

對安全Web裝置DNS服務進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[DNS概念](#)

[代理部署中的DNS服務](#)

[配置DNS設定](#)

[最佳實踐](#)

[在GUI中配置DNS](#)

[從CLI配置DNS](#)

[CLI DNS命令](#)

[建立手動記錄](#)

[dnsflush](#)

[advancedproxyconfig](#)

[DNS快取](#)

[從GUI清除DNS快取](#)

簡介

本文檔介紹域名服務(DNS)配置以及如何在Secure Web Appliance(SWA) (以前稱為WSA) 中進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- 已安裝物理或虛擬安全網路裝置(SWA)
- 許可證已啟用或已安裝
- 安全殼層(SSH)使用者端
- 安裝精靈已完成

- 對SWA的管理訪問

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

DNS概念

DNS是Internet中用於將對象名稱（通常是主機名）對映到Internet協定(IP)地址或其他資源記錄值的系統。

Internet的名稱空間被劃分為多個域，每個域內的名稱管理責任通常被委託給每個域內的系統。

域名空間被劃分為稱為區域的區域，這些區域是DNS樹中的委派點。

區域包含從某一點往下的所有域，但其他區域具有權威性的域除外。

區域通常具有權威名稱伺服器，通常不止一個。

在組織中，您可以擁有許多名稱伺服器，但Internet使用者端只能查詢根名稱伺服器知道的那些伺服器。

其他名稱伺服器只回答內部查詢。

DNS基於客戶端/伺服器模型。在此模型中，域名伺服器儲存有關DNS資料庫一部分的資料，並將其提供給透過網路查詢域名伺服器的客戶端。

名稱伺服器是在實體主機上執行的程式，用來儲存區域資料。作為域管理員，您可以設定名稱伺服器，該伺服器帶有描述一個或多個區域中主機的所有「資源記錄」(RR)的資料庫

代理部署中的DNS服務

在顯式部署中：代理運行DNS查詢

在透明部署中：DNS查詢在客戶端上運行。

配置DNS設定

您可以從圖形使用者介面(GUI)和命令列介面(CLI)配置DNS。

AsyncOS for Web可以使用網際網路根DNS伺服器或您自己的DNS伺服器。如果SWA使用Internet根伺服器，則可以指定用於特定域的備用伺服器。

由於備用DNS伺服器適用於單個域，因此它必須是該域的權威（提供最終的DNS記錄）。

AsyncOS支援分割DNS，其中內部伺服器是為特定域配置的，外部或根DNS伺服器是為其他域配置的。

如果SWA使用本地DNS伺服器，我們還可以指定異常域和關聯的DNS伺服器。

最佳實踐

安全最佳實踐表明，每個網路必須託管兩個DNS解析器：一個用於本地域內的權威記錄，另一個用於網際網路域的遞迴解析。

為了適應這一點，SWA允許為特定域配置DNS伺服器。

如果一個DNS伺服器可用於本地查詢和遞迴查詢，請考慮將其用於所有SWA查詢時將會增加的額外負載。

更好的選項是本地域使用內部解析器，外部域使用根網際網路解析器。這取決於管理員的風險設定檔和允差。

必須配置輔助DNS伺服器，以防主伺服器不可用。如果所有伺服器都配置了相同的優先順序，則會隨機選擇伺服器IP。

根據配置的伺服器數量，給定伺服器的超時會有所不同。查詢超時值如下表所示，最多六台DNS伺服器：

DNS伺服器數量	查詢超時 (按順序)
1	60
2	5、45
3	5、10、45
4	1、3、11、45
5	1、3、11、45、1
6	1、3、11、45、1、1

有關詳細資訊，請訪問：[思科網路安全裝置最佳實踐指南-思科](#)

在GUI中配置DNS

要透過GUI配置DNS，請執行以下步驟：

步驟 1. 從頂部選單中選擇Network

步驟 2. 選擇DNS

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy


External DLP Servers


Web Traffic Tap

Certificate Management

Cloud Services Settings


替代DNS伺服器覆蓋 (可選) : 域的授權DNS伺服器

 注意：AsyncOS不支援透明FTP請求的版本首選項。

 注意：在雲聯結器模式下，思科網路安全裝置僅支援IPv4

使用網際網路根DNS伺服器。當裝置無法訪問您網路上的DNS伺服器時，選擇使用網際網路根DNS伺服器進行域名服務查詢。

Internet根DNS伺服器不解析本地主機名。

 注意：如果需要裝置解析本地主機名，請使用本地DNS伺服器或從命令列介面(CLI)向本地DNS增加相應的靜態條目。

域搜尋清單：將請求傳送到裸主機名 (無點) 時使用的DNS域搜尋清單。 (「」)。


按照輸入的順序 (從左到右) ，依次嘗試指定的每個域，檢視是否可以找到與主機名加上域的DNS匹配。

DNS流量的路由表：指定DNS服務透過哪個介面路由流量。

等候逾時反向DNS查閱之前：等候逾時無回應的反向DNS查閱之前的等候時間(以秒為單位)。

當主要DNS伺服器傳回下列錯誤時，次要DNS伺服器會接收主機名稱查詢：

- 無錯誤，未收到答案部分
- 伺服器無法完成要求，沒有回應區段
- 名稱錯誤，未收到答案部分
- 未實現功能
- 伺服器拒絕回答查詢

 注意：AsyncOS在評估外部依賴關係之前會根據策略評估事務，以避免來自裝置的不必要外部通訊。例如，如果根據阻止未分類的URL的策略阻止某個事務，則該事務將不會因DNS錯誤而失敗。

