安全网络设备DNS服务故障排除

目录

简介

先决条件

- 要求
- 使用的组件

DNS概念

- 代理部署中的DNS服务

配置DNS设置

- 最佳实践
- 在GUI中配置DNS
- 从CLI配置DNS

CLI DNS命令

- 创建手动记录
- dnsflush
- advancedproxyconfig

DNS缓存

- 从GUI清除DNS缓存
- 从CLI清除DNS缓存
- 查看DNS缓存

排除DNS故障

- 查看DNS日志
  - 从GUI更改系统日志日志级别
  - 从CLI更改系统日志日志级别
- nslookup
- dig
- DNS响应缓慢
  - 修改访问日志以查看DNS统计信息
  - TrackstatLogs中的总体DNS响应时间
- 数据包捕获

L4TM

错误

- 通知页面
- 访问日志结果代码NONE
- 启动DNS缓存失败
- 查询DNS服务器时达到最大失败次数
- DNS_FAIL

相关内容

简介

本文档介绍域名服务(DNS)配置以及如何在Secure Web Appliance(SWA)中进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 已安装物理或虚拟安全网络设备(SWA)。
- 许可证已激活或已安装。
- 安全外壳(SSH)客户端。
- 安装向导已完成。

- 对SWA的管理访问。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

DNS概念

DNS是Internet中用于将对象名称（通常为主机名）映射到Internet协议(IP)地址或其他资源记录值的系统。

- Internet的域名空间被划分为多个域，每个域内的域名管理责任通常被委托给每个域内的系统。
- 域名空间被划分为称为区域的区域，这些区域是DNS树中的委派点。

区域包含从某一点向下的所有域，但其他区域具有权威性的域除外。区域通常具有权威域名服务器，通常不止一个。

在一个组织中，可以有许多名称服务器，但Internet客户端只能查询根名称服务器知道的那些服务器。

其他名称服务器仅应答内部查询。

DNS基于客户端/服务器模型。在此模型中，域名服务器存储关于DNS数据库一部分的数据，并将其提供给通过网络查询域名服务器的客户端。

名称服务器是在物理主机上运行并存储区域数据的程序。作为域的管理员，您可以设置名称服务器，其中包含所有描述一个或多个区域中主机的资源记录(RR)的数据库

代理部署中的DNS服务

在显式部署中：代理运行DNS查询

在透明部署中：DNS查询在客户端计算机上运行。

配置DNS设置

您可以从图形用户界面(GUI)和命令行界面(CLI)配置DNS。

AsyncOS for Web可以使用Internet根DNS服务器或您自己的DNS服务器。如果SWA使用Internet根DNS服务器，则可以指定用于特定域的备用服务器。

由于备用DNS服务器适用于单个域，因此它必须对该域具有权威性（提供最终的DNS记录）。

AsyncOS支持拆分DNS，其中，内部服务器针对特定域进行配置，外部或根DNS服务器针对其他域进行配置。

如果SWA用于本地DNS服务器，我们还可以指定例外域和关联的DNS服务器。

最佳实践

安全最佳实践建议每个网络必须托管两个DNS解析器：一个用于本地域内的权威记录，另一个用于递归解析Internet域。

为此，SWA允许为特定域配置DNS服务器。

如果一台DNS服务器可用于本地查询和递归查询，请考虑在所有SWA查询中使用它时增加的额外负载。

最佳选项是使用本地域的内部解析程序和外部域的根互联网解析程序。这取决于管理员风险简档和容差。

辅助DNS服务器必须配置，以防主要服务器不可用。如果所有服务器都配置了相同的优先级，则会随机选择服务器IP。

根据配置的服务器数量，给定服务器的超时值会有所不同。下表给出了最多六台DNS服务器的查询超时：

DNS服务器数量	查询超时（按顺序）
1	60
2	5、45
3	5、10 和 45
4	1、3、11、45
5	1、3、11、45、1
6	1、3、11、45、1、1

