



## راه اندازی و پیکربندی امن پروتکل SSL/TLS بر روی سرویس دهنده پست الکترونیک Zimbra 8

شماره مستند ..... APA-AMIRKABIR-13950623-1

تاریخ نگارش ..... ۲۳ شهریور ۱۳۹۵

شماره نگارش ..... ۷/۰

نگارش ..... آقای امیرکبیر

طبقه بندی ..... عادی

## فهرست مطالب

۱	مقدمه	۱
۲	تولید یک درخواست امضا گواهی	۲
۷	نصب گواهی SSL	۳
۷	تولید و نصب گواهی نامه SSL خود-امضا	۳-۱
۱۱	نصب گواهی SSL تجاری	۳-۲
۱۳	پیکربندی و ایمن سازی گواهی SSL	۴
۱۵	حل مشکل استفاده از RC4	۴-۱
۱۷	حل مشکل OpenSSL Padding Oracle	۴-۲
۱۸	حل مشکل پارامترهای ضعیف دیفی هلمن	۴-۳
۲۱	پشتیبانی از Strict Transport Security	۴-۴
۲۲	حل مشکلات امنیتی پروتکل SMTP	۴-۵
۲۴	منابع	۵

## ۱ مقدمه

شرکت‌ها و سازمان‌های کوچک عمدتاً از شرکت‌های سرویس‌دهنده Hosting برای پست الکترونیک خود استفاده می‌کنند اما شرکت‌های متوسط و بزرگ به دلیل مسائل امنیتی و حساسیت سرویس پست الکترونیک برای آنان، ناچار به استفاده از یک Mail Server اختصاصی در محل خود هستند.

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 و ایمن‌سازی پروتکل SSL/TLS بر روی Zimbra نسخه 8.6.0\_GA\_1194.NETWORK بیان شده است ولی تفاوت‌های موجود در برخی نسخه‌ها هم ذکر شده است.

## ۲ تولید یک درخواست امضا گواهی

برای تولید درخواست امضا گواهی، می‌بایست بر اساس مستندات مرکز صدور گواهی مورد نظر، کلید عمومی و خصوصی مربوط به سرویس دهنده خود را ایجاد نمایید. کلید خصوصی می‌بایست نزد شما به صورت محرمانه باقی بماند و حتی نباید برای مرکز صدور گواهی نیز ارسال شود. کلید عمومی در قالب CSR<sup>۱</sup> برای مرکز صدور گواهی ارسال می‌شود تا مرکز صدور گواهی پس از انجام بررسی‌های لازم آن را امضا کند. در حقیقت در CSR شما تنها کلید عمومی و دامنه/دامنه‌های مدنظر و مشخصات سازمان خود را برای مرکز صدور گواهی ارسال می‌کنید. با توجه به نوع گواهی مد نظر، مرکز صدور گواهی ممکن است مدارک دیگری را نیز از شما درخواست نماید. گرفتن گواهی دارای مراحل است که برای اطلاعات بیشتر در این زمینه می‌توانید 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>

در این گزارش مراحل ایجاد فایل CSR را در Zimbra بیان می‌کنیم. برای انجام این کار، مرورگر خود را باز کرده و به کنسول مدیریتی Zimbra وارد شوید و به مسیر Home > Configure > Certificates بروید:



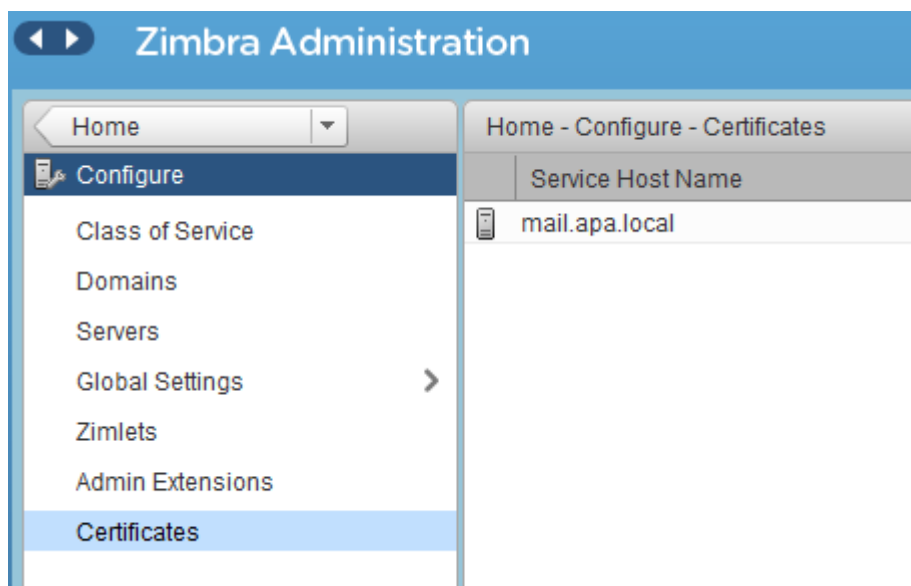
The screenshot shows the Zimbra Administration web interface. The top navigation bar includes 'Home', 'Monitor', 'Manage', 'Configure', 'Tools and Migration', 'Search', and 'Help Center'. The main content area displays a 'Summary' section with the following information:

- Zimbra Version: 8.6.0\_GA\_1153.FOSS
- Servers: 1
- Accounts: 1
- Domains: 1
- Class of Service: 2

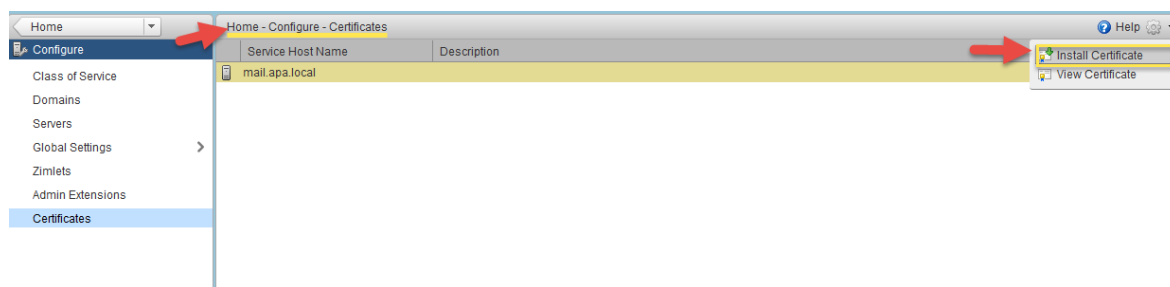
Below the summary, there is a '1 Get Started' button with a right-pointing arrow. Underneath this button, a list of steps is provided:

1. Install Certificates
2. Configure Default COS

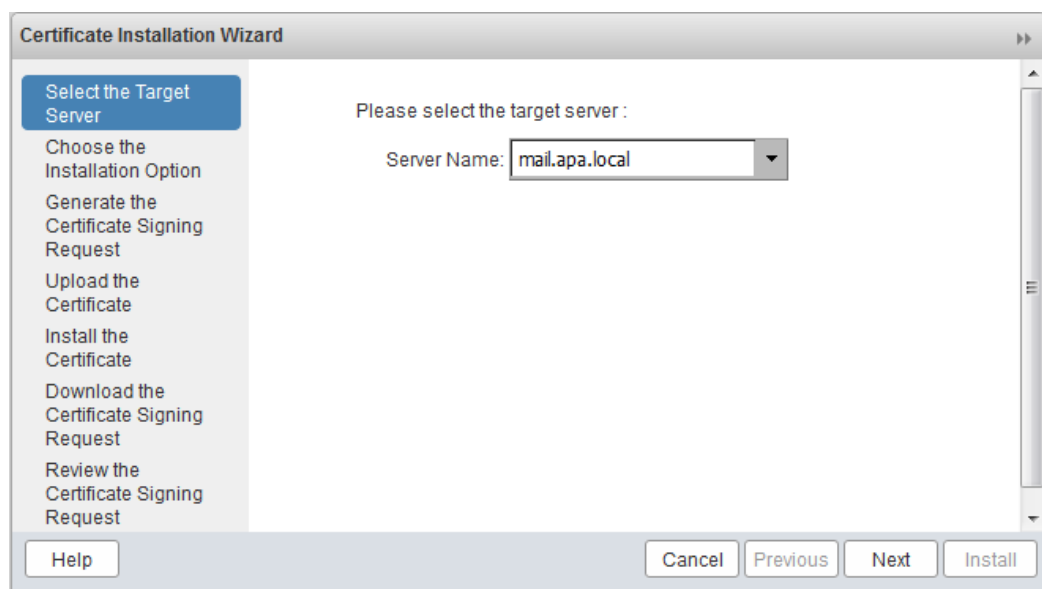
<sup>۱</sup> Certificate Signing Request



