Configuring Allowed TLS Versions and Ciphers for the Monitoring Station and Agents

Configuration of allowed TLS versions and ciphers for the Monitoring Station

Communications between the Monitoring Station and Agents

To configure communications between the Monitoring Station and Agents, add a list of allowed TLS versions and ciphers in *uptime.conf* using `clientSocketTlsVersion`, `clientSocketCiphers`, and ':' as delimiter, for example:

```
clientSocketTlsVersion= TLSv1.2
```

or

```
clientSocketTlsVersion= TLSv1:TLSv1.1:TLSv1.2
clientSocketCiphers=TLS_RSA_WITH_AES_256_CBC_SHA256
```

or

```
clientSocketCiphers= TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384:TLS_RSA_WITH_AES_256_CBC_SHA256
```

Web Application Monitoring

To configure web application monitoring, add a list of allowed TLS versions and ciphers in *uptime.conf* using `clientHttpCiphers`, `clientHttpTlsVersion`, and ':' as delimiter, for example:

```
clientHttpCiphers= TLS_RSA_WITH_AES_256_CBC_SHA256
```

or

```
clientHttpCiphers=TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384:TLS_RSA_WITH_AES_256_CBC_SHA256
clientHttpTlsVersion=TLSv1.2
```

or

```
clientHttpTlsVersion=TLSv1:TLSv1.1:TLSv1.2
```

For a full list of supported ciphers, see the **Java SE 7** column of the **Default Enabled Cipher Suites** table in http://docs.oracle.com/javase/7/docs/technotes/guides/security/SunProviders.html.

Configuration of allowed TLS versions and ciphers for Agents/Stunnel

In *uptmagnt.conf*, specify sslVersion and ciphers to allow specific TLS versions and ciphers, for example:

```
ciphers = ECDHE-ECDSA-AES256-SHA384:AES256-SHA256:PSK
```

or

```
ciphers = AES256-SHA256
```

To enable specific SSL/TLS versions, you first must disable all other possible versions. For example, to enable only TLSv1.2, add the following code to *uptmagnt.conf*:

```
options = NO_SSLv2
options = NO_SSLv3
options = NO_TLSv1
options = NO_TLSv1.1
```

To enable TLSv1.1 and TLSv1.2, use the following options:

```
options = NO_SSLv2
options = NO_SSLv3
options = NO_TLSv1
```

Review the following example of *uptmagnt.conf* with a specific TLS version and cipher:

```
cert = /etc/stunnel/uptmagnt.pem
exec = /opt/uptime-agent/bin/uptimeagent

options = NO_SSLv2
options = NO_SSLv3
options = NO_TLSv1
options = NO_TLSv1.1
ciphers=AES256-SHA256:PSK
```

For more information about Stunnel configuration, see https://www.stunnel.org/static/stunnel.html#OPTIONS, https://www.stunnel.org/pipermail/stunnel-users/2015-March/004985.html