有关详细信息，请访问：思科网络安全设备最佳实践指南 — 思科

在GUI中配置DNS

要从GUI配置DNS，请执行以下步骤：

步骤1.从顶部菜单中选择Network。

步骤2.选择DNS。

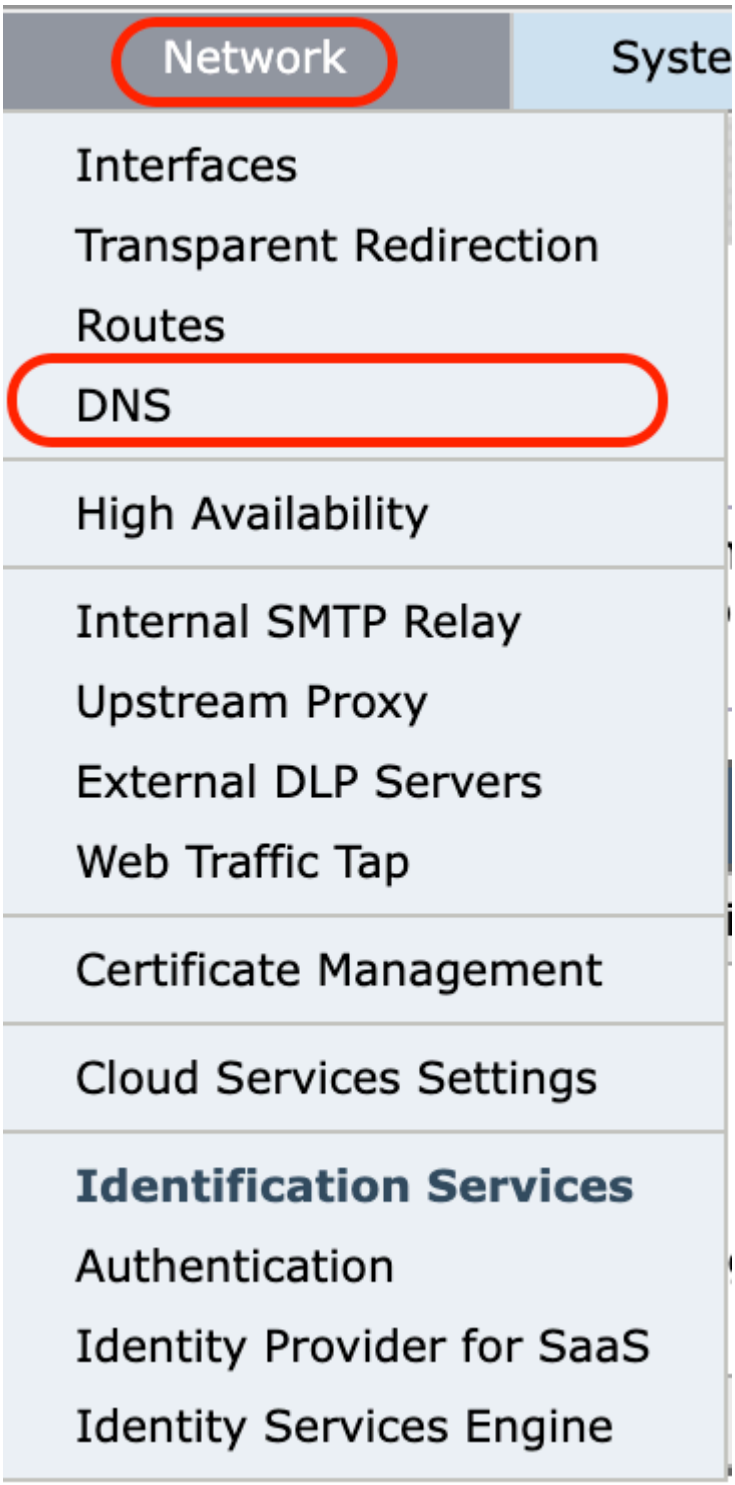
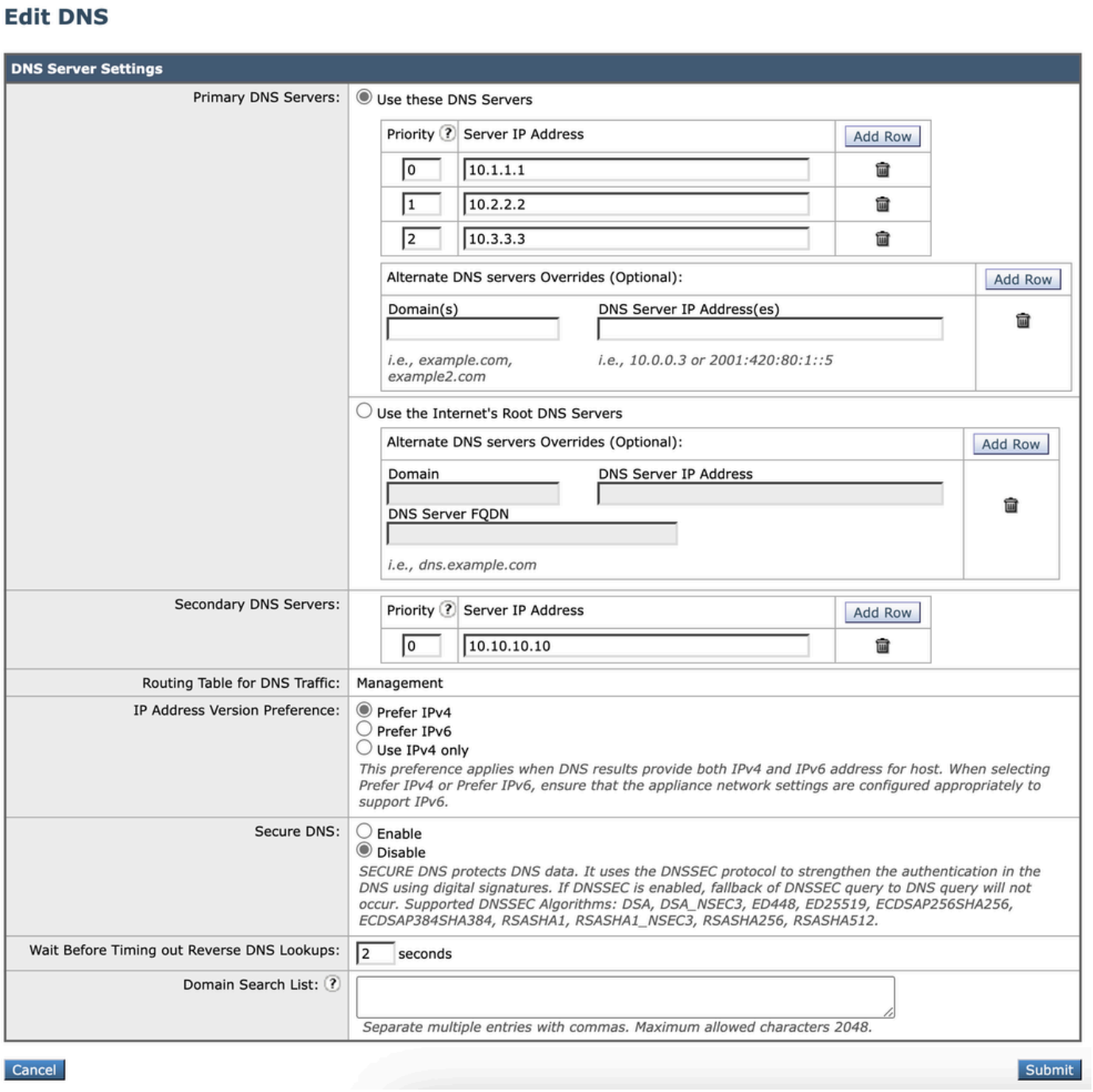