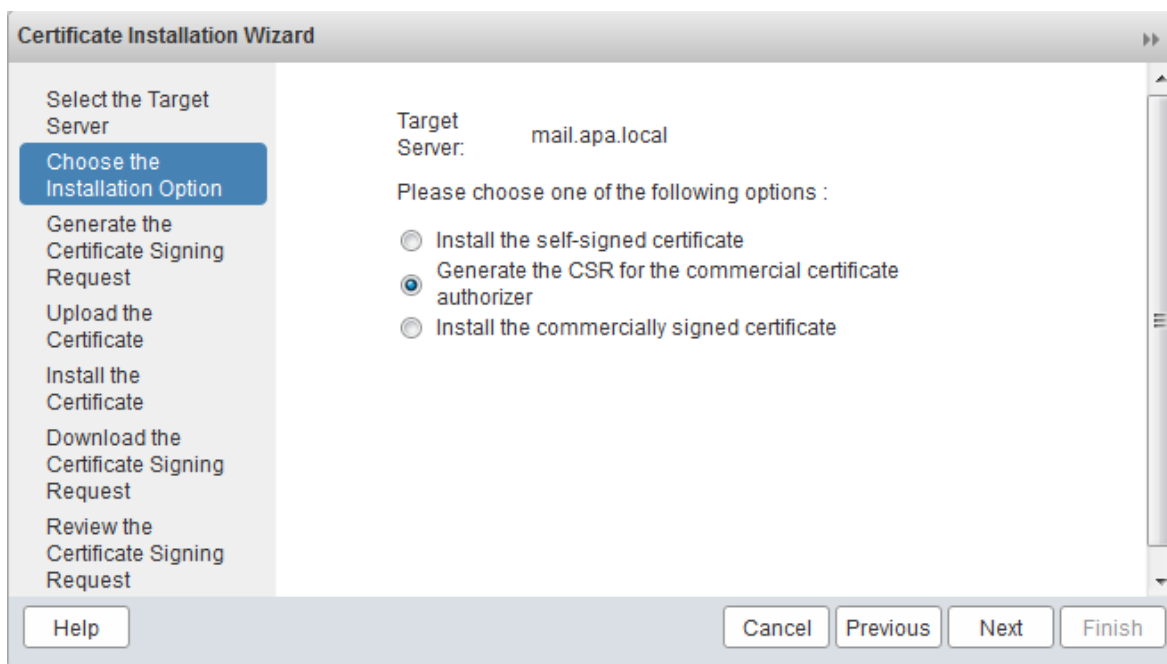
در پنجره کنسول مدیریتی وارد بخش تنظیمات شوید و سپس گزینه "Install Certificate" را انتخاب کنید:



سرور هدف را به منظور تولید فایل‌های SSL مانند CSR و کلید خصوصی، انتخاب کنید.



در گام بعد، گزینه "Generate the CSR for the commercial certificate authorizer" را به منظور تولید CSR برای یک مرکز صدور گواهی تجاری، انتخاب کنید.



در این پنجره، شما باید تنظیمات بعدی را انتخاب کنید:

- در ابتدا گزینه SHA256 را در قسمت digest انتخاب کنید. همچنین توجه کنید که گزینه SHA1 هم وجود دارد ولی از امنیت کافی برخوردار نیست.
- طول کلید را ۲۰۴۸ بیت یا بیشتر در نظر بگیرید.
- نام مشترک (CN)<sup>۱</sup> باید نام FQDN<sup>۲</sup> که شما می‌خواهید از آن استفاده کنید، باشد. اگر شما در حال استفاده از یک سرور تنها هستید، توصیه می‌شود که FQDN و نام میزبان<sup>۳</sup> یکسان باشند.
- اگر می‌خواهید از یک گواهی Wildcard (که این نوع گواهی همه زیر دامنه‌های دامنه اصلی را پوشش می‌دهد) برای Zimbra استفاده کنید، گزینه مربوطه را انتخاب کنید.
- در قسمت مربوط به SAN<sup>۴</sup> می‌توانید نام‌های دیگری را هم (اگر می‌خواهید از یک گواهی Multi-SAN استفاده کنید) انتخاب کنید.

<sup>۱</sup> Common Name

<sup>۲</sup> Fully Qualified Domain Name

<sup>۳</sup> Hostname

<sup>۴</sup> Subject Alternative Name

**Certificate Installation Wizard**

Choose the Installation Option

**Generate the Certificate Signing Request**

Upload the Certificate

Install the Certificate

Download the Certificate Signing Request

Review the Certificate Signing Request

Digest: sha256

Key Length: 2048

Common Name: mail.apa.local

Use Wildcard Common Name

Country Name: GB

State/Province: Lon

City: Lon

Organization Name: apa

Organizational Unit: apa

Subject Alternative Name:  Add

Note: Subject Alternative Name is used to set the SubjectAltName extension of the

Help Cancel Previous Next Finish

حالا فایل CSR شما آماده است و شما می‌توانید آن را دانلود کنید (یا از مسیر `/opt/zimbra/ssl/zimbra/commercial/commercial.csr` دریافت کنید) و به مرکز صدور گواهی SSL ارسال کنید. مرکز صدور گواهی، کلید عمومی شما را امضا کرده و یک فایل crt به شما تحویل می‌دهد.

**Certificate Installation Wizard**

Select the Target Server

Choose the Installation Option

Generate the Certificate Signing Request

Upload the Certificate

Install the Certificate

**Download the Certificate Signing Request**

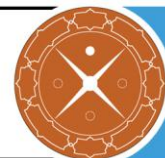
Review the Certificate Signing Request

Target Server: mail.apa.local

In order to obtain a commercially signed certificate, you must download the generated CSR and submit it to your commercial certificate authorizer. Once you get the certificate, please restart the Certificate Installation Wizard and choose the option Install the commercially signed certificate to complete the certificate installation.

[Download the CSR](#)

Help Cancel Previous Next Finish



به منظور چک کردن اعتبار CSR، می‌توانید به عنوان مثال از [اینجا](#) استفاده کنید.

