-23.5.tar.sha1sum
-rw-r--r--. 1  499  499        81 Mar  3 08:47 setup-23.5.tar.sha256sum
-rwxr-xr-x. 1  499  499      3684 Mar  3 08:50 setup.sh
-rw-r--r--. 1  499  499   4484966 Mar  3 08:47 sla_client_fingerprint
-rw-r--r--. 1  499  499       256 Mar  3 08:47 sla_client_fingerprint.sha256
drwxr-xr-x. 2  499  499       189 Mar  1 22:38 sla_client_sha256
-rw-r--r--. 1 root root 113295360 Mar  4 01:59 sla-redhat.23.5.tar
[root@sjx64117ab sla-redhat.23.5]# ./setup.sh -c install_config
```

Figure 102. Command Screen to Install

14. Once the script is successfully run, navigate to 'My servers' page in SLA UI. The server is marked as "Onboarded".

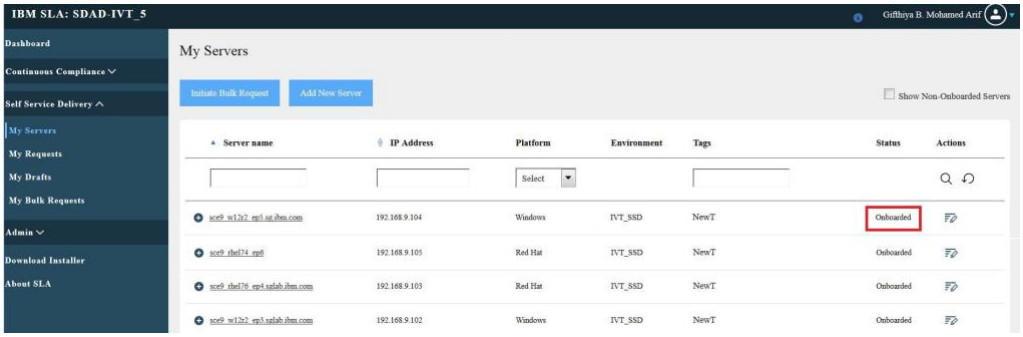


Figure 103. Server Onboarded

Note:

v Installation may get aborted if the server is not in whitelist.

v The above described steps are applicable for all the OS platforms.

15. If onboarding an endpoint through messaging services, you need not go through the entire server onboarding process for said servers via ProcessPortal. You will see the below notification when trying to onboard via ProcessPortal for the servers with messaging enabled.

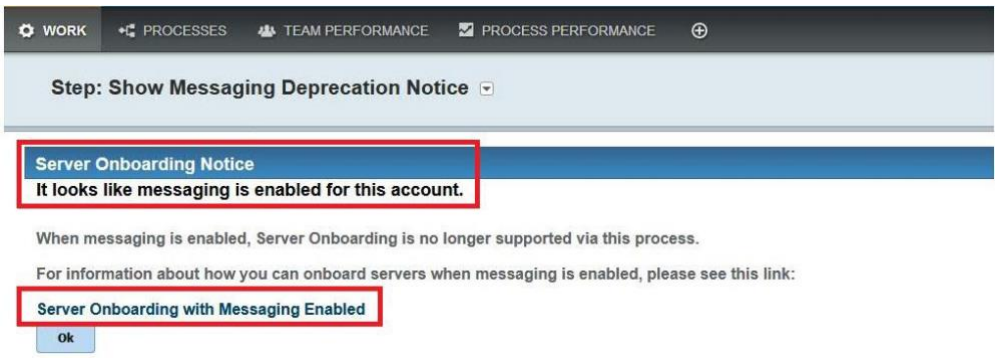


Figure 104. Server Onboarded

Installing SLA Client Using Same 'Batch' Name

You can install SLA Client Using same 'batch' name and successfully onboard a server in SLA UI.

1. You can onboard other endpoints of any platform with same batch name in install_config file.
2. Once the endpoint is onboarded through messaging model with the same batch name, click on 'My Bulk Requests' option under End Point Management in the left pane. My Bulk Requests screen appears with the endpoint bulk request details.

Figure 105. My Bulk Requests

3. 'Type' column value is displayed as '**<specified_batch_name>**'. For example, 'test batch 901' as displayed in the below image.

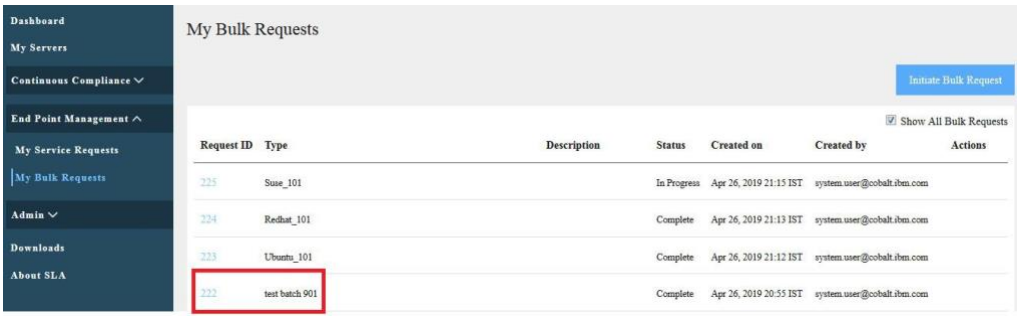


Figure 106. Same Batch Name

4. To view more details on the bulk request, click on the Request ID link and you will see the below screen with all the endpoint bundled together as one bulk request.
5. Click on "Download all reports" link to export and view the bulk request details.

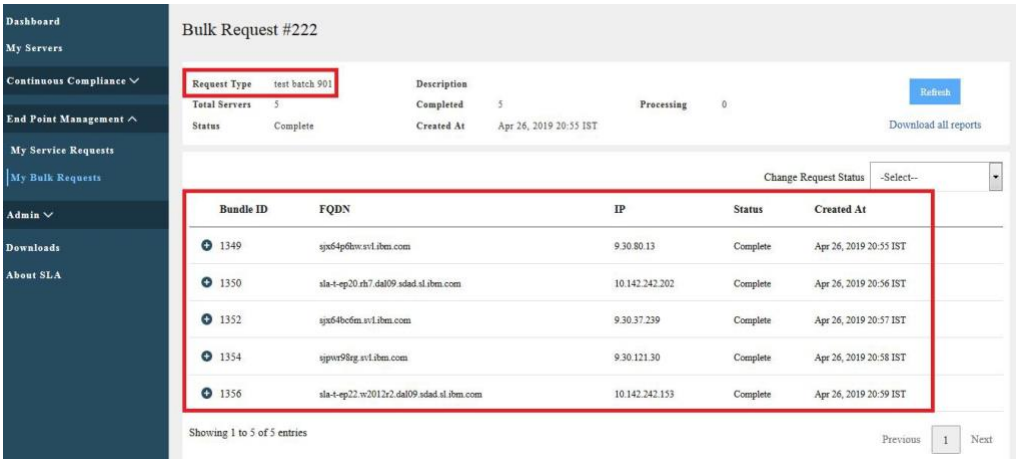


Figure 107. Bulk Requests Details

Installing SLA Client Using Different 'Batch' Name

You can install SLA Client using different 'batch' name other than the name mentioned in install_config file and successfully onboard a server in SLA UI.