Image-GUI — 配置DNS设置

步骤3.选择Edit Settings。
步骤4.根据需要配置DNS设置。



映像 — DNS配置

- 使用以下DNS服务器：设备可用于解析主机名的本地DNS服务器。
- 备用DNS服务器覆盖（可选）：域的授权DNS服务器。

注意：AsyncOS不遵循透明FTP请求的版本首选项。

注意：在云连接器模式下，思科网络安全设备仅支持IPv4

- 使用互联网根DNS服务器。当设备无法访问网络上的DNS服务器时，选择使用互联网根

DNS服务器进行域名服务查找。

Internet根DNS服务器无法解析本地主机名。

注意：如果需要设备解析本地主机名，请使用本地DNS服务器，或者从命令行界面(CLI)向本地DNS添加相应的静态条目。

- 域搜索列表：将请求发送到没有圆点的裸主机名时使用的DNS域搜索列表(.)。 按输入的顺序（从左到右）依次尝试指定的每个域，以查看是否可以找到主机名和域的DNS匹配。

- DNS流量的路由表：指定DNS服务路由流量通过的接口。
- Wait Before Timing out Reverse DNS Lookups：在无响应的反向DNS查找超时之前的等待时间（秒）。

当主DNS服务器返回以下错误时，辅助DNS服务器会收到主机名查询：

- “无错误”，未收到应答部分
- “Server failed to complete request”（服务器无法完成请求），无应答部分
- “名称错误”，未收到应答部分
- "未实现功能"
- "服务器拒绝回答查询"

注意：AsyncOS根据策略评估事务，然后再评估外部依赖项，以避免来自设备的不必要的外部通信。例如，如果根据阻止未分类的URL的策略阻止事务，则事务不会因DNS错误而失败。

- Priority:值0具有最高优先级。如果两者具有相同的优先级，则选择随机IP。

从CLI配置DNS

您可以使用dnsconfig从CLI配置DNS设置。

步骤1.在CLI中键入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.
[]>
```

步骤2.要将新的DNS服务器添加到列表，请键入NEW并按Enter。

第3步：在主DNS名称服务器或辅助DNS名称服务器之间进行选择，您要向其中添加新的名称服务器。

```
[]> 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
```

第4步：选择添加新的域名服务器或备用域服务器（条件转发域名）

```
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
```

步骤5.提供新域名服务器的IP地址

步骤6.为新添加的域名服务器提供优先级。

```
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
```

步骤7.按Enter退出向导。

步骤8.键入commit以保存更改。



注意：要编辑或删除任何名称服务器，可以从dnsconfig中选择EDIT和DELETE。

通过SETUP选项，您可以配置DNS缓存时间和脱机DNS检测设置：

```
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 compatibilit
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缓存的最小TTL（以秒为单位）：此选项用于配置SWA缓存记录的最小秒数。有关详细信息，请访问本文档中的DNS缓存部分。
- 输入将本地DNS服务器视为脱机之前失败的尝试次数：如果DNS服务器未响应任何DNS查询

，计数器将启动。当达到此定义的值时，该名称服务器被视为脱机DNS服务器，并且SWA避免在预定义持续时间内将DNS查询发送到该名称服务器（“下一步”选项）。 当DNS服务器标记为脱机时，您会看到以下错误消息：

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

- 输入轮询脱机本地DNS服务器的间隔（以秒为单位）：当标记为脱机的DNS服务器在此时间间隔（以秒为单位）之后，SWA开始向该名称服务器发送DNS查询，并且该DNS服务器的计数器未应答重置为零。

CLI DNS命令

创建手动记录

要创建手动记录，不能使用或编辑Hosts文件。可以在CLI中的dnsconfig中使用localhosts隐藏命令。

注意：更改此配置后，必须提交更改。

```
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从DNS缓存表中删除所有缓存的DNS记录：

```
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（临时重定向）状态代码指示目标资源临时驻留在不同的统一资源标识符(URI)下，并且如果用户代理执行到该URI的自动重定向，则不得更改请求方法。由于重定向会随时间更改，因此客户端必须继续使用原始有效请求URI。

更多详细信息：什么是HTTP 307临时重定向状态代码 — Kinsta

这些选项控制SWA在透明代理部署中评估客户端请求时如何确定要连接的IP地址。收到请求后，SWA会看到目标IP地址和主机名。SWA必须决定是信任用于TCP连接的原始目标IP地址，还是执行自己的DNS解析并使用解析的地址。默认值为0 =始终按顺序使用DNS应答，这意味着SWA不信任客户端提供IP地址。

选项1:SWA尝试连接由客户端提供的IP地址，但如果失败，则回退到解析地址。解析的地址用于策略评估（Web类别、Web信誉等）。

选项2: SWA仅使用客户端提供的地址进行连接，不会回退。解析的地址用于策略评估（Web类别、Web信誉等）。

选项3: SWA仅使用客户端提供的地址进行连接，不会回退。客户端提供的IP地址用于策略评估（Web类别、Web信誉等）。

所选择的选项取决于管理员在确定给定主机名的解析地址时在客户端中必须信任多少。如果客户端是下游代理，请选择选项3以避免不必要的DNS查找增加延迟。

DNS缓存

为了提高效率和性能，思科SWA存储您最近连接的域的DNS条目。DNS缓存允许SWA避免对相同域执行过多的DNS查找。DNS缓存条目由于记录的TTL（生存时间）而过期。