優先順序：值為0時優先順序最高。如果兩者具有相同的優先順序，則會選擇隨機IP。

從CLI配置DNS

可以使用CLI中的dnsconfig配置DNS設定。

步驟 1.在CLI中鍵入dnsconfig：

```
SWA_CLI> dnsconfig
```

```
Currently using the local DNS cache servers:
```

1. Priority: 0 10.1.1.1
2. Priority: 1 10.2.2.2
3. Priority: 2 10.3.3.3

```
Currently using the following Secondary DNS cache servers :
```

1. Priority: 0 10.10.10.10

```
Choose the operation you want to perform:
```

- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
- SEARCH - Configure DNS domain search list.

```
[>
```

步驟 2.要將新的DNS伺服器增加到清單，請鍵入NEW並按Enter。

步驟 3.選擇主要DNS名稱伺服器或次要DNS名稱伺服器，以便新增新的名稱伺服器。

```
[> NEW
```

```
Do you want to make changes in the Primary DNS nameserver list or secondary DNS nameserver list?
```

1. Make changes to the primary DNS nameserver
2. Make changes to the secondary DNS nameserver

```
[> 1
```

步驟 4.選擇新增名稱伺服器或替代網域伺服器（條件式轉寄網域名稱）

```
Do you want to add a new local DNS cache server or an alternate domain server?
```

1. Add a new local DNS cache server.
2. Add a new alternate domain server.

```
[> 1
```

步驟 5. 提供新名稱伺服器的IP地址

步驟 6.為新增的名稱伺服器提供優先順序。

```
Please enter the IP address of your DNS server.
```

```
Separate multiple IPs with commas.
```

```
[> 10.4.4.4
```

```
Please enter the priority for 10.4.4.4.
```

```
A value of 0 has the highest priority.
```

```
The IP will be chosen at random if they have the same priority.
```

[0]> 4

Currently using the local DNS cache servers:

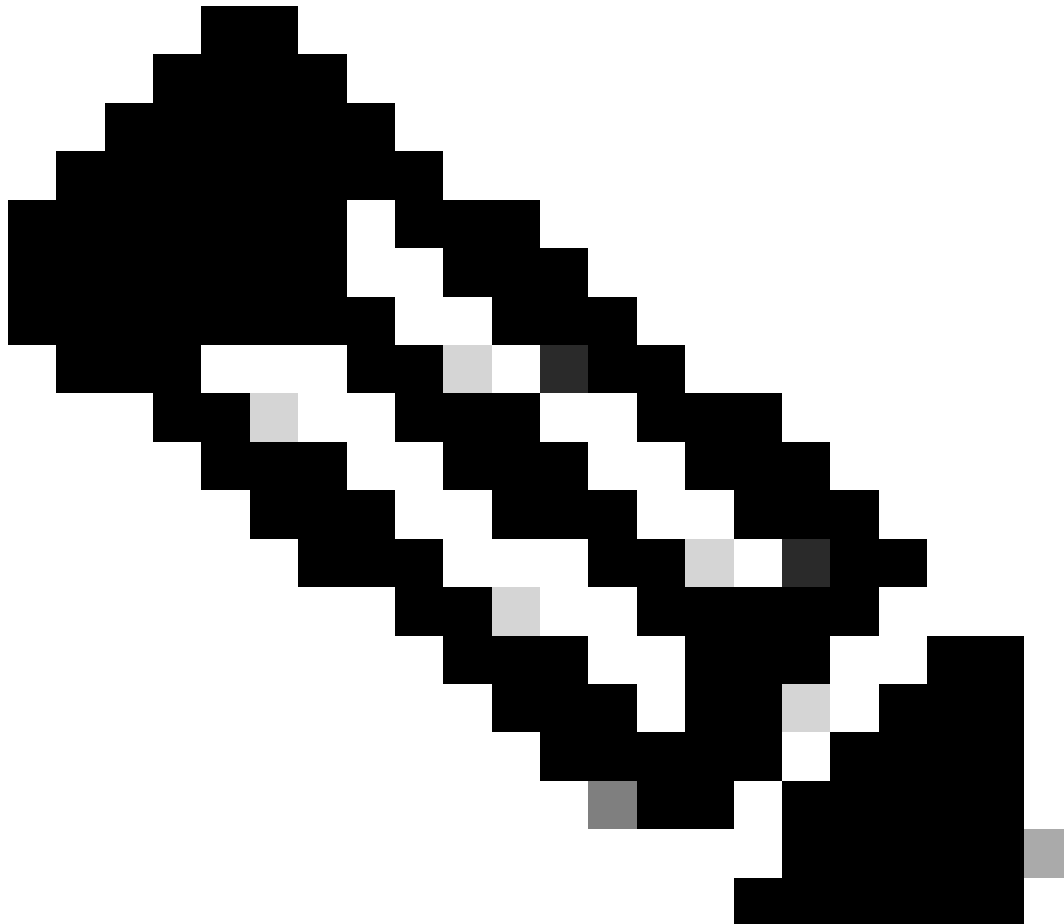
1. Priority: 0 10.1.1.1
2. Priority: 1 10.2.2.2
3. Priority: 2 10.3.3.3
4. Priority: 4 10.4.4.4

Currently using the following Secondary DNS cache servers :

1. Priority: 0 10.10.10.10

步驟 7.按Enter退出嚮導。

步驟 8.鍵入commit以儲存更改。



注意：要編輯或刪除任何名稱伺服器，可以從dnsconfig中選擇EDIT和DELETE。

透過SETUP選項，可以配置DNS快取時間和離線DNS檢測設定：

```
SWA_CLI> dnsconfig
....
[ ]> setup
Do you want the Gateway to use the Internet's root DNS servers or would you like it to use your own DNS
1. Use Internet root DNS servers
2. Use own DNS cache servers
[2]> 2

Enter the number of seconds to wait before timing out reverse DNS lookups.
[20]>

Enter the minimum TTL in seconds for DNS cache.
[1800]>

Do you want to enable Secure DNS? [N]> N
Warning: Ensure that you configure the DNS server with DNSSEC because there is no backward compatibility.
Failing to do so can result in invalid response with an unresolved hostname.

You must use FQDN with the hostname for the local and private domains.

Enter the number of failed attempts before considering a local DNS server offline.
[100]>

Enter the interval in seconds for polling an offline local DNS server.
[5]>
```

