



راه اندازی و پیکربندی امن پروتکل SSL/TLS بر روی سرویس دهنده وب Glassfish 4.1

شماره مستند APA-AMIRKABIR-13950728-1
تاریخ نگارش ۲۸ مهر ۱۳۹۵
شماره نگارش ۱/۰
نگارش آپای امیرکبیر
طبقه بندی عادی

فهرست مطالب

۱	مقدمه	۱
۲	فعال سازی ارتباطات HTTPS	۲
۵	پیکربندی امن پروتکل SSL/TLS	۳
۵	غیرفعال سازی SSLv2 و SSLv3	۳-۱
۵	روش اول: کنسول مدیریتی	۳-۱-۱
۶	روش دوم: ویرایش domain.xml	۳-۱-۲
۷	غیرفعال سازی الگوریتم های رمزنگاری ضعیف	۳-۲
۱۰	منابع	۴

۱ مقدمه

برای تأمین محرمانگی و جامعیت داده‌های مبادله شده می‌توان از پروتکل‌های استاندارد که بدین منظور طراحی شده استفاده کرد. در حال حاضر مهم‌ترین پروتکل رمزنگاری که در سطح اینترنت برای رمزنگاری داده‌های لایه کاربرد و تأمین امنیت ارتباطات استفاده می‌شود، پروتکل SSL/TLS است. در این گزارش مراحل نصب گواهی‌نامه SSL و امن‌سازی پروتکل SSL/TLS بر روی سرویس‌دهنده وب Glassfish نسخه ۴,۱ بیان شده است.

۲ فعال سازی ارتباطات HTTPS

برای پیکربندی سرویس دهنده HTTPS و استفاده از این پروتکل ابتدا باید گواهی نامه دیجیتال مربوطه را از مراکز صدور گواهی (CA)^۱ معتبر دریافت کرد (یا گواهی خود-امضا را تولید کرد). گرفتن گواهی دارای مراحل است که برای اطلاعات بیشتر در این زمینه می توانید به گزارش ارائه شده توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر که در آدرس زیر قرار دارد مراجعه کنید:

<http://apa.aut.ac.ir/?p=971>

مراحل قرار دادن گواهی نامه دیجیتال در GlassFish به صورت زیر است:

قبل از انجام هر کاری، از فایل های این زیرشاخه نسخه پشتیبان تهیه کنید:

\$GFHOME/domains/yourdomain/config

این مراحل عبارتند از:

۱. یک کلید خصوصی تولید کنید.
۲. یک درخواست امضای گواهی نامه (CSR)^۲ بسازید.
۳. CSR را به مرکز صدور گواهی ارسال کنید.
۴. گواهی نامه امضا شده خود را وارد کنید.
۵. تنظیمات ضروری Glassfish را انجام دهید.

در ابتدا، اجازه دهید کلید خصوصی خود را بسازیم. شما می توانید بر روی keystore موجود در Glassfish کار کنید یا می توانید یک keystore جدید بسازید و سپس آن را در keystore مربوط به Glassfish وارد کنید. برای امنیت بیشتر، ما یک keystore جدید ساختیم و کلید خصوصی را توسط آن تولید کردیم:

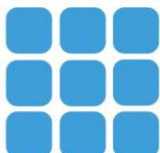
```
cd ~
mkdir ssl-stuff
cd ssl-stuff
keytool -keysize 2048 -genkey -alias yourdomain.com -keyalg RSA -dname
"CN=www.yourdomain.com,O=Your Organization,L=Your City,S=Your State,C=Your
Country Code like US, CH or TR" -keystore keystore.jks -keypass changeit -storepass
changeit
```

حالا کلید خصوصی در فایل keystore.jks تولید شده است. در دستور زیر، ما از 'changeit' به عنوان کلمه عبور کلید و کلمه عبور keystore استفاده می کنیم.

```
keytool -certreq -alias yourdomain.com -keystore keystore.jks -storepass changeit -
keypass changeit -file server.csr
```

^۱ Certificate Authority

^۲ Certificate signing request



این نتایج در یک درخواست امضا شدن گواهی نامه قرار دارند (server.csr). در حال حاضر ما دو فایل در اختیار داریم:

- keystore.jks
- server.csr

مرحله بعد فرستادن فایل server.csr به یکی از مراکز صدور گواهی و دریافت گواهی نامه امضا شده است. مراکز صدور گواهی به دنبال نتایج whois دامنه شما هستند و اگر آن‌ها آدرس پست الکترونیک نماینده فنی را پیدا کنند، گواهی نامه امضا شده را به این آدرس پست الکترونیک ارسال می‌کنند. اگر آدرس پست الکترونیک وجود نداشته باشد، آن‌ها یک کد در اختیار شما قرار می‌دهند (مانند abcd123) و از شما می‌خواهند که یا یک زیردامنه با آن کد اضافه کنید و یا اینکه یک صفحه html با نام این کد ایجاد کنید (و همچنین با محتوای پر شده توسط کد).

