E メール セキュリティ アプライアンスのためのデンマーク人

目次

概要

この資料は ESA 送信 メール フローのためのデンマーク人実装を記述したものです。

前提条件

ESA 概念および設定の一般的な知識。

デンマーク人を設定する必要条件:

- DNSSEC 可能な DNS リゾルバ
- AsyncOS 12.0 の ESA またはより新しい

背景説明

デンマーク人は送信 メール 検証のための ESA 12 に導入されました。

指定 Entities （ デンマーク人 ）の DNS ベース 認証。

- デンマーク人は DNSSEC を使用してドメイン名に結合 されるように X.509 デジタル証明書がするインターネット セキュリティ プロトコルです。 （ RFC 6698 ）
- DNSSEC は公開キー暗号化の使用によって DNS レコードを保護するための IETF 仕様の収

集です。（非常に基本的な説明。 RFC 4033、RFC 4034 および RFC 4035）

実装に関する問題

ESA が dnssec 可能な DNS リゾルバを利用することを確認して下さい。

dnssec/DANE クエリを行う DNS 機能がデンマーク人を設定するために必要となります。

ESA DNS デンマーク人機能をテストするために簡単なテストは ESA CLI ログオンから実行されたことができます。

CLI コマンドは行いますドメインが通過デンマーク人確認が可能であるかどうか確かめるために複雑なクエリーを「daneverify」。

既知よいドメインと同じコマンドが dnssec クエリを解決する ESA 機能を確認するのに使用することができます。

「ietf.org」はグローバルに既知出典です。 DNS リゾルバが可能なデンマーク人であるかどうか CLI コマンドを「実行して」確かめます daneverify。

有効な PASS: デンマーク人可能な DNSサーバ「デンマーク人成功」は ietf.org のために起因します

```
> 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.
```

無効 FAIL: NON-DANE ietf.org のための可能な DNSサーバ「偽」結果

```
> daneverify ietf.org

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

有効な FAIL: cisco.com > cisco を設定しませんでしたデンマーク人を daneverify。 これは dnssec 可能なリゾルバからの期待された結果です。

