Troubleshoot Kerberos

The following will help you troubleshoot common issues with Kerberos authentication.

Common issues with Kerberos authentication:

1. Clock skew too great while getting initial credentials error.

   Solution: The Active directory and the RiskVision Server must not be more than 5 minutes apart. The clocks on both servers have to be in sync.

2. Defective token detected (Mechanism level: GSSHeader did not find the right tag)

   Solution: This can happen if the browser cannot negotiate the request with the Kerberos Distribution Center or the Active Directory.

   For Mozilla Firefox:

   Setup the following environment variables:

   - NSPR_LOG_FILE = c:/moz.log
   - NSPR_LOG_MODULES = negotiateauth:5

   Verify the Firefox configurations. Restart Firefox and check logs under C:/moz.log. If Firebug is enabled, check the header details. If the response is ":401 UnAuthorized," most likely, the issue is with the keytab files.

3. Cannot load keytab files on RiskVision Server startup

   Solution: The keytab files are loaded during startup. If the version number (kvno) is incorrect, the keytab will not be loaded. The best approach to generate the keytab files on the Active Directory is by using the ktpass command. The ktab command is known to cause issues due to the kvno number.

4. Server not found in Kerberos database

   Solution: This happens if the same SPN is mapped to multiple accounts or hostnames on the Active Directory. Unregister the SPN for other accounts on the Active Directory server by running the following command:

   setspn -D service/name hostname

5. Error 400 Bad Request

   Solution: If user has many groups in Active Directory then request size might be more for Kerberos Authentication which can lead to 400 Bad Request. In order to resolve this issue please perform below changes:

   1. Go to `<%AGILIANCE_HOME%>\apache2\conf\extra`
   2. Open `httpd-ssl.conf` using text editor and add below directive under

   LimitRequestFieldSize 16380The default value for LimitRequestFieldSize is 8190, as per our requirement the size can be increase.

6. Error 413 - Request Entity Too Large

   Solution: When users encounters the error 413, then we need to perform below changes in Apache Web Server.

   1. Go to `<%AGILIANCE_HOME%>\apache2\conf\extra`
   2. Open httpd-ssl.conf using text editor and add below directive under `LimitRequestBody 0`
   3. Go to `<%AGILIANCE_HOME%>\apache2\conf\extra,` in the `workers.properties` file add: `worker.agl_tomcat.max_packet_size=65536`
   4. Restart Apache Service
   5. Go to < `%AGILIANCE_HOME%>\Tomcat\conf` , in `server.xml` file add the packetsize `packetSize="65536"`
      Example:

      ```
      enableLookups="false"
      protocol="AJP/1.3"
      packetSize="65536"
      connectionTimeout="900000"
      backlog="200"
      maxThreads="300"
      debug="0"
      URIEncoding="UTF-8"/>
      ```

   6. `Restart Tomcat Service`

`If error still exists then we need to increase packet size.`