DNS快取的最小TTL秒數：此選項用於配置SWA快取記錄的最短秒數。有關詳細資訊，請參閱本文檔中的DNS快取部分。

輸入將本地DNS伺服器視為離線前嘗試失敗的次數：如果DNS伺服器未響應任何DNS查詢，計數器將啟動。

當達到此定義值時，該名稱伺服器被視為離線DNS伺服器，SWA避免在預定義的時間段內向該名稱伺服器傳送DNS查詢（Next選項）。

當DNS伺服器標籤為os offline時，您會看到以下錯誤消息：

```
30 Jun 2023 07:37:03 +0200    Reached maximum failures querying DNS server 10.1.1.1
```

輸入輪詢離線的本機DNS伺服器的間隔（秒）：當標示為離線的DNS伺服器在此時間間隔（秒）之後，SWA開始將DNS查詢傳送至該名稱伺服器，該DNS伺服器失敗的回應計數器會重設為零。

CLI DNS命令

建立手動記錄

若要建立手動「A記錄」，您無法使用或編輯Hosts檔案。可以在CLI中的dnsconfig中使用localhosts隱藏命令。

注意：更改此配置後必須提交更改。

dnsconfig

Currently using the local DNS cache servers:

1. Priority: 0 10.1.1.1
2. Priority: 0 10.2.2.2

Choose the operation you want to perform:

- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
- SEARCH - Configure DNS domain search list.

[> localhosts

Local IP to Host mappings:

Choose the operation you want to perform:

- NEW - Add new local IP to host mapping.
- DELETE - Delete an existing mapping.

```
[> new
```

Enter the IP address of the host you are adding.

```
[> 10.20.30.40
```

Enter the canonical host name and any additional aliases (separate values with spaces)

```
[> ManualHostEntry.cisco.com
```

dnsflush

dnsflush從DNS快取表中刪除所有快取的DNS記錄：

```
SWA_CLI> dnsflush
```

Are you sure you want to clear out the DNS cache? [N]> Y

advancedproxyconfig

```
advancedproxyconfig
```

Choose a parameter group:

- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
- CONTENT-ENCODING - Block content-encoding types
- SCANNERS - Scanner related parameters

```
[> DNS
```

Enter values for the DNS options:

Enter the URL format for the HTTP 307 redirection on DNS lookup failure.

```
[%P://www.%H.com/%u]>
```

Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure?

```
[Y]>
```

Would you like proxy not to automatically failover to DNS results when upstream proxy (peer) is unresponsive?

```
[N]>
```

Select one of the following options:

0 = Always use DNS answers in order

1 = Use client-supplied address then DNS

2 = Limited DNS usage
3 = Very limited DNS usage

For options 1 and 2, DNS will be used if Web Reputation is enabled.
For options 2 and 3, DNS will be used for explicit proxy requests, if there is no upstream proxy or in the event the configured upstream proxy fails.

For all options, DNS will be used when Destination IP Addresses are used in policy membership.

Find web server by:
[0]>

HTTP 307 (臨時重定向) 狀態代碼指示目標資源臨時駐留在不同的統一資源識別符號(URI)下，並且如果使用者代理執行到該URI的自動重定向，則不得更改請求方法。由於重定向會隨時間而變化，因此客戶端必須繼續使用原始的有效請求URI。

有關詳細資訊：[什麼是HTTP 307臨時重定向狀態代碼- Kinsta](#)

在透明代理部署中評估客戶端請求時，這些選項控制SWA如何決定要連線的IP地址。收到請求後，WSA會看到目標IP地址和主機名。SWA必須決定是信任用於TCP連線的原始目標IP地址，還是執行自己的DNS解析並使用解析的地址。預設值為「0 = Always use DNS answers in order」，這意味著SWA不信任客戶端提供IP地址。

選項1：SWA嘗試客戶端提供的IP地址進行連線，如果失敗，則返回解析地址。解析的地址用於策略評估(Web類別、Web信譽等)。

選項2：SWA僅使用客戶端提供的地址進行連線，不回退。解析的地址用於策略評估(Web類別、Web信譽等)。

選項3：SWA僅使用客戶端提供的地址進行連線，不回退。客戶端提供的IP地址用於策略評估(Web類別、Web信譽等)。

選擇的選項取決於管理員在確定給定主機名的解析地址時必須給予客戶端多少信任。如果客戶端是下行代理，請選擇選項3以避免不必要的DNS查詢增加延遲。

DNS快取

為了提高效率和效能，思科SWA會為您最近連線的域儲存DNS條目。DNS快取允許SWA避免對相同域執行過多的DNS查詢。DNS快取條目由於記錄的TTL (生存時間) 而過期。

當DNS伺服器中記錄的TTL大於SWA dnsconfig cache TTL時間時，dns快取將使用DNS伺服器中的TTL。

當DNS伺服器中記錄的TTL小於SWA dnsconfig cache TTL時間時，dns快取將使用WSA dnsconfig設定中的TTL。



注意：SWA有兩個DNS快取，其中一個用於代理進程，另一個用於內部進程。

預設情況下，無論記錄TTL如何，SWA都會快取DNS記錄至少30分鐘。現代網站大量使用內容交付

網路(CDN)，由於IP地址經常變化，因此其TTL記錄會較低。

這可能導致客戶端為給定伺服器快取一個IP地址，而SWA為同一伺服器快取另一個地址。要解決此問題，可以從dsnconfig CLI命令的SETUP部分將SWA預設TTL降低到五分鐘。

