Risoluzione dei problemi relativi al servizio DNS Secure Web Appliance

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Concetto DNS

- Servizio DNS in distribuzioni proxy

Configura impostazioni DNS

- Procedure ottimali
- Configurazione di DNS nella GUI
- Configurare DNS da CLI

Comandi DNS CLI

- Crea registrazione manuale
- dnsflush
- configurazione avanzata

cache DNS

- Cancellazione della cache DNS dalla GUI

Introduzione

In questo documento viene descritta la configurazione del DNS (Domain Name Service) e la procedura per la risoluzione dei problemi in Secure Web Appliance (SWA), precedentemente noto come WSA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Installazione di Physical o Virtual Secure Web Appliance (SWA) completata
- Licenza attivata o installata
- Client Secure Shell (SSH)
- Installazione guidata completata

- Accesso amministrativo all'SWA

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Concetto DNS

Il DNS è il sistema in Internet che esegue il mapping dei nomi degli oggetti (in genere nomi host) in indirizzi IP (Internet Protocol) o altri valori di record di risorse.

Lo spazio dei nomi di Internet è suddiviso in domini e la responsabilità della gestione dei nomi all'interno di ogni dominio è delegata, in genere, ai sistemi all'interno di ogni dominio.

Lo spazio dei nomi di dominio è suddiviso in aree denominate zone che rappresentano punti di delega nella struttura DNS.

Una zona contiene tutti i domini da un certo punto verso il basso, ad eccezione di quelli per i quali altre zone sono autorevoli.

Una zona dispone in genere di un server dei nomi autorevole, spesso più di uno.

In un'organizzazione è possibile disporre di molti server dei nomi, ma i client Internet possono eseguire query solo su quelli noti ai server dei nomi principali.

Gli altri server dei nomi rispondono solo alle query interne.

Il DNS si basa su un modello client/server. In questo modello i server dei nomi archiviano i dati relativi a una parte del database DNS e li forniscono ai client che eseguono query sul server dei nomi in tutta la rete.

I server dei nomi sono programmi che vengono eseguiti su un host fisico e memorizzano i dati delle zone. In qualità di amministratore di un dominio, è necessario configurare un server dei nomi con il database di tutti i record di risorse (RR) che descrivono gli host della zona o delle zone

Servizio DNS in distribuzioni proxy

Nella distribuzione esplicita: il proxy esegue query DNS

Nella distribuzione trasparente: le query DNS vengono eseguite sul client.

Configura impostazioni DNS

È possibile configurare il DNS sia dall'interfaccia grafica utente (GUI) che dall'interfaccia della riga di comando (CLI).

AsyncOS for Web può utilizzare i server DNS radice Internet o i propri server DNS. Se i servizi

SWA utilizzano server radice Internet, è possibile specificare server alternativi da utilizzare per domini specifici.

Poiché un server DNS alternativo si applica a un singolo dominio, deve essere autorevole (fornire record DNS definitivi) per tale dominio.

AsyncOS supporta la suddivisione del DNS quando i server interni sono configurati per domini specifici e i server DNS esterni o radice sono configurati per altri domini.

Se SWA utilizza un server DNS locale, è inoltre possibile specificare i domini di eccezione e il server DNS associato.

Procedure ottimali

In base alle procedure consigliate per la sicurezza, ogni rete deve ospitare due resolver DNS, uno per i record autorevoli da un dominio locale e uno per la risoluzione ricorsiva dei domini Internet.

Per risolvere questo problema, l'SWA consente di configurare i server DNS per domini specifici.

Nel caso di un server DNS disponibile sia per le query locali che per quelle ricorsive, considerare il carico aggiuntivo che verrebbe aggiunto se fosse utilizzato per tutte le query SWA.

L'opzione migliore può essere quella di utilizzare il resolver interno per i domini locali e i resolver Internet radice per i domini esterni. Ciò dipende dal profilo di rischio e dalla tolleranza dell'amministratore.

