適用於電子郵件安全裝置的DANE

目錄

簡介

本文檔介紹ESA出站郵件流的DANE實施。

必要條件

ESA概念和配置的一般知識。

實施DANE的要求：

- 支援DNSSEC的DNS解析程式
- 使用AsyncOS 12.0或更高版本的ESA

背景資訊

DANE已引入ESA 12用於出站郵件驗證。

命名實體的DNS型驗證(DANE)。

- DANE是一種網際網路安全協定，允許X.509數位證書使用DNSSEC繫結到域名。(RFC 6698)
- DNSSEC是一組IETF規範，用於通過使用公鑰加密來保護DNS記錄。(非常簡單的解釋。RFC 4033、RFC 4034和RFC 4035)

實施注意事項

驗證ESA是否使用支援dnssec的DNS解析程式。

實施DANE需要DNS功能來執行dnssec/DANE查詢。

要測試ESA DNS DANE功能，可從ESA CLI登入執行簡單測試。

CLI命令「daneverify」將執行複雜的查詢，以驗證域是否能夠通過DANE驗證。

同一命令可用於確認已知正常的域，以確認ESA解析dnssec查詢的能力。

「ietf.org」是全域性已知源。執行cli命令「daneverify」將驗證DNS解析程式是否支援DANE。

有效通行證：ietf.org的DANE支援DNS伺服器「DANE成功」結果

```
> daneverify ietf.org

SECURE MX record(mail.ietf.org) found for ietf.org
SECURE A record (4.31.198.44) found for MX(mail.ietf.org) in ietf.org
Connecting to 4.31.198.44 on port 25.
Connected to 4.31.198.44 from interface 216.71.133.161.
SECURE TLSA record found for MX(mail.ietf.org) in ietf.org
Checking TLS connection.
TLS connection established: protocol TLSv1.2, cipher ECDHE-RSA-AES256-GCM-SHA384.
Certificate verification successful
TLS connection succeeded ietf.org.
DANE SUCCESS for ietf.org
DANE verification completed.
```

無效失敗：不支援DANE的DNS伺服器「BOGUS」結果對於ietf.org

```
> daneverify ietf.org

BOGUS MX record found for ietf.org
DANE FAILED for ietf.org
DANE verification completed.
```

有效失敗：daneverify cisco.com >思科尚未實施DANE。這是支援dnssec的解析程式的預期結果。

```
> daneverify cisco.com

INSECURE MX record(alln-mx-01.cisco.com) found for cisco.com
INSECURE MX record(alln-mx-01.cisco.com) found. The command will still proceed.
INSECURE A record (173.37.147.230) found for MX(alln-mx-01.cisco.com) in cisco.com
Trying next MX record in cisco.com
INSECURE MX record(rcdn-mx-01.cisco.com) found for cisco.com
INSECURE MX record(rcdn-mx-01.cisco.com) found. The command will still proceed.
INSECURE A record (72.163.7.166) found for MX(rcdn-mx-01.cisco.com) in cisco.com
Trying next MX record in cisco.com
INSECURE MX record(aer-mx-01.cisco.com) found for cisco.com
INSECURE MX record(aer-mx-01.cisco.com) found. The command will still proceed.
INSECURE A record (173.38.212.150) found for MX(aer-mx-01.cisco.com) in cisco.com
DANE FAILED for cisco.com
DANE verification completed.
```

如果以上測試「有效」工作：

- 謹慎的方法是在新增域配置檔案之前測試每個域。
- 更積極的方法是在預設目標控制配置檔案上配置DANE並檢視通過/失敗的人員。

Mail Direction確定DANE是否將進行驗證。

已配置「RELAY」操作的發件人組/郵件流策略將執行DANE驗證。

配置了「接受」操作的發件人組/郵件流策略將不執行DANE驗證。

> **注意**：如果ESA在預設策略上啟用目的地控制「DANE」，**則存在交付失敗的風險。** 如果某個內部擁有的域（如RAT中列出的域）同時通過RELAY和ACCEPT郵件流策略，同時為該域提供SMTP路由。