1. You can onboard other endpoints of any platform with different batch name other than the name mentioned in install_config file.
2. Once the endpoint is onboarded through messaging model with the different batch name, click on 'My Bulk Requests' option under End Point Management. My Bulk Requests screen appears with the endpoint bulk request details.

Figure 108. My Bulk Requests Option

3. Different requests IDs are created for onboarded endpoints. Below is an example of different batch name.

Figure 109. Different Batch Name

4. To view more details on the bulk request, click on the Request ID link and you will see the below screen with the specific endpoint details.
5. Click on "Download all reports" link to export and view the bulk request details.

Figure 110. Bulk Requests Details

Validate the Endpoint and Config File before Onboarding

A PowerShell script on Window, and a Perl script on Linux/AIX are provided as a mean to validate and detect potential issues before and actual run of the installation. No change to endpoint will be made by that script.

It is a prerequisite to have Perl available on Linux/AIX endpoints to utilize this feature.

1. In the "CC Enhanced UI" page, click 'Downloads' in the left navigation panel and select 'Download Validation Script'.

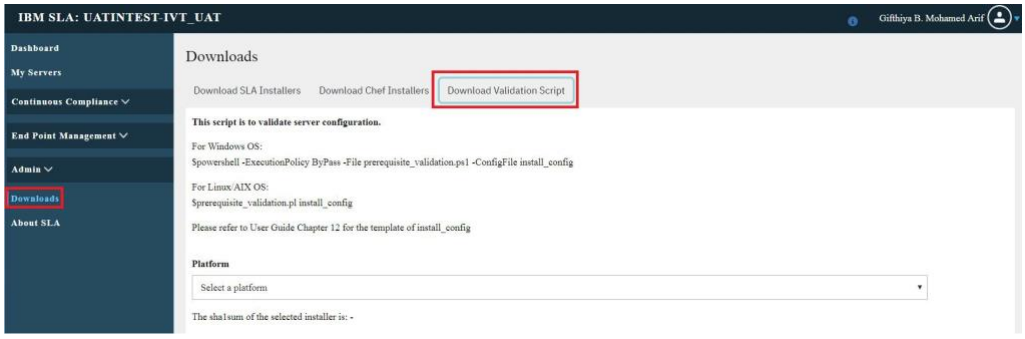


Figure 111. SLA UI → CC Enhance UI → Download →Download Validation Script

2. Select the platform on which you would run the validation script and click 'Download'.

   Note: The validation scripts are different for Windows/ Linux/ AIX and could not be used interchangeably.

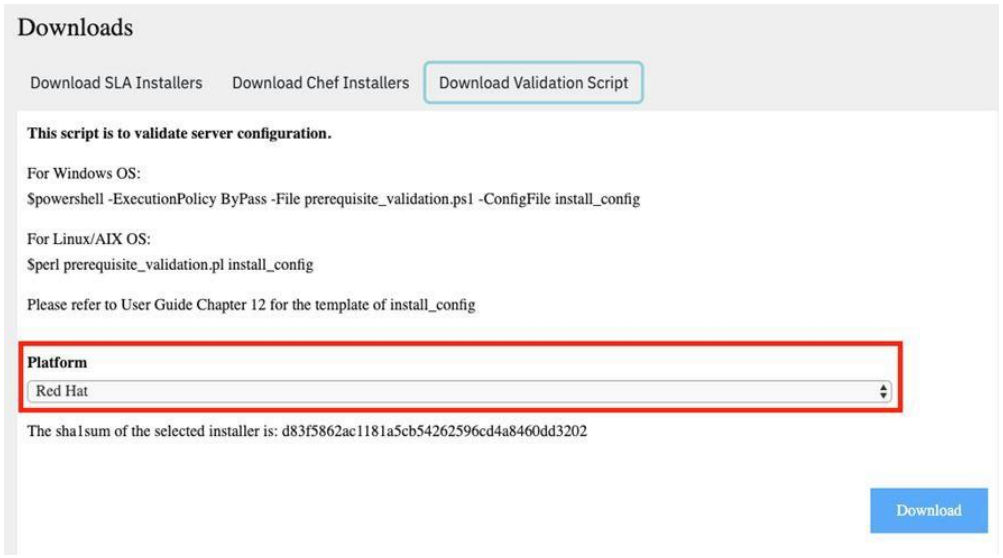


Figure 112. Select Platform for Validation

3. The sha1sum of the installer will be displayed on the UI, which could be used to validate the integrity of the downloaded file.

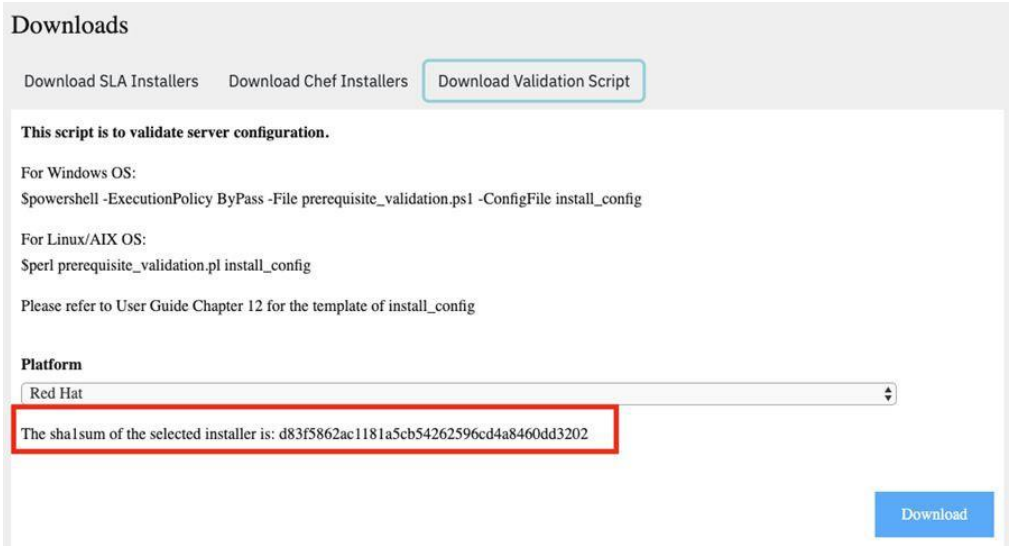


Figure 113. Sha1sum of the Selected Installer

4. Copy the validation script to the target endpoint.
5. Run the below command to validate the endpoint and configuration file prepared in section "Download the SLA Client Installer" on page 101 (step 9).

   For Windows:

   `$powershell -ExecutionPolicy ByPass -File prerequisite_validation.ps1 -ConfigFile install_config`

   For Linux/AIX:

   `$perl prerequisite_validation.pl install_config`

   An output similar to below screenshot appears.