```
> 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.
```

上記のテスト「有効な」作業:

- 用心深いアプローチはドメインのためにプロファイルを追加する前に各ドメインをテストすることです。
- より積極的なアプローチはデフォルト 宛先制御プロファイルのデンマーク人を設定し、だれをパス/失敗するか見ることです。

Mail 方向はデンマーク人が確認したかどうか確認します。

送信側 グループ/peform デンマーク人確認をために設定される「リレー」操作がある Mail フロー ポリシー。

送信側 グループ/」設定される操作を受け入れることを「持っている Mail フロー ポリシーは pefor デンマーク人確認。

> **注意**： ESA が持っていれば Desination は**デフォルトポリシー**で有効に なる「デンマーク人」を制御します**壊れる配信リスクがあります。** RATS にリストされている物のような内部で所有されたドメイン パススルー リレーはおよびドメインのための SMTP ルートの存在と結合されるメール フロー ポリシーを受け入れます。

SMTP ルーティング

デンマーク人は SMTP ルーティングで「宛先ホスト USEDNS」がに「」。設定されなければ失敗します

日和見主義デンマーク人はバウンス プロファイル タイマーが切れるまで配信キューでそれらが含まれているメッセージを提供しません。

これは、なぜですか。 デンマーク人確認 gets は SMTP ルートが本当宛先の修正で、正しく DNS を使用しないかもしれないのでスキップしました。

ソリューション： 明示的に SMTP ルーティングが含まれているドメインのデンマーク人確認を無効に するために宛先 コントロール プロファイルを作成して下さい

日和見主義必須デンマーク人かデンマーク人

次のルックアップはデンマーク人確認の間に実行された。

各確認はそれに続く確認を行うためにコンテンツを入れます。

- MXレコード ルックアップはかどうか、不確かセキュア、>>> 偽確認します
- レコード ルックアップはかどうか >>> セキュア不確か > 偽確認します

- TLSA はルックアップを確認しますかどうか、セキュア、>>> 偽不確か、NXDOMAIN 記録します
- 失敗される Certificate verify >> 成功

安全性：

- DNS は信頼のチェーンの上の RRSIG によって検証された署名された RRSIG DS および DNSKEY が、含まれているセキュリティ記録の存在を確認しました。

不確か:

- DNS はドメインを持っていません現在の dnssec によって有効に されるレコードを判別します。

偽:

- 不完全な、しかし提供 dnssec エントリは失敗するかもしれません確認。
- 期限切れのキーによる無効レコード。
- 信頼のチェーンの抜けたレコードかキー。

NXDOMAIN

- 該当レコードなし DNS で。

上のレコード チェックの組み合せおよび確認結果は「デンマーク人成功を判別します | デンマーク人失敗 | TLS へのデンマーク人フォールバック」。

例えば: example.com の MXレコードのために送信 される RRSIG がない場合 example.com に DNSKEY レコードがあるかどうか親ゾーン（ .com ）は、example.com がレコードに署名する必要があることを示しますチェックされ。 この検証は達されるルート ゾーン（ 。 ）キー verification.is の信頼仕上げのチェーンの上で続き ESA が期待するものをルート ゾーンのキーは一致する（ 自動更新済を RFC5011 に基づいて得る ） ESA のハードコードされた値。

デンマーク人 MANDATORY

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

デンマーク人 MANDATORY

注: 日和見主義デンマーク人は**好まれる TLS のように動作しません。** 下記の図 FAIL の処理部分はデンマーク人生じましたり、必須か日和見主義のために渡しません。 メッセージは配信キューにタイマーが切れるまで、それから配信終わります残ります。