از مرکز صدور گواهی، معمولاً شما باید دو فایل دریافت کنید:

- گواهی نامه امضا شده خود را که معمولاً اینگونه نام‌گذاری می‌شود: yourdomain.com.crt
- ریشه گواهی نامه (شما ممکن است بیش از یک فایل دریافت کنید. در بعضی موارد مراکز صدور گواهی، گواهی نامه‌های میانی را ارسال می‌کنند).

مرحله بعد، وارد کردن keystore مورد استفاده در keystore مربوط به Glassfish است:

```
keytool -importkeystore -srckeystore ~/ssl-stuff/keystore.jks -destkeystore  
$GLASSFISHHOME/domains/yourdomain/config/keystore.jks
```

هم اکنون، مرحله نهایی که باید بر روی keystore انجام شود، وارد کردن گواهی نامه امضا شده است. در ابتدا ما باید ریشه گواهی نامه را در keystore مربوط به Glassfish وارد کنیم.

```
cd $GLASSFISH_HOME/domains/yourdomain/config keytool -import -v -trustcacerts -alias root  
-file gd_bundle.crt -keystore keystore.jks -keypass changeit -storepass changeit
```

سپس گواهی نامه امضا شده خود را وارد کنید:

```
keytool -import -v -trustcacerts -alias yourdomain.com -file yourdomain.com.crt -keystore  
keystore.jks -keypass changeit -storepass changeit
```

حال بخش مربوط به keystore تمام شده است. شما باید چیزی شبیه این داشته باشید:

```
keytool -list -keystore keystore.jks
```

```
Keystore-Typ: JKS
```

```
Keystore-Provider: SUN
```

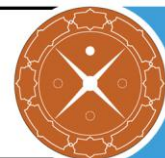
```
....
```

```
root, 03.06.2011, trustedCertEntry,
```

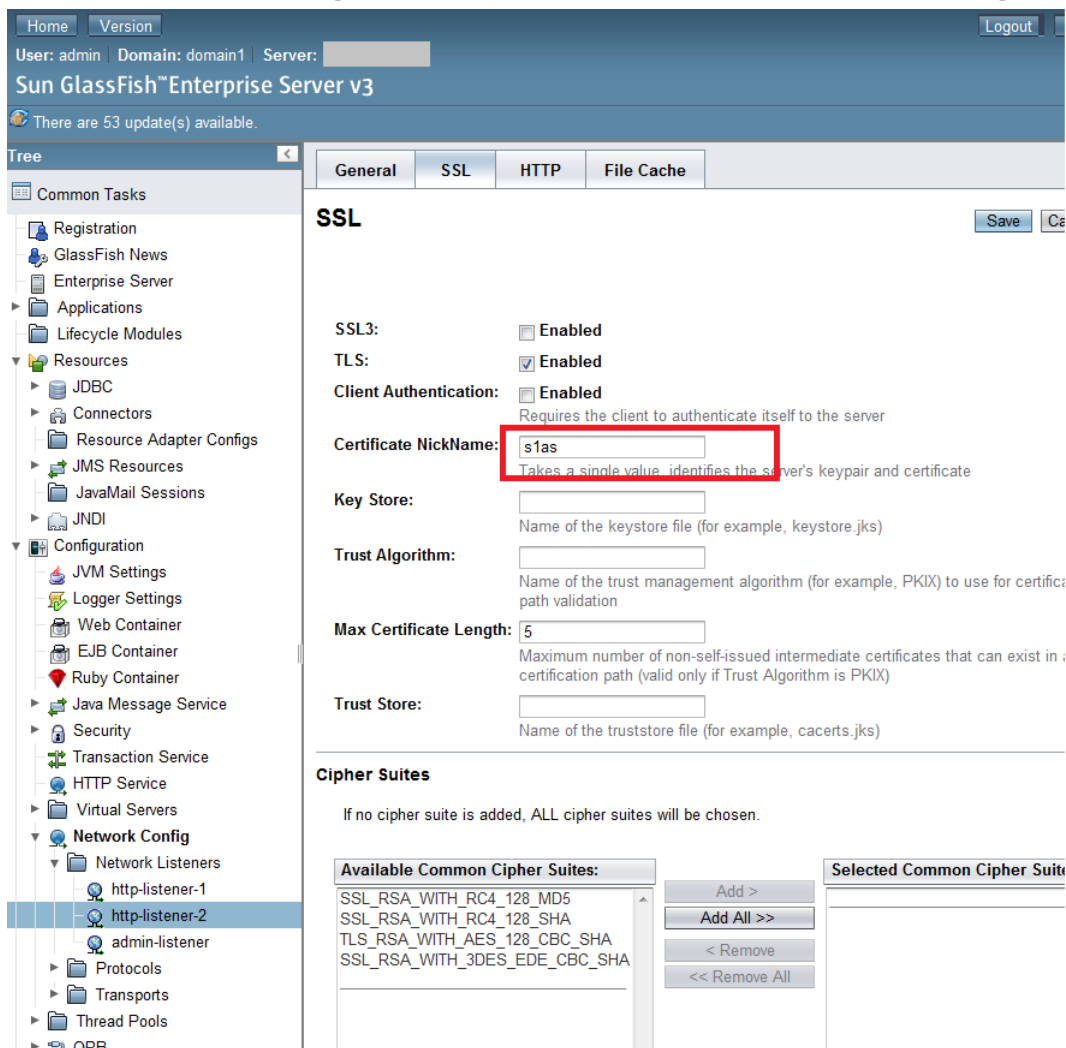
```
Zertifikatsfingerabdruck (MD5): XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX
```

```
yourdomain.com, 03.06.2011, PrivateKeyEntry,
```

