

Web UI のセキュリティ強化

この付録では、次の項について説明します。

• Web UI のセキュリティ強化 (1ページ)

Web UI のセキュリティ強化

HTTPS を使用してセキュアソケットレイヤ (SSL) プロトコルで接続すると、Web UI は Java 仮想マシン (JVM) のデフォルトの暗号を使用します。これらの暗号には通常、弱い暗号セッションキーが含まれており、システムセキュリティに影響を与える可能性があります。システムを強化する場合は、次のように暗号を調整します。

(注) Cisco Prime Network Registrar 11.0 のデフォルトのインストールは、Transport Layer Security (TLS)
1.2 で動作します。必要に応じて、古い TLS のバージョンで動作するように構成を変更できます。

- ステップ1 /var/nwreg2/{local | regional }/tomcat/con フォルダにある server.xml ファイルを開きます。
- ステップ2 以下の推奨される sslEnabledProtocol と暗号を使用するか、セキュリティ要件に従って設定します。詳細に ついては、オンラインで入手可能な tomcat SSL/TLS 設定ドキュメントを参照してください。

<Connector port="\${cnrui.https.port}" protocol="com.cisco.cnr.webui.tomcat.SecureHTTP"

relaxedQueryChars='[]'

maxConnections="1024" maxThreads="150" SSLEnabled="true" scheme="https" secure="true"

clientAuth="false"

keystoreFile="..."

keystorePass="..."

ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA384,

compression="on"

```
compressionMinSize="2048"
```

noCompressionUserAgents="gozilla, traviata"

URIEncoding="UTF-8"

compressableMimeType="text/html,text/xml,text/plain, text/css,text/javascript, application/x-javascript,application/javascript"

sslEnabledProtocols="TLSv1.2"/>

(注) keystoreFile および keystorePass の値は、インストールに固有です。これらの値は、Cisco Prime Network Registrar が起動されるたびに上書きされるため、変更しないでください。

ステップ3 Cisco Prime Network Registrar を再起動して、変更を有効にします。