```
===== Prerequisite validation begin =====
Config loaded:
owner => automate
account_gcsc => example
timezone => America/New_York
kafka_ip => 1.1.1.200
fqdn => myredhatserver.example.com
group => automate
batch => test_batch_1
network_name => n1
platform => redhat
ipaddress => 1.1.1.2
kafka_url => something.sdad.sl.ibm.com:9093
Check config entries: PASS
All mandatory config entries are defined

Check platform: PASS
Platform value: redhat is valid

Check timezone: PASS
Timezone value: America/New_York is valid

CHECK Available space on /opt/IBM/cobalt: PASS
/opt/IBM/cobalt has recommended minimum free space of 5 GB. 35.2051 GB free space is available

CHECK Available Memory: PASS
Available Memory : 32007 MB. Recommended memory 512 MB

CHECK Directory /tmp permission: PASS
/tmp is accessible
```

Figure 114. Validation Output

6. Examine the validation result, and fix if any issue found.

Setup the File Caching Server or Pre-stage the Chef Client Package (Optional)

Setup the File Caching Server or pre-stage the Chef Client package to reduce network traffic and speed up the installation the Chef Client package.

Performing the following steps will result in the faster onboarding process and the lesser onboarding failure. However, they are not mandatory and not performing them will not deter you from successful endpoint onboarding.

During the SLA Client installation, the installer will connect to the SLA Server to download the Chef Client, which is a separate component of the SLA solution. It may take a long time for SLA to copy the package to the endpoints and would incur additional network traffic. This may lead to the onboarding failure especially when there is a network bandwidth limitation in the environment. SLA provides two (2) options to optimize the onboarding process:

1. Setup a File Caching Server (FCS)

   A File Caching Server is an server setup in the client network that serves the required files. This will improve the performance because the traffic between the FCS and the endpoint needs to travel a shorter route, and sometimes it would even be in the same LAN, which would usually have much higher bandwidth. There are multiple ways to setup the FCS each provides different pros and cons. Refer to Appendix E, "Setting Up A File Caching Service (FCS)," on page 125 for more details on FCS.

2. Pre-stage the Chef Client package on endpoint

   Alternatively, the account could download and copy the Chef Client package to the endpoint before the installation.

   a. Download the Chef Client package

      The package could be downloaded from the SLA Enhanced UI by nagivating to the 'Downloads' page, select "Download Chef Installers", and choose the respective platform on which you would want to install SLA Client.

      Note: The package for each platform is different and could not be used interchangeably. The sha1sum of the package is shown on the UI which can be used to validate the integrity of the downloaded file.

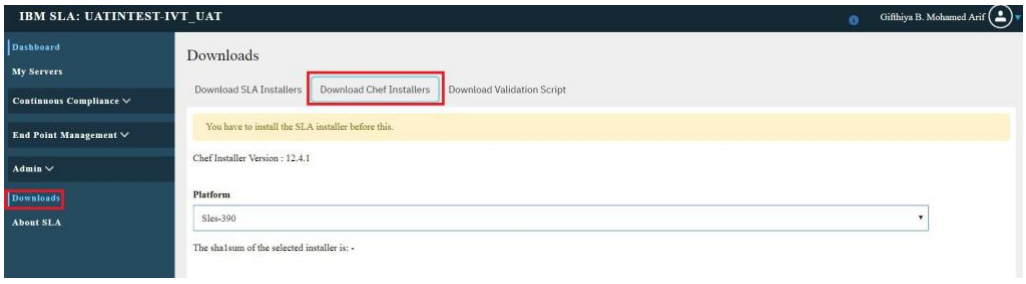


Figure 115. My Servers

   b. Copy the package to the target endpoint

      The Chef Client package need to be placed in the below directory:

      Windows: **`C:\temp\chef\`**

      Linux/ AIX:**`/tmp/chef`**

Any additional automation tool could be used to facilitate this step.

Install SLA Client

Once all the prerequisites and validations are completed, the endpoint could be onboarded anytime by logging on to the endpoint and run the below command:

1. Windows
   - v Run the installer as member of Local Administrators group
   - v **<installer_extract_dir>\setup.bat-c <path\config_file>**
2. Linux/AIX
   - v Run the installer as root or with appropriate sudo (or other) privileges on Linux / AIX
   - v **<installer_extract_dir>/setup.sh -c<path/config_file>**

Verify the SLA Client Installation

Once the setup is completed successfully, below steps could be performed to validate the installation status. All the checks should pass, otherwise further investigation should be performed.

1. **On Endpoint:**

   Once the installation is finished successfully, below steps could be performed to validate the Service/ Daemon process is running:

   - v Windows: Open the 'Service' tool and ensure a new service called 'SLA Client' is running.

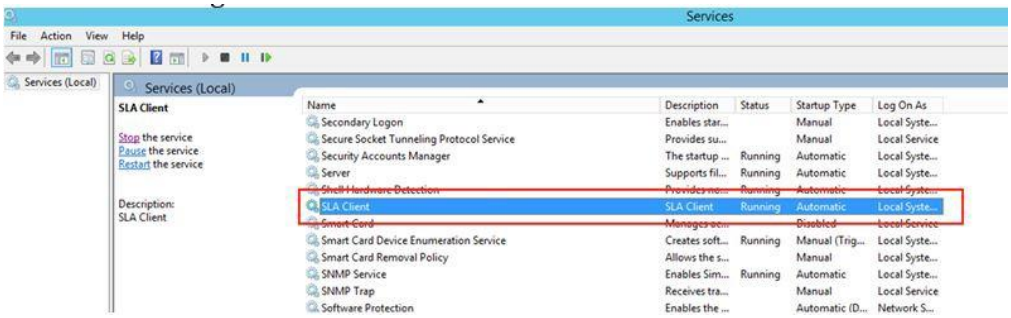


Figure 116. SLA Client in Service Tool

   - v Linux/ AIX: Use 'ps' or the below command to verify /opt/IBM/cobalt/sla/messenger/bin/sla-client is being run by a Ruby process.

