CyberRes

Troubleshooting SSC and Scancentral upgrade issues

Richard Pinaroc
Fortify Security Support Engineer
richard.pinaroc@microfocus.com

Topics

SSC upgrade

- Checking database collation
- SSC migration script
- Seed bundles
- Tomcat and Java version
- Logs

Scancentral upgrade

- Controller
- Sensors
- Clients
- Logs

Database Collation

Before any SSC upgrade, please make a FULL backup of the SSC database.

SSC database needs to be case sensitive and supported collations are documented in the SSC System Requirement guide. Many of the information that will be discussed today can be found in this document.

https://www.microfocus.com/documentation/fortify-software-security-center/

MySQL

```
SELECT default_character_set_name, default_collation_name FROM information_schema.schemata  WHERE schema_name = 'ssc';
+----------------------------+------------------------+
| default_character_set_name | default_collation_name |
+----------------------------+------------------------+
| latin1                     | latin1_general_cs      |
+----------------------------+------------------------+
```

Microsoft SQL Server

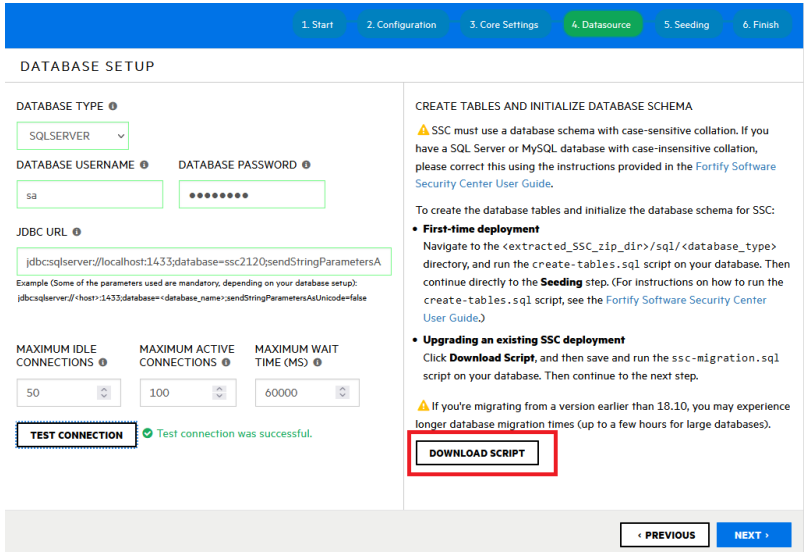
```
SELECT cast(name as varchar(10)) as Name, cast(collation_name as varchar(30)) as Collation FROM sys.databases WHERE name = 'ssc';

Name       Collation
---------- ------------------------------
ssc        SQL_Latin1_General_CP1_CS_AS
```

Oracle

```
SELECT @@character_set_database, @@collation_database;
```

SSC migration script

This script is generated under the Database Setup section by using the “DOWNLOAD SCRIPT” button. The generated ssc-migration.sql is uploaded to the database server machine which is then executed against the SSC database. This script updates the tables to the latest version.



If any error(s) occur please open a ticket with Fortify Technical Support and provide the ssc logs and ssc-migration.sql file. ***Do not continue or attempt to modify the script to get rid of error messages or try to install any seed bundles***.

Seeding

Always use the correct seed bundles that come with the latest version that are bundled with the SSC installation files.
Eg
SSC 21.2.x
Fortify_Process_Seed_Bundle-**2021_Q4_0001**.zip
Fortify_Report_Seed_Bundle-**2021_Q4_0001**.zip

SSC 20.2.x
Fortify_Process_Seed_Bundle-**2020_Q3_0002**.zip
Fortify_Report_Seed_Bundle-**2020_Q3_0002**.zip

When error occurs during the seeding stage, provide the SSC logs and the following SQL output to Fortify Technical Support.

```
select  * from seedhistory order by seedDate ASC;
```

Tomcat and Java version

SSC 18.10 - Tomcat 8 and Java 8
SSC 18.20-20.10 - Tomcat 9 and Java 8
SSC 20.2.x-21.2.x - Tomcat 9 and Java 11

SSC System Requirement guide can be found here,

https://www.microfocus.com/documentation/fortify-software-security-center/

Tomcat and Java version

Things to verify if Tomcat is running the correct Java version is to open Tomcat's Catalina log and look for the following lines,

16-May-2022 11:46:11.264 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Java Home: C:_Java\jdk-11.0.6
16-May-2022 11:46:11.264 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Version: 11.0.6+8-LTS

If Tomcat is running as a Windows service and the wrong Java version is used, the service needs to be recreated as the Java version is hard-coded in the Windows system registry.

1. Uninstall the Tomcat Wndows service

eg Tomcat\bin\service.bat" **remove** "<service_name>"

2. update the Windows JRE_HOME system environment variable to point to the correct Java home folder
eg JRE_HOME=path\java11

3. create the new Tomcat Windows service

eg Tomcat\bin\service.bat" **install** "<service_name>"

Logs to provide to Micro Focus

Provide the following logs,

- Tomcat **catalina.YYYY-MM-DD.log**
- **ssc.log** and **ssc_audit.log**
- For report related issues include the **ssc_birtrunner.log**
- For plugin, eg Jira Bug Tracker, related issues include the FORTIFY_HOME\ssc\plugin-framework\logs**plugin-framework.log**

For debugging other issues like email notification not working, LDAP or SAML configuration issues, the following can be added to FORTIFY_HOME\ssc\config\log4j.xml without restarting Tomcat.
Should be only used for debugging purposes as this will cause the ssc.log file size to grow quickly and the logs to rollover sooner.

