ZephyrTel

Service Gateway 5.1.2.0

Release Notes and Installation Instructions

Original filename: Service Gateway 5.1.2.0 Patch Release Notes.pdf

Generated on: 05/18/2020 10:37 AM

Contents

Introduction

This document describes the changes included in this patch to Service Gateway, along with the patch installation instructions. This patch can only be applied directly to version 5.1.1 of Service Gateway. Earlier versions must first be upgraded to 5.1.1.

Enhancements

The following new features and enhancements are included in this patch:

ZenDesk 1982975 - Protect automatic hw-fw creation through regex

A bug in a recent firmware version for a device resulted in a random UUID being sent as the new version number in the BOOT Inform message, but any subsequent Inform messages from that device had the correct firmware version from that point onward. The issue is that a new firmware record would be created in the database for each device that was upgraded.

To protect against this Service Gateway will now use a regular expression to blacklist version numbers. If an incoming version number matches this regular expression the firmware version is replaced with another constant value, so even if a new firmware record is created, only one new record is created regardless of the number of devices being processed.

To configure this functionality four new system preferences have been added, to define blacklists for both firmware versions as well as hardware revisions:

- Firmware Version Blacklist Regular Expression
- Firmware Version Blacklist Target Value
- Hardware Revision Blacklist Regular Expression
- Hardware Revision Blacklist Target Value

Note that all these preferences default to empty values. If the Regular Expression preference is empty, the versions will not be validated, and the previous functionality will be used. If the Regular Expression preferences have values defined, then the specified regular expression will be used to validate the version number. If the regular expression matches, then the version is blacklisted and will not be used. If a value is specified for the Target Value preference, that value will instead be used as the version number, and the processing will continue as before, meaning that a new firmware or hardware record will be created if it does not already exist. Note that if a version is blacklisted and no Target Value has been specified, a default version of 'Service.Gateway' will be used.

ZenDesk 2080268 - Associate a custom file type to a script template

It is now possible to specify a file type for a script file template. The default value, when a new script file template is created, is 'Configuration'.

Issues Addressed

The following issues have been addressed by this patch.

ZenDesk 2013550 - Missing index on nc_cpe column nc_cpe_remote_addr

The index has been added.

ZenDesk 2127584 - Account for user system locked for 30 minutes at user cache expiry

The custom Weblogic security provider would cache some users in order to reduce hits on the database. If the cache expired and there was a database error when trying to retrieve the new value and the maximum number of login failures happened during that time, the user would get locked out for the default 30 minutes by Weblogic.

The security provider has been updated to re-use the previously cached value if any database error occurs when the cached entry is expired.

ZenDesk 2127588 - Stopping one managed server causes the ACS to no longer send traffic to its cluster

The InitialContext was not being reinitialized on failover, resulting in the ACS server not reconnecting to the cluster when a managed server went down. The InitialContext is now reinitialized properly in failover situations.

ZenDesk 2130375 - WLST login goes through the SG security provider plugin

The custom Weblogic security module includes two components, and the solution to this issue is two-fold. First, only a configuration change was needed for the authentication module. The authentication providers listed in the Weblogic console had to be re-ordered to ensure that the custom authentication module was listed last. Also, both the built-in Weblogic provider as well as the custom Service Gateway provider needed to have their control flags set to 'SUFFICIENT'.

Secondly, the custom role mapping provider needed a code change, as all configured role mappers get invoked. A new property, EXEMPT_USERS, has been added to servicegateway.properties. It can contain a comma-delimited list of users who are exempt from the custom role mapper. This would typically be Weblogic console users. The list will default to the 'weblogic' user if the property is not specified. The custom role mapper will check this property first, and will only retrieve roles fromt the database for users who are not exempt.

ZenDesk 2140352 - compile method should replace servicegateway by sprtSgName in EJB names

The template processing has been updated to dynamically update the JNDI names for the configuration templates (stored in SPRT_SG_TC_PLUGIN.INSTANCE_CONF_JNDI) if the Service Gateway application name is anything other than the default value of 'servicegateway'.

ZenDesk 2140355 - timer job should replace servicegateway by sprtSgName in EJB names

The timer has been updated to dynamically update the JNDI names for the timer jobs (defined in servicegateway_timer.properties) if the Service Gateway application name is anything other than the default value of 'servicegateway'.

ZenDesk 2140381 - CSR firmware upgrade automatically retries after 5 minutes

Service Gateway was treating any timeout from the ACS API as a failed attempt to contact that ACS API, and would automatically try the next one in the list, if more than one was defined. This included any timeout imposed by Apache Tomcat *after* the connection with the ACS API had already been established.

