Solucionar problemas del servicio DNS de dispositivo web seguro

Contenido

Introducción

Este documento describe la configuración del Servicio de nombres de dominio (DNS) y cómo solucionar problemas en el Dispositivo web seguro (SWA) anteriormente conocido como WSA.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo web seguro (SWA) físico o virtual instalado
- Licencia activada o instalada
- Cliente de Secure Shell (SSH)
- El asistente de configuración ha finalizado
- Acceso administrativo al SWA

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Concepto de DNS

DNS es el sistema de Internet que asigna nombres de objetos (normalmente nombres de host) a direcciones de protocolo de Internet (IP) u otros valores de registro de recursos.

El espacio de nombres de Internet se divide en dominios y la responsabilidad de administrar los nombres de cada dominio se delega, normalmente, en los sistemas de cada dominio.

El espacio de nombres de dominio se divide en áreas denominadas zonas que son puntos de delegación en el árbol DNS.

Una zona contiene todos los dominios desde un determinado punto hacia abajo, excepto aquellos para los que otras zonas son autoritativas.

Una zona suele tener un servidor de nombres autoritativo, a menudo más de uno.

En una organización, puede tener muchos servidores de nombres, pero los clientes de Internet sólo pueden consultar los que conocen los servidores de nombres raíz.

Los otros servidores de nombres sólo responden a consultas internas.

DNS se basa en un modelo cliente/servidor. En este modelo, los servidores de nombres almacenan datos sobre una parte de la base de datos DNS y la proporcionan a los clientes que consultan el servidor de nombres en la red.

Los servidores de nombres son programas que se ejecutan en un host físico y almacenan datos de zona. Como administrador de un dominio, se configura un servidor de nombres con la base de datos de todos los registros de recursos (RR) que describen los hosts de la zona o zonas

Servicio DNS en implementaciones de proxy

En la implementación explícita: el proxy ejecuta consultas DNS

En la implementación transparente: las consultas de DNS se ejecutan en el cliente.

Configurar los parámetros de DNS

Puede configurar DNS tanto desde la interfaz gráfica de usuario (GUI) como desde la interfaz de línea de comandos (CLI).

AsyncOS para Web puede utilizar los servidores DNS raíz de Internet o sus propios servidores DNS. Si SWA utiliza servidores raíz de Internet, puede especificar los servidores alternativos que se utilizarán para dominios específicos.

Dado que un servidor DNS alternativo se aplica a un único dominio, debe ser autoritativo (proporcionar registros DNS definitivos) para dicho dominio.

AsyncOS admite DNS dividido en el que los servidores internos se configuran para dominios específicos y los servidores DNS raíz o externos se configuran para otros dominios.

Si SWA utiliza un servidor DNS en las instalaciones, también podemos especificar dominios de excepción y el servidor DNS asociado.

Prácticas recomendadas

Las prácticas recomendadas de seguridad sugieren que cada red debe alojar dos resoluciones DNS: una para los registros autorizados de un dominio local y otra para la resolución recursiva de dominios de Internet.

Para ello, el SWA permite configurar servidores DNS para dominios específicos.

En el caso de un servidor DNS disponible tanto para consultas locales como recursivas, considere la carga adicional que esto agregaría si se utiliza para todas las consultas SWA.

La mejor opción puede ser utilizar la resolución interna para dominios locales y la resolución raíz de Internet para dominios externos. Esto depende del perfil de riesgo y la tolerancia del administrador.

Los servidores DNS secundarios deben configurarse en caso de que el principal no esté disponible. Si todos los servidores se configuran con la misma prioridad, la IP del servidor se elegirá aleatoriamente.

Dependiendo del número de servidores configurados, el tiempo de espera para un servidor determinado varía. El tiempo de espera para una consulta se indica en esta tabla, para un máximo de seis servidores DNS:

Número de servidores DNS	Tiempo de espera de consulta (en secuencia)
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

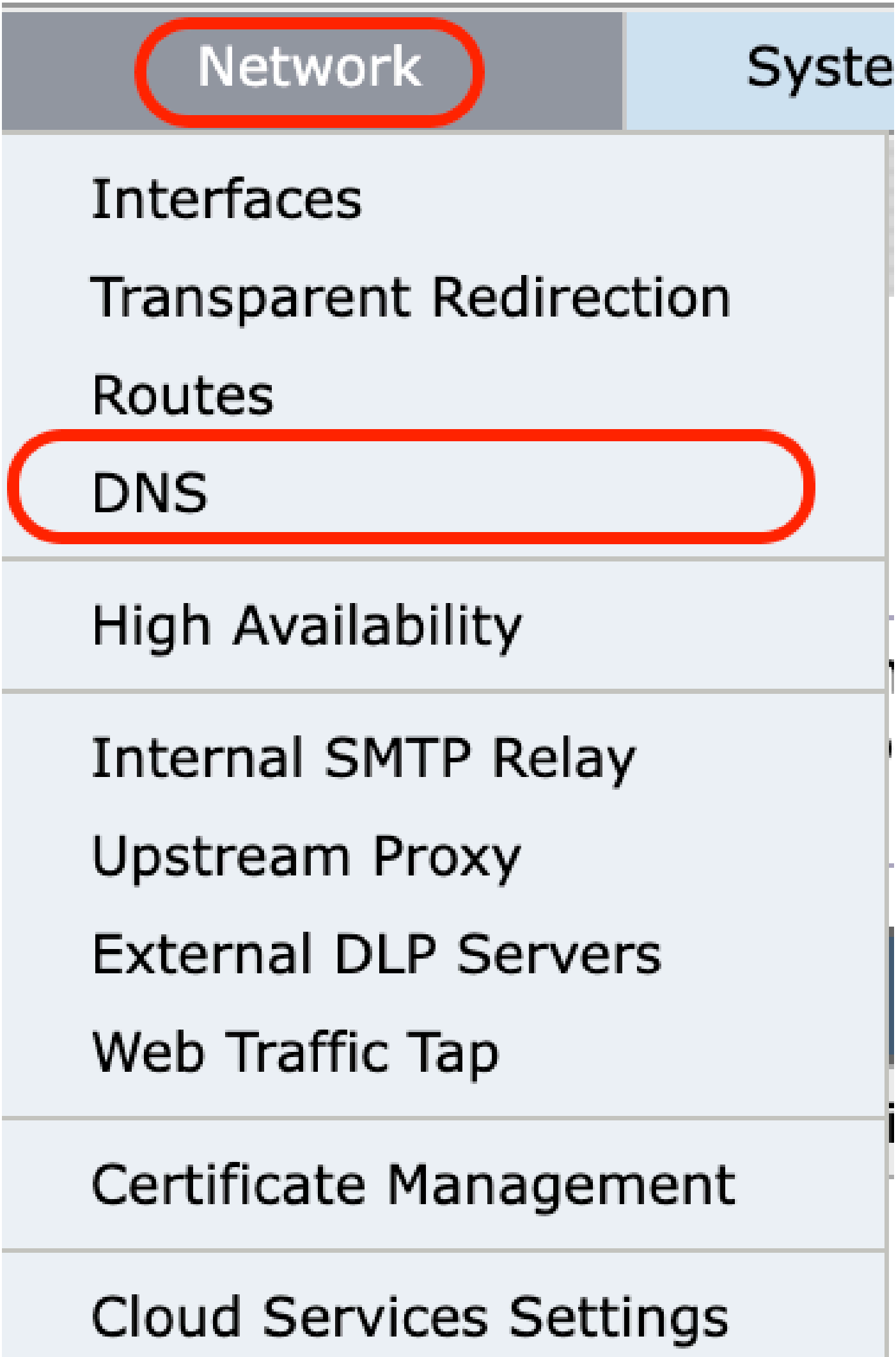
Para obtener más información, visite: Directrices sobre prácticas recomendadas de Cisco Web Security Appliance: Cisco