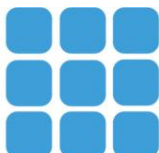
```
Zertifikatsfingerabdruck (MD5): XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX
```



مرحله نهایی این فرآیند استفاده از دامنه alias به عنوان نام مستعار گواهی نامه بر روی Glassfish است.



The screenshot shows the administration console for Sun GlassFish Enterprise Server v3. The left sidebar contains a tree view with categories like Common Tasks, Resources, Configuration, and Network Config. The main area displays the SSL configuration page, which includes sections for SSL, Ciphers Suites, and Trust Store. The 'Certificate NickName' field is highlighted with a red box and contains the value 's1as'. Below the SSL section, there is a 'Ciphers Suites' section with a list of available common cipher suites and buttons to add or remove them.



۳ پیکربندی امن پروتکل SSL/TLS

در این بخش چگونگی پیکربندی امن پروتکل SSL/TLS را در سرویس‌دهنده وب GlassFish بیان می‌کنیم. مواردی همچون استثنا کردن برخی الگوریتم‌های رمز به منظور کاهش حملاتی شبیه به CRIME، FREAK و LogJAM، غیرفعال سازی نسخه‌های ناامن SSL و برقرار کردن رمزنگاری‌های قوی که از (FS) Forward Secrecy پشتیبانی می‌کنند را بیان می‌کنیم. برای بررسی وضعیت امنیتی پروتکل SSL/TLS سرویس‌دهنده خود، می‌توانید به ابزاری که بدین منظور توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر طراحی شده و در آدرس زیر قرار دارد، مراجعه کنید.

<https://sslcheck.certcc.ir>

۱-۳ غیرفعال سازی SSLv2 و SSLv3

SSLv2 و SSLv3 (به خاطر حمله POODLE) ناامن هستند و باید غیرفعال شوند. در ادامه دو روش را برای غیرفعال کردن نسخه‌های ناامن SSL را بیان می‌کنیم.

۳-۱-۱ روش اول: کنسول مدیریتی

برای هر کدام از تنظیمات شما:

- وارد منوی Protocols شوید، که می‌توانید آن را در زیرمجموعه Network Config پیدا کنید.
 - برای هر کدام از شنودهایی که لیست شده است، بر روی نام شنودکننده کلیک کنید:
 - بررسی کنید که گزینه Security تیک خورده باشد، شما نمی‌توانید SSL3 را از طریق کنسول مدیریتی غیرفعال کنید مگر اینکه Security فعال شده باشد.
 - با فرض اینکه گزینه Security تیک خورده باشد، به تب SSL بروید و تیک مربوط به گزینه SSL3 را بردارید.
 - بر روی Save کلیک کنید و به شنودکننده بعدی بروید.
- هنگامی که شما SSL3 را برای هر کدام از شنودکننده‌ها غیرفعال کرده باشید، شما باید دامنه خود را راه اندازی مجدد کنید تا تغییرات حاصل شود. قبل از اینکار، شما همچنین باید SSL3 را بر روی شنودکننده‌های IIOP نیز غیرفعال کنید، بنابراین بر هر کدام از تنظیمات خود باید مراحل زیر را انجام دهید:
- به بخش شنودکننده‌های IIOP خود بروید، که در بخش ORB قرار دارد.
 - برای هر کدام از شنودکننده‌ها، بر روی نام شنودکننده کلیک کنید، سپس:
 - بررسی کنید که گزینه Security تیک خورده باشد، شما نمی‌توانید SSL3 را از طریق کنسول مدیریتی غیرفعال کنید مگر اینکه Security فعال شده باشد.
 - با فرض اینکه گزینه Security تیک خورده باشد، به تب SSL بروید و تیک مربوط به گزینه SSL3 را بردارید.

○ بر روی Save کلیک کنید و به شنود کننده بعدی بروید.

● دامنه را راه اندازی مجدد کنید.

این روش احتمالاً راحت ترین راه برای غیرفعال کردن SSL3 است، مخصوصاً اگر شما در حال تنظیم و نصب یک GlassFish جدید باشید. در هنگام نصب یک GlassFish جدید، شما فقط دو مورد از تنظیمات را ویرایش کنید و هر مورد جدید ساخته شده می تواند تنظیمات خود را از آن جا کپی کند.

۳-۱-۲ روش دوم: ویرایش domain.xml

غیرفعال کردن SSL3 از طریق فایل تنظیمات دامنه کمی پیچیده تر است، اما اگر شما بدانید دقیقاً در حال چه کاری هستید، می توان آن را نسبت به روش کنسول مدیریتی سریع تر انجام داد، مخصوصاً اگر شما ارتباطات HTTPS یا گروه های تنظیمات زیادی داشته باشید.

فایلی که شما به دنبال آن هستید، فایل domain.xml است، که می توانید آن را در زیرمجموعه \$GF_INSTALL/glassfish/domains/\$DOMAIN/config پیدا کنید که \$GF_INSTALL دایرکتوری است که GlassFish را بر روی آن نصب کردید و \$DOMAIN نام دامنه شما است (نام پیش فرض آن، domain1 است). اگرچه قبل از شروع به ویرایش فایل، بهتر است که دامنه خود را متوقف کنید، چراکه هنگامی که دامنه همچنان فعال است، امکان دارد تغییراتی بر روی فایل domain.xml اعمال کند که وقتی شما خودتان در حال اعمال تغییرات مورد نظر هستید، ممکن است مورد تأیید شما نباشد.

نام پیش فرض شنودکننده HTTP، http-listener-2 است. در تگ های این پروتکل، چیزی که شما می بینید احتمالاً شبیه این است:

```
<protocol name="http-listener-2" security-enabled="true">
  <http max-connections="250" default-virtual-server="server">
    <file-cache></file-cache>
  </http>
  <ssl classname="com.sun.enterprise.security.ssl.GlassfishSSLImpl"
cert-nickname="slas"></ssl>
</protocol>
```

برای غیرفعال کردن SSL3، ssl-enabled=false را بین تگ های <ssl> اضافه کنید، که به این صورت در می آید:

```
<protocol name="http-listener-2" security-enabled="true">
  <http max-connections="250" default-virtual-server="server">
    <file-cache></file-cache>
  </http>
  <ssl ssl3-enabled=false
classname="com.sun.enterprise.security.ssl.GlassfishSSLImpl" cert-
nickname="slas"></ssl>
</protocol>
```


روش غیرفعال کردن SSL3 مشابه روش غیرفعال کردن شنودکننده‌های HTTP است، در نتیجه، این تغییرات را اعمال کنید.

فایل اصلی شما احتمالاً چیزی شبیه به این است:

```
<iiop-listener address="0.0.0.0" port="3820" id="SSL" security-  
enabled="true">  
  <ssl classname="com.sun.enterprise.security.ssl.GlassfishSSLImpl"  
cert-nickname="slas"></ssl>  
</iiop-listener>  
<iiop-listener address="0.0.0.0" port="3920" id="SSL_MUTUALAUTH"  
security-enabled="true">  
  <ssl classname="com.sun.enterprise.security.ssl.GlassfishSSLImpl"  
cert-nickname="slas" client-auth-enabled="true"></ssl>  
</iiop-listener>
```