The application has been updated with a configurable timeout (the default is 5000 milliseconds), and if a timeout with the ACS API occurs in less than that time, it is treated as the ACS API being offline, and the application will try the next one in the list, if any are defined. If the timeout happens after that time, then it is treated as a successful attempt to contact the ACS API, but the timeout was due to another reason. In this situation, the application does not use the next ACS API in the list. In this later case, an WARN level log message, as shown below, will be written to the application log file:

```
Connection with ACS API timed out after X milliseconds: <Exception Name>
```

This log message will show the actual time elapsed, as well as the exception that occurred, as a means to assist with tuning the timeout value.

A new Preference called "ACS API Offline Retry Timeout" has been added under the CWMP section of system preferences to configure this timeout value to your environment. The default value is 5000 ms.

ZenDesk 2147686 - TR-157 ChangeDUState wrongly implemented

The definition of the Operations element for the ChangeDUState RPC method was changed in TR-069 Amendment 5 to no longer be an array. The Service Gateway implementation for this RPC method has been updated to match the latest release of the specification (Amendment 6).

ZenDesk 2147827 - ACS warns for Unrecognized Inform EventCode:13 WAKEUP

The ACS was incorrectly looking for the string '13 WAKE UP' instead of '13 WAKEUP' for the list of known event codes. This has been corrected.

Patch Contents

In addition to this document, the patch includes the following files:

- packages/servicegateway-cwmp-5.1.2.0.011.tar.gz
- packages/servicegateway-integration.jar
- packages/servicegateway-jboss-5.1.2.0.011.tar.gz
- packages/servicegateway-openfire-5.1.2.0.011.tar.gz
- packages/servicegateway-stun-5.1.2.0.011.tar.gz
- packages/servicegateway-timer-5.1.2.0.011.tar.gz
- packages/servicegateway-weblogic-5.1.2.0.011.tar.gz
- packages/sprtWeblogicSecurityProviders.jar
- patch/sql/OracleDBChangesFrom5.1.1.0_DDL.sql
- patch/sql/OracleDBChangesFrom5.1.1.0_DML.sql
- patch/NewUIProperties.txt

These files will be updated in various locations to address the issues described above.

This patch updates the Service Gateway EAR file. Once this patch is applied to Service Gateway 5.1.1, the Service Gateway EAR file version will be:

- ServiceGateway 5.1.2.0.011

Additionally, the patch also includes the following directories which contain files required by the installer itself:

- bin
- configuration
- etc
- interface
- lib
- scripts
- sql
- utils

Before Upgrading

Backups

Regular backups of the database and file systems should be performed prior to performing an upgrade.

Installation Instructions

This patch is packaged with a web-based installer to ease the upgrade process. The installer is used in the same way as during a new install.

It is necessary to run the installer on all servers that make up the Service Gateway installation. This is so that the installer can update, at minimum, patch level information on each server.

Prior to upgrading any server, the ACS servers must be shut down and all user interface and EAI activity must cease.

Perform the upgrades to the Application Servers and Database Schema first. When patching a WebLogic clustered environment, the Admin server must be patched before any managed servers are patched. WebLogic servers must be running before the patch process can be started. Ensure that the WebLogic configuration is not locked.

Once the application servers and database schema have been successfully upgraded, proceed with the upgrade of each ACS server. The ACS upgrade will automatically restart the ACS.

The steps to upgrade each server are as follows:

1. Extract the contents of the patch archive to a temporary location.

2. Copy the JDBC driver for the database to the root directory of the extracted patch contents.

3. Enter the "bin" directory and start the run script appropriate to the operating system. run.bat for Windows, and run.sh for Solaris or Linux.

4. Under Windows, the default web browser is automatically launched and directed at http://localhost:8888/. On Solaris or Linux, a web browser must be launched from any computer on the network and directed at the installation site manually. The installer listens for HTTP connections on port 8888 of the server the installer is running on.

5. After accessing the installer web UI, select "Update an existing instance" and click "Next".

6. Once the target instance has been selected and the license agreement has been accepted, the patch prerequisite scripts will run. If they are all successful, clicking "Next" will start the upgrade process.

Troubleshooting and Manual Installation

If the installer fails for any reason, installer.log should be backed up to a safe location so that there is no loss of information needed to diagnose the problem and understand the current state of the application. This file should be sent to Aptean Technical Support for review. Manual patch and rollback instructions are available to Aptean technicians to assist in recovery from a failed upgrade.

Updated Service Gateway Integration JAR

The patch contains a new copy of servicegateway-integration.jar, which is used by all utilities that interface with Service Gateway. Any custom code or integration applications must be updated to use the new integration jar file.

New UI Properties for Translation

New UI properties have been added. These are already present in the EAR file that has been deployed, so no further action is required. However, if any translations have been created for the installation, the new tokens will need to be translated and added to the translated properties files. A list of the new tokens can be found in the NewUIProperties.txt file included with the upgrade package.

Database Changes

A new column, FILE_TYPE, has been added to the SPRT_SG_TCP_CWMPTEMPLATE_I table.

The column VALUE in the SPRT_EC_SYSTEM_PREF table had been made nullable.

Integration Interface Changes

There are no changes to the EAI Web Services in this release.