Configurar DNS en la GUI

Para configurar DNS desde la GUI, siga estos pasos:

Paso 1. Elija Red en el menú superior

Paso 2. Elija DNS


Network
Syste
Interfaces
Transparent Redirection
Routes
DNS
High Availability
Internal SMTP Relay
Upstream Proxy
External DLP Servers
Web Traffic Tap
Certificate Management
Cloud Services Settings

Sustituciones de servidores DNS alternativos (opcional): servidores DNS autorizados para dominios

Nota: AsyncOS no respeta la preferencia de versión para las solicitudes FTP transparentes.

Nota: en el modo de conector de nube, Cisco Web Security Appliance solo admite IPv4

Utilice los servidores DNS raíz de Internet. Elija utilizar los servidores DNS de raíz de Internet para las búsquedas del servicio de nombres de dominio cuando el dispositivo no tiene acceso a los servidores DNS de la red.

Los servidores DNS raíz de Internet no resuelven los nombres de host locales.

Nota: Si necesita que su dispositivo resuelva los nombres de host locales, utilice un servidor DNS local o agregue las entradas estáticas adecuadas al DNS local desde la interfaz de línea de comandos (CLI).

Lista de búsqueda de dominios: lista de búsqueda de dominios DNS que se utiliza cuando se envía una solicitud a un nombre de host sin software específico (sin punto " . ").

Los dominios especificados se intentarán cada uno por separado, en el orden especificado (de izquierda a derecha), para ver si se encuentra una coincidencia de DNS para el nombre de host más el dominio.

Tabla de enrutamiento para tráfico DNS: especifica la interfaz a través de la cual el servicio DNS enruta el tráfico.

Wait Before Timing Out Reverse DNS Lookups: Tiempo de espera en segundos antes de que se agote el tiempo de espera de las búsquedas de DNS inversas que no responden.

Los servidores DNS secundarios reciben consultas de nombre de host cuando los servidores DNS primarios devuelven estos errores:

· Sin errores, no se recibe sección de respuesta
· El servidor no ha podido completar la solicitud, sección sin respuesta
· Error de nombre, no se recibió sección de respuesta
· Función no implementada
· El servidor se negó a responder la consulta

Nota: AsyncOS evalúa las transacciones en función de las políticas antes de evaluar las dependencias externas para evitar la comunicación externa innecesaria del dispositivo. Por ejemplo, si una transacción se bloquea en función de una política que bloquea las URL no clasificadas, la transacción no fallará en función de un error de DNS.

Prioridad: Un valor de 0 tiene la prioridad más alta. Se selecciona una IP aleatoria si ambas tienen la misma prioridad.

Configurar DNS desde CLI

Puede utilizar dnsconfig desde CLI para configurar los parámetros de DNS.

Paso 1. Escriba dnsconfig en CLI:

```
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.
[]>
```

Paso 2. Para agregar un nuevo servidor DNS a la lista, escriba NEW y presione Entrar.

Paso 3. Elija entre Primary DNS nameservers o Secondary DNS nameservers, a los que desea agregar un nuevo nameserver.

```
[]> 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
```

Paso 4. Elija agregar un nuevo servidor de nombres o un servidor de dominios alternativo (nombre de dominio de reenvío condicional)

```
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
```

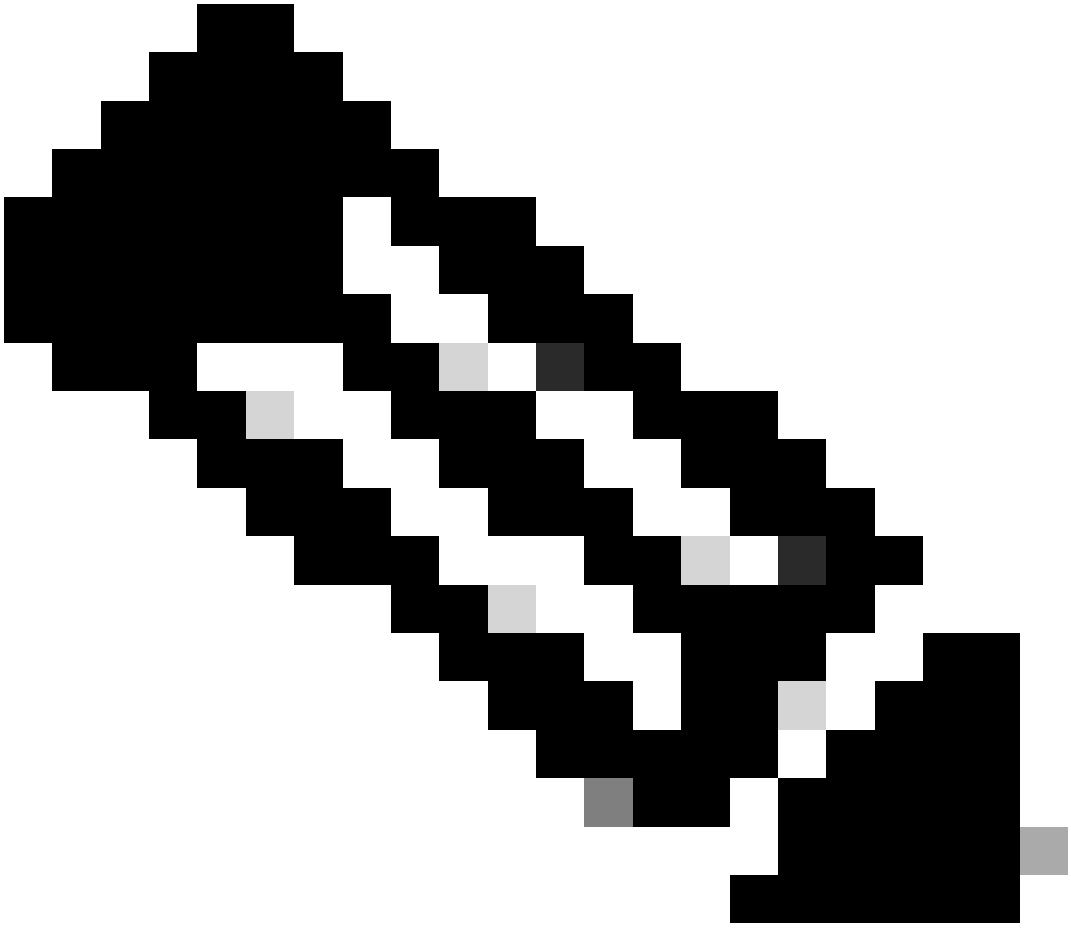
Paso 5. Proporcione la dirección IP del nuevo servidor de nombres

Paso 6. Proporcione la prioridad para el servidor de nombres recién agregado.

```
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
```

Paso 7. Pulse Intro para salir del asistente.