例如，如果DNS配置中的「DNS快取的最小TTL（以秒為單位）」已設定為10分鐘，並且一條記錄的TTL為5分鐘，則快取記錄的TTL將增加到10分鐘。

另一方面，如果記錄的TTL設定為15分鐘，則SWA會在快取中儲存15分鐘的記錄。

但是，有時需要清除條目的DNS快取。損壞或過期的DNS快取條目偶爾會導致向遠端主機傳遞時出現問題。


此問題通常發生在裝置因網路移動或其他情況而離線之後。

從GUI清除DNS快取

步驟 1. 從頂部選單中選擇Network

步驟 2. 選擇DNS

步驟 3. 選擇Clear DNS Cache

 注意：重新填充快取時，此命令可能導致臨時效能下降

從CLI清除DNS快取

Cisco WSA中的DNS快取可以透過CLI中的dnsflushcommand清除。

檢視DNS快取

在SWA中，無法從CLI或GUI檢視快取的DNS記錄。

注意：您無法通過nslookup查詢DNS快取。

DNS故障排除

檢視DNS日誌

與Web代理元件相關的某些日誌型別未啟用。主要Web代理日誌型別（稱為「預設代理日誌」）預設啟用，捕獲所有Web代理模組的基本資訊。

每個Web Proxy模組也有自己的記錄型別，您可以視需要手動啟用。

系統記錄、記錄DNS、錯誤及確認活動。預設為啟用

 提示：如果您將系統日誌的日誌級別更改為DEBUG，則可以看到DNS查詢和響應。您可以從GUI和CLI更改日誌級別。

從GUI變更系統記錄檔記錄層級

步驟 1.從頂部選單選擇System Administrations

步驟 2.選擇日誌訂閱

步驟 3.選擇系統日誌

步驟 4.在日誌級別部分選擇調試

步驟 5.提交

步驟 6.提交更改

Edit DNS

DNS Server Settings																			
Primary DNS Servers:	<input checked="" type="radio"/> Use these DNS Servers <table border="1"><thead><tr><th>Priority ?</th><th>Server IP Address</th><th></th></tr></thead><tbody><tr><td><input type="text" value="0"/></td><td><input type="text" value="10.1.1.1"/></td><td><input type="button" value="Add Row"/> </td></tr><tr><td><input type="text" value="1"/></td><td><input type="text" value="10.2.2.2"/></td><td><input type="button" value="Add Row"/> </td></tr><tr><td><input type="text" value="2"/></td><td><input type="text" value="10.3.3.3"/></td><td><input type="button" value="Add Row"/> </td></tr></tbody></table> <table border="1"><thead><tr><th colspan="2">Alternate DNS servers Overrides (Optional):</th><th><input type="button" value="Add Row"/></th></tr></thead><tbody><tr><td><input type="text" value="Domain(s)"/> <small>i.e., example.com, example2.com</small></td><td><input type="text" value="DNS Server IP Address(es)"/> <small>i.e., 10.0.0.3 or 2001:420:80:1::5</small></td><td></td></tr></tbody></table>	Priority ?	Server IP Address		<input type="text" value="0"/>	<input type="text" value="10.1.1.1"/>	<input type="button" value="Add Row"/>	<input type="text" value="1"/>	<input type="text" value="10.2.2.2"/>	<input type="button" value="Add Row"/>	<input type="text" value="2"/>	<input type="text" value="10.3.3.3"/>	<input type="button" value="Add Row"/>	Alternate DNS servers Overrides (Optional):		<input type="button" value="Add Row"/>	<input type="text" value="Domain(s)"/> <small>i.e., example.com, example2.com</small>	<input type="text" value="DNS Server IP Address(es)"/> <small>i.e., 10.0.0.3 or 2001:420:80:1::5</small>	
Priority ?	Server IP Address																		
<input type="text" value="0"/>	<input type="text" value="10.1.1.1"/>	<input type="button" value="Add Row"/>																	
<input type="text" value="1"/>	<input type="text" value="10.2.2.2"/>	<input type="button" value="Add Row"/>																	
<input type="text" value="2"/>	<input type="text" value="10.3.3.3"/>	<input type="button" value="Add Row"/>																	
Alternate DNS servers Overrides (Optional):		<input type="button" value="Add Row"/>																	
<input type="text" value="Domain(s)"/> <small>i.e., example.com, example2.com</small>	<input type="text" value="DNS Server IP Address(es)"/> <small>i.e., 10.0.0.3 or 2001:420:80:1::5</small>																		
	<input type="radio"/> Use the Internet's Root DNS Servers <table border="1"><thead><tr><th colspan="2">Alternate DNS servers Overrides (Optional):</th><th><input type="button" value="Add Row"/></th></tr></thead><tbody><tr><td><input type="text" value="Domain"/> <small>i.e., dns.example.com</small></td><td><input type="text" value="DNS Server IP Address"/> <input type="text" value="DNS Server FQDN"/></td><td></td></tr></tbody></table>	Alternate DNS servers Overrides (Optional):		<input type="button" value="Add Row"/>	<input type="text" value="Domain"/> <small>i.e., dns.example.com</small>	<input type="text" value="DNS Server IP Address"/> <input type="text" value="DNS Server FQDN"/>													
Alternate DNS servers Overrides (Optional):		<input type="button" value="Add Row"/>																	
<input type="text" value="Domain"/> <small>i.e., dns.example.com</small>	<input type="text" value="DNS Server IP Address"/> <input type="text" value="DNS Server FQDN"/>																		
Secondary DNS Servers:	<table border="1"><thead><tr><th>Priority ?</th><th>Server IP Address</th><th></th></tr></thead><tbody><tr><td><input type="text" value="0"/></td><td><input type="text" value="10.10.10.10"/></td><td><input type="button" value="Add Row"/> </td></tr></tbody></table>	Priority ?	Server IP Address		<input type="text" value="0"/>	<input type="text" value="10.10.10.10"/>	<input type="button" value="Add Row"/>												
Priority ?	Server IP Address																		
<input type="text" value="0"/>	<input type="text" value="10.10.10.10"/>	<input type="button" value="Add Row"/>																	
Routing Table for DNS Traffic:	Management																		
IP Address Version Preference:	<input checked="" type="radio"/> Prefer IPv4 <input type="radio"/> Prefer IPv6 <input type="radio"/> Use IPv4 only <small>This preference applies when DNS results provide both IPv4 and IPv6 address for host. When selecting Prefer IPv4 or Prefer IPv6, ensure that the appliance network settings are configured appropriately to support IPv6.</small>																		
Secure DNS:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <small>SECURE DNS protects DNS data. It uses the DNSSEC protocol to strengthen the authentication in the DNS using digital signatures. If DNSSEC is enabled, fallback of DNSSEC query to DNS query will not occur. Supported DNSSEC Algorithms: DSA, DSA_NSEC3, ED448, ED25519, ECDSAP256SHA256, ECDSAP384SHA384, RSASHA1, RSASHA1_NSEC3, RSASHA256, RSASHA512.</small>																		
Wait Before Timing out Reverse DNS Lookups:	<input type="text" value="2"/> seconds																		
Domain Search List: ?	<input type="text"/> <small>Separate multiple entries with commas. Maximum allowed characters 2048.</small>																		