SMTP 路由

除非將「目標主機」配置為「USEDNS」，否則在SMTP路由上DANE將失敗。

在退回配置檔案計時器過期之前，DANE機會不會傳送郵件，這些郵件將包含在傳送隊列中。

為什麼？將跳過DANE驗證，因為SMTP路由將是對實際目標的修改，可能不能正確使用DNS。

解決方案：建立目標控制配置檔案以顯式禁用包含SMTP路由的域的DANE驗證

DANE機會主義或DANE必備

在DANE驗證期間將執行下列查詢。

每個驗證饋送內容以執行隨後的驗證。

- MX記錄查詢驗證是否>>安全、不安全、偽造
- 記錄查詢驗證是否>>>安全不安全>偽造
- TLSA記錄查詢驗證是否>>安全、不安全、偽造、NXDOMAIN
- 證書驗證>>成功，失敗

安全：

- DNS已驗證是否存在包含RRSIG驗證的已簽名RRSIG DS和DNSKEY的安全記錄（位於信任鏈的上方）。

不安全：

- DNS確定域中不存在已啟用dnssec的記錄。

假冒產品：

- 不完整，但存在的dnssec條目可能無法通過驗證。
- 由於金鑰過期，記錄無效。
- 信任鏈中缺少記錄或金鑰。

NXDOMAIN

- 在DNS中找不到記錄。

上述記錄檢查和驗證結果的組合將確定「DANE成功」| DANE失敗 | DANE回退到TLS。"

例如：如果沒有為example.com的MX記錄傳送RRSIG，則會檢查父區域(.com)以檢視example.com是否具有DNSKEY記錄，指示example.com應對其記錄進行簽名。通過達到根區域(.)金鑰驗證，此驗證將繼續在信任鏈上完成，並且根區域的金鑰與ESA預期匹配（ESA上的硬編碼值，基於RFC5011自動更新）。

DANE必填

MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed	DANE Fail
Secure	Secure	Insecure		DANE Fail
Secure	secure	NXDOMAIN		DANE Fail
Secure	Secure	Bogus		DANE Fail
Secure	Insecure			DANE Fail
secure	Bogus			DANE Fail
Insecure	Secure	Secure	Success	DANE Fail
Insecure	Secure	Secure	Fail	DANE Fail
Insecure	Secure	Insecure		DANE Fail
Insecure	Secure	NXDOMAIN		DANE Fail
Insecure	Secure	Bogus		DANE Fail
Insecure	Insecure			DANE Fail
Insecure	Bogus			DANE Fail
Bogus				DANE Fail

DANE必填

附註：DANE機會主**義不像TLS首選的那樣運行。**下圖中的ACTION部分會導致DANE FAIL，不會為Mandatory或Opportitional提供。消息將保留在傳送隊列中，直到計時器過期，然後傳送終止。