```
AIX 7.1 - Technology Level 0 - Service Pack 10
# ps -ef | grep sla
    root 5636320 6357134   0 10:41:34  pts/0  0:00 grep sla
automate 6750214       1   0   Apr 04      -  3:19 /opt/IBM/cobalt/rubies/ruby-2.4.5/bin/ruby /opt/IBM/
cobalt/sla/messenger/bin/sla-client -d --pid /opt/IBM/cobalt/sla_client.pid -c /opt/IBM/cobalt/sla/sla_
config.yml
#
```

Figure 117. SLA Client Run by Ruby Process

2. **On SLA Enhanced UI:**
   a. **Check Server Status (via SLAUI)**
      1) Navigate to 'My Servers' page, and validate the target server is in 'Onboarded' status.

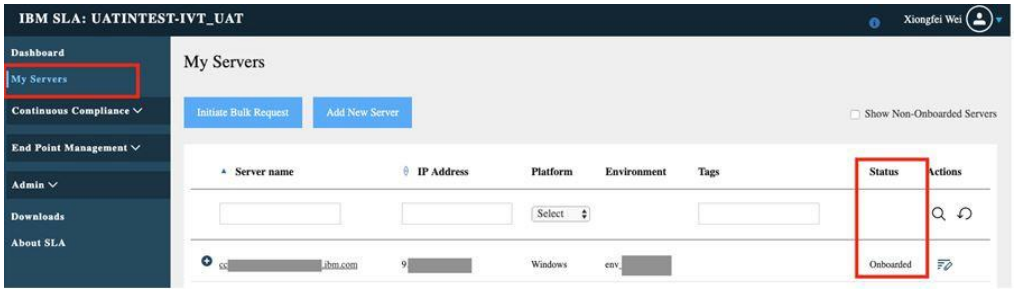


Figure 118. Server Status through SLAUI

b. Check Initial Inspection Run Status (via SLAUI)

1) Once the server is marked as 'Onboarded', a "Server Compliance" task will be triggered in a few minutes. Refer to "CC User Guide, **Chapter 7: Server Inspection.**

2) Click the respective server name in 'My Servers' page to track the task status.

3) Check the entry in 'Pending Requests' and 'Request History' tab.

The task will initially appears in 'Pending Requests' tab once it is created and while it's executing.

The request moves to 'Request History' after the execution.

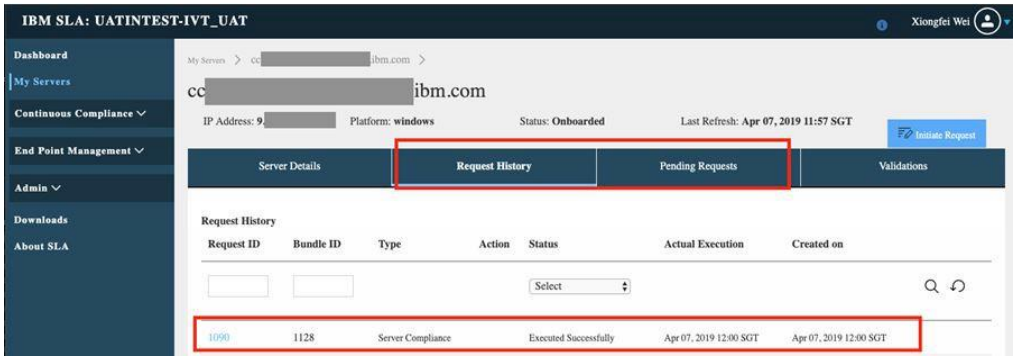


Figure 119. Initial Inspection Run Status through SLAUI

c. Check Initial Inspection Report after Inspection Run Completes (via SLAUI)

Once the "Server Compliance" task is completed, the Initial Inspection Report will appear in "Server Overrides" page as shown in screenshot below. Refer to "CC User Guide, Chapter 7: Server Inspection to find more about the Inspection Run and about how to interpret the report.

Figure 120. Initial Inspection Report after Inspection Run

Post-Onboarding Scripts

Once the server onboarding via messaging is completed, run the below scripts to collect all the files required for debug, if endpoint is not reachable via EE or Kafka is down.

1. Navigate to SLA UI → Downloads → Download Validation Scripts. You will see the below screen providing the scripts to run on different platforms.
   a. Windows: start Powershell and execute command:

      powershell -ExecutionPolicy ByPass -File prerequisite_validation.ps1

   b. Linux/AIX: at command line and execute command:

      perl prerequisite_validation.pl

   A file named "validation_[start_time].tar.gz" contains gathered debug information will be created under:

   a. Windows: C:\IBM\cobalt\
   b. Linux/AIX: /opt/IBM/cobalt/

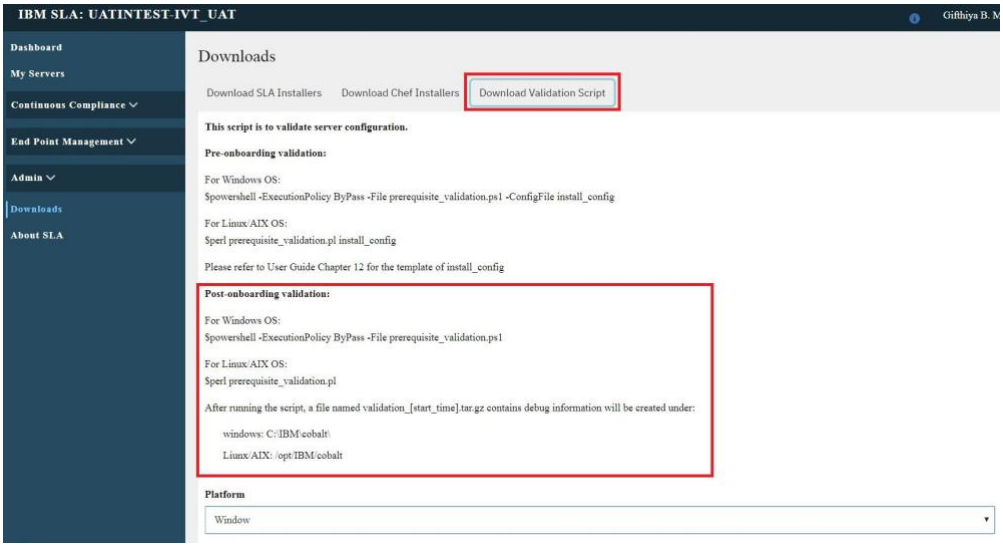


Figure 121. Download Validation Script

Serviceability

Chef upgrade on all prod endpoints and perform a symlink based approach, similar to the SLA Client.

Refactor Folder Structure of Chef 12.12.13.2 to make use of sym-link referencing a version chef. This makes management/ upgrading chef easier, and more consistent with the current deployment of SLA components.

Main Changes to Endpoint, Chef application and configuration are not symbolic linked to versioned chef.

Below are the examples:

```
drwxr-xr-x.  3 automate automate   24 Apr  8 02:43 rubies
-rw-r--r--.  1 automate automate    0 Apr  8 02:45 install_lock
drwxr-xr-x. 14 automate automate 4096 Apr  8 02:45 setup.24.2
-rw-r--r--.  1 automate automate    0 Apr  8 20:16 registration_lock
drwxr-xr-x.  4 automate automate   39 Apr  8 20:23 config
drwxr-xr-x.  4 automate automate   29 Apr  8 21:41 var
drwxr-xr-x.  7 automate automate   98 Apr  8 22:48 chef.12.12.13.2
drwxr-xr-x.  7 automate automate   98 Apr  8 22:57 chef.12.12.13.3
lrwxrwxrwx.  1 automate automate   35 Apr  8 23:36 bin -> /opt/IBM/cobalt/chef.12.12.13.3/bin
lrwxrwxrwx.  1 automate automate   39 Apr  8 23:36 include -> /opt/IBM/cobalt/chef.12.12.13.3/incl
lrwxrwxrwx.  1 automate automate   55 Apr  8 23:36 sla_chef_client_version -> /opt/IBM/cobalt/chef
lrwxrwxrwx.  1 automate automate   24 Apr  8 23:36 sla -> /opt/IBM/cobalt/sla.24.2
lrwxrwxrwx.  1 automate automate   37 Apr  8 23:36 share -> /opt/IBM/cobalt/chef.12.12.13.3/share
lrwxrwxrwx.  1 automate automate   35 Apr  8 23:36 lib -> /opt/IBM/cobalt/chef.12.12.13.3/lib
lrwxrwxrwx.  1 automate automate   35 Apr  8 23:36 etc -> /opt/IBM/cobalt/chef.12.12.13.3/etc
drwxr-xr-x.  9 automate automate 4096 Apr  8 23:36 sla.24.2
```

Repo Affected

sla-client-setup

v chef.rb

v installer.rb

v cli.rb

sla-client-manager

v version.rb

ccssd-core

v - xeng.rake

ccssd-resource

v 12.13.13.3 tar ball and zip

Scenarios : Fresh Installation

Before Setup

v No Chef installed

After Setup

v Chef 12.13.13.3 installed, and symbolic linked

Setup Failed

Scenarios : Upgrade from existing older sla version, for example 23.5 or 23.2 or no SLA

Before Setup

v Chef 12.4.1 or Chef 12.12.13.1 or Chef 12.12.13.2 Installed

After Setup

v Chef 12.13.13.3 installed, and symbolic linked

v Previous Chef is backuped into their respective versioned folder.
  For example chef.12.13.13.2

Setup Failed

v Chef 12.13.13.2 restored, base on best effort basis

v Chef Config Restored

Scenarios : Rerunning same setup again

Before Setup

v Chef 12.13.13.3

After Setup

v Chef 12.13.13.3 installed, and symbolic linked

Setup Failed

v No changes, Chef 12.13.13.3 installed, and symbolic linked

Appendix A. CC Policies Documentation and Source Code Reference

A read-only version of CC policies documentation and source code is available for the user's reference. All CC cookbooks are now available on git repository. Follow the instruction on the **CC Policies Documentation and Source Code** page on the global support wiki to log on to the git repository to view the CC policies documentation and source code.

For detailed information on CC policy for Oracle Database support, refer to the Oracle Policy User guide on **Continuous Compliance (CC) Oracle Policy User Guide**

For detailed information on CC policy for WebSphere Application support, refer to the WAS Policy User Guide on **Continuous Compliance (CC) WebSphere Application Server (WAS) Policy User Guide**

For detailed information on CC policy for MS SQL support, refer to the MS SQL Policy User Guide on **Continuous Compliance (CC) MS SQL Policy User Guide**

Appendix B. Information on how SLA Manages the Onboarding Password

This section will provide you with the information on how SLA manages the onboarding and steady-state passwords as well as the password related work flow of onboarding and offboarding a server.

1. Server Group Password
   - v Assume you have a server group "G1" with credential type "windows_local" and the password for automate id is "PWA".
   - v The password, PWA, is stored in a safe vault. No one except the person who set the value knows the password.
2. Preparing Endpoints for Onboarding
   - v Before onboarding endpoints A, B and C to server group G1, set the password of the "automate" id in the endpoints to "OBD_PASS".
   - v OBD_PASS is onboarding password. It is a configuration item in SLA.
   - v If you want to change the value of OBD_PASS, you can go through SLA support to set it to a new value. And then set the new onboarding password value to automate id of the endpoints to be onboarded.
3. Onboarding Endpoints
   - v During onboarding of endpoint A, B and C, SLA uses OBD_PASS to authenticate the endpoints to install SLA client.
   - v Once SLA client is installed and configured properly, SLA update the automate id's password in endpoint A, B and C to server group G1's password, which is PWA.
4. Normal Authentication Flow after Onboarding
   - v You now have a server group G1 with the password PWA and endpoints A, B and C with the password PWA.
   - v SLA now uses PWA to authenticate the endpoints A, B and C.
5. Scenarios that SLA will change password on endpoints

   After password A, B and C are successfully onboarded, there are **two scenarios** in which SLA will change the endpoint password.

   a. If your account is set to get password auto-update, SLA will update the password of the automate id in all endpoints at a regular preset interval.

      The password auto-update will be triggered only if at least one endpoint under the same server group, for example endpoint A under server group G1, is in Enforcement or Inspection mode and its password is expiring soon.

      In that case, SLA will generate a new random password, for example "PWC", and reset the password of the automate id in all endpoints under G1, endpoint A, B and C in this case, to PWC.

      This process will happen in the following sequence.

      - v SLA uses PWA to access endpoints.
      - v SLA updates the passwords in endpoints to PWC.
      - v SLA set server group G1's password to PWC.
      - v From then on, SLA will use PWC to access endpoints

      For more information on password auto-update, see “Windows Endpoint Password Auto Update to Support Password Expiration Rule” on page 52.

b. If an endpoint, for example endpoint A, is to be offboarded, SLA will update the password of the automate id in endpoint A.

   This process will happen in the following sequence.

   - Assuming that scenario 5a has not happened yet, SLA uses PWA to access endpoint A.
   - SLA removes SLA Clients in endpoint A.
   - Once cleanup is done, SLA reset endpoint A's password to OBD_PASS.

The prerequisites for aforementioned work flow are as follows.

- Manage Windows local account password is enabled. (EE config COBALT_MANAGE_PASSWORD_WINDOWS_LOCAL is set to true)
- Windows local account onboarding password is set.

Important:

- For endpoints in statuses 'pre-boarding', 'onboarding', 'onboarding aborted' and 'offboarded', SLA uses OBD_PASS (onboarding password) to access the endpoints.
- For endpoints in statuses 'onboarded' and 'offboarding', SLA uses the password set in endpoint's server group (steady-state password) to access the endpoints.
- All endpoints in the same server group must have same automate id password.
- Changing the password of a server group through the "Server Group Management" option only changes the password stored by SLA. It does not sync the new password to the servers under the server group. You must make sure password of all the servers under the same server group are updated to the new value by making necessary manual password updates in each endpoint.

Appendix C. CC_Policy_Enforcer Compliance Profile

In previous versions of the SLA solution, the Account Security Focal would need to reference the release notes of each policy to understand and manage each individual policy version and what they do to decide on which policy version to run. New in this release, the ASF will create an environment and associate a release level with it. This release level will contain all of the versions of the policies that will be required to bring the managed servers into security compliance.

How is it determined which policies will be part of a release level? A policy hierarchy has been developed in which each policy level will specify the versions of policies that it depends upon. Any policy that is prefixed with cc_ is considered a "wrapper" policy whose purpose is to contain details about the policies it references.