که باید به صورت زیر تغییر یابد:

```
<iiop-listener address="0.0.0.0" port="3820" id="SSL" security-  
enabled="true">  
  <ssl ssl3-enabled="false"  
classname="com.sun.enterprise.security.ssl.GlassfishSSLImpl" cert-  
nickname="slas"></ssl>  
</iiop-listener>  
<iiop-listener address="0.0.0.0" port="3920" id="SSL_MUTUALAUTH"  
security-enabled="true">  
  <ssl ssl3-enabled="false"  
classname="com.sun.enterprise.security.ssl.GlassfishSSLImpl" cert-  
nickname="slas" client-auth-enabled="true"></ssl>  
</iiop-listener>
```

و شما SSL3 را از هر دو شنود کننده غیرفعال کرده‌اید.

مطمئن شوید که SSL3 را هم بر روی اتصالات و هم بر روی هر دو گروه تنظیمات، غیرفعال کرده باشید، شما باید توجه داشته باشید که شنودکننده‌ها یک بار در default-config و بار دیگر در server-config تنظیم شده‌اند.

۲-۳ غیرفعال سازی الگوریتم‌های رمزنگاری ضعیف

Forward Secrecy اطمینان می‌دهد که صحت^۱ یک کلید جلسه^۲ حتی وقتی که کلیدهای زیادی مورد مخاطره قرار گرفتند، حفظ می‌شود. FS کامل^۳ این مورد را با استخراج یک کلید جدید برای هر جلسه، به انجام می‌رساند.

^۱ Integrity

^۲ Session Key

^۳ Perfect Forward Secrecy

این بدان معناست که زمانی که کلید خصوصی به مخاطره افتاد، نمی‌تواند برای رمزگشایی ترافیک SSL مورد استفاده قرار گیرد.

برای غیرفعال کردن الگوریتم‌های رمزنگاری ضعیف باید در فایل پیکربندی domain.xml، تغییراتی اعمال کنیم و نام این الگوریتم‌ها را حذف کنیم. برای غیرفعال کردن الگوریتم‌های رمزنگاری ضعیف، باید دو پارامتر زیر را به درستی مقدار دهی کنیم.

۱. ssl2ciphers

این پارامتر شامل لیستی از الگوریتم‌های رمزنگاری SSL2 است که از طریق کاما (,) از هم جدا شده‌اند. الگوریتم‌هایی که به صورت صریح در این لیست نیابند، بدان معنی است که غیرفعال هستند. اگر از این پارامتر در فایل پیکربندی استفاده نشود، بدان معنی است که همه الگوریتم‌های رمزنگاری (که پشتیبانی می‌شوند) فعال هستند. مقادیر مجاز برای این پارامتر شامل موارد زیر هستند:

- rc4
- rc4export
- rc2
- rc2export
- idea
- des
- desede3

۲. ssl3tlsciphers

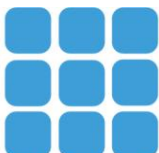
این پارامتر شامل لیستی از الگوریتم‌های رمزنگاری SSL3 و/یا TLS است که از طریق کاما (,) از هم جدا شده‌اند. الگوریتم‌هایی که به صورت صریح در این لیست نیابند، بدان معنی است که غیرفعال هستند. اگر از این پارامتر در فایل پیکربندی استفاده نشود، بدان معنی است که همه الگوریتم‌های رمزنگاری (که پشتیبانی می‌شوند) فعال هستند. مقادیر مجاز برای این پارامتر شامل موارد زیر هستند:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_WITH_NULL_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_NULL_SHA

باید دقت کنید که الگوریتم‌های ضعیف مانند RC4 را از لیست بالا حذف کرده و همیشه این پیکربندی را با جدیدترین توصیه‌های امنیتی به‌روز رسانی کنید. به عنوان مثال رمزنگاری‌های زیر، Forward Security را پشتیبانی نمی‌کنند و باید غیرفعال شوند:



- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA



۴ منابع

1. https://docs.oracle.com/cd/E18930_01/html/821-2432/gkyba.html
2. http://docs.oracle.com/cd/E18930_01/html/821-2433/create-ssl-1.html#SJSASEEREFMANcreate-ssl-1
3. <https://docs.oracle.com/cd/E19798-01/821-1794/aeogl/index.html>
4. <http://www.aliok.com.tr/techposts/2011-06-04-using-your-ssl-certificate-on-glassfish-3.html>
5. <http://blog.c2b2.co.uk/2014/11/disabling-ssl3-in-glassfish-41.html>