Paso 8. Escriba commit para guardar los cambios.



Nota: Para editar o eliminar cualquier servidor de nombres, puede seleccionar EDIT y DELETE en dnsconfig.

En la opción SETUP puede configurar los valores de tiempo de caché DNS y detección de DNS sin conexión:

```
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]>
```

TTL mínimo en segundos para caché DNS: Esta opción sirve para configurar el mínimo de segundos que SWA almacenó en caché un registro. Para obtener más información, visite la sección Caché DNS de este documento.

Introduzca el número de intentos fallidos antes de considerar un servidor DNS local sin conexión: Si el servidor DNS no responde a ninguna consulta DNS, se inicia el contador.

Cuando alcanza este valor definido, ese servidor de nombres se considera como servidor DNS sin conexión y SWA evita enviar la consulta DNS a ese servidor de nombres durante un tiempo predefinido (opción Siguiente).

Cuando el servidor DNS está marcado como desconectado, puede ver este mensaje de error:

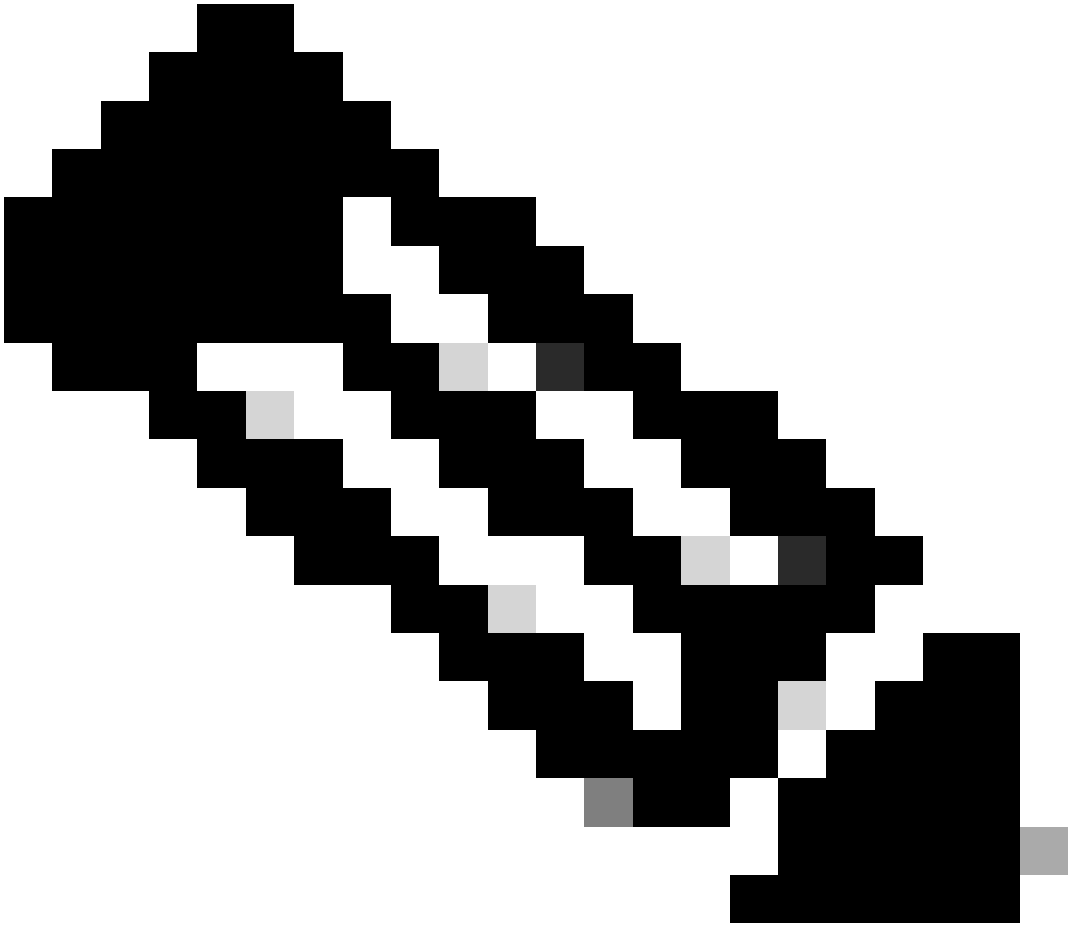
```
30 Jun 2023 07:37:03 +0200    Reached maximum failures querying DNS server 10.1.1.1
```

Introduzca el intervalo en segundos para sondear un servidor DNS local sin conexión: cuando un servidor DNS marcado como sin conexión, después de este intervalo de tiempo (en segundos), SWA comienza a enviar una consulta DNS a ese servidor de nombres y el contador para ese servidor DNS fallido se restablece en cero.

Comandos DNS de CLI

Crear registro manual

Para crear un "registro A manual" no puede utilizar ni editar el archivo Hosts. Puede utilizar el comando localhosts hidden de dnsconfig en la CLI.



Nota: Debe registrar los cambios después de cambiar esta configuración.

```
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 quita todos los registros DNS almacenados en caché de la tabla de caché DNS:

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

advanced proxyconfig