Email notification issues:
<Logger name="org.springframework.web.servlet.DispatcherServlet" level="debug"/>

LDAP related issues:
<Logger name="com.fortify.manager.service.ldap" level="debug"/>
<Logger name="com.fortify.manager.security.ldap" level="debug"/>
<Logger name="com.fortify.manager.service.fulltext.LdapIndexHelper" level="debug"/>
<Logger name="com.fortify.manager.BLL.impl.LdapBLLImpl" level="debug"/>

SAML SSO related issue:
<Logger name="org.springframework.security.saml" level="debug"/>
<Logger name="org.opensaml" level="debug"/>
<Logger name="PROTOCOL_MESSAGE" level="debug”/>

Logs to provide to Micro Focus

To help debug 401 Access denied or permission related issues when using the REST API, the best way to see what token is being used is to show the token in Tomcat's user access log. ***This should only be done for debugging purposes as exposing the token in the log can be a security risk.***

This can be done by backing up and updating Tomcat\conf\server.xml and appending the string, eg "**%{Authorization}i**", to the pattern attribute for the AccessLogValve class name. Pay attention to the letter "**i**" at the end of the patter. A Tomcat restart will be required after making the change.
eg

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
        prefix="localhost_access_log" suffix=".txt"
        pattern="%h %l %u %t &amp;quot;%r&amp;quot; %s %b %{Authorization}i" />
```

The following output will be captured in Tomcat's localhost_access_log.YYYY-MM-DD.txt when using the REST API to login to SSC
Eg

```
127.0.0.1 - - [09/May/2022:10:36:58 -0600] "GET /ssc/api/v1/projectVersions?q=id%3A%2210001%22&start=0&limit=50 HTTP/1.1" 200 854 FortifyToken <token>
```

Scancentral

Controller

Before any upgrade, please backup the following Scancentral Controller folders and config file,

Fortify_ScanCentral_Controller_<ver>\tomcat**cloudCtrlDb**
Fortify_ScanCentral_Controller_<ver>\tomcat**jobFiles**
Fortify_ScanCentral_Controller_<ver>\tomcat\webapps\scancentral-ctrl\WEB-INF\classes**config.properties**

The Scancentral user guide says to upgrade the Controller before upgrading the clients, sensors, and SSC. **The Controller version needs to match the SSC version.**

The hardest part is merging the old config.properties with the new config.properties. As the new config.properties will have new property fields.

Controller

The steps to upgrade the Controller can be found the Scancentral user guide under the “About Upgrading ScanCentral SAST Components” section. The most basic upgrade is installing the latest Controller version and replacing the **cloudCtrlDb** and **jobFiles** folder and replacing the config.properties with the new merged copy.

Complex upgrade would be copying the old tomcat\conf\server.xml and configuring SSL.

More information in upgrading the Controller can be found in the Scancentral user guide.

https://www.microfocus.com/documentation/fortify-software-security-center/

Sensor

Sensor are easy to configure which is installing the latest SCA version and updating the credentials in the following properties,

Fortify_SCA_and_Apps_<ver>\Core\config\client.properties
Fortify_SCA_and_Apps_<ver>\Core\config\worker.properties

They should match the credentials set in the Controller's config.properties.
eg
worker shared secret, either plaintext password or password encoded by pwtool can be used
worker_auth_token=CHANGEME123!

client shared secret, either plaintext password or password encoded by pwtool can be used
client_auth_token=CHANGEME321!

client.properties

```
client_auth_token=CHANGEME321!
pwtool_keys_file=
```

worker.properties

```
worker_auth_token=CHANGEME123!
pwtool_keys_file=
```

Client

Upgrading the client is pretty simple by extracting the Fortify_ScanCentral_Client_<version>_x64.zip or if using the embedded client which is already bundled in the latest SCA version.

The latest Controller tomcat has a Scancentral client bundled under Tomcat\client folder. This zip file is used to update a scancentral client if the Controller's config.properties has client_auto_update property set to true.

eg client_auto_update=true

Any issues with the client should send the "**scancentral.log**" found under FORTIFY_HOME\scancentral-21.1.2\log folder.

More information on upgrading the client can be found in the Scancentral user guide.

Logs to provide to Micro Focus

Any issues related to Scancentral, provide the following logs,

- Controller's scancentralCtrl.log

- Client/Sensor scancentral.log (if using the latest 21.2.3 add –debug argument to get more information via the command line)
  eg scancentral –debug –url http://localhost:8282/scancentral-ctrl worker

- SSC logs eg ssc.log and ssc_audit.log (FPR upload issues)

- SCA logs (translation or scan issues)

- If using a plugin, eg Azure DevOps or Jenkins, include the job's output log. If using the AzureDevOps plugin, run the pipeline with "Enable system diagnostics" to get better debug output.

Thank you