DANE機會主義

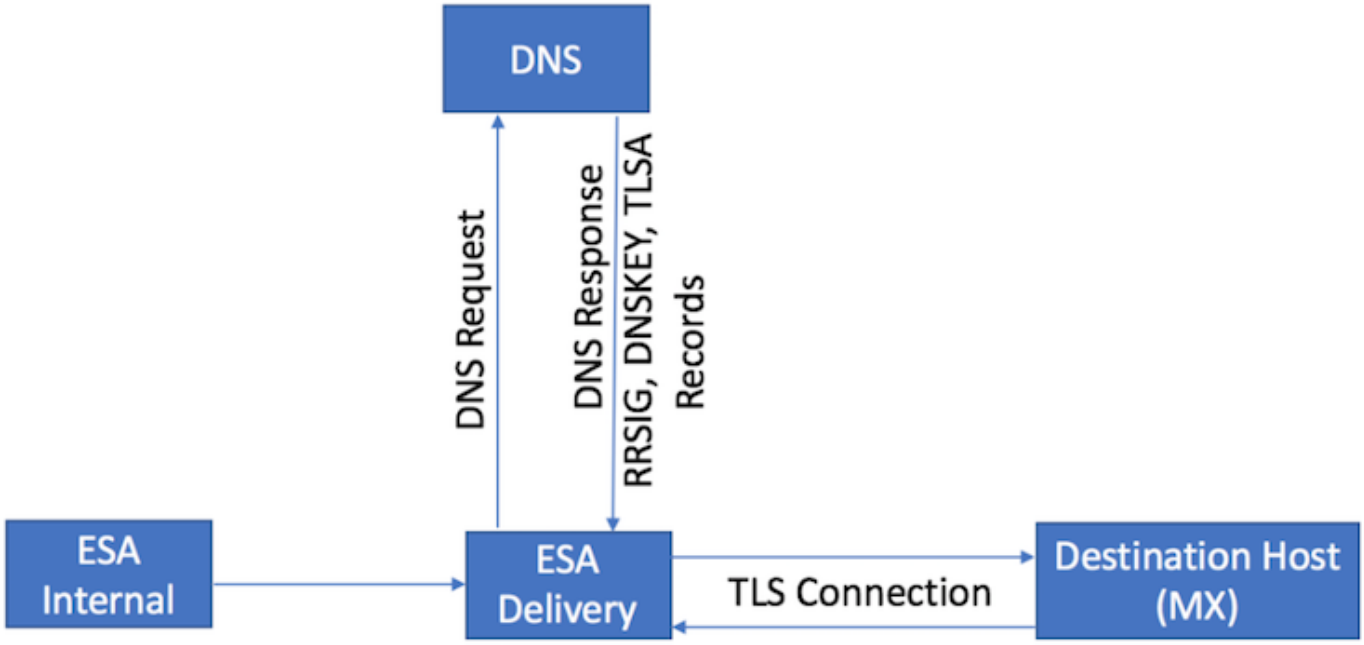
MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed →	DANE Fail
Secure	Secure	Insecure		Fallback to opportunistic TLS flow
Secure	secure	NXDOMAIN		Fallback to opportunisticTLS flow
Secure	Secure	Bogus	→	DANE Fail
Secure	Insecure	Mail will not be delivered for the marked arrows		Fallback to opportunistic TLS flow
secure	Bogus		→	DANE Fail
Insecure	Secure	Secure		Fallback to opportunisticTLS flow
Insecure	Secure	Insecure		Fallback to opportunisticTLS flow
Insecure	Secure	NXDOMAIN		Fallback to opportunisticTLS flow
Insecure	Secure	Bogus	→	DANE Fail
Insecure	Insecure			Fallback to opportunisticTLS flow
Insecure	Bogus			DANE Fail
Bogus			→	DANE Fail

DANE機會主義

在多裝置環境中啟用DANE

下圖說明了在多裝置環境中啟用DANE時的工作流程。

如果環境有多層ESA裝置，其中一層用於掃描，另一層用於傳送消息確保DANE僅在直接連線到外部目標的裝置上配置。



多ESA設計。在交付ESA上配置的DANE

管理多個DNS解析器

如果一個ESA配置了多個DNS解析器（少數支援DNSSEC的解析器，少數不支援DNSSEC的解析器），Cisco建議為支援DNSSEC的解析器配置更高的優先順序（更低的數值），以防止不一致。