#### Certificate information

**Common name:** mail.apa.local

**Organization:** apa

**Organizational unit:** apa

**City/locality:** Lon

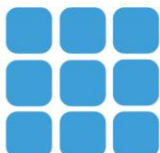
**State/province:** Lon

**Country:** GB

**Signature algorithm:** SHA256

**Key algorithm:** RSA

**Key size:** 2048



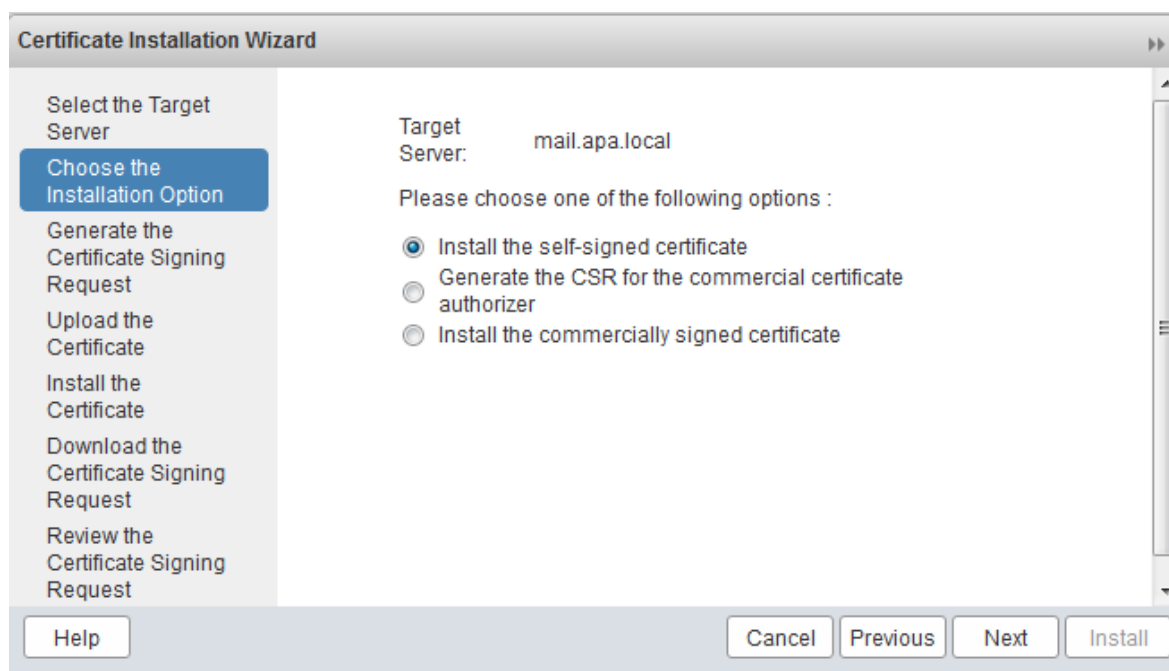


## ۳ نصب گواهی SSL

به منظور گرفتن گواهی SSL برای zimbra یک پنجره جدید از Certificate Installation Wizard باز کنید (این ابزار در واقع به شما کمک خواهد کرد تا یک گواهی را به سرعت بسازید و اعمال کنید). در اینجا مشاهده می‌کنید که دو روش (خود-امضا و تجاری) برای این کار وجود دارد که در ادامه آن‌ها را شرح می‌دهیم.

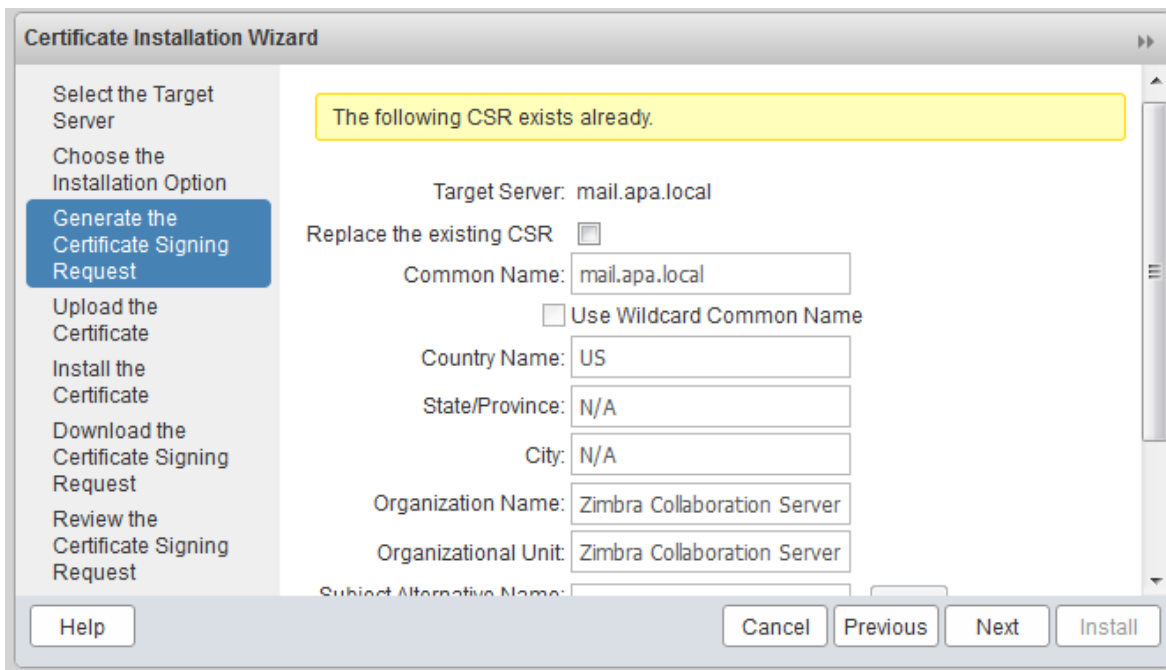
### ۳-۱ تولید و نصب گواهی نامه SSL خود-امضا

گواهی خود-امضا<sup>۱</sup> به گواهی‌ای گفته می‌شود که خود zimbra آن را امضا می‌کند. این گواهی رایگان است و ممکن است مرورگرها آن را یک گواهی صادره از CA نامعتبر تشخیص دهند. برای تولید گواهی خود-امضا، به مسیر **Configure > Select Install Certificate** بروید و گام‌های زیر را دنبال کنید.  
در گام اول گزینه "Install the self-signed certificate" را انتخاب کنید:



<sup>۱</sup> Self-Signed

با بررسی گزینه‌های مورد نظر به مرحله بعد بروید.



Certificate Installation Wizard

Select the Target Server

Choose the Installation Option

Generate the Certificate Signing Request

Upload the Certificate

Install the Certificate

Download the Certificate Signing Request

Review the Certificate Signing Request

The following CSR exists already.

Target Server: mail.apa.local

Replace the existing CSR

Common Name: mail.apa.local

Use Wildcard Common Name

Country Name: US

State/Province: N/A

City: N/A

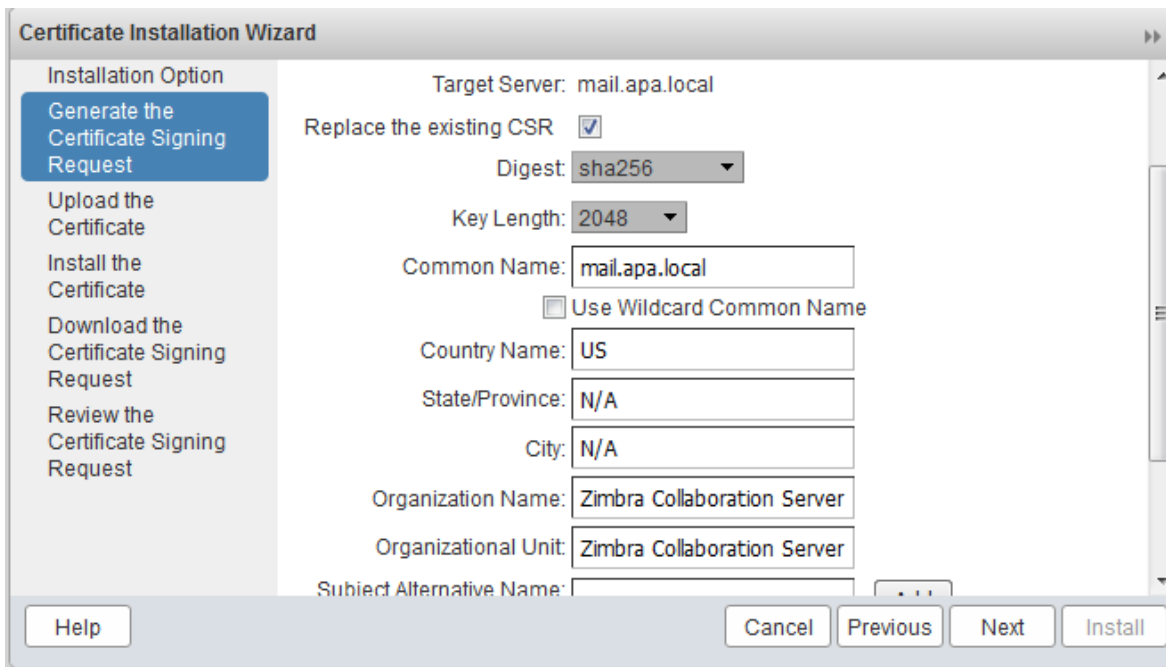
Organization Name: Zimbra Collaboration Server