- 当DNS服务器中记录的TTL大于SWA dnsconfig cache TTL时间时，dns cache使用来自DNS服务器的TTL。
- 如果DNS服务器中记录的TTL小于SWA dnsconfig cache TTL时间，则dns cache使用SWA dnsconfig设置中的TTL。

⚠ 警告：SWA具有两个DNS缓存，一个用于代理进程，另一个用于内部进程。

默认情况下，无论记录TTL如何，SWA都将DNS记录缓存至少30分钟。大量使用内容交付网络(CDN)的现代网站会拥有较低的TTL记录，因为其IP地址经常更改。

这可能会导致客户端缓存给定服务器的IP地址，并且SWA缓存同一服务器的不同地址。为此，SWA默认TTL可以从dsnconfig CLI命令中的SETUP部分降低到5分钟。

例如，如果DNS配置中DNS缓存的最小TTL（以秒为单位）已设置为10分钟，而一条记录的TTL为5分钟，则缓存记录的TTL将增加到10分钟。

另一方面，如果记录的TTL设置为15分钟，则SWA将记录在其缓存中存储15分钟。但是，有时需要清除条目的DNS缓存。损坏或过期的DNS缓存条目有时会导致向远程主机传送时出现问题。此问题通常发生在设备因网络移动或其他情况而离线之后。