```
 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]>
```

El código de estado HTTP 307 (Redirección temporal) indica que el recurso de destino reside temporalmente bajo un identificador uniforme de recursos (URI) diferente y que el agente de usuario NO DEBE cambiar el método de solicitud si realiza una redirección automática a dicho URI. Dado que la redirección puede cambiar con el tiempo, el cliente debe continuar utilizando el URI de solicitud efectivo original.

Más detalles sobre : Cuál es el código de estado de redirección temporal HTTP 307 - Kinsta

Estas opciones controlan la forma en que SWA decide la dirección IP a la que conectarse al evaluar una solicitud de cliente en una implementación de proxy transparente. Cuando se recibe una solicitud, WSA ve una dirección IP de destino y un nombre de host. SWA debe decidir si confía en la dirección IP de destino original para la conexión TCP o si realiza su propia resolución DNS y utiliza la dirección resuelta. El valor predeterminado es"0 = Utilizar siempre las respuestas DNS en orden", lo que significa que SWA no confía en el cliente para proporcionar la dirección IP.

Opción 1: SWA intenta la dirección IP proporcionada por el cliente para la conexión, pero vuelve a la dirección resuelta si falla. La dirección resuelta se utiliza para la evaluación de políticas (categoría web, reputación web y demás).

Opción 2: SWA sólo utiliza la dirección proporcionada por el cliente para la conexión y no retrocede. La dirección resuelta se utiliza para la evaluación de políticas (categoría web, reputación web y demás).

Opción 3: SWA solo utiliza la dirección proporcionada por el cliente para la conexión y no retrocede. La dirección IP proporcionada por el cliente se utiliza para la evaluación de políticas (categoría web, reputación web y demás).

La opción elegida depende de cuánta confianza debe depositar el administrador en el cliente al determinar la dirección resuelta para un nombre de host determinado. Si el cliente es un proxy descendente, elija la opción 3 para evitar la latencia añadida de búsquedas de DNS innecesarias.

Caché DNS

Para aumentar la eficacia y el rendimiento, Cisco SWA almacena entradas DNS para los dominios a los que se ha conectado recientemente. La memoria caché DNS permite a SWA evitar búsquedas DNS excesivas de los mismos dominios. Las entradas de la caché DNS caducan debido al TTL (tiempo de vida) del registro.

Cuando el TTL del registro en el servidor DNS es mayor que el tiempo TTL de la caché de dnsconfig de SWA, la caché de dns utiliza el TTL del servidor DNS.

Cuando el TTL del registro en el servidor DNS es menor que el tiempo TTL de la caché de dnsconfig de SWA, la caché de dns utiliza el valor TTL de dnsconfig de WSA.

⚠ Precaución: SWA tiene dos memorias caché DNS, una está diseñada para el proceso de proxy y la otra se utiliza para el proceso interno.

De forma predeterminada, el SWA almacenó en caché los registros DNS durante un mínimo de 30 minutos, independientemente del registro TTL. Los sitios web modernos que hacen un uso intensivo de las redes de distribución de contenido (CDN) tendrían registros TTL bajos, ya que sus direcciones IP cambian con frecuencia.