Organizational Unit: Zimbra Collaboration Server

Subject Alternative Name:

Help Cancel Previous Next Install

ابتدا باید مطمئن شوید که طول کلید ۲۰۴۸ بیتی انتخاب کرده‌اید و همین‌طور باقی فیلدها هم باید به درستی بررسی شوند.



Certificate Installation Wizard

Installation Option

Generate the Certificate Signing Request

Upload the Certificate

Install the Certificate

Download the Certificate Signing Request

Review the Certificate Signing Request

Target Server: mail.apa.local

Replace the existing CSR

Digest: sha256

Key Length: 2048

Common Name: mail.apa.local

Use Wildcard Common Name

Country Name: US

State/Province: N/A

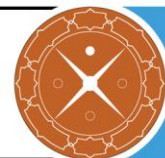
City: N/A

Organization Name: Zimbra Collaboration Server

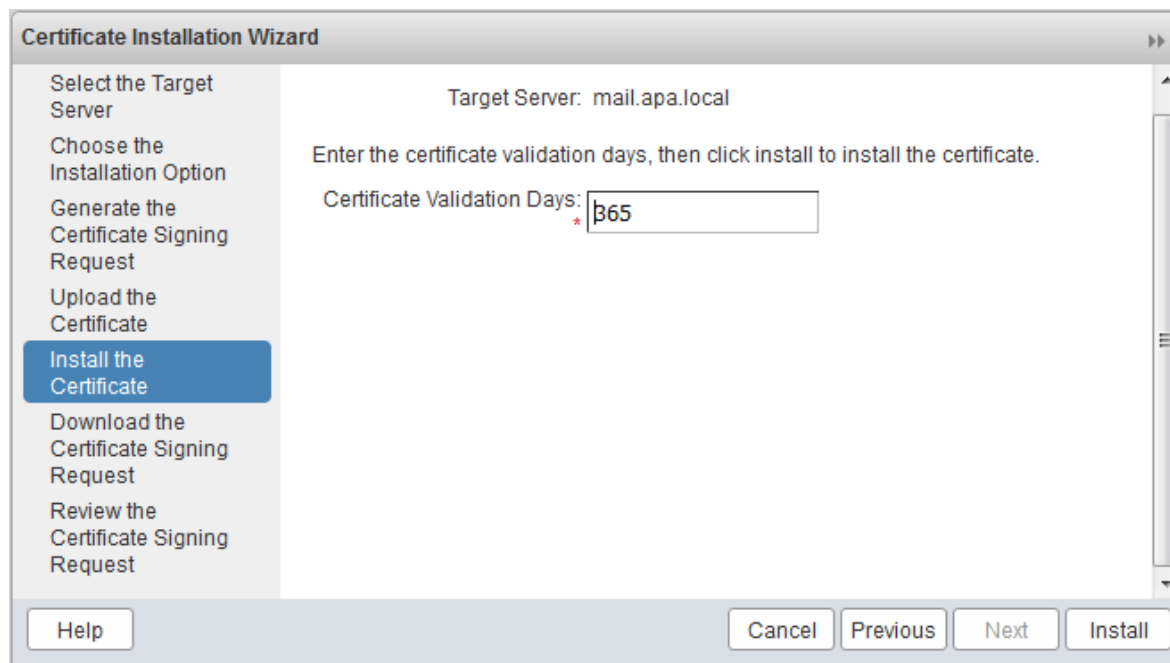
Organizational Unit: Zimbra Collaboration Server

Subject Alternative Name:

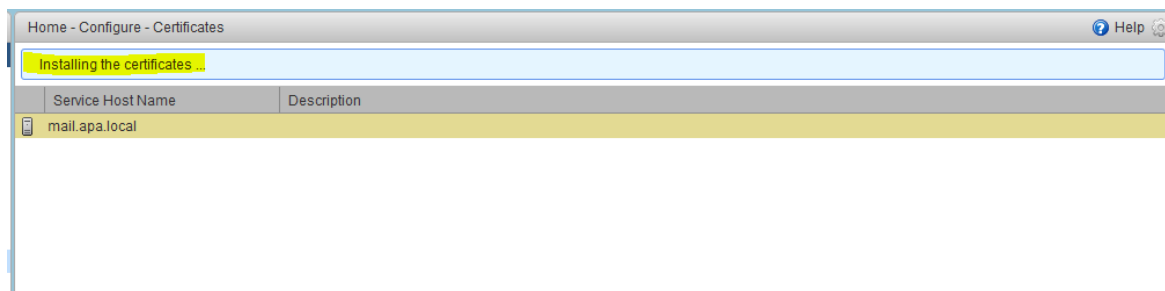
Help Cancel Previous Next Install



در این قسمت شما می‌توانید مدت زمان مدنظر خود را به منظور اعتبار گواهی SSL وارد کنید. به خاطر آورید که این یک گواهی خود-امضا است و اگر شما نقشه‌ای برای تعویض آن در آینده ندارید، می‌توانید زمانی بیشتر از یک سال را انتخاب کنید و سپس دکمه Install را بزنید.



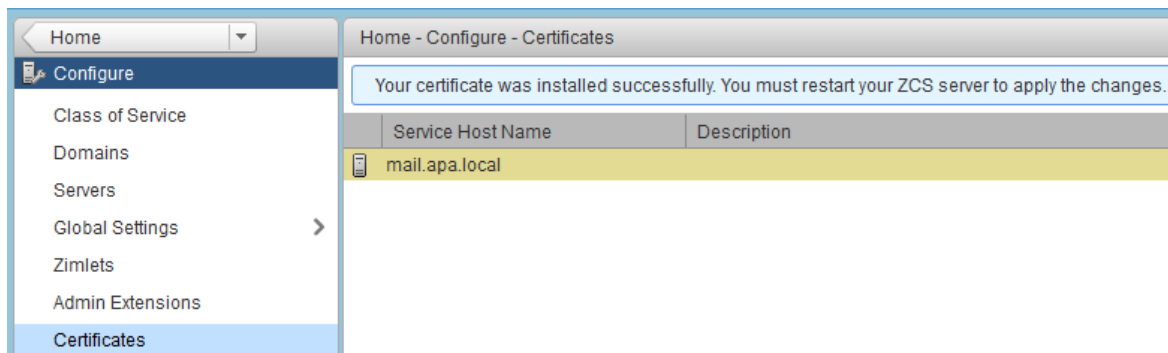
مشاهده می‌کنید گواهی SSL خود-امضا هم اکنون در سرور Zimbra در حال نصب است:



هنگامی که فرآیند نصب به پایان رسید، باید سرور ZCS را به منظور اعمال تغییرات، راه‌اندازی مجدد<sup>۱</sup> نمود.