Cancel

Submit

從CLI更改系統日誌日誌級別

步驟 1.登入到CLI

步驟 2.鍵入logconfig

步驟 3.選擇編輯

步驟 4.輸入與System_Logs相關的編號

步驟 5. 按下Enter直到您達到[記錄]層級

步驟 6.選擇用於調試的4號

步驟 7.按Enter鍵，直到您退出嚮導

步驟 8.要儲存更改，請鍵入commit。

```
SWA_CLI> logconfig


Currently configured logs:
...
42. "system_logs" Type: "System Logs" Retrieval: FTP Poll
...

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- HOSTKEYCONFIG - Configure SSH host keys.
- AUDITLOGCONFIG - Adjust settings for audit logging.
[> EDIT

Enter the number of the log you wish to edit:
[> 42 <--- in this example the System_logs is number 42

Please enter the name for the log:
[system_logs]>

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 4
....
SWA_CLI> commit
```

 提示：完成故障排除後，請確保將日誌級別改回資訊，否則磁碟輸入/輸出(I/O)將承受巨大負載，並且日誌檔案將快速填充。

nslookup

使用nslookup命令可檢視不同FQDN的SWA中的名稱解析響應。

在此範例中，第一次嘗試解析名稱時，TTL設定為30分鐘。

在第二次嘗試時，我們可以看到TTL小於30分鐘，這表示已從快取中解析此記錄。

```
SWA_CLI> nslookup
```

```
Please enter the host or IP address to resolve.
```

```
[> cisco.com
```

```
Choose the query type:
```

1. A the host's IP address
2. AAAA the host's IPv6 address
3. CNAME the canonical name for an alias
4. MX the mail exchanger
5. NS the name server for the named zone
6. PTR the hostname if the query is an Internet address,

```
otherwise the pointer to other information
```

7. SOA the domain's "start-of-authority" information
8. TXT the text information

```
[1]> 1
```

```
A=10.20.3.15 TTL=30m
```

```
TSWA_CLI> nslookup
```

```
Please enter the host or IP address to resolve.
```

```
[> cisco.com
```

```
Choose the query type:
```

1. A the host's IP address
2. AAAA the host's IPv6 address
3. CNAME the canonical name for an alias
4. MX the mail exchanger
5. NS the name server for the named zone
6. PTR the hostname if the query is an Internet address,

```
otherwise the pointer to other information
```

7. SOA the domain's "start-of-authority" information
8. TXT the text information

```
[1]> 1
```

```
A=10.20.3.15 TTL=28m 49s
```

dig

dig是另一個用於查詢DNS記錄的有用命令。使用挖掘，您可以指定要查詢的源介面或DNS伺服器：

在本示例中，查詢來自伺服器10.1.1.1的A記錄


```
dig @10.1.1.1 www.cisco.com A
```

```
; <<> DiG 9.16.8 <<> @10.1.1.1 www.cisco.com A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58012
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 2cbc212c0877096701000000623db99b050bda7f896790e3 (good)
;; QUESTION SECTION:
;www.cisco.com.                IN      A

;; ANSWER SECTION:
www.cisco.com.                3600    IN      CNAME   origin-www.cisco.com.
www.cisco.com.                5       IN      A       10.20.3.15

;; Query time: 115 msec
;; SERVER: 10.1.1.1#53(10.1.1.1)
;; WHEN: Fri Mar 25 12:46:19 GMT 2022
;; MSG SIZE rcvd: 111
```

dig的用法：

```
dig [-s <source IP>] [-t] [-x <IP Address>] [@<IP address>] hostname [qtype]
```

Query a DNS server.

