

# 第4章 GWS邮件管理

## 练习1

略

## DNS介绍

CNAME记录、TXT记录、MX记录、SPF、DKIM和DMARC 还有NS记录、A记录等。

Name/Host/Alias	Record Type	Priority	Value/Answer/Destination
Blank or @	A	NA	216.239.32.21
Blank or @	MX	1	ASPMX.L.GOOGLE.COM
Blank or @	MX	5	ALTI.ASPMX.L.GOOGLE.COM
Blank or @	MX	10	ASPMX3.GOOGLEMAIL.COM
mail	CNAME	NA	ghs.googlehosted.com.
Blank or @	TXT	NA	google-site-verification=6tTalLzrBX_Ks69jle8
www	CNAME	NA	ghs.googlehosted.com.

## 练习2

参考链接<https://support.google.com/a/answer/140034>



1.先要创建用户账号（应该是指邮箱）然后再将MX记录转到GWS上 2.TTL默认是3600，但正常使用Gmail后可以改为86400，这样更新频率会改为每天1次 3.如果是要把现行的邮箱系统转移到GWS上，可以保留现在的MX记录，但调低优先级（比如将优先级改为10+），当所有邮箱都经由Google后，再删除原MX记录，这样保证不会有邮件丢失

## 练习3

检查MX 工具URL为<https://toolbox.googleapps.com/apps/checkmx/>

Domain name

example.com RUN CHECKS!

---

DKIM selector (optional)

---

## ! trident365.com

There were some critical problems detected with this domain. Mail-flow is probably affected. Please refer to the corresponding help articles.

- |   |  |   |                                     |
|---|--|---|-------------------------------------|
| ! | <a href="#">SPF must allow Google servers to send mail on behalf of your domain.</a> | ? | <a href="#">Help center article</a> |
| ! | <a href="#">Domain must have at least one mail server.</a>                           | ? | <a href="#">Help center article</a> |
| ▲ | DKIM is not set up.  | ? | <a href="#">Help center article</a> |
| ▲ | DMARC is not set up.   | ? | <a href="#">Help center article</a> |
| ▲ | <a href="#">MTA-STS DNS Record.</a>  |   |                                     |
| ▲ | <a href="#">No Google mail exchangers found. Relayhost configuration?</a>            | ? | <a href="#">Help center article</a> |

点击报警会给出解决方法

## 测试1

*You need to make a change to your MX records and you want the change to be implemented as soon as possible. What approach can you take?*

1. Change your MX records in the admin console and reduce the Time to Live (TTL) value to one hour. Once the change has been implemented revert the TTL value to 24 hours
2. **Make the change in your DNS console and reduce the Time to Live (TTL) value to 1 hour. Once the change has been implemented revert the TTL value to 24 hours**
3. Change your MX records in the admin console and reduce the Time to Live (TTL) value to one hour
4. Make the change in your DNS console and reduce the Time to Live (TTL) value to 1 hour

*Which type of DNS record determines where mail destined for your domain is routed?*

1. **MX Record**
2. TXT Record
3. NS Record
4. CNAME Record

In general, from where would you manage your domain's DNS records?

1. All of the options here
2. In your local DNS files
3. **In your domain registrar console**
4. In the Google Workspace admin console

What are common uses for a DNS TXT record when using Google Workspace? (Choose 2)

1. Customise a Google service address
2. Control inbound mail to your domain
3. **Domain verification**
4. **Email security records**

## 邮件安全

3招 SPF DKIM 和 DMARC  
 SPF: verify the domain you own  
 DKIM: prevent email spoofing on outbound message by adding an encrypted header  
 DMARC: tell email servers how to handle messages that fail SPF/DKIM checks

## 练习1

SPF 通过添加TXT记录到DNS中 Xserver中已经有一条记录了，现在在后面追加

```
include:_spf.google.com ~all
```


记录生效需要24小时左右 参考链

接：<https://support.google.com/a/answer/33786#zippy=%2Cspf-%E8%AE%B0%E5%BD%95%E7%A4%BA%E4%BE%8B>

## 练习2

The screenshot shows the 'Authenticate email' settings page in the Google Workspace Admin console. The page is titled 'Authenticate email' and shows the status as 'Not authenticating email'. The selected domain is 'trident365.com'. The status is 'Not authenticating email' and the message says 'You must update the DNS records for this domain. To start authenticating email for the domain selected above, enter the following DNS TXT record into your domain provider's DNS settings page. Then click 'Start authentication.''. The DNS Host name (TXT record name) is empty, and the TXT record value is empty. A red arrow points to the 'GENERATE NEW RECORD' button. A note at the bottom says 'It may take up to 48 hours for DNS changes to fully propagate.'.

# Generate new record

 You must wait 24 to 72 hours after enabling Gmail with a registered domain before you can create a DKIM record. [Learn more.](#)

If you are currently authenticating email from this domain, generating a new TXT record will stop authentication until you restart it and wait for DNS to update.