<sup>۱</sup> restart





The screenshot shows the Zimbra Admin Console interface. On the left is a navigation menu with 'Certificates' selected. The main content area is titled 'Home - Configure - Certificates' and displays a success message: 'Your certificate was installed successfully. You must restart your ZCS server to apply the changes.' Below the message is a table with two columns: 'Service Host Name' and 'Description'. The table contains one entry: 'mail.apa.local'.

به منظور انجام این عمل، دستور زیر را در کنسول توسط کاربر Zimbra وارد کنید:

```
su zimbra  
zmcontrol restart
```

اگر شما به <https://mail.domain.com> بروید، مشکل گواهی SSL را در مرورگر خود به شکل زیر خواهید داشت.

The certificate is not trusted because the issuer certificate is unknown.  
The server might not be sending the appropriate intermediate certificates.  
An additional root certificate may need to be imported.  
The certificate is only valid for [mail.apa.local](mailto:mail.apa.local)

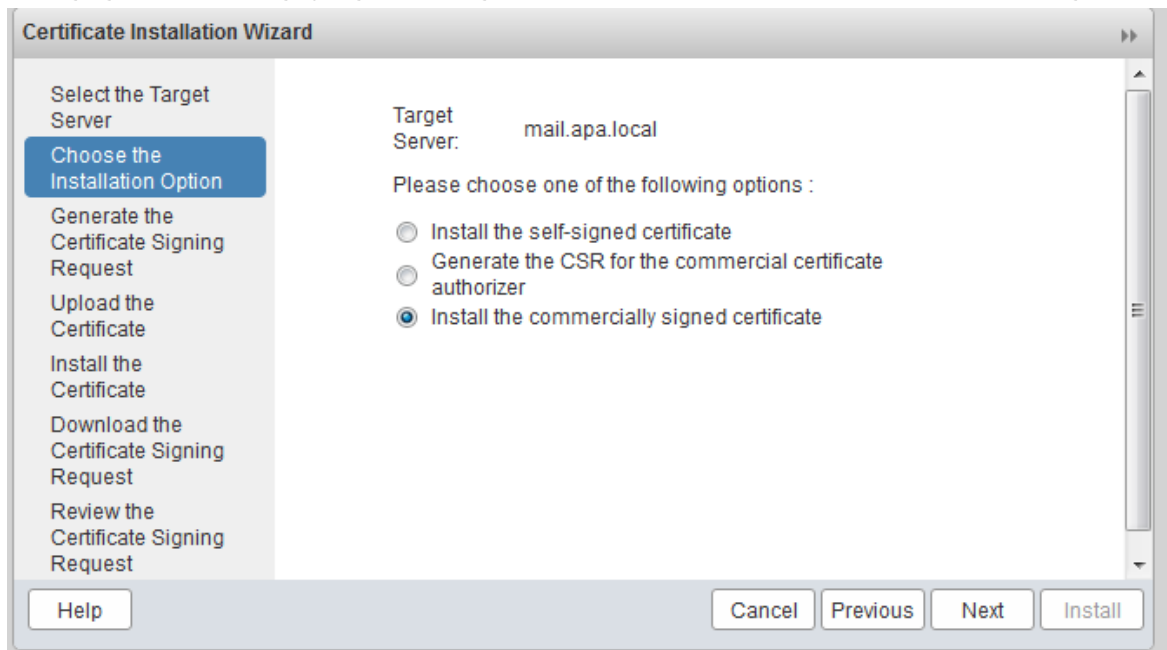
Error code: SEC\_ERROR\_UNKNOWN\_ISSUER

[Add Exception...](#)



## ۲-۳ نصب گواهی SSL تجاری

گواهی‌های تجاری، وابسته به انتخاب شما دارای هزینه‌های مختلفی هستند که باید جزئیات دقیق مراحل اداری را از مرکز صدور گواهی مورد نظر پیگیری کنید. برای نصب یک گواهی تجاری در zimbra، در این قسمت گزینه "Install the commercial signed certificate" را انتخاب کرده و برای ادامه Next را بزنید:

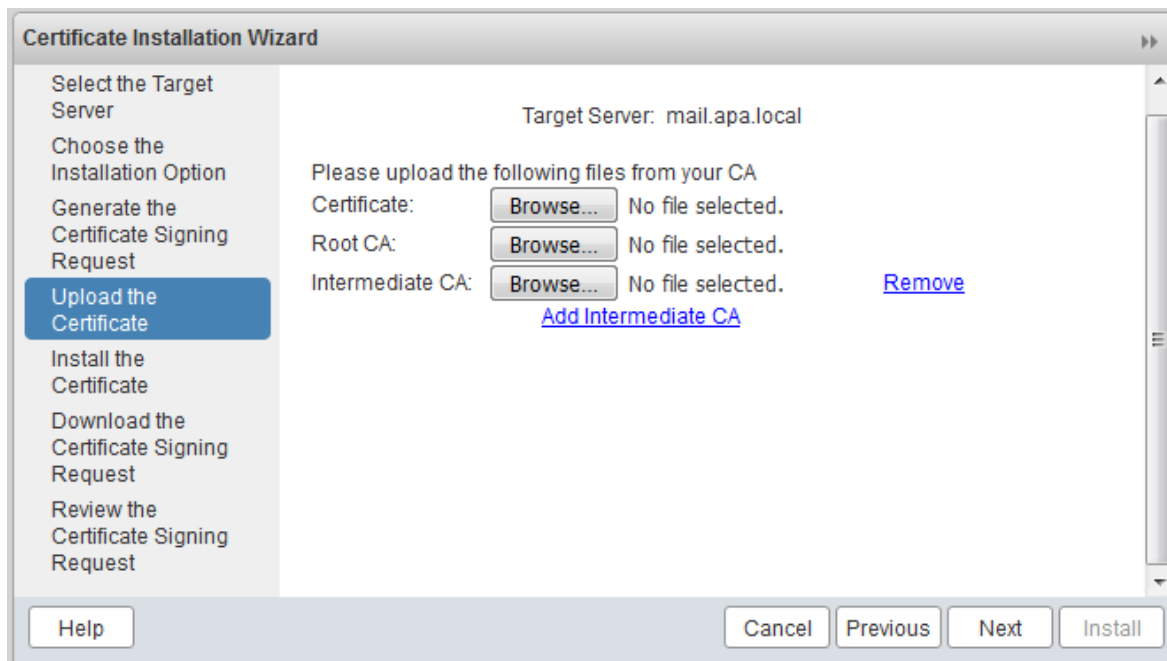


فایل‌های ضروری‌ای که قبلاً گرفته‌اید را بارگذاری کنید:

- گواهی‌نامه: فایل گواهی SSL (.cert)
- CA ریشه: گواهی‌های SSL مربوط به CA ریشه (.cert)
- CA میانی: CAهای میانی (.cert)

ممکن است در این قسمت گزینه‌های دیگری برای وارد کردن CA میانی باشد که اگر شما تنها یک گواهی میانی را از CA خود گرفته‌اید، می‌توانید موارد دیگر را نادیده بگیرید.

روی گزینه "Install" کلیک کنید:



و در آخر سرویس‌های Zimbra را به منظور اعمال تغییرات، راه‌اندازی مجدد کنید.