Se il server primario non è disponibile, è necessario configurare i server DNS secondari. Se tutti i server sono configurati con la stessa priorità, l'indirizzo IP del server viene scelto in modo casuale.

A seconda del numero di server configurati, il timeout per un determinato server varia. Il timeout per una query è indicato in questa tabella, per un massimo di sei server DNS:

Numero di server DNS	Timeout query (in sequenza)
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

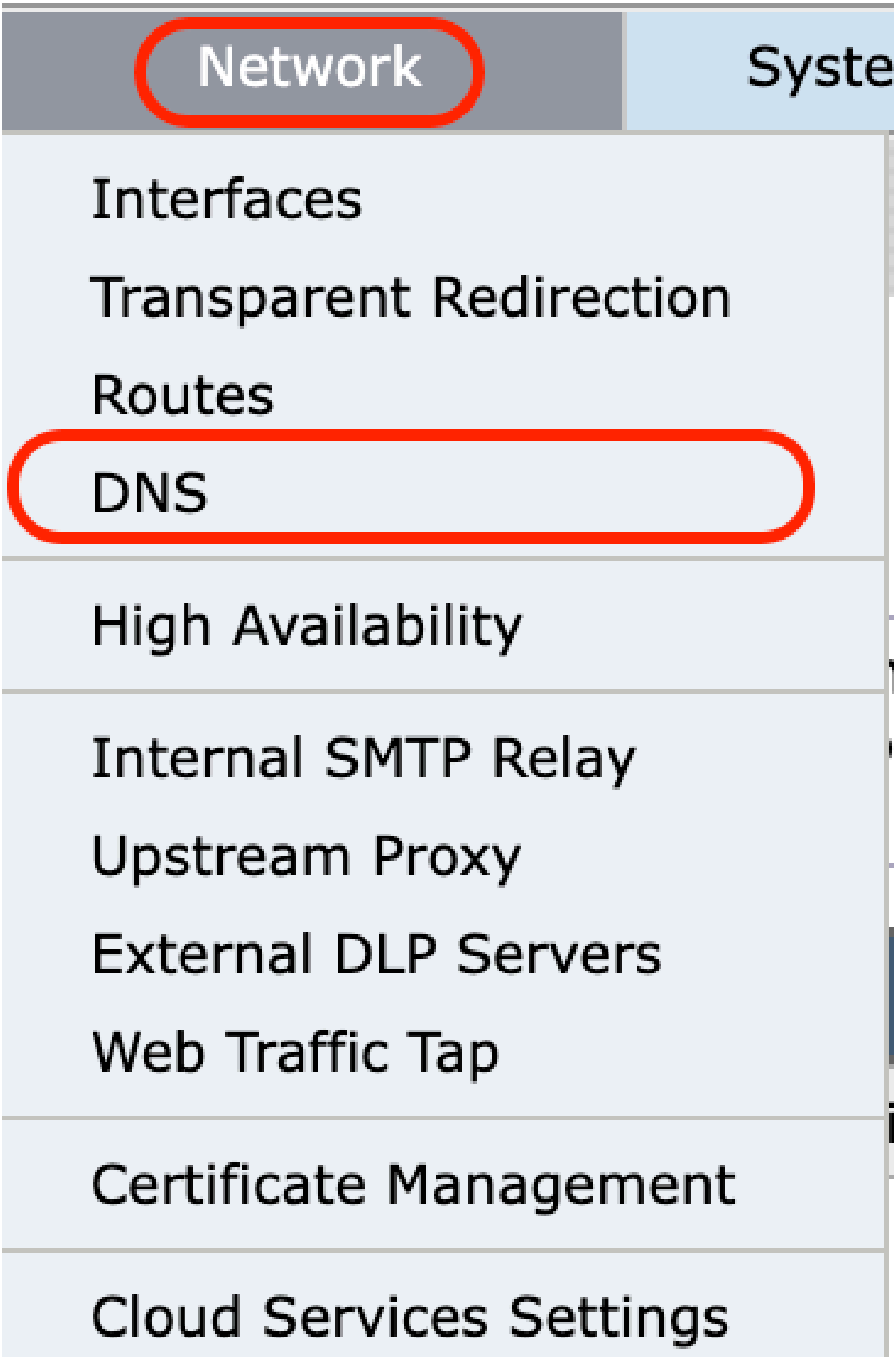
Per ulteriori informazioni, visitare il sito Web: Cisco Web Security Appliance Best Practices Guidelines - Cisco