Select DKIM key bit length

2048 ▼

Prefix selector (optional)

google

CANCEL GENERATE

生成后长这个样子

Status: Not authenticating email

You must update the DNS records for this domain.

To start authenticating email for the domain selected above, enter the following DNS TXT record into your domain provider's DNS settings page. Then click "Start authentication."

DNS Host name (TXT record name):  
google.\_domainkey

TXT record value:

v=DKIM1; k=rsa;  
p=MIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBChKCAGEAs1ap/h/3GcUga0iQOiqIRQ/6786OfROCx4LIsXHA5MjsXokNH99or  
hTDKhrWZX6JL/cKGYsjZZF...NmfQ+/pLWfPHvuZ6  
br3Wsq...NGL7up0Tlhqv/UVbw8F1Z  
91/kOZQdfel...ynnyETLfEGVF33IBPgwIDAQAB

GENERATE NEW RECORD

 It may take up to 48 hours for DNS changes to fully propagate.

START AUTHENTICATION

生成的记录在Xserver的DNS DKIM记录中已经有了，一模一样。参考链接：  
<https://support.google.com/a/answer/174124>

## 练习3

```
✓ _dmarc.trident365.com      TXT      v=DMARC1; p=none; rua=mailto:admin@trident365.com      3600      0
```

这条TXT记录告诉收件邮箱服务器，如果判定Fail如何操作，这里是通知管理员。

## 测试2

*What is the main purpose of a Sender Policy Framework (SPF) record?*

1. **It specifies which servers/domains can send messages on your behalf**
2. It can be used to verify that message content is authentic and has not changed
3. It defines the action to take on suspicious incoming messages

*You have been asked to implement DomainKeys Identified Mail (DKIM) for your organization. How would you do this?*

1. Enable DKIM from Apps > Google Workspace > Gmail > Authenticate email
2. Enable DKIM directly in your DNS records
3. Generate a key from your DNS records and add it to the Google Workspace admin console. Then Enable DKIM from Apps > Google Workspace > Gmail > Authenticate email
4. **Generate a DKIM record from Apps > Google Workspace > Gmail > Authenticate email. Add the record to your DNS records and then start authentication from the admin console**

*What policy defines what to do if an incoming message is not authenticated?*

1. SPF
2. DKIM
3. All of the options here
4. **DMARC**

*DKIM adds an encrypted signature to the header of all outgoing messages. What happens if you don't turn on email signing with your own domain DKIM key?*

1. Gmail signs all outgoing messages with a temporary key generated for your domain
2. **Gmail signs all outgoing messages with this default DKIM domain key d=\*.gappssmtp.com**
3. Gmail signs all outgoing messages with a key generated using the From address in the message
4. Messages are sent as normal with no additional headers

## 邮件安全配置

对于未受信任的发件人的加密附件，处理方式是隔离。

Apps > Google Workspace > Settings for Gmail > Safety

**即便你把某一个域加为安全，但这里的设定仍然会生效。各自相互独立**

## 练习2

对于外包人员，禁止他们的自动转发邮件到个人邮箱，并且禁止POP和IMAP，但那些开户GWS Sync的人例外。

Apps > Google Workspace > Settings for Gmail > End User Access

现在Rules也会终止工作

## 测试3

*The attachment section in the Gmail Safety settings page allows you to protect against malicious attachments. What actions can you perform on a suspicious attachment? (Choose 2)*

1. Keep email in inbox without warning
2. **Move email to spam**
3. Send to a designated user
4. **Keep email in inbox and show warning**

*You have enabled protection against anomalous attachment types in emails from the Gmail > Safety page but you are finding some emails with valid attachment types are not being delivered. How can*

*you resolve this?*

1. Ask each user to create an allowlist of allowable file types
2. **Add an allowlist of allowable file types to the entry in the Attachments section on the Safety page**
3. Have all messages that trigger this setting delivered to a quarantine and then release the messages manually
4. You cannot control what file types are considered anomalous so you must disable this protection to allow messages to be delivered

*What are valid reasons for allowing per-user outbound gateways in your organization? (Choose 2)*

1. **An outbound gateway ensures that the same mail server delivers all messages from otherdomain and that server has a record that the mail has been sent**
2. Mail delivery times are improved because messages bypass the Gmail servers
3. **An outbound gateway can prevent the appearance of “on behalf of” addresses in the From field**
4. Allows your users to send mail from their business and personal Gmail account from one inbox

*Google recommends against the use of the Image URL proxy allowlist?*

1. **True**
2. False

From:

<https://www.trident365.com/> - 三叉戟

Permanent link:

[https://www.trident365.com/doku.php?id=resources:courses:gws\\_c4&rev=1737639805](https://www.trident365.com/doku.php?id=resources:courses:gws_c4&rev=1737639805)

Last update: **2025/01/23 22:43**