cc_policy_enforcement profile: At the top-level of the hierarchy will be the cc_policy_enforcement profile. This is the profile that contains the logic to determine what is installed on a box and run the appropriate policies. It will contain a list of "component policies" that it depends upon and their specific versions. This profile serves as the "Release Manifest". The version number on this profile will be kept in sync with each release. This profile should be specified when a server is onboarded to the solution.

The version of cc_policy_enforcer that gets executed will depend upon the version associated to the environment that this server belongs to. Once that is established, then the individual policy versions that ultimately get executed will be governed by the hierarchy and versions contained within a release.

If the customer has created a custom compliance profile and assigned it to a managed server, then that profile will contain the cc_policy_enforcer role in its runlist, and thus the version hierarchy will be inherited. Any policy attribute overrides or customizations associated with the compliance profile would actually be stored as attributes of this custom compliance profile.

A managed server must have either cc_policy_enforcer profile in its runlist OR a custom compliance role that contains the cc_policy_enforcer profile in its runlist.

Component Policy: A “component policy" is a wrapper policy that is used to group together all policies related to a software "component". Examples of a "component" would include an Operating System such as Linux or some other middleware software such as MySQL. The "component policy" will contain a list of "policy metadata policies" that it depends upon along with their specific versions.

Policy Metadata Policy: A "policy metadata policy" is a wrapper policy that is used to store metadata about a "policy". The metadata stored in these policies is used to describe the policy and the attributes that can be customized within a policy. The "policy metadata policy" will contain a reference to the "policy" that it wraps and its specific version.

Policy: A "policy" contains the actual implementation of the logic necessary to enforce a policy and the default attributes that are used when enforcing it. These policies may come from a variety of sources (e.g. ASCE, open source community

etc). Each "policy" will have a version number. The version number will be dependent upon the group or organization that is contributing the policy.

Appendix D. Valid Timezone Values In Install Configuration File

Etc/UTC	Asia/Baku	Asia/Tokyo	Europe/Madrid
Africa/Algiers	Asia/Bangkok	Asia/Tokyo	Europe/Minsk
Africa/Cairo	Asia/Bangkok	Asia/Ulaanbaatar	Europe/Moscow
Africa/Casablanca	Asia/Chongqing	Asia/Urumqi	Europe/Moscow
Africa/Harare	Asia/Colombo	Asia/Vladivostok	Europe/Paris
Africa/Johannesburg	Asia/Dhaka	Asia/Yakutsk	Europe/Prague
Africa/Monrovia	Asia/Dhaka	Asia/Yekaterinburg	Europe/Riga
Africa/Nairobi	Asia/Hong_Kong	Asia/Yerevan	Europe/Rome
America/Argentina/Buenos_Aires	Asia/Irkutsk	Atlantic/Azores	Europe/Samara
America/Bogota	Asia/Jakarta	Atlantic/Cape_Verde	Europe/Sarajevo
America/Caracas	Asia/Jerusalem	Atlantic/South_Georgia	Europe/Skopje
America/Chicago	Asia/Kabul	Australia/Adelaide	Europe/Sofia
America/Chihuahua	Asia/Kamchatka	Australia/Brisbane	Europe/Stockholm
America/Denver	Asia/Karachi	Australia/Darwin	Europe/Tallinn
America/Godthab	Asia/Karachi	Australia/Hobart	Europe/Vienna
America/Guatemala	Asia/Kathmandu	Australia/Melbourne	Europe/Vilnius
America/Guyana	Asia/Kolkata	Australia/Melbourne	Europe/Volgograd
America/Halifax	Asia/Kolkata	Australia/Perth	Europe/Warsaw
America/Indiana/Indianapolis	Asia/Kolkata	Australia/Sydney	Europe/Zagreb
America/Juneau	Asia/Kolkata	Europe/Amsterdam	Pacific/Apia
America/La_Paz	Asia/Krasnoyarsk	Europe/Athens	Pacific/Auckland
America/Lima	Asia/Kuala_Lumpur	Europe/Belgrade	Pacific/Auckland
America/Lima	Asia/Kuwait	Europe/Berlin	Pacific/Chatham
America/Los_Angeles	Asia/Magadan	Europe/Berlin	Pacific/Fakaofo
America/Mazatlan	Asia/Muscat	Europe/Bratislava	Pacific/Fiji
America/Mexico_City	Asia/Muscat	Europe/Brussels	Pacific/Guadalcanal
America/Mexico_City	Asia/Novosibirsk	Europe/Bucharest	Pacific/Guam
America/Monterrey	Asia/Rangoon	Europe/Budapest	Pacific/Honolulu
America/Montevideo	Asia/Riyadh	Europe/Copenhagen	Pacific/Majuro
America/New_York	Asia/Seoul	Europe/Dublin	Pacific/Midway
America/Phoenix	Asia/Shanghai	Europe/Helsinki	Pacific/Midway
America/Regina	Asia/Singapore	Europe/Istanbul	Pacific/Noumea
America/Santiago	Asia/Srednekolymsk	Europe/Kaliningrad	Pacific/Pago_Pago
America/Sao_Paulo	Asia/Taipei	Europe/Kiev	Pacific/Port_Moresby
America/St_Johns	Asia/Tashkent	Europe/Lisbon	Pacific/Tongatapu
America/Tijuana	Asia/Tbilisi	Europe/Ljubljana	
Asia/Almaty	Asia/Tehran	Europe/London	
Asia/Baghdad	Asia/Tokyo	Europe/London	

Figure 122. Valid Timezone Values

Appendix E. Setting Up A File Caching Service (FCS)

There are two (2) options to deploy the File Caching Server:

1. A plain HTTP/HTTPS static file server, in which user will put the new packages after every package release
2. A http server that is configured as a File Caching (Proxy) Server with direct connection to SLA's EE server in backend – Same solution as the current Nginx installed on SASg.

Deploy A plain HTTP/HTTPS (static) file server

Reusing an existing http server as the plain HTTP/HTTPS (static) file server. This process is applicable for Account Team.

When using an existing http server, the following requirement must be met:

1. The File Caching Server need to be a http/https server that servers the required files.
2. The artifact repository URL / file path need to meet below standard:
   a. The final download URL will be in the format <artifact repository URL>/<SLA predefined sub-path>/<SLA predefined filename>
   b. The <artifact repository URL> could be any path with http/https protocol, e.g. https://my.cache.server:9043/parent/path
   c. The <SLA predefined sub-path> are predefined path by SLA, e.g. /shared/. SLA may change that path or add additional paths for different purpose with advance notice
   d. The <SLA predefined filename> would be same file name as the file downloaded from SLAUI's 'Download' page, and would be the actual file name to be downloaded, e.g. chef-client-cobalt-12.12.13.2-win.zip. For this example, the final download path would be **`https://my.cache.server:9043/parent/path/shared/chef-client-cobalt-12.12.13.2-win.zip`**
3. In case a http server is provided, no connection verification will be performed
4. In case a https server is provided,
   a. the FCS need to be accessed using FQDN. The FQDN must match the CN of the https certificate.
   b. create a SR ticket, assign to Ops team, to request upload the https certificate to EE, and repack the SLA installer:
      1) Get the https certificate, and name it as **fcs_cert.pem**
      2) Attach **fcs_cert.pem** in the SR ticket
5. You will need to download updated sla installers from SLAUI installer download page to install on new endpoints
6. Artifact repository URL need to be configured on Server Group Management page.

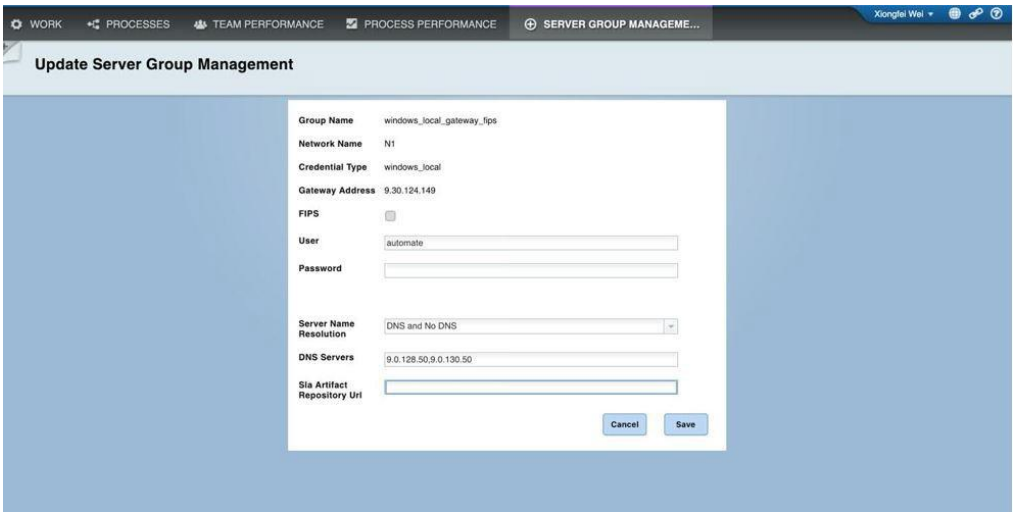


Figure 123. Artifact Repository - Static File Server

7. Download all the chef clients from SLAUI Chef Client download page, and copy into the corresponding path of the File Caching Server.
   a. This step needs to be done again when there is new release of chef client.

Setup for Plain HTTP/HTTPS Static File Server

Prerequisites

1. Server: Nginx 1.12.2 or newer can be installed on the server. Recommended: RHEL 7.4 or newer.
2. The server need to be accessed using FQDN. The FQDN must match the CN of the https certificate.

Setup Steps (Based on RHEL7.4)

1. Upload the staging.zip to the designated File Caching Server and unzip it.
2. Connect to the File Caching Server as an admin or sudo user.
3. Go to the folder where staging.zip is unzipped and make sure the following files exist in that folder:
   a. generate_keys.sh
   b. nginx.conf
   c. sla_staging.conf
4. Install nginx on the server:

```
sudo yum install epel-release
sudo yum install nginx
```

5. Start nginx and add firewall rule

```
sudo systemctl start nginx
sudo firewall-cmd --permanent --zone=public --add-port=3333/tcp
```

6. Create SSL Certificate for nginx.

   Note:

   a. The CN of the SSL certificate must be the same as the hostname or FQDN to access the file caching server.
   b. By default, *generate_keys.sh* reads FQDN (using 'hostname -f') of the server and use that FQDN as the SSL certificate CN. You can provide a different FQDN to the script instead of using the default one.

```
chmod +x ./generate_keys.sh
```

c. To generate SSL certificate using the default FQDN:

```
./generate_keys.sh
```

d. To generate SSL certificate using a different FQDN. Please replace ***myhost.mydomain.com*** with the actual FQDN you want to use to access the file caching server.

```
./generate_keys.sh myhost.mydomain.com
sudo mkdir -p /etc/nginx/ssl/
sudo cp ./tmp/fcs_cert.* /etc/nginx/ssl/
```

7. Copy nginx configure files.

```
sudo cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.`date +"%Y%m%d%H%M%S"`
sudo cp ./nginx.conf /etc/nginx/
sudo cp ./sla_staging.conf /etc/nginx/conf.d/
```

8. Create folder /sasg/Nginx/www/shared/

```
sudo mkdir -p /sasg/Nginx/www/shared/
```

9. Go to SLAUI Chef Client Download page, download all the chef clients on the page, and copy into /sasg/Nginx/www/shared/ of the file caching server.

   Note: This step needs to be done again when there is new release of chef client.

10. Update folder permission

```
sudo chown -R nginx:nginx /sasg/Nginx/
```

11. Restart nginx

```
sudo systemctl restart nginx
```

12. Create a SR ticket, assign to Ops team, request to upload fcs_cert.pem to EE, and repack the SLA installer.
    a. Get **/etc/nginx/ssl/fcs_cert.pem** from the File Caching Server
    b. Attach **fcs_cert.pem** in the SR
13. Artifact repository URL need to be configured on Server Group Management page. The URL shall be https://[fcs_hostname]:3333

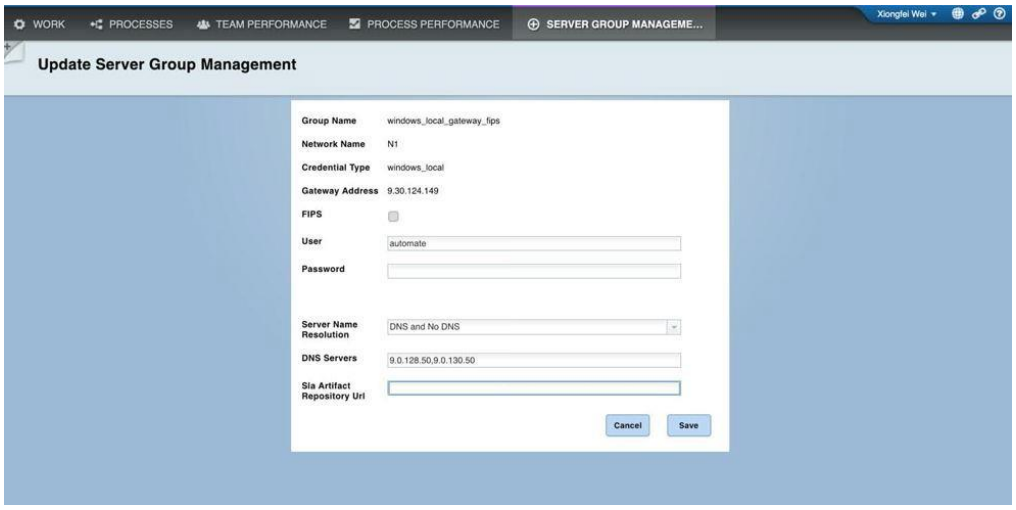


Figure 124. Artifact Repository URL on Server Group Management

14. The updated SLA installers need to be downloaded from SLAUI installer download page to install on new endpoints.

Reusing an Existing HTTP Server

When using an existing http server, the following requirement must be met:

1. The http server has the ability to be used as caching proxy server.
2. The file caching (proxy) server shall pass http requests to **`https://ee_host:3333`**
3. The cache size shall be set to 10G or larger
4. Chef client files shall be cached for 28 days
5. The artifact repository URL / file path need to meet below standard:
   a. The final download URL will be in the format <artifact repository URL>/<SLA predefined sub-path>/<SLA predefined filename>
   b. The <artifact repository URL> could be any path with http/https protocol, e.g. https://my.cache.server:9043/parent/path
   c. The <SLA predefined sub-path> are predefined path by SLA, e.g. /shared/. SLA may change that path or add additional paths for different purpose with advance notice
   d. The <SLA predefined filename> would be same file name as the file downloaded from SLAUI's 'Download' page, and would be the actual file name to be downloaded, e.g. chef-client-cobalt-12.12.13.2-win.zip. For this example, the final download path would be **`https://my.cache.server:9043/parent/path/shared/chef-client-cobalt-12.12.13.2-win.zip`**
6. In case a http server is provided, no connection verification will be performed
7. In case a https server is provided
   a. The FCS need to be accessed using FQDN. The FQDN must match the CN of the https certificate.
   b. Create a SR ticket, assign to Ops team, to request upload the https certificate to EE, and repack the SLA installer:
      1) Get the https certificate, and name it as **fcs_cert.pem**
      2) Attach **fcs_cert.pem** in the SR ticket
8. The updated sla installers need to be downloaded from SLAUI installer download page to install on new endpoints
9. Artifact repository URL need to be configured on Server Group Management page.

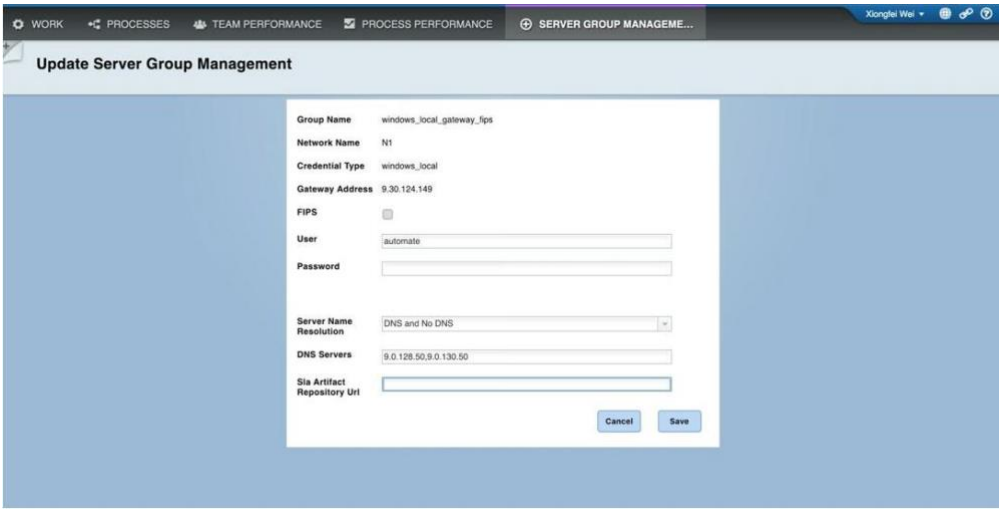


Figure 125. Artifact Repository - Reusing an existing HTTP server

Setup for File Caching (Proxy) Server

Prerequisites

1. Server: Nginx 1.12.2 or newer can be installed on the server. Recommended: RHEL 7.4 or newer.
2. The server need to be accessed using FQDN. The FQDN must match the CN of the https certificate.

Setup steps (Based on RHEL 7.4)

1. Upload the fcs.zip to the designated File Caching Server and unzip it.
2. Connect to the File Caching Server as an admin or sudo user.
3. Go to the folder where fcs.zip is unzipped and make sure the following files exist in that folder:
   a. generate_keys.sh
   b. nginx.conf
   c. sla_fcs.conf
4. Install nginx on the server:

```
sudo yum install epel-release
sudo yum install nginx
```

5. Start nginx and add firewall rule.

```
sudo systemctl start nginx
sudo firewall-cmd --permanent --zone=public --add-port=3333/tcp
```

6. Create SSL Certificate for nginx.

   Note:

   a. The CN of the SSL certificate must be the same as the hostname or FQDN to access the file caching server.
   b. By default, generate_keys.sh reads FQDN (using 'hostname -f') of the server and use that FQDN as the SSL certificate CN. You can provide a different FQDN to the script instead of using the default one.

```
chmod +x ./generate_keys.sh
```

   c. To generate SSL certificate using the default FQDN:

```
./generate_keys.sh
```

d. To generate SSL certificate using a different FQDN, replace ***myhost.mydomain.com*** with the actual FQDN you want to use to access the file caching server.