从GUI清除DNS缓存

步骤1.从顶部菜单中选择Network。

步骤2.选择DNS。

步骤3.选择清除DNS缓存。

⚠ 警告：重新填充缓存时，此命令可能会导致临时性能下降

从CLI清除DNS缓存

Cisco SWA中的DNS缓存可通过CLI中的dnsflush命令清除。

查看DNS缓存

在SWA中从CLI或GUI查看缓存的DNS记录没有选项。

注意：无法通过nslookup查询DNS缓存。

排除DNS故障

查看DNS日志

与Web代理组件相关的某些日志类型未启用。默认情况下，会启用主网络代理日志类型（称为“默认代理日志”），并捕获所有Web代理模块的基本信息。

每个Web代理模块也有其自己的日志类型，您可以根据需要手动启用该日志类型。

系统日志、记录DNS、错误和提交活动。默认情况下启用

 提示：如果将系统日志的日志级别更改为DEBUG，您可以看到DNS查询和响应。您可以从GUI和CLI更改日志级别。

从GUI更改系统日志日志级别

第1步：从顶部菜单中选择系统管理。

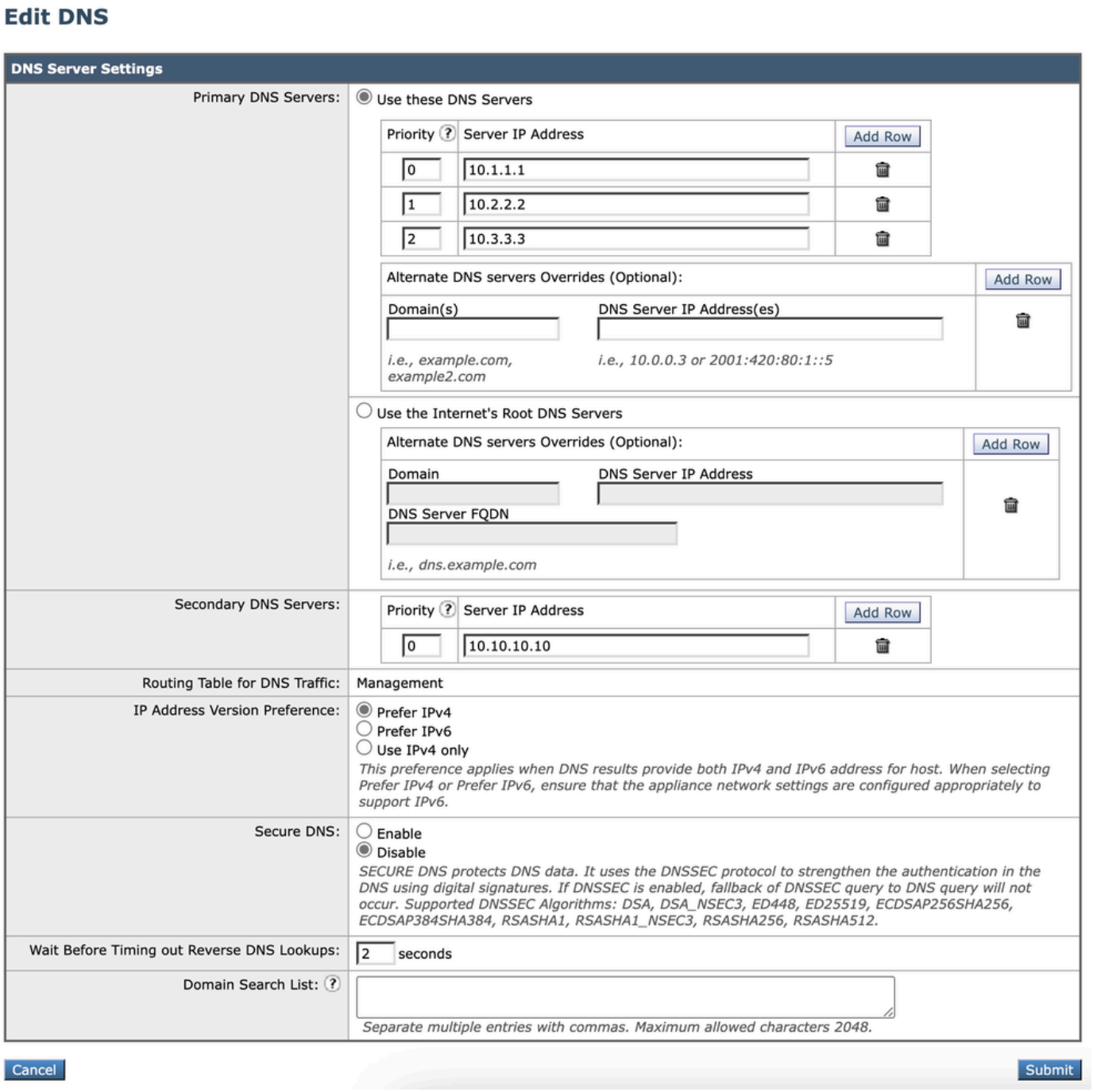
步骤2.选择Log Subscriptions。

步骤3.选择System Logs。

步骤4.在日志级别部分中选择DEBUG。

步骤5.提交。

步骤6.提交更改。



映像 — 更改系统日志，日志级别

从CLI更改系统日志日志级别

步骤1.登录到CLI。

步骤2.键入logconfig。

步骤3.选择EDIT。

步骤4.输入与System_Logs关联的编号。

步骤5.按Enter直到达到日志级别。

步骤6.选择用于调试的编号4

步骤7.按Enter键，直到退出向导。

步骤8.要保存更改，请键入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：完成故障排除后，请确保将日志级别改回信息，否则磁盘输入/输出(I/O)会产生巨大的负载，而且日志文件填充速度会过快。

nslookup

使用nslookup命令查看不同FQDN的SWA中的名称解析响应。

在本示例中，第一次尝试解析名称时，TTL设置为30分钟。

在第二次尝试时，我们可以看到TTL小于30分钟，这表示已从缓存解析此记录。

```
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是查询DNS记录的另一个有用命令。使用dig，您可以指定要查询的源接口或DNS服务器：

在本示例中，查询来自服务器10.1.1.1的A记录

```
 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的使用：

```
dig [-s ] [-t] [-x


     ] [@


      ] hostname [qtype]

        Query a DNS server.

        @



        - 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：您可以选择源IP以选择要从哪个接口查询名称解析。

DNS响应缓慢

如果加载全部或部分URL花费的时间较长（与刷新同一页面相比），最好检查DNS响应时间。SWA中有两个选项可用于检查DNS响应时间：

- 配置AccessLogs自定义字段。
- 跟踪统计日志。

修改访问日志以查看DNS统计信息

您可以修改Accesslogs以查看每个Web请求的DNS时间。

步骤1.登录GUI。

第2步：从“系统管理”(System Administration)菜单中，选择“日志订阅”(Log Subscriptions)。

步骤3.在日志名称(Log Name)列中，点击访问日志(accesslogs)或新创建的的名称。在本示例中,TAC_access_logs。

步骤4.在自定义字段(Custom Fields)部分，粘贴以下字符串：

