[V8] FAQ: How to improve security of connection to AhsayCBS (Strong Cipher, TLS protocol and PFS)

Article ID: 8116
Reviewed: 2021-05-04

Product Version:
AhsayCBS: 8.1 to 8.x
OS: All platforms

Description

This article outlines how to improve security of connection to AhsayCBS by:

- Usage of strong cipher and TLS protocol
- Support of perfect forward secrecy (PFS)

Important: You can only perform the following steps if you DO NOT have any version 6 AhsayOBM / ACB client connecting to your CBS server.

Steps

Refer to the following steps for detail:

- **Change the TLS setting**:

  1. Browse to the following path on the AhsayCBS server:

     %CBS_Installation_Home%/conf

  2. Open the server.xml file with a text editor:

     server.xml

```
    …
    …
    <Connector maxKeepAliveRequests="9999"
keepAliveTimeout="30000" address="0.0.0.0" scheme="https"
enableLookups="false" socket.txBufSize="43800"
    connectionUploadTimeout="900000" acceptCount="200"
secure="true" URIEncoding="utf-8" sendReasonPhrase="true"
protocol="org.apache.
    maxHttpHeaderSize="8192" redirectPort="443"
executor="tomcatThreadPool-https-0.0.0.0-443"
disableUploadTimeout="false" coyote.
    http11.Http11NioProtocol" SSLEnabled="true" port="443"
socket.rxBufSize="25188" connectionTimeout="10000"
maxConnections="500">
        <SSLHostConfig disableCompression="true"
caCertificateFile="${catalina.base}/conf/ca.crt"
insecureRenegotiation="false"
        honorCipherOrder="false" ciphers="HIGH:!aNULL:!MD5"
disableSessionTickets="false"
protocols="+TLSv1+TLSv1.1+TLSv1.2"
        certificateVerification="false"
certificateVerificationDepth="10">
        …
```

3. Edit the line from

   protocols="TLSv1+TLSv1.1+TLSv1.2"

   to

   protocols="TLSv1.2":

   server.xml

```
    …
    …
    <Connector maxKeepAliveRequests="9999"
keepAliveTimeout="30000" address="0.0.0.0" scheme="https"
enableLookups="false" socket.txBufSize="43800"
    connectionUploadTimeout="900000" acceptCount="200"
secure="true" URIEncoding="utf-8" sendReasonPhrase="true"
protocol="org.apache.
    maxHttpHeaderSize="8192" redirectPort="443"
executor="tomcatThreadPool-https-0.0.0.0-443"
disableUploadTimeout="false" coyote.
    http11.Http11NioProtocol" SSLEnabled="true" port="443"
socket.rxBufSize="25188" connectionTimeout="10000"
maxConnections="500">
        <SSLHostConfig disableCompression="true"
caCertificateFile="${catalina.base}/conf/ca.crt"
insecureRenegotiation="false"
        honorCipherOrder="false" ciphers="HIGH:!aNULL:!MD5"
disableSessionTickets="false" protocols="TLSv1.2"
        certificateVerification="false"
certificateVerificationDepth="10">
        …
```

- **Change the cipher settings**:

1. Browse to the following path on the AhsayCBS server:

   %CBS_Installation_Home%/conf

2. Open the server.xml file with a text editor:

server.xml

```
    …
    …
    <Connector maxKeepAliveRequests="9999"
keepAliveTimeout="30000" address="0.0.0.0" scheme="https"
enableLookups="false" socket.txBufSize="43800"
    connectionUploadTimeout="900000" acceptCount="200"
secure="true" URIEncoding="utf-8" sendReasonPhrase="true"
protocol="org.apache.
    maxHttpHeaderSize="8192" redirectPort="443"
executor="tomcatThreadPool-https-0.0.0.0-443"
disableUploadTimeout="false" coyote.
    http11.Http11NioProtocol" SSLEnabled="true" port="443"
socket.rxBufSize="25188" connectionTimeout="10000"
maxConnections="500">
        <SSLHostConfig disableCompression="true"
caCertificateFile="${catalina.base}/conf/ca.crt"
insecureRenegotiation="false"
        honorCipherOrder="false" ciphers="HIGH:!aNULL:!MD5"
disableSessionTickets="false" protocols="TLSv1.2"
        certificateVerification="false"
certificateVerificationDepth="10">
        …
```

   - Option 1 - For AhsayCBS server with version 7 and 8 backup clients:

     Edit the line from

     ciphers="HIGH:!aNULL:!MD5"

     to

     ciphers="TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256"

server.xml

```
    …
    …
    <Connector maxKeepAliveRequests="9999" keepAliveTimeout="30000" address="0.0.0.0" scheme="https" enableLookups="false"
socket.txBufSize="43800"
    connectionUploadTimeout="900000" acceptCount="200" secure="true" URIEncoding="utf-8" sendReasonPhrase="true"
protocol="org.apache.
    maxHttpHeaderSize="8192" redirectPort="443" executor="tomcatThreadPool-https-0.0.0.0-443" disableUploadTimeout="false"
coyote.
    http11.Http11NioProtocol" SSLEnabled="true" port="443" socket.rxBufSize="25188" connectionTimeout="10000"
maxConnections="500">
        <SSLHostConfig disableCompression="true" caCertificateFile="${catalina.base}/conf/ca.crt" insecureRenegotiation="false"
        honorCipherOrder="false" ciphers="TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256"
        disableSessionTickets="false" protocols="TLSv1.2" certificateVerification="false" certificateVerificationDepth="10">
        …
```

   - Option 2 - For AhsayCBS server with version 8 backup clients only (DO NOT use this

option if there is version 7 AhsayOBM / ACB client connecting to your CBS):

Edit the line from

ciphers="HIGH:!aNULL:!MD5"

to

ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256"

server.xml

```
    …
    …
    <Connector maxKeepAliveRequests="9999" keepAliveTimeout="30000" address="0.0.0.0"
scheme="https" enableLookups="false" socket.txBufSize="43800"
    connectionUploadTimeout="900000" acceptCount="200" secure="true"
URIEncoding="utf-8" sendReasonPhrase="true" protocol="org.apache.
    maxHttpHeaderSize="8192" redirectPort="443" executor="tomcatThreadPool-
https-0.0.0.0-443" disableUploadTimeout="false" coyote.
    http11.Http11NioProtocol" SSLEnabled="true" port="443" socket.rxBufSize="25188"
connectionTimeout="10000" maxConnections="500">
        <SSLHostConfig disableCompression="true"
caCertificateFile="${catalina.base}/conf/ca.crt" insecureRenegotiation="false"
        honorCipherOrder="false"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
        TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256" disableSessionTickets="false"
protocols="TLSv1.2" certificateVerification="false"
        certificateVerificationDepth="10">
        …
```

Keywords

seedload, import, local, cloud, network, removable, export, win

From:
https://wiki.ahsay.com/ - **Ahsay Wiki**

Permanent link:
https://wiki.ahsay.com/doku.php?id=public:8116_faq:how_to_improve_security_of_connection_to_cbs

Last update: **2021/12/14 10:45**