Esto podría dar lugar a que un cliente almacene en caché una dirección IP para un servidor determinado y SWA almacene en caché una dirección diferente para el mismo servidor. Para contrarrestar esto, el TTL predeterminado SWA se puede reducir a cinco minutos desde la sección SETUP en el comando dsnconfig CLI.

Por ejemplo, si el valor "TTL mínimo en segundos para la caché DNS" de la configuración DNS se ha establecido en 10 minutos y un registro tiene TTL de 5 minutos, el TTL del registro almacenado en caché aumenta a 10 minutos.

Por otra parte, si el TTL del registro se establece en 15 minutos, SWA almacena el registro durante 15 minutos en su caché.

Sin embargo, a veces es necesario borrar la memoria caché de DNS de las entradas. Las entradas de caché de DNS dañadas o caducadas pueden ocasionar problemas con la entrega a uno o varios hosts remotos.

Este problema suele producirse después de que el dispositivo haya estado fuera de línea para un traslado de red o cualquier otra circunstancia.

Borrar la caché DNS de la GUI

Paso 1. Elija Red en el menú superior

Paso 2. Elija DNS

Paso 3. Elija Clear DNS Cache

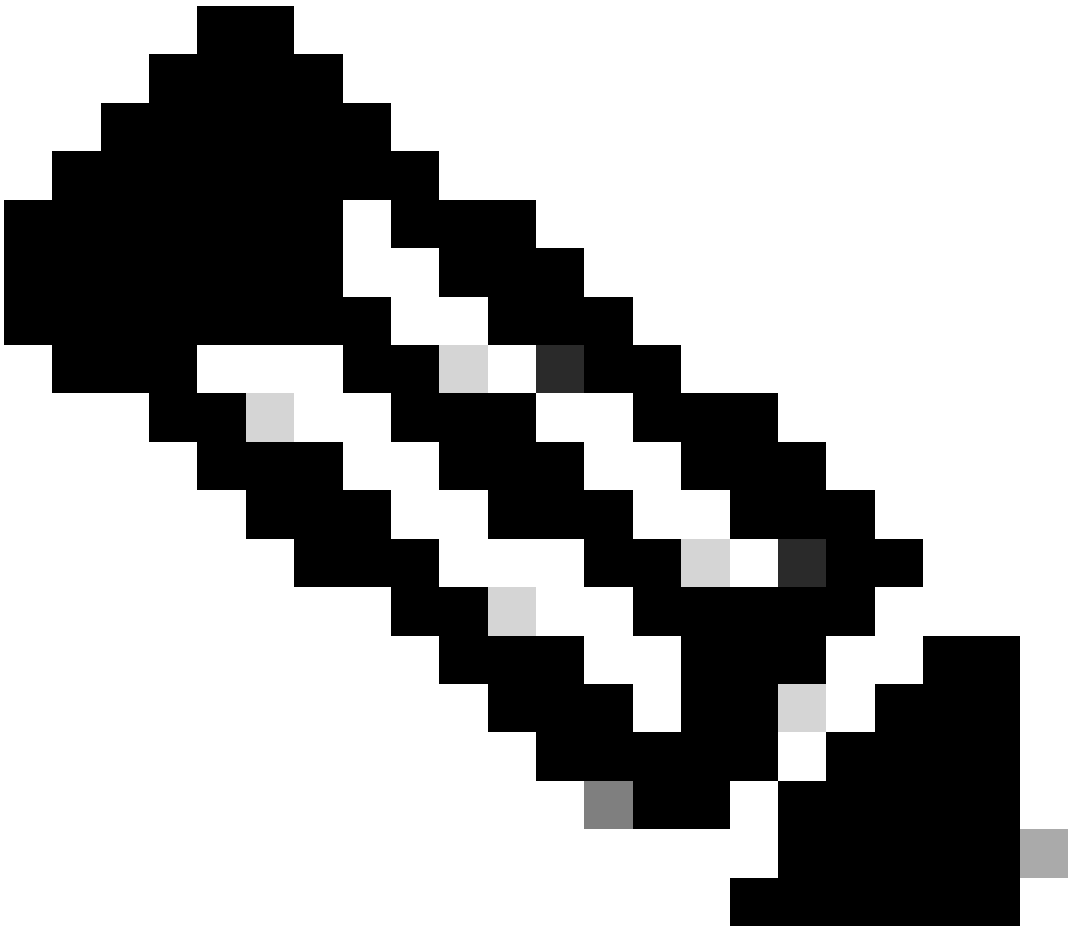
⚠ Precaución: este comando puede causar una degradación temporal del rendimiento mientras se vuelve a llenar la memoria caché

Borrar la caché DNS de CLI

La memoria caché DNS de Cisco WSA se puede borrar mediante el comando dnsflushde la CLI.

Ver caché DNS

No existe la opción de ver el registro DNS almacenado en caché en SWA desde CLI o GUI.



Nota: No puede consultar la caché DNS mediante nslookup.

Troubleshooting de DNS

Ver registros DNS

Algunos tipos de registro relacionados con el componente de proxy web no están habilitados. El tipo de registro de proxy web principal, denominado "Registros de proxy predeterminados", está habilitado de forma predeterminada y captura información básica sobre todos los módulos de proxy web.

Cada módulo Web Proxy también tiene su propio tipo de registro que puede activar manualmente según sea necesario.

Registros del sistema, Registros DNS, error y actividad de confirmación. que está habilitada de forma predeterminada

---

 Sugerencia: Si cambia el nivel de registro de registros del sistema a DEBUG, puede ver las consultas y respuestas de DNS.Puede cambiar el nivel de registro de GUI y CLI.

Cambiar el nivel de registro de registros del sistema desde GUI

Paso 1. Elija Administración del sistema en el menú superior

Paso 2. Elija Suscripciones de registro

Paso 3. Elija Registros del sistema

Paso 4. Elija DEBUG en la sección Log Level

Paso 5. Enviar

Paso 6. Registrar cambios

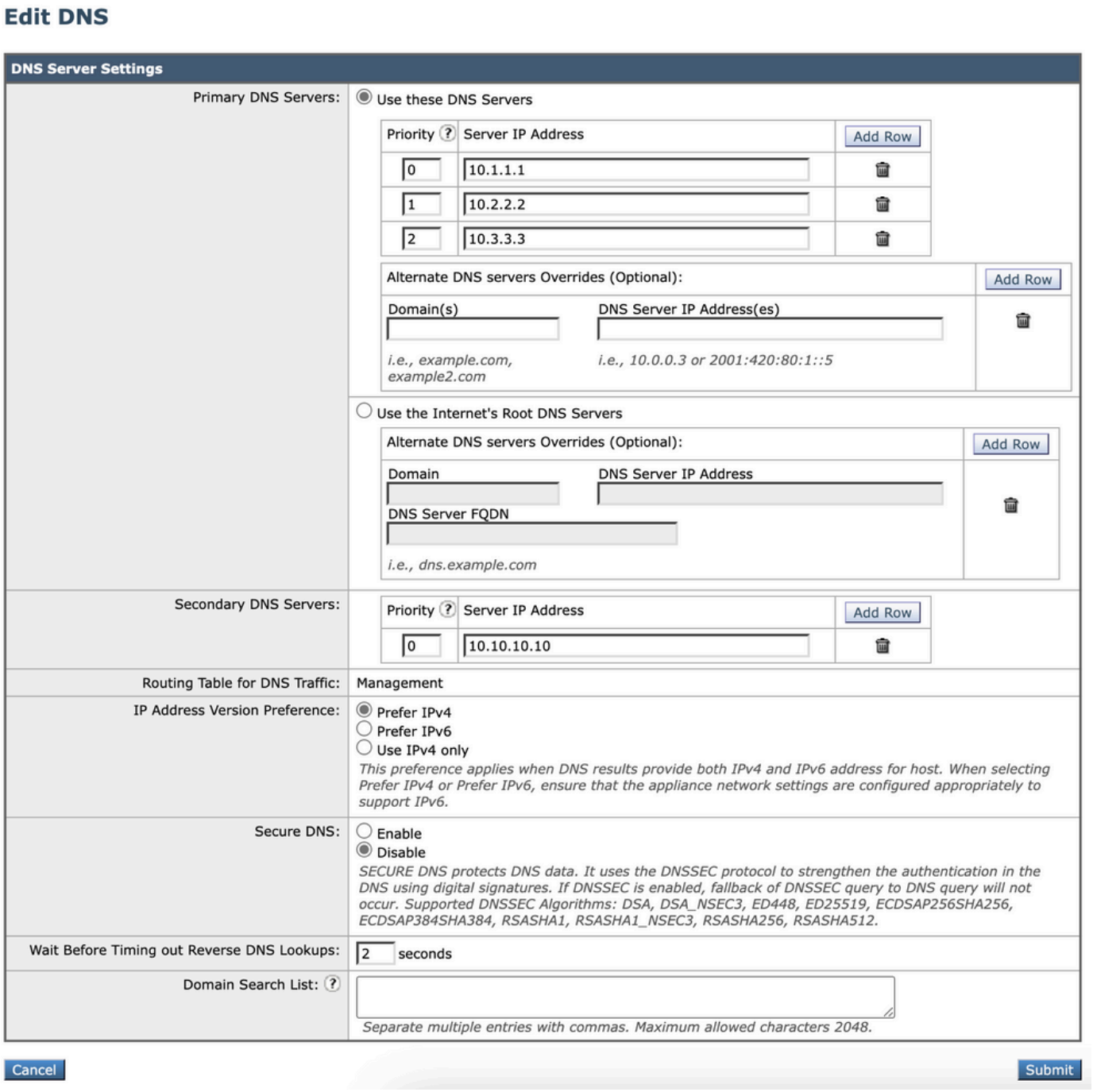


Imagen - Cambiar registros del sistema, nivel de registro

Cambiar el nivel de registro de registros del sistema desde CLI

Paso 1. Iniciar sesión en CLI

Paso 2. Escriba logconfig

Paso 3. Elija EDITAR

Paso 4. Introduzca el número asociado a System_Logs

Paso 5. Pulse Intro hasta que alcance el nivel de registro

Paso 6. Elija el número 4 que es para Debug

Paso 7. Pulse Intro hasta que salga del asistente

Paso 8. Para guardar los cambios, escriba 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
```