這可以防止不支援DNSSEC的解析程式將支援DANE的目標域分類為「偽造」。

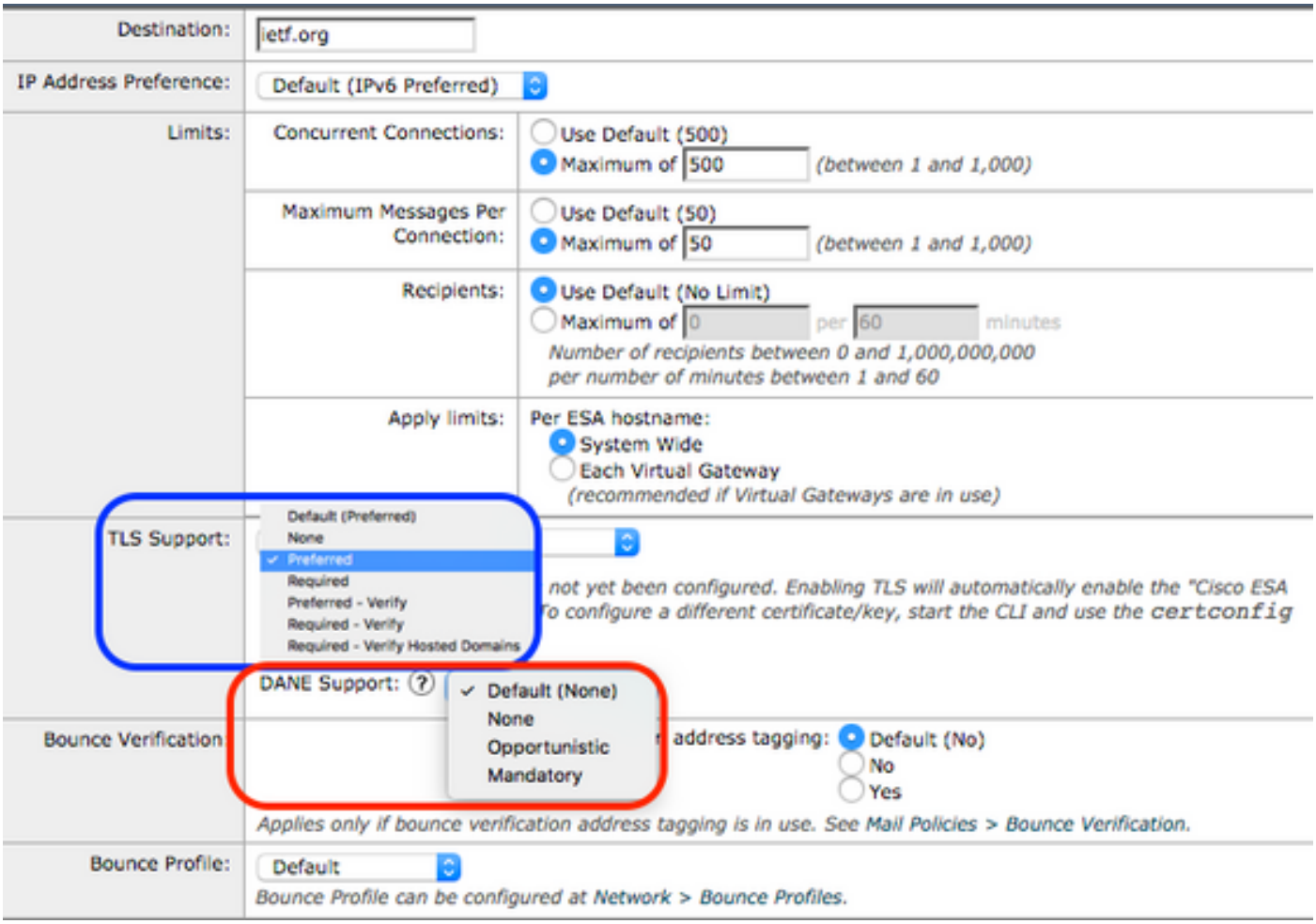
管理輔助DNS伺服器

當DNS解析程式不可訪問時，DNS會回退到輔助DNS伺服器。如果未在輔助DNS伺服器上配置DNSSEC，則支援DANE的目標域的MX記錄被分類為「偽造」。 這將影響報文的傳送，而無論DANE設定如何（機會性設定或強制性）。 思科建議您使用支援DNSSEC的輔助解析程式。

組態

為出站郵件流配置DANE。

1. Web導航至>郵件策略>目標控制>新增目標
2. 根據您的偏好完成配置檔案的頂部。
3. TLS 支援：**必須設定為「首選TLS」 |首選 — 驗證 |必需 |必需 — 驗證|必需 — 驗證託管域。"**
4. 啟用TLS支援後，DANE支援：下拉選單將變為活動狀態。
5. **DANE支援：選項包括「無」 |機會主義 |必填。**
6. 完成「DANE支援」選項後，提交並提交更改。



目的地控制設定檔 — DANE驗證

驗證DANE成功

交貨狀態

監控WebUI「Delivery Status」（傳送狀態）報告，以瞭解可能由DANE故障導致的任何意外的目標域建立。

在啟用服務之前執行此操作，然後定期執行幾天以確保持續成功。

ESA WebUI >監控>傳送狀態>檢查「活動接收人」列。

郵件日誌

日誌級別的預設郵件日誌資訊級別。

郵件日誌顯示DANE成功協商郵件的非常微妙的指示器。

出站的最終TLS協商將包含經過微幅修改的輸出，以便在日誌條目末尾包含域。

日誌條目將包含「TLS成功協定」，後跟「for domain.com」的TLS版本/密碼。

魔力來自「for」：

```
myesa.local> grep "TLS success.*for" mail_logs

Tue Feb  5 13:20:03 2019 Info: DCID 2322371 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-
GCM-SHA384 for karakun.com
```