日和見主義デンマーク人

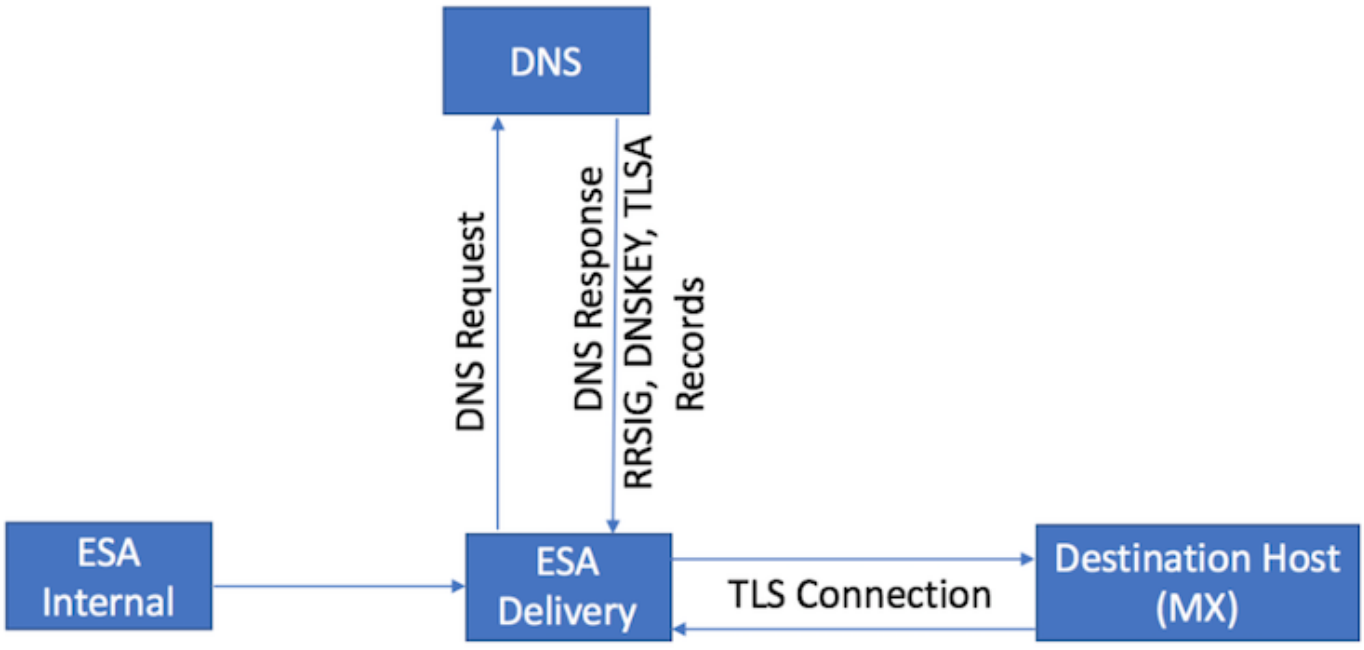
MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed →	DANE Fail
Secure	Secure	Insecure		Fallback to opportunistic TLS flow
Secure	secure	NXDOMAIN		Fallback to opportunisticTLS flow
Secure	Secure	Bogus	→	DANE Fail
Secure	Insecure	Mail 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

日和見主義デンマーク人

多重アプライアンス 環境のイネーブル デンマーク人

次の図は倍数アプライアンス 環境のデンマーク人を有効に するとき作業の流れを説明します。

環境に ESA アプライアンスのマルチプルレイヤがある場合、スキャンのための 1 つおよびメッセージを提供するための別のものは外部宛先に直接接続するアプライアンスだけでデンマーク人を設定されます確認します。



複数の ESA 設計。 配信 ESA で設定されるデンマーク人

複数の DNS リゾルバの管理

ESA に設定される複数の DNS リゾルバがある場合 DNSSEC をサポートしない DNSSEC を少数サポートする少数、Cisco は（数値防ぐ）高優先順位で DNSSEC 可能なリゾルバを設定することを推奨します、不整合を。

これは「偽」として宛先 ドメイン サポート デンマーク人を分類するために非DNSSEC 可能なリゾルバを防ぎます。

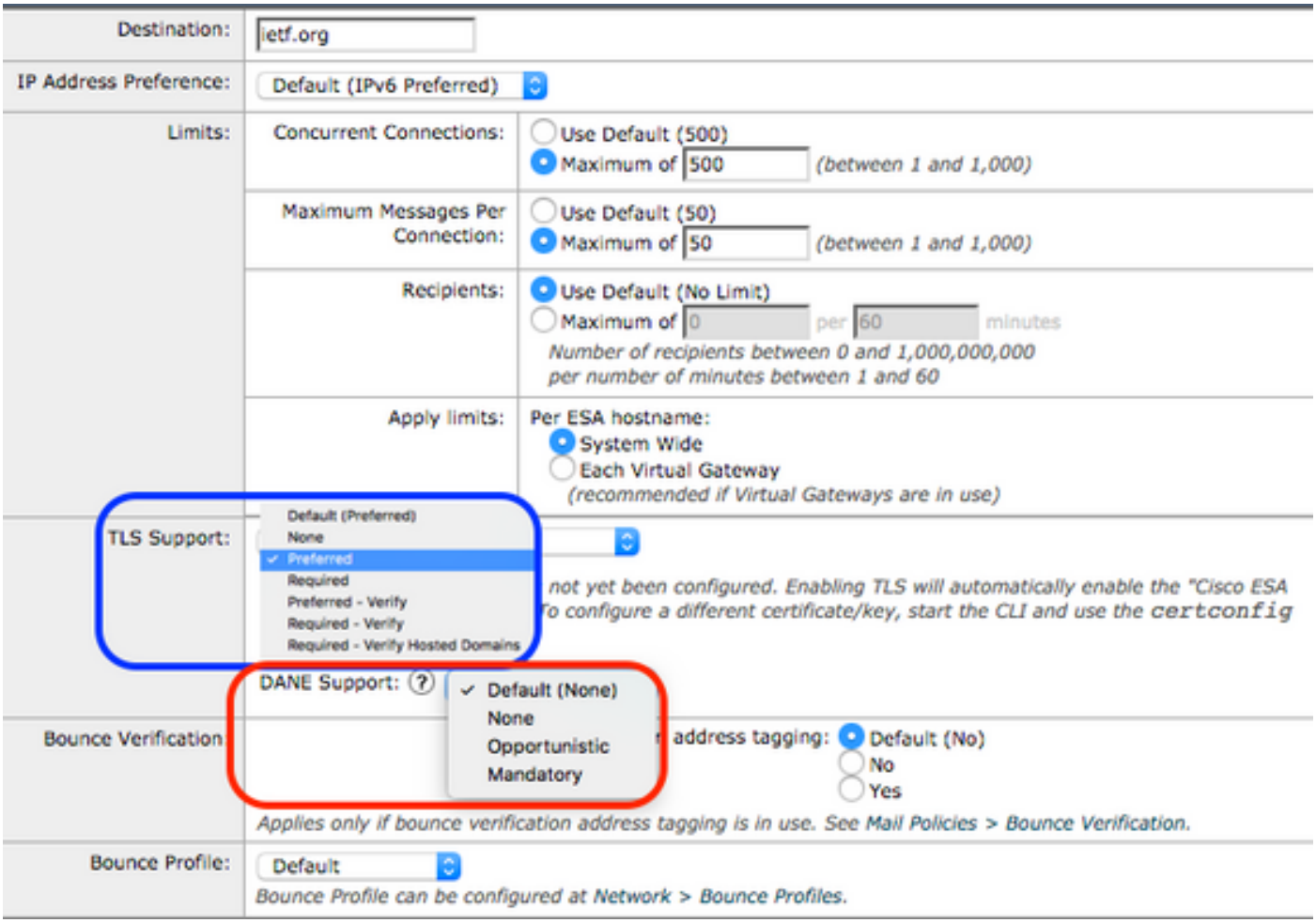
セカンダリDNSサーバの管理

DNS リゾルバが到達可能のとき、DNS はセカンダリDNSサーバに戻って下ります。 セカンダリDNSサーバの DNSSEC を設定しない場合、デンマーク人可能な宛先 ドメインのための MX レコードは「偽として分類されます」。 これはデンマーク人設定に関係なくメッセージ デリバリーに影響を与えます（日和見主義か必須）。 Cisco はセカンダリ DNSSEC 可能なリゾルバを使用するために推奨します。

設定

送信 メール フローのための設定デンマーク人。

1. Webui ナビゲートはへの > Mail ポリシー > 宛先 > Add 宛先を制御します
2. プリファレンスにプロファイルの上部分を完了して下さい。
3. TLS サポート: **「好まれる TLS に設定 されるために必要とされます | 優先 する-確認事項 | Required | 必須-確認事項| 必須-ホステッド ドメインを」。確認して下さい**
4. TLS サポートが有効に なったら、デンマーク人サポート: ドロップダウンメニューはアクティブになります。
5. **デンマーク人サポート: オプションは「どれも含まれていません | 日和見主義 | 必須。**
6. デンマーク人サポートオプションが完了したら、変更を入れ、保存して下さい。



宛先 コントロール プロファイル-デンマーク人は確認します

デンマーク人成功を確認して下さい

配信ステータス

デンマーク人失敗による宛先 ドメインのあらゆる故意ではない集結のための WebUI 「配信ステータス」レポートを、可能性としては監視して下さい。

サービスを、そして継続的成功を確認するために定期的に数日間有効に する前にこれを行って下さい。

ESA WebUI > モニタ > 配信ステータス > チェック「アクティブな受信者」カラム。

Mail ログ

デフォルト Mail は水平なログの情報レベルで記録 します。

メール ログはデンマーク人うまくネゴシエートされたメッセージのための非常に微妙なインジケーターを示します。

最終的な TLS ネゴシエーション 発信は Log エントリの端にドメインを含むためにわずかに修正された出力が含まれています。

Log エントリは「domain.com」のための TLS バージョン/暗号に先行している「TLS 成功プロトコル」が含まれています。

マジックはに「のための」あります:

```
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
```

Mail ログ デバッグ

デバッグ レベルのカスタム Mail ログは完全なデンマーク人および dnssec ルックアップを、期待されたネゴシエーション渡り、/失敗、成功インジケータ チェックの部分表示する。

> **注: デバッグ レベル ロギングのために設定される Mail ログはシステム 負荷および設定によって ESA の余分なリソースを消費するかもしれません。**

デバッグ レベル ロギングのために設定される Mail ログはシステム 負荷および設定によって ESA の余分なリソースを消費するかもしれません。

Mail ログは通常長時間のデバッグ レベルで維持されません。

デバッグ レベル ログはログオンします短いある一定の時間をメールの途方もない音量を生成するかもしれません。

頻繁な推奨事項は mail_logs_d のための追加ログ サブスクリプションを作成し、デバッグのための ロギングを設定 することです。

操作は既存の mail_logs に影響を防ぎ、サブスクリプションのために維持される ログの音量に操作を可能にします。

作成される ログの音量を制御するために 2-4 のファイルのようなより小さい数に維持するためにファイルの数を制限して下さい。

モニタリング、試用期間またはトラブルシューティングが完了したら、ログを無効に して下さい。

デバッグ レベルのために設定 される Mail ログは出力される非常に詳しいデンマーク人を示します:

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)
```

関連情報

- ESA ユーザ ガイド
- ESA リリース ノート
- ESA CLI リファレンス ガイド