Sugerencia: Una vez que haya solucionado el problema, asegúrese de volver a cambiar el nivel de registro a Información, de lo contrario habría una gran carga en el disco Entrada / Salida (E/S) y el archivo de registro se llenaría a rápido.

nslookup

Utilice el comando nslookup para ver la respuesta de resolución de nombres en SWA para diferentes FQDN.

En este ejemplo, en el primer intento de resolver el nombre, el TTL se establece en 30 minutos.

En el segundo intento, podemos ver que el TTL es inferior a 30 minutos, lo que indica que este registro se resolvió desde la memoria caché.

```
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
```

cavar

dig es otro comando útil para consultar los registros DNS. Con dig puedes especificar la interfaz de origen o el servidor DNS en el que queremos consultar:

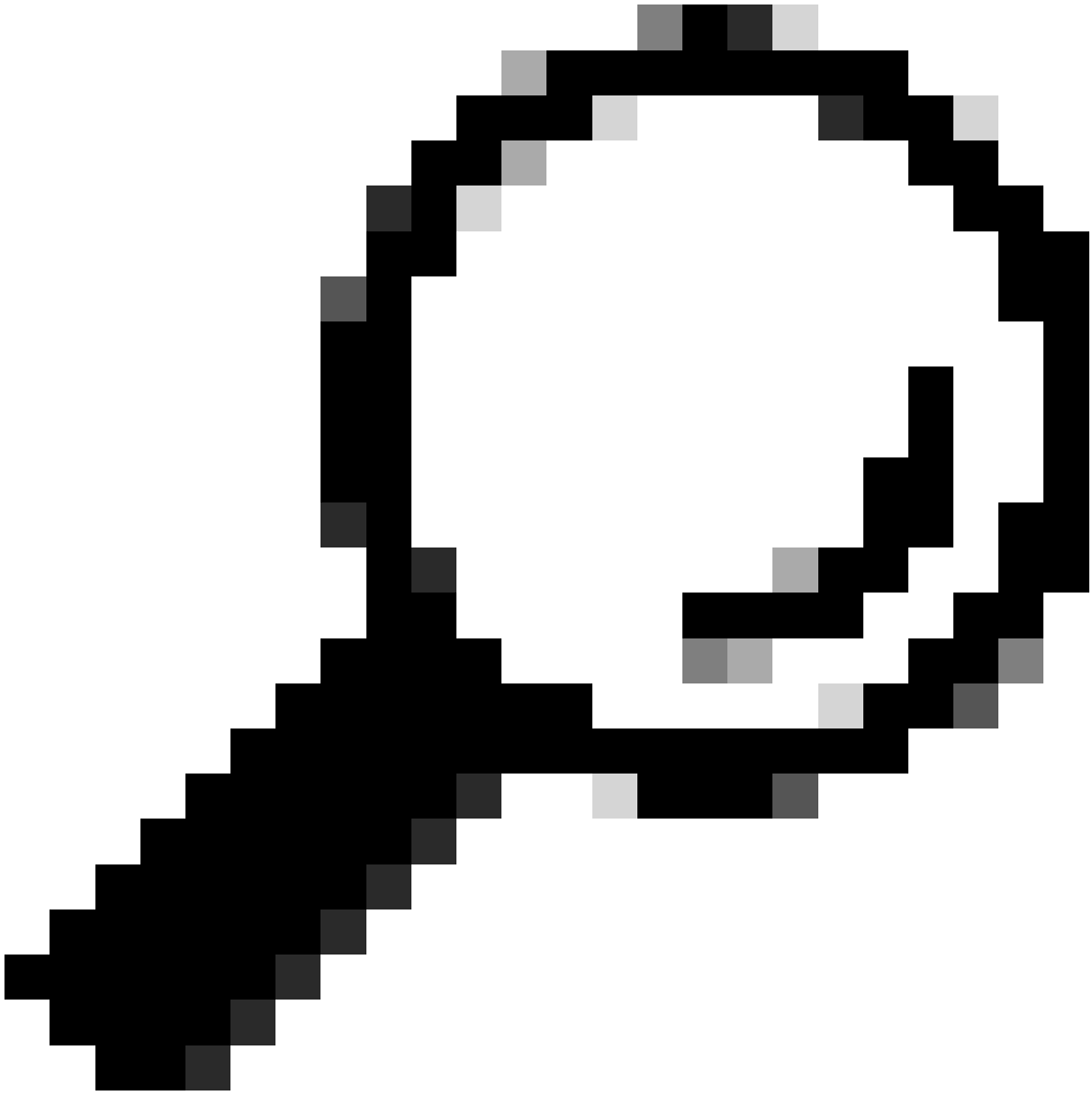
En este ejemplo, aquí está la consulta para A-Record del servidor 10.1.1.1

```
 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
```

El uso de dig:

```
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.
```



Sugerencia: Puede elegir la IP de origen para elegir desde qué interfaz desea consultar la resolución de nombres.

Respuesta de DNS lenta

Si la carga de todas o algunas URL tardó más tiempo (en comparación con cuando actualiza la misma página), es mejor comprobar el tiempo de respuesta de DNS. Hay dos opciones en SWA para verificar el tiempo de respuesta de DNS:

- Configure el campo personalizado AccessLogs.
- Registros de Trackstat.

Modificar registros de acceso para ver estadísticas de DNS

Puede modificar los registros de acceso para ver la hora de DNS de cada solicitud web.

Paso 1. Inicie sesión en GUI.

Paso 2. En el menú Administración del sistema, elija Registrar suscripciones.

Paso 3.En la columna Log Name, haga clic en accesslogs,o el nombre del recién creado. En este ejemplo, TAC_access_logs.

Paso 4.En la sección Campos personalizados, pegue esta cadena:

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

Paso 5.Enviar y confirmar cambios.

Nombre de campo personalizado	Campo personalizado	Registros W3C	Descripción
respuesta DNS	%:<d	x-p2p-dns-wait-time	Tiempo que tarda el proxy web en enviar la solicitud de DNS (petición de nombre de dominio) al proceso DNS del proxy web.
Total de DNS	%:>d	x-p2p-dns-svc-time	Tiempo que tarda el proceso DNS del proxy web en devolver un resultado DNS al proxy web.

Para obtener más información sobre cómo editar campos personalizados en los registros de acceso, puede visitar este enlace: Configure Performance Parameter in Access Logs - Cisco

Tiempo de respuesta DNS total en registros de Trackstat

Puede ver las estadísticas del servicio DNS y otros servicios internos en los registros de trackstat. Puede acceder a los registros de trackstats conectándose vía FTP a su SWA.

En este ejemplo, puede ver las estadísticas de caché y el número de respuestas DNS, categorizadas por el tiempo transcurrido desde el servidor DNS desde que se reinició SWA por última vez.

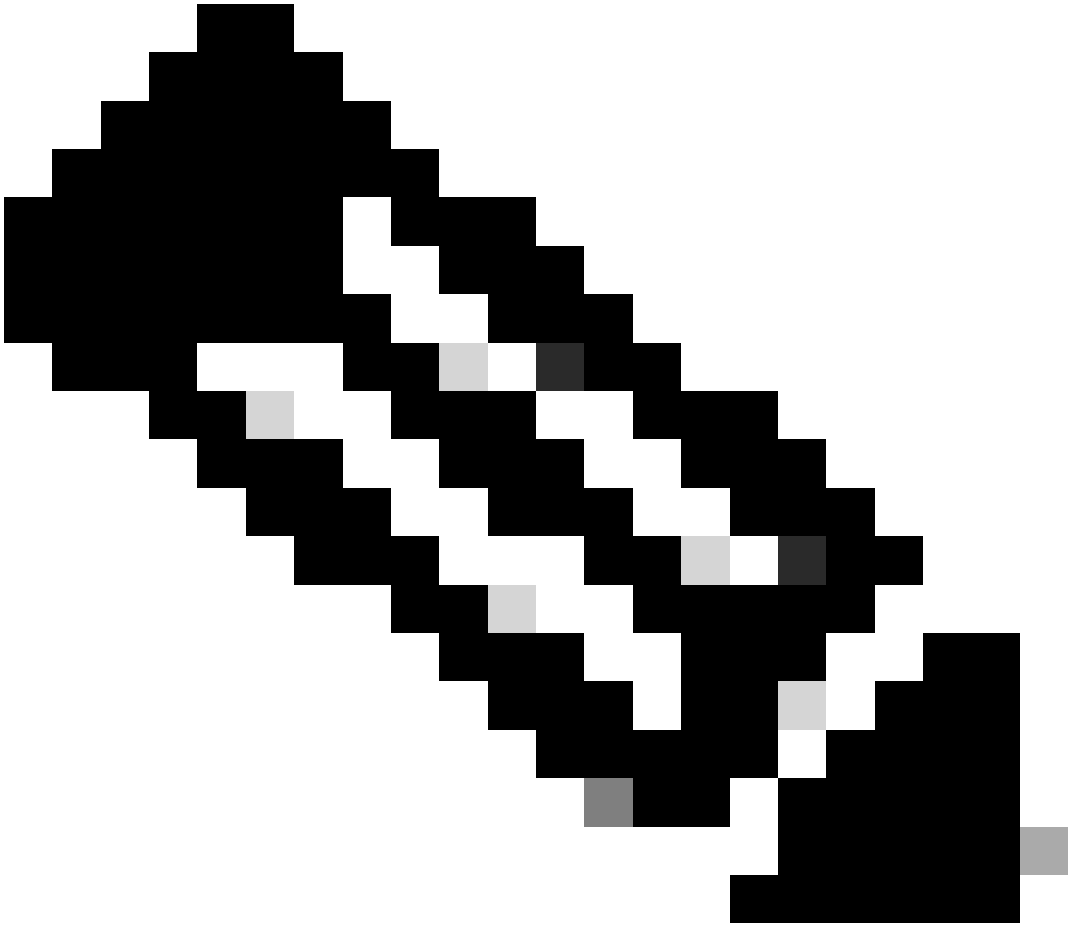
```
...
INFO: DNS Cache Stats: Entries 662, Expire 1697, Hits 88739, Misses 664, Reclaims 0
...
       DNS Time       1.0 ms    349
       DNS Time       1.6 ms    550
       DNS Time       2.5 ms    374
       DNS Time       4.0 ms    32
       DNS Time       6.3 ms    35
       DNS Time      10.0 ms    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
```

