

Hoe te gebruiken graven/nslookup om SPF, DKIM en DMARC Records voor een Domein te vinden?

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[SPF](#)

[DKIM](#)

[DMARC](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe het moet worden gebruikt `dig/nslookup` om SPF-, DKIM- en DMARC-records te vinden voor een domein op Email Security Applicatie (ESA) en Cloud Email Security (CES).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ESA op Async OS 10.0 of hoger
- Administratieve toegang tot het apparaat

Gebruikte componenten

De informatie in dit document is gebaseerd op alle ondersteunde ESA-hardwaremodellen en virtuele apparaten op Async OS 10.0 of hoger.

Typ de opdracht `Versie` om de versiegegevens van het apparaat via de CLI te controleren. In de GUI navigeer je naar **Monitor > System Status**.

Beide `nslookup` en `dig` opdrachten worden ondersteund op de huidige ESA/CES Async OS-releases. Deze opdrachten kunnen worden uitgevoerd via SSH/CLI-toegang tot het apparaat.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

De verstrekte steekproefoutput is voor domeinen `cisco.com` en `gmail.com` U kunt echter ook voor andere domeinen soortgelijke opdrachten gebruiken.

SPF

SPF-raadplegingen kunnen worden uitgevoerd met deze indelingen:

- `nslookup domeintekst`
- `dig domeintekst`

Opmerking: Shet woord vervangen `domain` met het juiste domein wil je omhoog kijken.

Voor domeinen waarin meerdere TXT-records zijn gepubliceerd, `nslookup` kan er niet in slagen om van SPF-records een lijst te maken. In dergelijke gevallen `dig` moet worden gebruikt.

Dit wordt in de voorbeeldoutput hier getoond voor `cisco.com`.

```
(Machine lab.esa.com)> nslookup cisco.com txt
TXT="google-site-verification=qPS9ZkoQ-Og1rBrM1_N7z-tNJNy2BVxE8lw6SB2iFdk"
TTL=21m 8s

(Machine lab.esa.com)> dig cisco.com txt
;; Warning: Message parser reports malformed message packet.
;; Truncated, retrying in TCP mode. ; <<>> DiG 9.11.2 <<>> cisco.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20648
;; flags: qr rd ra; QUERY: 1, ANSWER: 25, AUTHORITY: 0, ADDITIONAL: 0 ;; QUESTION SECTION:
;cisco.com. IN TXT ;; ANSWER SECTION:
cisco.com. 1782 IN TXT "fastly-domain-delegation-w049tcm0w48ds-341317-20210209"
cisco.com. 1782 IN TXT "v=spf1 redirect=spf._spf.cisco.com"
cisco.com. 1782 IN TXT "MS=ms35724259"
cisco.com. 1782 IN TXT "amazonses:QbUv5pPHGQxRylvKA0J7Y/biE9oR6MTxOTI1bZIfjsw="
cisco.com. 1782 IN TXT "fastly-domain-delegation-e9a758d22183504af2d5ab4d9a9853da-20210127"