@<IP address> - Query the DNS server at this IP address

hostname - Record that you want to look up.

qtype - Query type: A, PTR, CNAME, MX, SOA, NS, TXT

options:

-s IP Address

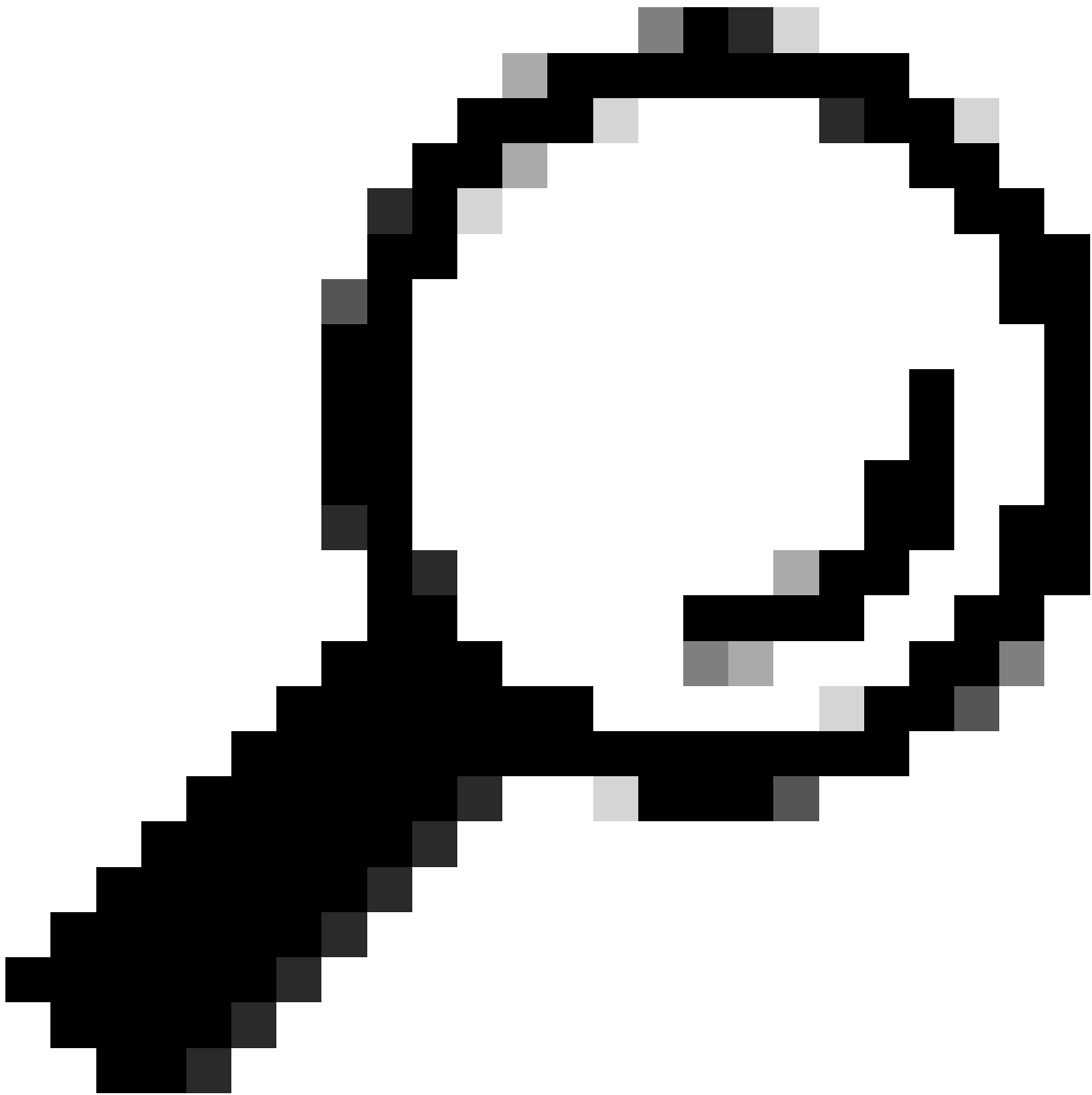
Specify the source IP address.

-t

Make query over tcp.

-x IP Address

Do a reverse lookup on this IP address.



提示：您可以選擇源IP以選擇要從哪個介面查詢名稱解析。

DNS響應緩慢

如果載入全部或部分URL的時間較長（與重新整理相同頁面時相比），最好檢查DNS回應時間。SWA中有兩個選項可用於檢查DNS響應時間：

- 配置AccessLogs自定義欄位。
- Trackstat日誌。

修改訪問日誌以檢視DNS統計資訊

您可以修改訪問日誌以檢視每個Web請求的DNS時間。

步驟 1.登入到GUI。

步驟 2.從System Administration選單中，選擇Log Subscriptions。

步驟3.從「日誌名稱」欄，按一下存取日誌或新建立的名稱。在本示例中，TAC_access_logs。

步驟4.在「自訂欄位」段落中貼上此字串：

```
[DNS response = %:<d, DNS total = %:>d]
```

步驟5.提交和提交更改。

自訂欄位名稱	自定義欄位	W3C日誌	說明
DNS響應	% : <d	x-p2p-dns-wait-time	Web代理將域名請求 (DNS)請求傳送到Web代理DNS進程所用的時間。
DNS總計	% : >d	x-p2p-dns-svc-time	Web代理DNS進程將DNS結果傳送回Web代理所用的時間。

有關如何編輯訪問日誌中的自定義欄位的詳細資訊，您可以訪問此連結：[在訪問日誌中配置效能引數-思科](#)

跟蹤器日誌中的總DNS響應時間

您可以在trackstat日誌中檢視DNS服務和其他內部服務的統計資訊。您可以透過透過FTP連線到SWA來訪問跟蹤統計日誌。

在此示例中，您可以看到快取統計資訊以及DNS響應數，這些響應數按SWA上次重新啟動以來從DNS伺服器經過的時間進行分類。

```
...  
INFO: DNS Cache Stats: Entries 662, Expire 1697, Hits 88739, Misses 664, Reclaims 0
```

```
...  
DNS Time      1.0 ms    349  
DNS Time      1.6 ms    550  
DNS Time      2.5 ms    374  
DNS Time      4.0 ms     32  
DNS Time      6.3 ms     35  
DNS Time     10.0 ms     37  
DNS Time     15.8 ms    301
```