## ۴ پیکربندی و ایمن‌سازی گواهی SSL

قبل از اینکه تنظیمات ایمن‌سازی SSL را انجام دهید، ابتدا با توجه به مراحل زیر، آخرین وصله<sup>۱</sup> مربوط به Zimbra را نصب کنید. در شکل زیر نسخه zimbra را قبل از نصب وصله، مشاهده می‌کنید:

```
zimbra@mail:~$ zmcontrol -v
Release 8.6.0.GA.1153.UBUNTU14.64 UBUNTU14_64 FOSS edition.
zimbra@mail:~$
```

و برای نصب وصله مورد نظر مراحل زیر را انجام می‌دهیم:

```
root@mail:/home/admin1#
root@mail:/home/admin1# cd zcs-patch-8.6.0_GA_1194
root@mail:/home/admin1/zcs-patch-8.6.0_GA_1194#
root@mail:/home/admin1/zcs-patch-8.6.0_GA_1194#
root@mail:/home/admin1/zcs-patch-8.6.0_GA_1194# ./installPatch.sh
Current Version: 8.6.0_GA_1153
Found Patch for 8.6.0_GA called 8.6.0_P6
Deploying patch for 8.6.0_GA
Updating files for package zimbra-core
/opt/zimbra/zimbramon/pylibs/state.py... copied.
/opt/zimbra/bin/zmtrainsa... copied.
/opt/zimbra/lib/jars/zimbracommon.jar... copied.
/opt/zimbra/libexec/zmfixperms... copied.
/opt/zimbra/lib/jars/zimbrastore.jar... copied.
/opt/zimbra/libexec/zmldapmmrtool... copied.
/opt/zimbra/conf/timezones.ics... copied.
/opt/zimbra/lib/jars/zimbraclient.jar... copied.
/opt/zimbra/lib/jars/zimbrasoap.jar... copied.
com_zimbra_attachcontacts...deployed...updated.
com_zimbra_url...deployed...updated.
Updating files for package zimbra-store
```

و در انتها مشاهده می‌کنید که وصله P6 روی Zimbra نصب شده است.

```
zimbra@mail:~$
zimbra@mail:~$ zmcontrol -v
Release 8.6.0.GA.1153.UBUNTU14.64 UBUNTU14_64 FOSS edition, Patch 8.6.0_P6.
zimbra@mail:~$
zimbra@mail:~$
```

در ادامه‌ی این گزارش، هدف پیکربندی امن پروتکل SSL/TLS است. برای کشف آسیب‌پذیری‌ها در سرور مورد نظر، ابتدا آن را توسط ابزار زیر که توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر طراحی شده است، بررسی کرده و سپس برای رفع مشکلات آن اقدام می‌کنیم:

<https://sslcheck.certcc.ir>

در دو شکل زیر، مشکلات امنیتی SSL و نمره دریافتی (از سایت <https://sslcheck.certcc.ir>) Zimbra را مشاهده می‌کنید که در ادامه قصد داریم این مشکلات را برطرف کرده تا نمره کامل دریافت گردد.

<sup>۱</sup> Patch



### جمع بندی مشکلات

#### مشکلات در گواهی دیجیتال

مستندات امن سازی

- گواهی نامعتبر
- سرور زنجیره کامل گواهی را ارائه نمی کند.

#### قدرت الگوریتم های رمزنگاری

مستندات امن سازی

- سرور از تعدادی دنباله های رمز ضعیف پشتیبانی میکند، که باید حذف شوند.

#### مقاومت در برابر حملات شناخته شده

مستندات امن سازی

- آسیب پذیر به Openssl padding oracle
- آسیب پذیر به RC4

### نمره وب سایت

#### نمره وب سایت: 11.25 از 20



پشتیبانی از پروتکل های امن



قدرت الگوریتم های رمزنگاری



گواهی دیجیتال



مقاومت در برابر حملات شناخته شده



## ۱-۴ حل مشکل استفاده از RC4

الگوریتم RC4 دارای نقاط ضعف قابل بهره‌برداری است و بهتر است از آن استفاده نشود. برای غیرفعال سازی آن در Zimbra، از دستورات زیر استفاده می‌کنیم. صحت اجرای این دستورات در ZCS 8.6، ZCS 8.5 و ZCS 8.0 بررسی شده است.

```
zmprov mcf zimbraReverseProxySSLCiphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128:AES256:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4'
```

```
zmproxycctl restart
```

```
zimbra@mail:/root$
zimbra@mail:/root$
zimbra@mail:/root$ zmprov mcf zimbraReverseProxySSLCiphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128:AES256:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4'
zimbra@mail:/root$
zimbra@mail:/root$
zimbra@mail:/root$ zmproxycctl restart
Stopping nginx...done.
Starting nginx...done.
zimbra@mail:/root$
zimbra@mail:/root$
```

حال بعد از غیرفعال سازی RC4، نمره کمی ارتقا پیدا کرده است که در شکل زیر قابل مشاهده است.

### جمع بندی مشکلات

**مشکلات در گواهی دیجیتال**

- گواهی نامعتبر
- سرور زنجیره کامل گواهی را ارائه نمی کند.

مستندات امن سازی

**قدرت الگوریتم های رمزنگاری**

- سرور از پارامترهای ضعیف تبادل کلید دیفی هلمن پشتیبانی می کند.