cisco.com. 1782 IN TXT "QuoVadis=94d4ae74-ecd5-4a33-975e-a0d7f546c801"
cisco.com. 1782 IN TXT "atlassian-domain-
verification=672RcADvt8BPqsb9gCN2ZC5DoTAhUT8abC1b1YKQxi/MHMaGoA/BuvjFMaWRtgd7"
cisco.com. 1782 IN TXT "google-site-verification=9M1QU9MMQ1jHLMUkONKe6QzZ-ZIGRv0BCD1_rY1Zdmc"
cisco.com. 1782 IN TXT "SFMC-o7HX74BQ79k7glpt_qj1F2vmZ09DpqLtYxKLwg87"
cisco.com. 1782 IN TXT "926723159-3188410"
cisco.com. 1782 IN TXT "docuSign=95052c5f-a421-4594-9227-02ad2d86dfbe"
cisco.com. 1782 IN TXT "amazonses:7LyikZmpuGja4+KbA4xX31N69yajYKLkHH4QJcWnuwo="
cisco.com. 1782 IN TXT "google-site-verification=qPS9ZkoQ-Og1rBrM1_N7z-tNJNy2BVxE8lw6SB2iFdk"
cisco.com. 1782 IN TXT
"zpSH7Ye/seY61hH8+Rq5Kb+ZJ9hDa+qeFBaD/6sPAAg+2P0kGdP0byHb1pFVK9uZgYF2AIosUSZq4MB17oydQ=="
cisco.com. 1782 IN TXT
"duo_sso_verification=AxenLdoqIXzjl2RJzE1BlOfkawDbDFlnbyvjAt8vcjKHBkvYwEMySDRk5QmBd66v"
cisco.com. 1782 IN TXT "facebook-domain-verification=1zoxo8z7t013gpruxmhc8dkerq47vh"
cisco.com. 1782 IN TXT "google-site-verification=lW5eqPMJI4VrLc28YW-JBkqA-FDNVnhFCXQVDVfQzTo"
cisco.com. 1782 IN TXT "facebook-domain-verification=qr2nigspzrpa96j1nd9criovuuwino"
cisco.com. 1782 IN TXT "apple-domain-verification=q0InipPgso3W8cmK"
cisco.com. 1782 IN TXT "identrust_validate=JnSSfW+y58dEQu6mVBe8lu1MGFepXI50P270E1ZZQmL"
cisco.com. 1782 IN TXT "onetrust-domain-verification=20345dd0c33946f299f14c1498b41f67"
cisco.com. 1782 IN TXT "mixpanel-domain-verify=2c6cb1aa-a3fb-44b9-ad10-d6b744109963"
cisco.com. 1782 IN TXT "identrust_validate=Wns4/AOM0Ij2kQCQhzvNbMcoBzxItOa+4407KF061Ip3"
cisco.com. 1782 IN TXT "docuSign=5e18de8e-36d0-4a8e-8e88-b7803423fa2f"
cisco.com. 1782 IN TXT "amazonses:mX+y1Qj+fJAFh9pr03yIR7YvjKZ1b0o5ABegqM/5pvI=" ; ; Query time: 0
```

```
msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 23 06:03:28 GMT 2021
;; MSG SIZE rcvd: 1756
```

```
(Machine lab.esa.com)> nslookup gmail.com txt
TXT="v=spf1 redirect=_spf.google.com"
TTL=30m
```

```
(Machine lab.esa.com)> dig gmail.com txt
```

```
; <<>> DiG 9.11.2 <<>> gmail.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14807
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0 ;; QUESTION SECTION:
;gmail.com. IN TXT ;; ANSWER SECTION:
gmail.com. 1800 IN TXT "v=spf1 redirect=_spf.google.com"
gmail.com. 1800 IN TXT "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8=" ;;
Query time: 85 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 23 06:05:38 GMT 2021
;; MSG SIZE rcvd: 148
```