```
[DNS response = %:

    d]
```

步骤5.提交并提交更改。

自定义字段名	自定义字段	W3C日志	描述

称			
DNS响应	%:<d	x-p2p-dns-wait-time	Web代理向Web代理DNS进程发送域名请求(DNS)请求所用的时间。
DNS总计	%:>d	x-p2p-dns-svc-time	Web代理DNS进程将DNS结果发送回Web代理所用的时间。

有关如何编辑Accesslogs中自定义字段的详细信息，您可以访问以下链接：Configure Performance Parameter in Access Logs - Cisco

Trackstat日志中的总体DNS响应时间

您可以在trackstat日志中查看DNS服务和其他内部服务的统计信息。您可以通过通过FTP连接到SWA来访问跟踪统计日志。

在本示例中，您可以看到缓存统计信息以及DNS响应数量，这些响应按SWA上次重新启动以来从DNS服务器经过的时间进行分类。

```
...
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，在最后一行中，它表示自上次重新启动SWA以来，190个DNS查询需要超过6,309毫秒（约6秒）才能完成。

要找出时间段内的确切数值，请减去开始时间和结束时间的这些值。

例如，要确定从上午10:00到上午11:00的DNS响应时间，请收集上午11:00的统计数据并从上午10:00的统计数据中减去这些统计数据。

结果是所需日期的DNS响应时间从上午10:00到上午11:00。



注意：跟踪统计信息日志每5分钟收集一次。

数据包捕获

您可以捕获数据包以查看DNS请求和响应，并仅过滤可用的DNS:端口 53.