DNS Time	25.1 ms	80
DNS Time	39.8 ms	136
DNS Time	63.1 ms	91
DNS Time	100.0 ms	12
DNS Time	158.5 ms	33
DNS Time	251.2 ms	14
DNS Time	398.1 ms	12
DNS Time	631.0 ms	45
DNS Time	1000.0 ms	120
DNS Time	1584.9 ms	73
DNS Time	2511.9 ms	296
DNS Time	3981.1 ms	265
DNS Time	6309.6 ms	190

例如，在最後一行中，它表明，自上次重新啟動SWA以來，190個DNS查詢需要超過6,309毫秒（約6秒）才能完成。

若要找出某個時間週期中的確切數字，請減去開始時間和結束時間的這些值。

例如，要確定上午10:00到上午11:00的DNS響應時間，請收集上午11:00的統計資訊，然後從上午10:00的統計資訊中減去這些統計資訊。

結果是所需日期的DNS響應時間是上午10:00到上午11:00。



注意：跟蹤統計日誌每5分鐘收集一次。

資料包捕獲

您可以捕獲資料包以檢視DNS請求和響應，並過濾可以使用的DNS：埠53。

從GUI啟動資料包捕獲：

步驟 1. 從右上角選擇支援和幫助

步驟 2. 選擇資料包捕獲

步驟3. (可選) 選擇Edit Settings以增加過濾器

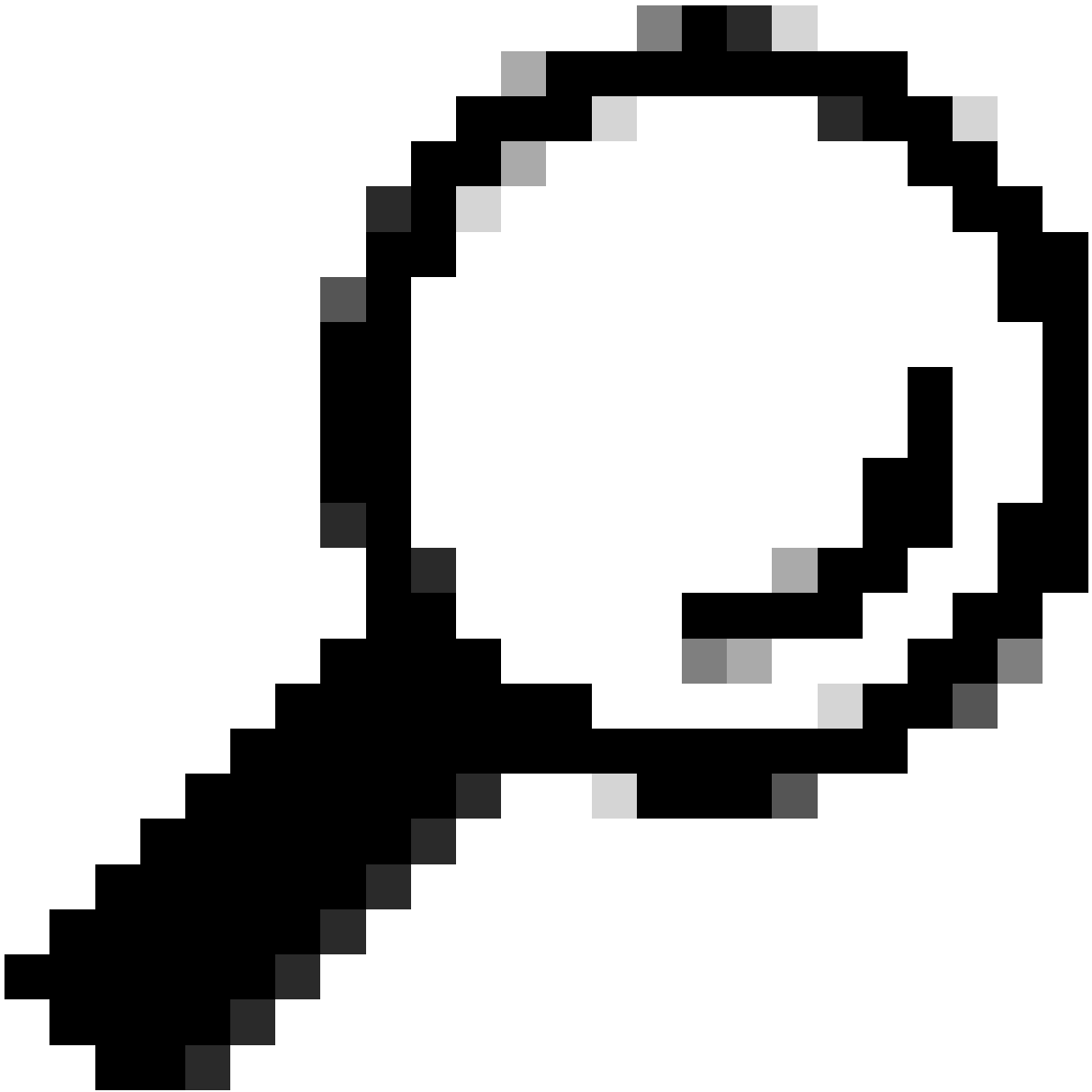
步驟4. (可選) 在Custom Filter部分選擇介面並鍵入埠53

步驟5. (選擇性) 選擇提交

Edit Packet Capture Settings

Packet Capture Settings	
Capture File Size Limit: ?	<input type="text" value="200"/> MB <small>Maximum file size is 200MB</small>
Capture Duration:	<input type="radio"/> Run Capture Until File Size Limit Reached <input type="radio"/> Run Capture Until Time Elapsed Reaches <input type="text"/> (e.g. 120s, 5m 30s, 4h) <input checked="" type="radio"/> Run Capture Indefinitely
<small>The capture can be ended manually at any time; use the settings above to specify whether the capture should end automatically.</small>	
Interfaces:	<input checked="" type="checkbox"/> M1 <input type="checkbox"/> P1 <input type="checkbox"/> P2
Packet Capture Filters	
Filters:	<small>All filters are optional. Fields are not mandatory.</small>
	<input type="radio"/> No Filters <input type="radio"/> Predefined Filters ?
	Ports: <input type="text"/>
	Client IP: <input type="text"/>
	Server IP: <input type="text"/>
	<input checked="" type="radio"/> Custom Filter ? <input type="text" value="port 53"/>
<small>Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.</small>	

映像-增加過濾器以捕獲DNS資料包



提示：提交資料包捕獲設定後可立即使用。確認更改以永久儲存這些設定以供將來使用。

步驟 6.選擇Start Capture。

步驟7. (可選) 如果需要解決特定站點或URL訪問問題，生成流量。

步驟 8.停止捕獲

步驟 9.等待頁面刷新，然後從「管理資料包捕獲檔案」清單中選擇第一個資料包捕獲

步驟 10.選擇下載檔案

L4TM

第4層流量監控器偵聽透過每個安全Web裝置上的所有埠傳入的網路流量，並將域名和IP地址與其自身資料庫表中的條目進行匹配，以確定是否允許傳入和傳出流量。

當內部客戶端感染惡意軟體並嘗試透過非標準埠和協定回撥電話時，L4流量監控器會阻止回撥電話活動退出公司網路。

預設情況下，L4流量監控器處於啟用狀態，並設定為監控所有埠上的流量，包括DNS和其他服務。