```
./generate_keys.sh myhost.mydomain.com
sudo mkdir -p /etc/nginx/ssl/
sudo cp ./tmp/fcs_cert.* /etc/nginx/ssl/
```

7. You need to update sla_fcs.confwith the actual EE IP.
8. Copy nginx configure files.

```
sudo cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.`date +"%Y%m%d%H%M%S"`
sudo cp ./nginx.conf /etc/nginx/
sudo cp ./sla_fcs.conf /etc/nginx/conf.d/
```

9. Create folder /sasg/Nginx/installer_cache.

```
sudo mkdir -p /sasg/Nginx/installer_cache
```

10. Update folder permission.

```
sudo chown -R nginx:nginx /sasg/Nginx/
```

11. Restart nginx.

```
sudo systemctl restart nginx
```

12. Create a SR ticket, assign to Ops team, request to upload fcs_cert.pem to EE, and repack the SLA installer.
    a. Get **/etc/nginx/ssl/fcs_cert.pem** from the File Caching Server
    b. Attach **fcs_cert.pem** in the SR
13. Artifact repository URL need to be configured on Server Group Management page. The URL shall be https://[fcs_hostname]:3333.

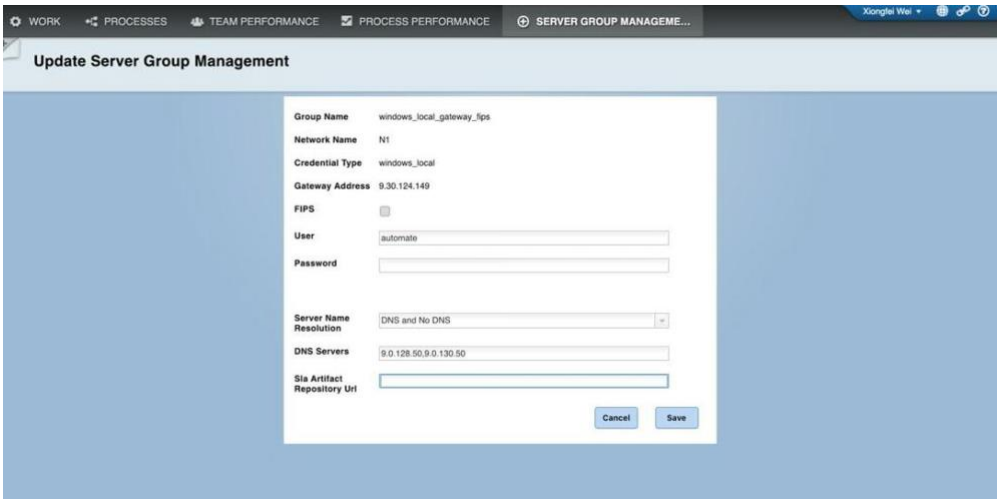


Figure 126. Artifact Repository - Proxy Server

14. The updated sla installers need to be download from SLAUI installer download page to install on new endpoints.

Alternatives for Deploying a File Caching Server

There is an alternative for deploying a File Caching Server.

User with System Admin or Onboarder role can download the SLA Instalelr and chef clients from SLAUI, download page. Once user downloads the files, they could use any of their automation process/tools to load the files into target folder

endpoints. During the Server Onboarding/Installation, the SLA installer will use the preloaded files instead of downloading them from a server.

1. The SLA Installer can be put into any directory for execution
2. The SLA custom Chef client need to be placed in C:\temp\chef folder for Windows, /tmp/chef folder for *nix

Manual Copy File Caching Server SSL Certificate to Endpoint

The file caching server SSL certificate can also be copied to the endpoint manually.

Before onboarding the endpoint

Note: It is suggested to upload the certificate to EE, repack the SLA installer, and download the updated SLA installer.

1. Copy fcs_cert.pem to the endpoint
2. Put fcs_cert.pem under the sla installer **certs** directory

After onboarding the endpoint

1. Copy fcs_cert.pem to the endpoint
2. Put fcs_cert.pem to the following directory:
   a. Windows: C:\IBM\cobalt\config\trusted_certs\
   b. *nix: /opt/IBM/cobalt/config/trusted_certs/

Create PEM File with Multiple SSL Certificate

When there are more than one file caching servers in one EE environment, a PEM file contains SSL certificates from all file caching servers need to be created.

1. Create a plain text file name as **fcs_cert.pem**.
2. Copy the content of each file caching server SSL certificate into **fcs_cert.pem**, each certificate shall start with a new line.
3. You may also add comments before each certificate.
4. Save **fcs_cert.pem**
5. The content looks like the below provided image.

```
-----BEGIN CERTIFICATE-----
MIIIgjCCB2qgAwIBAgIIO25QodIIAGIwDQYJKoZIhvcNAQELBQAwVDELMAkGA1UE
........
W8yNRCttwlen3ZJeChHRpoigd1IeAQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDjTCCAnWgAwIBAgIJAOvs7sz81GBqMA0GCSqGSIb3DQEBCwUAMF0xEzARBgNV
........
hQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIGjTCCBXWgAwIBAgIQB1bcrVT4VnHncFBc5Ox0GDANBgkqhkiG9w0BAQsFADBg
........
ag==
-----END CERTIFICATE-----
```

Figure 127. Content Without Comments

```
fcs 01 cert
=====================
-----BEGIN CERTIFICATE-----
MIIIgjCCB2qgAwIBAgIIO25QodIIAGIwDQYJKoZIhvcNAQELBQAwVDELMAkGA1UE
........
W8yNRCttwlen3ZJeChHRpoigd1IeAQ==
-----END CERTIFICATE-----

srv grp 01 fcs cert
=====================
-----BEGIN CERTIFICATE-----
MIIDjTCCAnWgAwIBAgIJAOvs7sz81GBqMA0GCSqGSIb3DQEBCwUAMF0xEzARBgNV
........
hQ==
-----END CERTIFICATE-----

win srv grp fcs cert
=====================
-----BEGIN CERTIFICATE-----
MIIGjTCCBXWgAwIBAgIQB1bcrVT4VnHncFBc5Ox0GDANBgkqhkiG9w0BAQsFADBg
........
ag==
-----END CERTIFICATE-----
```

Figure 128. Content With Comments

Upload File Caching Server SSL Certificate to EE

Operation Team has to upload File Caching Server SSL Certificate to EE.

1. Get the SSL Certificate from Account team.
2. Copy the SSL certificate to the server that hosts EE container.
   a. name the SSL certificate as fcs_cert.pem
   b. put it under /usr/ccssd/ee/certs/
3. On the server that hosts EE container, run the following command to repack the sla installers.

   ```
   /usr/ccssd/ee/reconfig_ee.sh
   ```

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy,

modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM® Corp. and Quantum in the U.S. and other countries.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Glossary

change freeze schedule A period of time when changes cannot be made to a managed server.

change request A request to make a change on a managed server.

change window A period of time when changes can be made to a managed server.

compliance policy A specific policy that is enforced on a managed server managed by Continuous Compliance.

compliance profile A named set of policies. A profile contains a set of policies and policy attribute settings that can be associated with a managed server such that it defines the continuous compliance policies that will apply to that managed server.

environment A categorization of sets of machines. For example: Test Environment, Development Environment.

managed server A server that is managed by CC.

override An act of setting a policy attribute with a value that overrides the default policy attribute value. Overrides can be set at different levels such as Policy, Environment or Node level

policy attributes The attributes of compliance policies that specify policy values.

recipe See compliance policy.

user group A group of users that can be assigned to a user role.

user role An association between user group and the operations and processes a user under that user group can perform on CC.

Printed in USA