郵件日誌調試

調試級別的自定義郵件日誌將顯示完整的DANE和dnssec查詢、預期的協商、通過/失敗的檢查部分以及成功指標。

> **附註**：**為調試級別日誌記錄配置的郵件日誌可能會消耗ESA上過多的資源，具體取決於系統負載和配置。**

為調試級別日誌記錄配置的郵件日誌可能會消耗ESA上過多的資源，具體取決於系統負載和配置。

郵件日誌通常不會在調試級別保留很長時間。

調試級別日誌可能會在短時間內生成大量郵件日誌。

一種常見的做法是為mail_logs_d建立額外的日誌訂閱，並為DEBUG設定日誌記錄。

該操作可防止對現有mail_logs的影響，並允許對為訂閱維護的日誌捲進行操作。

要控制建立的日誌量，請將要維護的檔案數限製為較小的檔案數，如2-4個檔案。

監控、試用期或故障排除完成後，禁用日誌。

為調試級別設定的郵件日誌顯示非常詳細的DANE輸出：

Success sample daneverify

```
daneverify ietf.org

SECURE MX record(mail.ietf.org) found for ietf.org
```

```
SECURE A record (4.31.198.44) found for MX(mail.ietf.org) in ietf.org
Connecting to 4.31.198.44 on port 25.
Connected to 4.31.198.44 from interface 194.191.40.74.
SECURE TLSA record found for MX(mail.ietf.org) in ietf.org
Checking TLS connection.
TLS connection established: protocol TLSv1.2, cipher DHE-RSA-AES256-GCM-SHA384.
Certificate verification successful
TLS connection succeeded ietf.org.
DANE SUCCESS for ietf.org
DANE verification completed.
```

debug level mail logs during the above 'daneverify' exeuction.
Sample output from the execution of the daneverify ietf.org will populate the dns lookups within the mail logs

```
Mon Feb 4 20:08:47 2019 Debug: DNS query: Q('ietf.org', 'MX')
Mon Feb 4 20:08:47 2019 Debug: DNS query: QN('ietf.org', 'MX', 'recursive_nameserver0.parent')
Mon Feb 4 20:08:47 2019 Debug: DNS query: QIP ('ietf.org','MX','194.191.40.84',60)
Mon Feb 4 20:08:47 2019 Debug: DNS query: Q ('ietf.org', 'MX', '194.191.40.84')
Mon Feb  4 20:08:48 2019 Debug: DNSSEC Response data([(0, 'mail.ietf.org.')], secure, 0, 1800)
Mon Feb 4 20:08:48 2019 Debug: DNS encache (ietf.org, MX, [(8496573380345476L, 0, 'SECURE', (0,
'mail.ietf.org'))])
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q('mail.ietf.org', 'A')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QN('mail.ietf.org', 'A',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QIP ('mail.ietf.org','A','194.191.40.84',60)
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q ('mail.ietf.org', 'A', '194.191.40.84')
Mon Feb  4 20:08:48 2019 Debug: DNSSEC Response data(['4.31.198.44'], secure, 0, 1800)
Mon Feb 4 20:08:48 2019 Debug: DNS encache (mail.ietf.org, A, [(8496573380345476L, 0, 'SECURE',
'4.31.198.44')])
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q('mail.ietf.org', 'AAAA')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QN('mail.ietf.org', 'AAAA',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QIP ('mail.ietf.org','AAAA','194.191.40.84',60)
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q ('mail.ietf.org', 'AAAA', '194.191.40.84')
Mon Feb 4 20:08:48 2019 Warning: Received an invalid DNSSEC Response:
DNSSEC_Error('mail.ietf.org', 'AAAA', '194.191.40.84', 'DNSSEC Error for hostname mail.ietf.org
(AAAA) while asking 194.191.40.84. Error was: Unsupported qtype') of qtype AAAA looking up
mail.ietf.org
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q('mail.ietf.org', 'CNAME')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QN('mail.ietf.org', 'CNAME',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QIP ('mail.ietf.org','CNAME','194.191.40.83',60)
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q ('mail.ietf.org', 'CNAME', '194.191.40.83')
Mon Feb 4 20:08:48 2019 Debug: DNSSEC Response data([], , 0, 1800)
Mon Feb 4 20:08:48 2019 Debug: Received NODATA for domain mail.ietf.org type CNAME
Mon Feb 4 20:08:48 2019 Debug: No CNAME record(NoError) found for domain(mail.ietf.org)

Mon Feb  4 20:08:49 2019 Debug: DNS query: Q('_25._tcp.mail.ietf.org', 'TLSA')
Mon Feb 4 20:08:49 2019 Debug: DNS query: QN('_25._tcp.mail.ietf.org', 'TLSA',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:49 2019 Debug: DNS query: QIP
('_25._tcp.mail.ietf.org','TLSA','194.191.40.83',60)
Mon Feb 4 20:08:49 2019 Debug: DNS query: Q ('_25._tcp.mail.ietf.org', 'TLSA', '194.191.40.83')
Mon Feb  4 20:08:49 2019 Debug: DNSSEC Response
data(['0301010c72ac70b745ac19998811b131d662c9ac69dbdbe7cb23e5b514b56664c5d3d6'], secure, 0,
1800)
Mon Feb  4 20:08:49 2019 Debug: DNS encache (_25._tcp.mail.ietf.org, TLSA, [(8496577312207991L,
0, 'SECURE', '0301010c72ac70b745ac19998811b131d662c9ac69dbdbe7cb23e5b514b56664c5d3d6')])
```