Por ejemplo, en la última línea, indica que 190 consultas DNS tardaron más de 6.309 milisegundos (aproximadamente 6 segundos) en finalizar desde que SWA se reinició por última vez.

Para averiguar el número exacto en un período de tiempo, reste estos valores para la hora de inicio y la hora de finalización.

Por ejemplo, para identificar el tiempo de respuesta de DNS de 10:00 a 11:00, recopile estadísticas para 11:00 a.m. y reste las estadísticas de 10:00 a.m.

El resultado es el tiempo de respuesta de DNS de 10:00 a 11:00 a.m. para la fecha deseada.



Nota: Los registros de estadísticas de seguimiento se recopilan cada 5 minutos.

Captura de paquete

Puede capturar paquetes para ver las solicitudes y respuestas de DNS, para filtrar solo por DNS puede utilizar: puerto 53 .

Para iniciar la captura de paquetes desde la GUI:

Paso 1. Elija Soporte y Ayuda en la esquina superior derecha

Paso 2. Elija Captura de paquetes

Paso 3. (Opcional) Elija Editar configuración para agregar filtro

Paso 4. (Opcional) Elija sus interfaces y escriba el puerto 53 en la sección Filtro personalizado

Paso 5. (Opcional) Seleccione Ejecutar

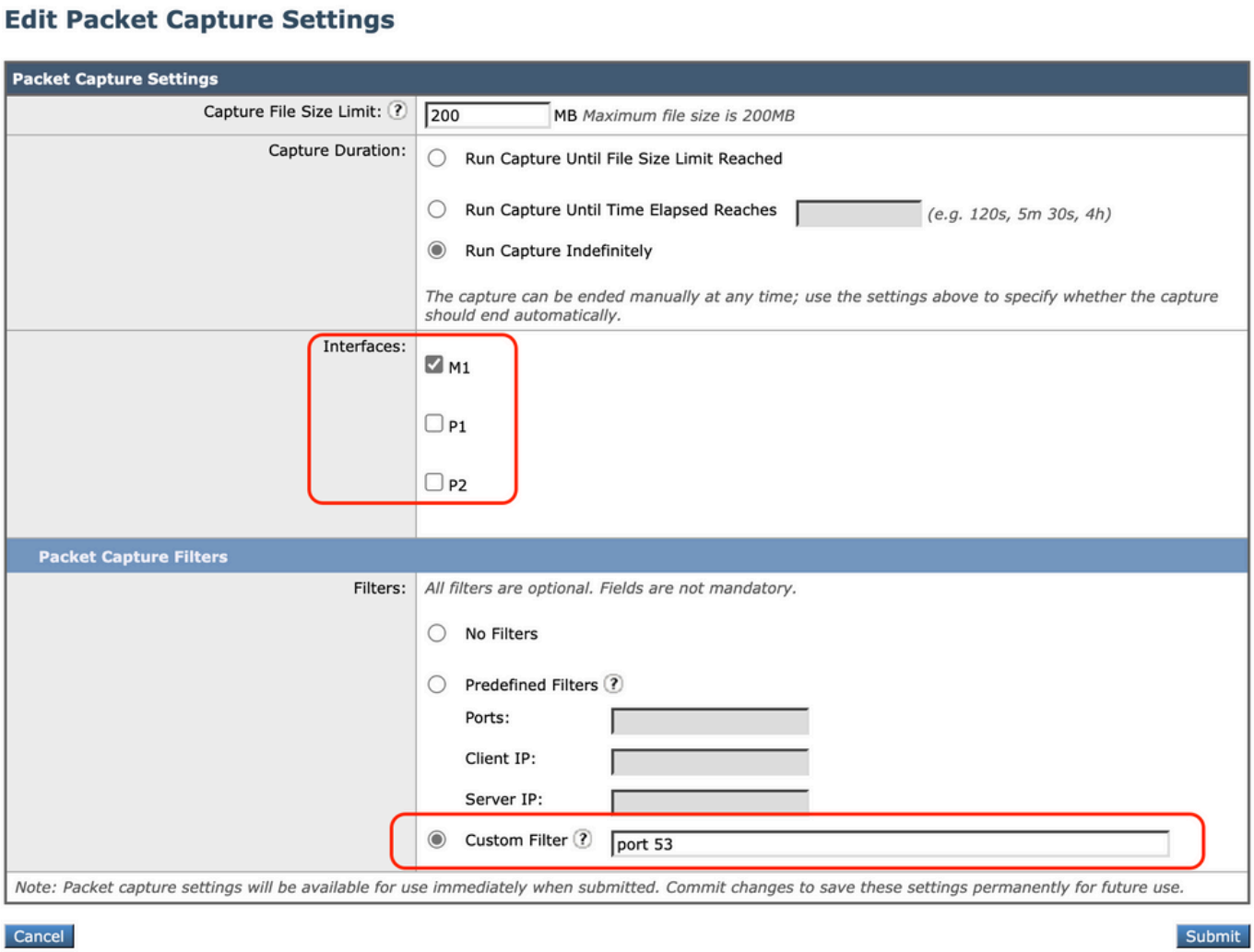
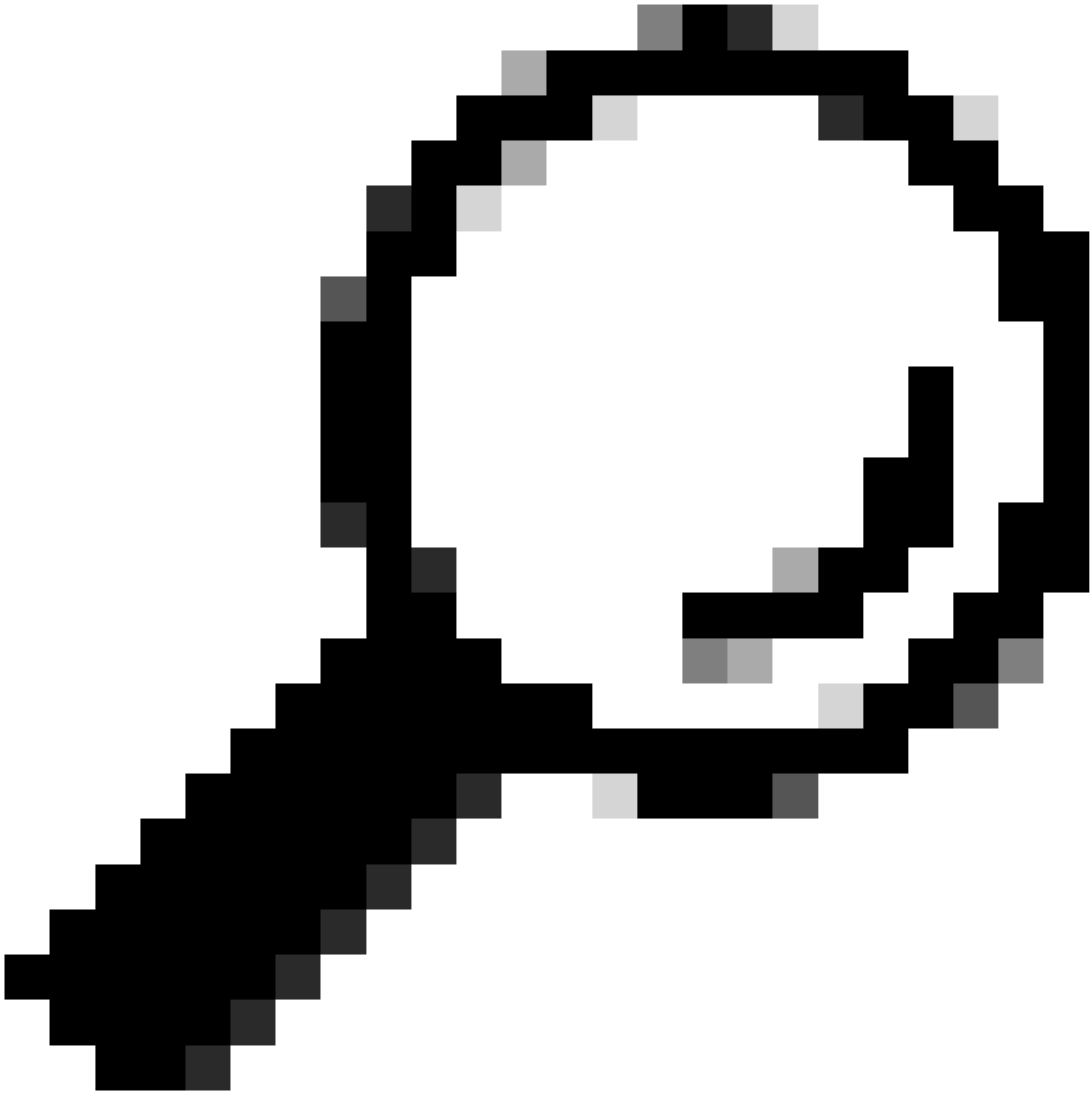