Configurazione di DNS nella GUI

Per configurare il DNS dalla GUI, attenersi alla seguente procedura:

Passaggio 1. Scegli rete dal menu in alto

Passaggio 2. Scegli 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

Override di server DNS alternativi (facoltativo): server DNS autorevoli per i domini

Nota: AsyncOS non rispetta la preferenza di versione per le richieste FTP trasparenti.

Nota: in modalità Cloud Connector, Cisco Web Security Appliance supporta solo IPv4

Utilizzare i server DNS radice Internet. Scegliere di utilizzare i server DNS radice Internet per le ricerche dei servizi dei nomi di dominio quando l'accessorio non ha accesso ai server DNS della rete.

I server DNS radice Internet non risolvono i nomi host locali.

Nota: se l'accessorio deve risolvere i nomi host locali, utilizzare un server DNS locale oppure aggiungere le voci statiche appropriate al DNS locale dall'interfaccia della riga di comando (CLI).

Elenco di ricerca dei domini: elenco di ricerca dei domini DNS utilizzato quando una richiesta viene inviata a un nome host nudo (senza punto ". ").

I domini specificati vengono tentati a turno, nell'ordine immesso (Da sinistra a destra), per verificare se è possibile trovare una corrispondenza DNS per il nome host più dominio.

Tabella di routing per il traffico DNS: specifica l'interfaccia attraverso cui il servizio DNS instrada il traffico.

Attendi prima del timeout Ricerche DNS inverse: tempo di attesa in secondi prima del timeout delle ricerche DNS inverse non reattive.

I server DNS secondari ricevono query sui nomi host quando i server DNS primari restituiscono questi errori:

· Nessun errore, nessuna sezione di risposta ricevuta
· Il server non è riuscito a completare la richiesta, nessuna sezione di risposta
· Errore di nome, nessuna sezione di risposta ricevuta
· Funzione non implementata
· Il server si è rifiutato di rispondere alla query

Nota: AsyncOS valuta le transazioni in base ai criteri prima di valutare le dipendenze esterne per evitare inutili comunicazioni esterne dall'accessorio. Ad esempio, se una transazione viene bloccata in base a un criterio che blocca gli URL non classificati, la transazione non avrà esito negativo in base a un errore DNS.

Priorità: il valore 0 ha la priorità più alta. Se entrambi hanno la stessa priorità, viene selezionato un

indirizzo IP casuale.

Configurare DNS da CLI

È possibile utilizzare dnsconfig da CLI per configurare le impostazioni DNS.

Passaggio 1. Digitare dnsconfig nella 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.
[]>
```

Passaggio 2. Per aggiungere un nuovo server DNS all'elenco, digitare NEW e premere Invio.

Passaggio 3. Scegliere tra i server dei nomi DNS primari o i server dei nomi DNS secondari, a cui si desidera aggiungere un nuovo server dei nomi.

```
[]> 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
```

Passaggio 4. Scegliere se aggiungere un nuovo server dei nomi o un server di dominio alternativo (nome di dominio con inoltro condizionale)