fail sample daneverify

[]> thinkbeyond.ch

INSECURE MX record(thinkbeyond-ch.mail.protection.outlook.com) found for thinkbeyond.ch
INSECURE MX record(thinkbeyond-ch.mail.protection.outlook.com) found. The command will still proceed.
INSECURE A record (104.47.9.36) found for MX(thinkbeyond-ch.mail.protection.outlook.com) in thinkbeyond.ch
Trying next A record (104.47.10.36) for MX(thinkbeyond-ch.mail.protection.outlook.com) in thinkbeyond.ch
INSECURE A record (104.47.10.36) found for MX(thinkbeyond-ch.mail.protection.outlook.com) in thinkbeyond.ch
DANE FAILED for thinkbeyond.ch
DANE verification completed.

mail_logs

Sample output from the execution of he danverify thinkbeyond.ch will populate the dns lookups within the mail logs

```
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond.ch', 'MX')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond.ch', 'MX',
'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond.ch','MX','194.191.40.84',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond.ch', 'MX', '194.191.40.84')
Mon Feb  4 20:15:52 2019 Debug: DNSSEC Response data([(10, 'thinkbeyond-
ch.mail.protection.outlook.com.')], insecure, 0, 3600)
Mon Feb 4 20:15:52 2019 Debug: DNS encache (thinkbeyond.ch, MX, [(8502120882844461L, 0,
'INSECURE', (10, 'thinkbeyond-ch.mail.protection.outlook.com'))])
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond-ch.mail.protection.outlook.com', 'A')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond-ch.mail.protection.outlook.com', 'A',
'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','A','194.191.40.83',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com', 'A',
'194.191.40.83')
Mon Feb  4 20:15:52 2019 Debug: DNSSEC Response data(['104.47.9.36', '104.47.10.36'], insecure,
0, 10)
Mon Feb 4 20:15:52 2019 Debug: DNS encache (thinkbeyond-ch.mail.protection.outlook.com, A,
[(8497631700844461L, 0, 'INSECURE', '104.47.9.36'), (8497631700844461L, 0, 'INSECURE',
'104.47.10.36')])
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond-ch.mail.protection.outlook.com',
'AAAA')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond-ch.mail.protection.outlook.com',
'AAAA', 'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','AAAA','194.191.40.84',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com',
'AAAA', '194.191.40.84')
Mon Feb 4 20:15:52 2019 Debug: DNSSEC Response data([], , 0, 32768)
Mon Feb 4 20:15:52 2019 Debug: Received NODATA for domain thinkbeyond-
ch.mail.protection.outlook.com type AAAA
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME', 'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','CNAME','194.191.40.83',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME', '194.191.40.83')
Mon Feb 4 20:15:53 2019 Warning: Received an invalid DNS Response: SERVER FAILED to IP
194.191.40.83 looking up thinkbeyond-ch.mail.protection.outlook.com
Mon Feb 4 20:15:53 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','CNAME','194.191.40.84',60)
Mon Feb 4 20:15:53 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME', '194.191.40.84')
Mon Feb 4 20:15:54 2019 Warning: Received an invalid DNS Response: SERVER FAILED to IP
194.191.40.84 looking up thinkbeyond-ch.mail.protection.outlook.com
Mon Feb 4 20:15:54 2019 Debug: No CNAME record() found for domain(thinkbeyond-
ch.mail.protection.outlook.com)
```

相關資訊

- ESA使用手冊
- ESA發行說明
- ESA CLI參考指南