有關第4層流量監控器的詳細資訊，請參閱使用手冊。

錯誤

通知頁面

預設情況下，SWA會顯示通知頁面，通知使用者他們已被阻止以及阻止的原因

檔案名稱和通知標題：ERR_DNS_FAIL (DNS失敗)

描述：當要求的URL包含無效的網域名稱時，顯示的錯誤頁面。

通知文本：此主機名<hostname >的主機名解析 (DNS查詢) 失敗。

Internet地址可能拼錯或過時，主機<hostname >可能暫時不可用，或者DNS伺服器可能無響應。

請檢查輸入的Internet地址的拼寫。如果正確，請稍後再嘗試此請求。

This Page Cannot Be Displayed

The host name resolution (DNS lookup) for this host name (invalidurl.cisco.com) has failed. The Internet address may be misspelled or obsolete, the host (invalidurl.cisco.com) may be temporarily unavailable, or the DNS server may be unresponsive.

Please check the spelling of the Internet address entered. If it is correct, try this request later.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Sun, 02 Jul 2023 12:16:14 CEST

Username:

Source IP: 10.61.66.65

URL: GET http://invalidurl.cisco.com/

Category: Computers and Internet

Reason: UNKNOWN

Notification: DNS_FAIL

存取日誌結果代碼無

accesslog檔案中的事務結果代碼描述裝置如何解析客戶端請求。如果在訪問日誌中，Result Code為NONE，這意味著事務出錯。例如，DNS故障或網關超時。

```
1688292974.527 20 10.61.66.65 NONE/503 0 GET http://invalidurl.cisco.com/ - NONE/invalidurl.cisco.com -
```

無法啟動DNS快取

如果在重新啟動裝置時生成帶有「Failed to bootstrap the DNS cache」消息的警報，則意味著系統無法聯絡其主DNS伺服器。

如果DNS子系統在建立網路連線之前上線，則可能在開機時發生。如果在其他時間出現此消息，則可能表明存在網路問題，或者DNS配置未設定為有效的伺服器

查詢DNS伺服器時達到失敗次數上限

如果在SWA中配置的一台或多台DNS伺服器未回覆DNS查詢，則SWA會將其視為離線，並且不會將DNS查詢傳送給這些伺服器，但需要預先定義的時間量。有關詳細資訊，請參閱本文的從CLI配置DNS。

DNS_FAIL

當SWA收到HTTP請求且無法解析主機名時，預設情況下，SWA將返回如下回覆：

```
GET http://cisco HTTP/1.1
User-Agent: curl/7.19.7 (universal-apple-darwin10.0) libcurl/7.19.7 OpenSSL/0.9.8l zlib/1.2.3
Host: hostname
Accept: */*
Proxy-Connection: Keep-Alive

HTTP/1.1 307 Temporarily Moved for Domain Name Expansion
Mime-Version: 1.0
Date: Wed, 15 Sep 2022 13:05:02 EST
Proxy-Connection: keep-alive
Location: http://www.cisco.com/
Content-Length: 2068
```

此功能稱為「伺服器名稱擴充」。

WSA在嘗試重定向主機名解析客戶端的預期頁面時執行此操作。

您可以更改「DNS查詢失敗時的HTTP 307重定向的URL格式」，有關詳細資訊，請參閱本文的advanceproxyconfig部分。

WSA將返回ServFail的DNS請求視為故障。

例如，NXDOMAIN會傳回「DNS_FAIL」而非「SERVER_NAME_EXPANSION」

相關資訊

[Cisco Secure Web Appliance AsyncOS 15.0使用手冊](#)

[使用安全Web裝置最佳實踐-思科](#)

[Cisco Content Hub -域名系統簡介](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。