要从GUI开始数据包捕获，请执行以下操作：

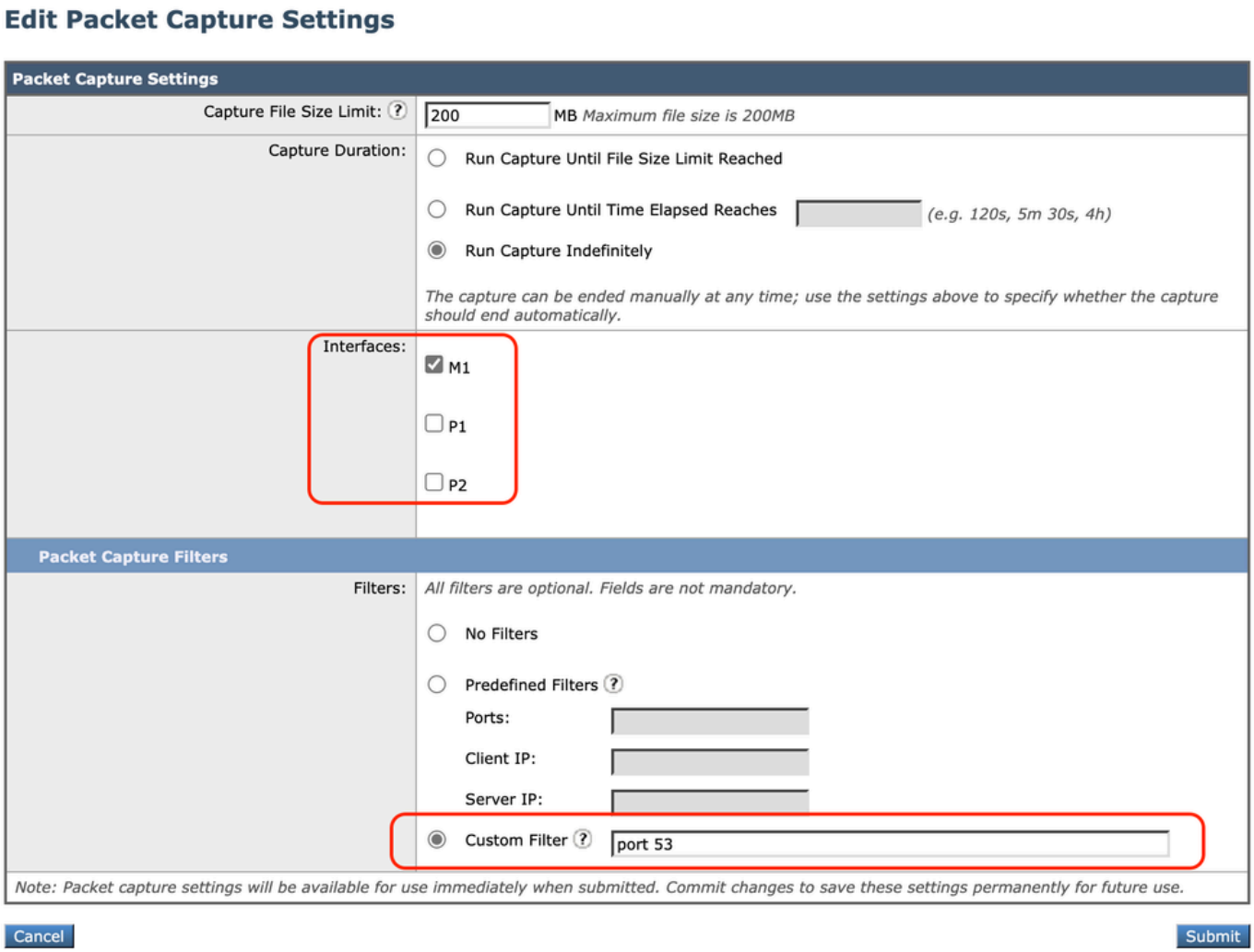
步骤1.从右上角选择支持和帮助

步骤2.选择Packet Capture

步骤3.（可选）选择Edit Settings以添加过滤器

步骤4.（可选）在Custom Filter（自定义过滤器）部分选择接口并键入端口53

第5步（可选）选择提交



映像 — 添加过滤器以捕获DNS数据包

提示：数据包捕获设置可在提交时立即使用。确认更改以永久保存这些设置以供将来使用。

步骤6.选择Start Capture。

第7步（可选）如果需要排除特定站点或URL访问故障，生成流量。

步骤8.停止捕获

步骤9.等待页面刷新，然后从“管理数据包捕获文件”列表中选择第一个数据包捕获。

步骤10.选择Download File

L4TM

第4层流量监控器会侦听通过每个安全Web设备上所有端口传入的网络流量，并将域名和IP地址与其自身数据库表中的条目进行匹配，以确定是否允许传入和传出流量。当内部客户端受到恶意软件感染并尝试通过非标准端口和协议进行回拨时，L4流量监控器会阻止回拨活动退出公司网络。

默认情况下，L4流量监控器启用并设置为监控所有端口上的流量，包括DNS和其他服务。

有关第4层流量监控器的详细信息，请参阅用户指南。

错误

通知页面

默认情况下，SWA显示通知页面，通知用户他们已被阻止以及阻止的原因

- 文件名和通知标题:ERR_DNS_FAIL（DNS故障）
- 说明：当请求的URL包含无效域名时显示的错误页面。
- 通知文本：此主机名<hostname >的主机名解析（DNS查找）失败。
- Internet地址可能拼写错误或过时，主机<hostname >可能暂时不可用，或者DNS服务器可能无响应。
- 请检查输入的Internet地址的拼写。如果正确，请稍后尝试此请求。



映像 — DNS失败错误

访问日志结果代码NONE

accesslog文件中的事务结果代码描述设备如何解析客户端请求。如果在访问日志中，结果代码为NONE，这意味着事务中有错误。例如，DNS故障或网关超时。

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

启动DNS缓存失败

如果设备重新启动时生成了带有“Failed to bootstrap the DNS cache”消息的警报，则意味着系统无法联系其主要DNS服务器。

如果DNS子系统在建立网络连接之前联机，则可能在启动时发生这种情况。如果此消息在其他时间出现，则可能表示存在网络问题或DNS配置未设置为有效的服务器

查询DNS服务器时达到最大失败次数

如果在SWA中配置的一个或某些DNS服务器未回复DNS查询，SWA会将其视为脱机，并且不会在预定义的时间段内向它们发送DNS查询。有关详细信息，请参阅本文中的从CLI配置DNS。

DNS_FAIL

当SWA收到HTTP请求失败解析主机名时，默认情况下，SWA将返回如下回复：

```
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
```

此功能称为服务器名称扩展。
SWA在尝试重定向主机名解析客户端的预期页面时执行此操作。

在DNS查找失败时，可以更改HTTP 307重定向的URL格式。 有关详细信息，请参阅本文中的advanceproxyconfig部分。

SWA将返回ServFail的DNS请求视为故障。

例如，NXDOMAIN将返回DNS_FAIL，而不是SERVER_NAME_EXPANSION。

相关内容

- 思科安全Web设备AsyncOS 15.0用户指南
- 使用安全Web设备最佳实践 — 思科
- Cisco Content Hub — 域名系统简介

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。