```
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
```

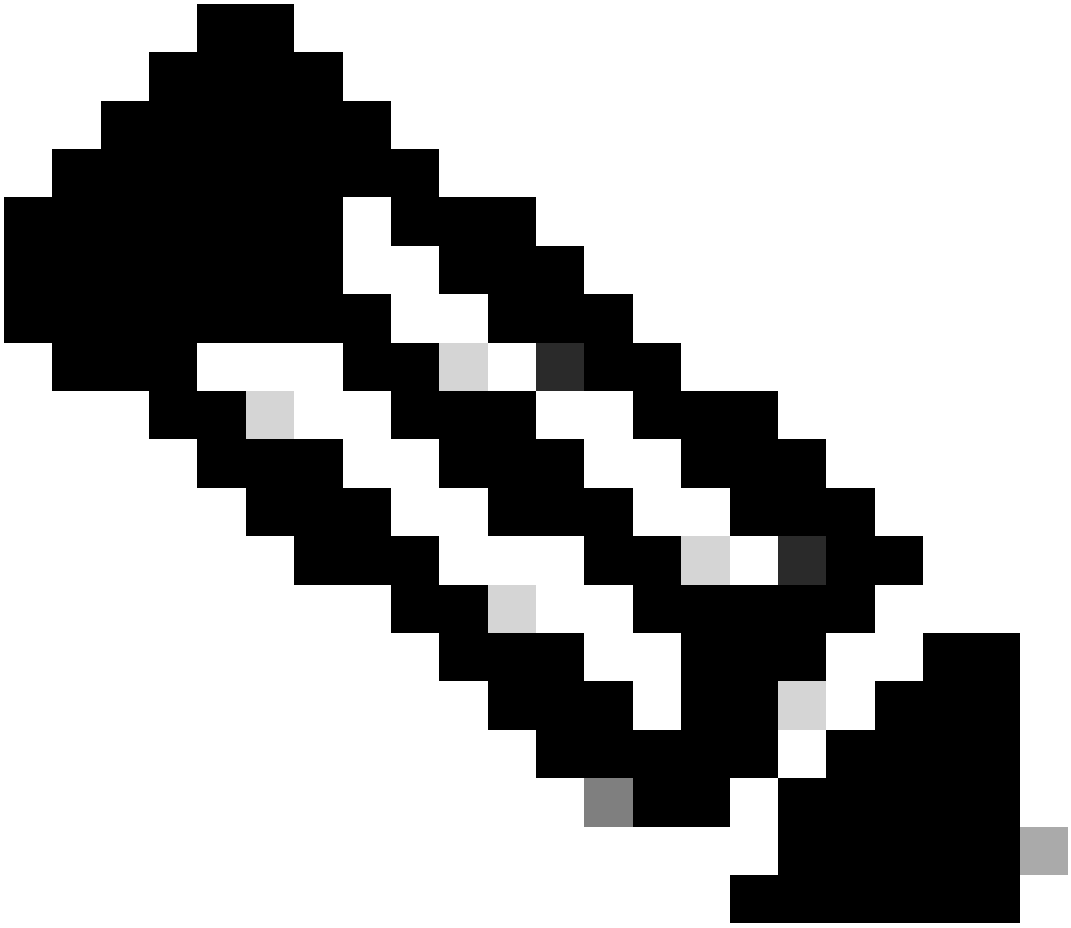
Passaggio 5. Specificare l'indirizzo IP del nuovo server dei nomi

Passaggio 6. Specificare la priorità per il server dei nomi appena aggiunto.

```
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
```

Passaggio 7. Premere Invio per uscire dalla procedura guidata.

Passaggio 8. Digitare commit per salvare le modifiche.



Nota: per modificare o eliminare qualsiasi server dei nomi è possibile scegliere MODIFICA ed ELIMINA da dnsconfig.

Dall'opzione SETUP è possibile configurare l'ora della cache DNS e le impostazioni di rilevamento DNS offline:

```
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 minimo in secondi per la cache DNS: questa opzione consente di configurare i secondi minimi in cui SWA ha memorizzato nella cache un record. per ulteriori informazioni, vedere la sezione relativa alla cache DNS in questo documento.

Immettere il numero di tentativi non riusciti prima di considerare offline un server DNS locale: se il server DNS non risponde ad alcuna query DNS, il contatore viene avviato.

Quando raggiunge questo valore definito, il server dei nomi viene considerato come server DNS non in linea e SWA evita di inviare la query DNS a tale server dei nomi per una durata predefinita (opzione Avanti).