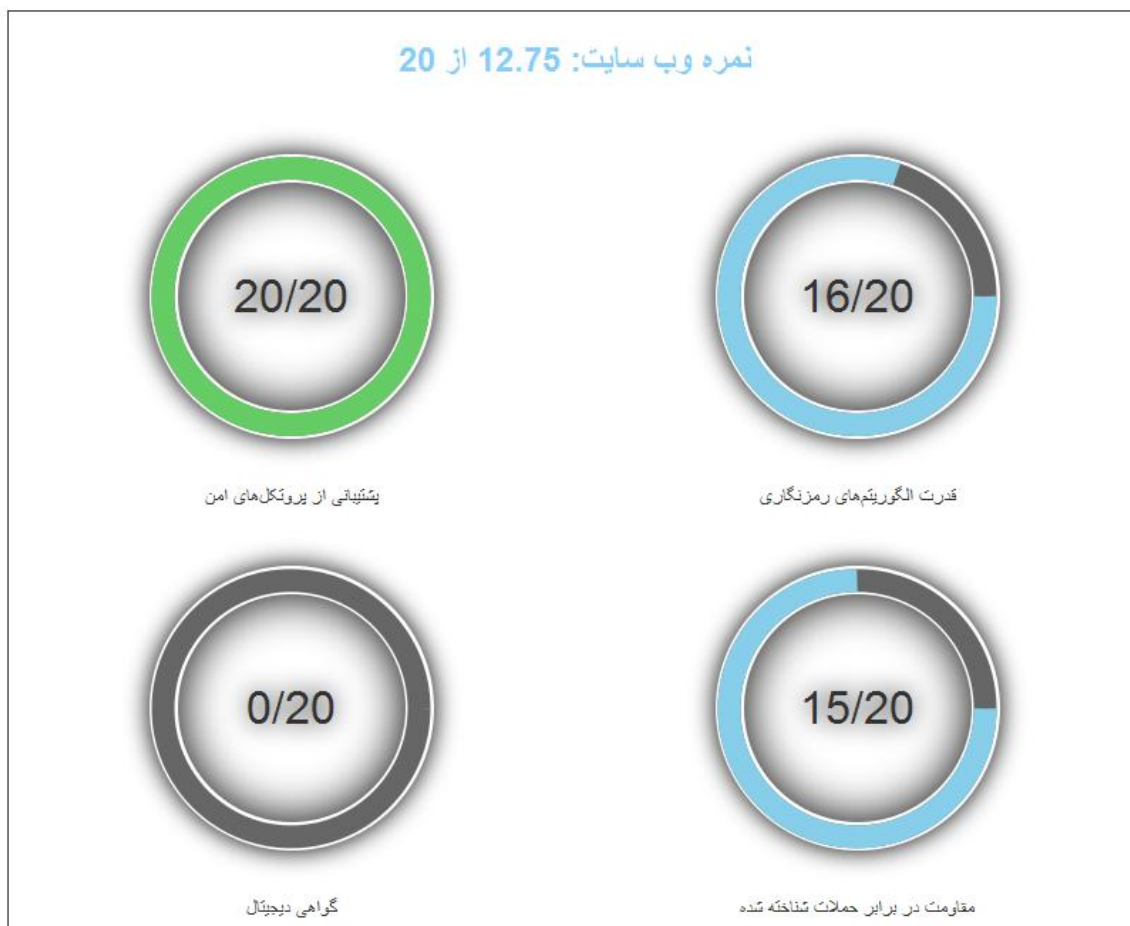
مستندات امن سازی

**مقاومت در برابر حملات شناخته شده**

- آسیب پذیر به Openssl padding oracle

مستندات امن سازی

### نمره وب سایت



## ۲-۴ حل مشکل OpenSSL Padding Oracle

هنگامی که ارتباط از AES CBC استفاده می‌کند و سرور AES-IN را پشتیبانی می‌کند، حمله‌کننده man-in-the-middle با استفاده از این آسیب‌پذیری می‌تواند ترافیک را رمزگشایی کند. برای برطرف کردن این آسیب‌پذیری باید OpenSSL مورد استفاده در Zimbra به روز رسانی شود که به صورت زیر می‌توان این کار را انجام داد:

(as root)

- 1) cd /opt/zimbra
- 2) mv openssl-OLDVERSION openssl-OLDVERSION.OLD
- 3) tar xzf /tmp/openssl-NEWVERSION.tgz

(as user zimbra)

- 4) su - zimbra
- 5) zmcontrol restart

همان‌طور که در شکل زیر مشاهده می‌کنید، این آسیب‌پذیری برطرف شده است.

### جمع بندی مشکلات

#### مشکلات در گواهی دیجیتال

مستندات امن سازی

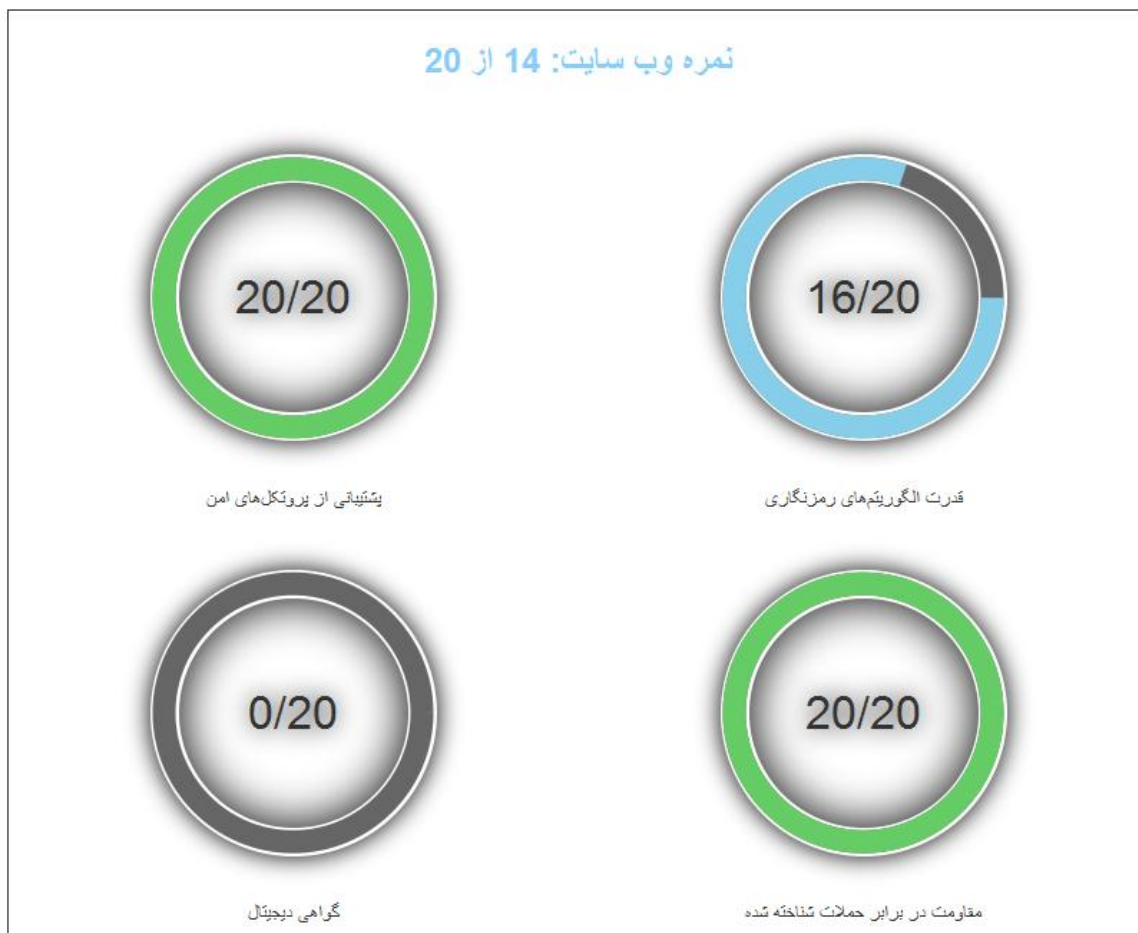
- گواهی نامعتبر
- سرور زنجیره کامل گواهی را ارائه نمی‌کند.

#### قدرت الگوریتم های رمزنگاری

مستندات امن سازی

- سرور از پارامترهای صحیح تبادل کلید دیفی هلمن پشتیبانی می‌کند.

نمره وب سایت



### ۳-۴ حل مشکل پارامترهای ضعیف دینی هلمن

به منظور حل این مشکل، شما می‌توانید سرور خود را به صورت زیر پیکربندی کنید. صحت اجرای این دستورات در ZCS 8.5 و ZCS 8.6 بررسی شده است.

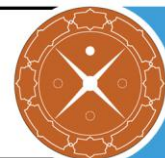
```
cd /opt/zimbra/conf
openssl dhparam -out dhparams.pem 2048
chown zimbra:zimbra dhparams.pem
```

و بعد از آن به ویرایش فایل‌های زیر بپردازید:

- /opt/zimbra/conf/nginx/templates/nginx.conf.web.https.default.template
- /opt/zimbra/conf/nginx/templates/nginx.conf.web.https.template

و خط زیر را در آنها (به صورتی که در شکل‌های زیر نشان داده شده است) اضافه کنید:

```
ssl_dhparam /opt/zimbra/conf/dhparams.pem;
```



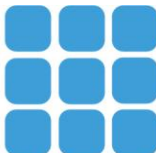
```
root@mail:~#
root@mail:~# cd /opt/zimbra/conf
root@mail:/opt/zimbra/conf# openssl dhparam -out dhparams.pem 2048
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+.....
.....+.....+.....+.....+.....
.....+.....
```

```
root@mail:/opt/zimbra/conf# chown zimbra:zimbra dhparams.pem
root@mail:/opt/zimbra/conf#
```

```
ssl_certificate_key      ${ssl.key.default};
ssl_verify_client       ${ssl.clientcertmode.default};
ssl_verify_depth        ${ssl.clientcertdepth.default};
ssl_dhparam /opt/zimbra/conf/dhparams.pem;
include                  ${core.includes}/${core.cprefix}.web.https.mode-${web.mailmode};
```

```
ssl_certificate_key      ${ssl.key};
ssl_verify_client       ${ssl.clientcertmode};
ssl_dhparam /opt/zimbra/conf/dhparams.pem;
include                  ${core.includes}/${core.cprefix}.web.https.mode-${web.mailmode};
```

```
zimbra@mail:/root$
zimbra@mail:/root$ zmprov mcf zimbraReverseProxySSLCiphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128:AES256:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4'
zimbra@mail:/root$
zimbra@mail:/root$
zimbra@mail:/root$ zmproxctl restart
Stopping nginx...done.
Starting nginx...done.
zimbra@mail:/root$
```



همان طور که در شکل زیر قابل مشاهده است، این مشکل برطرف شده و نمره کامل دریافت شده است.