Imagen - Agregar filtro para capturar paquetes DNS



Sugerencia: la configuración de captura de paquetes está disponible para utilizarla inmediatamente después de enviarla. Realice los cambios necesarios para guardar esta configuración de forma permanente para su uso futuro.

Paso 6. Elija Iniciar captura.

Paso 7. (Opcional) Generar tráfico, si necesita solucionar problemas de acceso a sitios o URL específicos.

Paso 8. Detener captura

Paso 9. Espere a que se actualice la página y, a continuación, seleccione la primera captura de paquetes de la lista "Administrar archivos de captura de paquetes"

Paso 10. Elija Descargar archivo

L4TM

El Monitor de tráfico de Capa 4 escucha el tráfico de red que llega a través de todos los puertos de cada Dispositivo web seguro y compara los nombres de dominio y las direcciones IP con las entradas de sus propias tablas de base de datos para determinar si se debe permitir el tráfico entrante y saliente.

Cuando los clientes internos se infectan con malware e intentan comunicarse por teléfono a través de puertos y protocolos no estándar, el monitor de tráfico L4 impide que la actividad de comunicación telefónica salga de la red corporativa.

De forma predeterminada, el Monitor de tráfico L4 está habilitado y configurado para supervisar el tráfico en todos los puertos, incluidos DNS y otros servicios.

Para obtener más información sobre el monitor de tráfico de capa 4, consulte la guía del usuario.

Errores

Página de notificación

De forma predeterminada, SWA muestra una página de notificación para informar a los usuarios de que se han bloqueado y del motivo del bloqueo

Nombre de archivo y título de notificación: ERR_DNS_FAIL (fallo de DNS)

Descripción: página de error que se muestra cuando la URL solicitada contiene un nombre de dominio no válido.

Texto de notificación: Error en la resolución del nombre de host (búsqueda de DNS) para este nombre de host <nombre de host >.

La dirección de Internet puede estar mal escrita u obsoleta, el host <nombre de host > puede no estar disponible temporalmente o el servidor DNS puede no responder.

Compruebe que ha escrito correctamente la dirección de Internet. Si es correcto, intente esta solicitud más tarde.

Imagen - Error DNS FAIL

Código de resultado de AccessLog NINGUNO

Los códigos de resultado de la transacción del archivo accesslog describen cómo resuelve el dispositivo las solicitudes de los clientes. Si en el registro de acceso el código de resultado es NONE, significa que hubo un error en la transacción. Por ejemplo, un fallo de DNS o un tiempo de espera de gateway.

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

Error al iniciar la caché DNS

Si se genera una alerta con el mensaje "Failed to bootstrap the DNS cache" (Error al iniciar la caché DNS) cuando se reinicia un dispositivo, significa que el sistema no ha podido ponerse en contacto con sus servidores DNS principales.

Esto puede suceder en el momento del arranque si el subsistema DNS se conecta antes de que se establezca la conectividad de red. Si este mensaje aparece en otras ocasiones, podría indicar problemas de red o que la configuración de DNS no está establecida en un servidor válido

Fallos máximos alcanzados al consultar el servidor DNS

Si uno o algunos de los servidores DNS configurados en SWA no respondieron a las consultas

DNS, SWA las considera como sin conexión y no les envía las consultas DNS durante un período de tiempo predefinido. Para obtener más información, lea "Configurar DNS desde CLI" en este artículo.

DNS_FAIL

Cuando SWA recibe una solicitud HTTP yno puede resolver el nombre de host, SWA devolverá de forma predeterminada una respuesta como:

```
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
```

Esta función se denomina "expansión del nombre del servidor".
WSA hace esto en los intentos de que el nombre de host redirigido resuelva la página esperada para el cliente.

Puede cambiar el "formato de URL para la redirección HTTP 307 en caso de fallo en la búsqueda de DNS", para obtener más información consulte la sección advanced proxyconfig de este artículo.

WSA trata la solicitud DNS que devuelve ServFail como una falla.
Por ejemplo, NXDOMAIN devolvería "DNS_FAIL" en lugar de "SERVER_NAME_EXPANSION"

Información Relacionada

Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance

Uso de las prácticas recomendadas de los dispositivos web seguros: Cisco

Cisco Content Hub: Introducción al sistema de nombres de dominio

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).