DKIM

DKIM lookups kunnen worden uitgevoerd met deze formaten:

- nslookup selector._domainkey.domain txt
- dig selector._domainkey.domain txt

Opmerking: Vervang de woorden **selector** en **domain** met de DKIM-selector en -domein wil je omhoog kijken.

```
(Machine lab.esa.com)> nslookup iport._domainkey.cisco.com txt
TXT="v=DKIM1;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCctxGhJnvNpdcQLJM6a/0otvdpzFIJuo73OYFuw6/8bXcf8/p5JG/iME
1r9fUlrNZs3kMn9ZdPYvTyRbyZ0UyMrsM3ZN2JAIop3M7sitqHgp8pbORFgQyZxq+L23I2cELq+qw
tbanjWJzEPpVvrvbuz9QL8CUtS+V5N5ldq8L/lwIDAQAB;"
TTL=1d
```

```
(Machine lab.esa.com)> dig iport._domainkey.cisco.com txt
```

```
; <<>> DiG 9.11.2 <<>> iport._domainkey.cisco.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21671
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0 ;; QUESTION SECTION:
;iport._domainkey.cisco.com. IN TXT ;; ANSWER SECTION:
iport._domainkey.cisco.com. 86400 IN TXT "v=DKIM1;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCctxGhJnvNpdcQLJM6a/0otvdpzFIJuo73OYFuw6/8bXcf8/p5JG/iME
1r9fUlrNZs3kMn9ZdPYvTyRbyZ0UyMrsM3ZN2JAIop3M7sitqHgp8pbORFgQyZxq+L23I2cELq+qw
tbanjWJzEPpVvrvbuz9QL8CUtS+V5N5ldq8L/lwIDAQAB;"
;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 23 06:41:31 GMT 2021
;; MSG SIZE rcvd: 285
```

```
(Machine lab.esa.com)> dig 20161025._domainkey.gmail.com TXT
```

```
; <<>> DiG 9.11.2 <<>> 20161025._domainkey.gmail.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11798
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0 ;; QUESTION SECTION:
20161025._domainkey.gmail.com. IN TXT ;; ANSWER SECTION:
20161025._domainkey.gmail.com. 1800 IN TXT "k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAviPGBk4ZB64UfSqWyAicdR7lodhytae+EYRQVtKDhM+1mXjEqR
tP/pDT3sBhazkMA48n2k5NJUyMEo08nc2r6sUA+/Dom5jRBZp6qDKJOwjJ5R/OpHamlRG+YRJQqR"
"tqEgSiJWG7h7efGYWmh4URhFM9k9+rmG/CwCgwx7Et+c8OMlngaLl04/bPmfpjdEyLWyNimk761CX6KymzYiRDnz1MOJOJ7
OzFaS4PFbVLn0m5mf0HVntBpPwWuCNvaFVflUYxEyblbB6h/oWOPGbz0SgtRA47SHV53SwZjIsVpb
q4LxUW9IxAEWyzGcSgZ4n5Q8X8TndowsDUzoccPFghdwIDAQAB"
;; Query time: 174 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 23 06:45:01 GMT 2021
;; MSG SIZE rcvd: 462
```

```
(Machine lab.esa.com)> nslookup 20161025._domainkey.gmail.com TXT
```

```
TXT="k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAviPGBk4ZB64UfSqWyAicdR7lodhytae+EYRQVtKDhM+1mXjEqR
tP/pDT3sBhazkMA48n2k5NJUyMEo08nc2r6sUA+/Dom5jRBZp6qDKJOwjJ5R/OpHamlRG+YRJQqR"
"tqEgSiJWG7h7efGYWmh4URhFM9k9+rmG/CwCgwx7Et+c8OMlngaLl04/bPmfpjdEyLWyNimk761CX6KymzYiRDnz1MOJOJ7
OzFaS4PFbVLn0m5mf0HVntBpPwWuCNvaFVflUYxEyblbB6h/oWOPGbz0SgtRA47SHV53SwZjIsVpb
q4LxUW9IxAEWyzGcSgZ4n5Q8X8TndowsDUzoccPFghdwIDAQAB"
TTL=30m
```

DMARC

DMARC lookups kunnen worden uitgevoerd met deze formaten:

- nslookup _dmarc.domain tekst
- dig _dmarc.domain tekst

Opmerking: Shet woord vervangen domain met het domein wil je graag omhoog kijken.

```
(Machine lab.esa.com)> nslookup _dmarc.cisco.com txt
```

```
TXT="v=DMARC1; p=quarantine; pct=0; fo=1; ri=3600; rua=mailto:cisco@rua.agari.com;
ruf=mailto:cisco@ruf.agari.com"
TTL=30m
```

```
(Machine lab.esa.com)> dig txt _dmarc.cisco.com
```

```
; <<>> DiG 9.11.2 <<>> _dmarc.cisco.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24522
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0 ;; QUESTION SECTION:
_dmarc.cisco.com. IN TXT ;; ANSWER SECTION:
_dmarc.cisco.com. 1800 IN TXT "v=DMARC1; p=quarantine; pct=0; fo=1; ri=3600;
rua=mailto:cisco@rua.agari.com; ruf=mailto:cisco@ruf.agari.com"
;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 23 06:34:15 GMT 2021
;; MSG SIZE rcvd: 155
```

```
(Machine lab.esa.com)> nslookup _dmarc.gmail.com txt
TXT="v=DMARC1; p=none; sp=quarantine; rua=mailto:mailauth-reports@google.com"
TTL=30m
```

```
(Machine lab.esa.com)> dig _dmarc.gmail.com txt
```

```
; <<>> DiG 9.11.2 <<>> _dmarc.gmail.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28370
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0 ;; QUESTION SECTION:
;_dmarc.gmail.com. IN TXT ;; ANSWER SECTION:
_dmarc.gmail.com. 1800 IN TXT "v=DMARC1; p=none; sp=quarantine; rua=mailto:mailauth-
reports@google.com"
;; Query time: 85 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 23 06:35:18 GMT 2021
;; MSG SIZE rcvd: 118
```

Gerelateerde informatie

- [Cisco e-mail security applicatie – eindgebruikershandleiding](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.