### جمع بندی مشکلات

#### مشکلات در گواهی دیجیتال

- گواهی نامعتبر
  - سرور زنجیره کامل گواهی را ارائه نمی کند.
- مستندات امن سازی

### جمع بندی قابلیت های پیشنهادی

- بهتر است پشتیبانی از **Strict Transport Security** به قابلیت های سرور اضافه شود.
- مستندات امن سازی

### نمره وب سایت

#### نمره وب سایت: 15 از 20



پشتیبانی از پروتکل های امن



قدرت الگوریتم های رمزنگاری



گواهی دیجیتال



مقاومت در برابر حملات شناخته شده

## ۴-۴ پشتیبانی از Strict Transport Security

Strict Transport Security یک بهبود امنیتی برای برنامه‌های تحت وب است که از HTTPS استفاده می‌کند. این بهبود امنیتی سبب می‌شود که مرورگر به صورت خودکار تمامی ارتباطات را به صورت https یا امن برقرار نماید و از برقراری ارتباط به صورت http (حتی در صورت درخواست کاربر) جلوگیری کند.

برای انجام این کار نیاز است تا دستورات زیر را اجرا کنید که صحت اجرای این دستورات در ZCS 8.7، ZCS 8.0 و ZCS 8.6 بررسی شده است:

```
zmprov mcf +zimbraResponseHeader "Strict-Transport-Security: max-age=31536000"
```

```
zmcontrol restart
```

در صورتی که دستور وارد شده در کادر بالا این مشکل را برطرف نکرد، می‌توانید از دستورات زیر استفاده کنید.

نیاز است تا بعد از گزینه `ssl_verify_depth` در دو فایل زیر:

- `/opt/zimbra/conf/nginx/templates/nginx.conf.web.https.default.template`
- `/opt/zimbra/conf/nginx/templates/nginx.conf.web.https.template`

خط، `add_header Strict-Transport-Security max-age=15768000;` اضافه گردد.

```
root@mail:/opt/zimbra/conf#
root@mail:/opt/zimbra/conf# vim /opt/zimbra/conf/nginx/templates/nginx.conf.web.https.default.template
# HTTPS Proxy Default Configuration
#
server
{
    ${core.ipboth.enabled}listen          [::]:${web.https.port} default;
    ${core.ipv4only.enabled}listen       ${web.https.port} default;
    ${core.ipv6only.enabled}listen       [::]:${web.https.port} default ipv6only=on;
    server_name                          ${web.server_name.default}.default;
    client_max_body_size                  0;
    ssl                                   on;
    ssl_protocols                        ${web.ssl.protocols};
    ssl_prefer_server_ciphers            ${web.ssl.preferserverciphers};
    ssl_ciphers                          ${web.ssl.ciphers};
    ssl_ecdh_curve                       ${web.ssl.ecdh.curve};
    ssl_certificate                      ${ssl.crt.default};
    ssl_certificate_key                  ${ssl.key.default};
    ssl_verify_client                    ${ssl.clientcertmode.default};
    ssl_verify_depth                     ${ssl.clientcertdepth.default};
    add_header Strict-Transport-Security max-age=15768000;
    ssl_dhparam /opt/zimbra/conf/dhparams.pem;
    include                              ${core.includes}/${core.cprefix}.web.https.mode-${web.mailmode};
}
```



```
root@mail:/opt/zimbra/conf#
root@mail:/opt/zimbra/conf# vim /opt/zimbra/conf/nginx/templates/nginx.conf.web.https.template
! (explode domain (vhn))
# HTTPS Proxy Configuration
#
server
{
    server_name                ${vhn};
    ${core.ipboth.enabled}listen                ${vip}:${web.https.port};
    ${core.ipv4only.enabled}listen                ${vip}:${web.https.port};
    ${core.ipv6only.enabled}listen                ${vip}:${web.https.port} ipv6only=on;

    client_max_body_size        0;
    ssl                         on;
    ssl_protocols                ${web.ssl.protocols};
    ssl_prefer_server_ciphers    ${web.ssl.prefer_server_ciphers};
    ssl_ciphers                  ${web.ssl.ciphers};
    ssl_ecdh_curve               ${web.ssl.ecdh.curve};
    ssl_certificate              ${ssl.crt};
    ssl_certificate_key          ${ssl.key};
    ssl_verify_client            ${ssl.clientcertmode};
    add_header Strict-Transport-Security max-age=15768000;
    ssl_dhparam /opt/zimbra/conf/dhparams.pem;
    include                      ${core.includes}/${core.prefix}.web.https.mode-${web.mailmode};
}
```

شکل زیر نشان می‌دهد که این مشکل حل شده است.

## جمع بندی مشکلات

### مشکلات در گواهی دیجیتال

مستندات امن سازی

- گواهی نامعتبر
- سرور زنجیره کامل گواهی را ارائه نمی‌کند.

## ۴-۵ حل مشکلات امنیتی پروتکل SMTP

- غیر فعال کردن الگوریتم‌های رمزنگاری ضعیف:

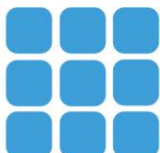
### For ZCS 8.5 , 8.6

```
zmprov mcf zimbraMtaSmtpdTlsCiphers high
zmprov mcf zimbraMtaSmtpdTlsProtocols '!SSLv2,!SSLv3'
zmprov mcf zimbraMtaSmtpdTlsMandatoryCiphers high
zmprov mcf zimbraMtaSmtpdTlsExcludeCiphers 'aNULL,MD5,DES'
Zmcontrol restart
```

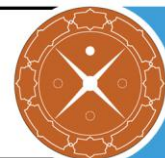
### For ZCS 8.0 and previous

```
zmlocalconfig -e smtpd_tls_ciphers=high
postconf -e smtpd_tls_protocols=!SSLv3,!SSLv2
zmlocalconfig -e smtpd_tls_mandatory_ciphers=high
postconf -e smtpd_tls_exclude_ciphers=aNULL,MD5,DES
```

بعد از ۲ دقیقه، postfix به‌روز رسانی می‌شود.







• حل مشکل استفاده از پارامترهای ضعیف دیفی هلمن:

برای حل این مشکل، مسیر کلیدهای دیفی هلمن که قبلاً تولید کردیم را به فایل مورد نظر اضافه می‌کنیم.

```
zimbra@mail:~/postfix/conf$  
zimbra@mail:~/postfix/conf$ vim main.cf  
smtpd_helo_required = yes  
in_flow_delay = 1s  
transport_maps = proxy:ldap:/opt/zimbra/conf/ldap-transport.cf  
smtpd_tls_dh1024_param_file = /opt/zimbra/conf/dhparams.pem
```

Zmcontrol restart





## منابع ۵

- 1 [https://wiki.zimbra.com/wiki/Administration\\_Console\\_and\\_CLI\\_Certificate\\_Tools](https://wiki.zimbra.com/wiki/Administration_Console_and_CLI_Certificate_Tools)
- 2 <https://www.ssllsupportdesk.com/ssl-installation-instructions-for-zimbra-8-x-x>
- 3 [https://wiki.zimbra.com/wiki/Cipher\\_suites](https://wiki.zimbra.com/wiki/Cipher_suites)
- 4 <https://wiki.zimbra.com/wiki/Security/Collab/logjam>
- 5 [https://wiki.zimbra.com/wiki/Postfix\\_PCI\\_Compliance\\_in\\_ZCS](https://wiki.zimbra.com/wiki/Postfix_PCI_Compliance_in_ZCS)