Quando il server DNS è contrassegnato come offline, è possibile visualizzare questo messaggio di errore:

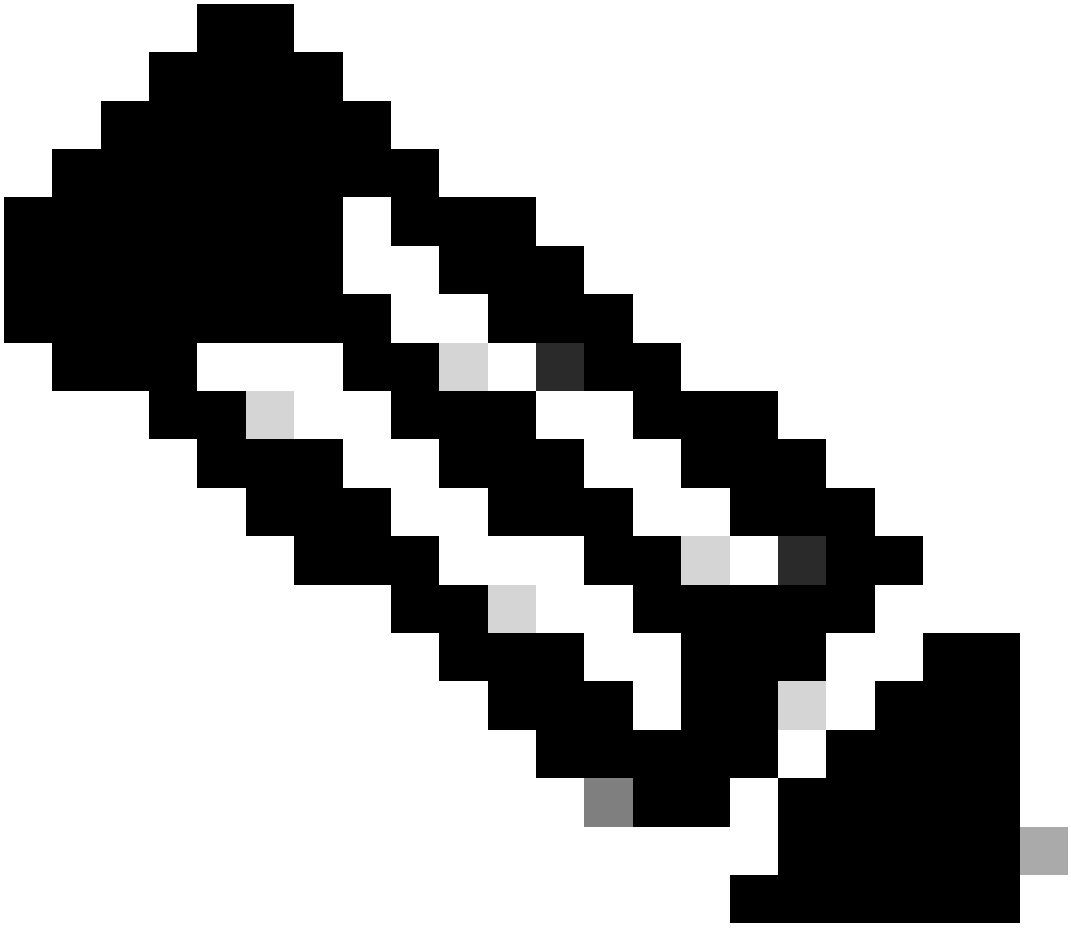
```
30 Jun 2023 07:37:03 +0200    Reached maximum failures querying DNS server 10.1.1.1
```

Immettere l'intervallo in secondi per il polling di un server DNS locale offline: quando un server DNS contrassegnato come offline, dopo questo intervallo di tempo (in secondi), SWA inizia a inviare la query DNS a tale server dei nomi e il contatore per tale server DNS risposta non riuscita viene azzerato.

Comandi DNS CLI

Crea registrazione manuale

Per creare manualmente "Un record" non è possibile utilizzare o modificare il file Hosts. È possibile usare il comando localhosts hidden da dnsconfig nella CLI.



Nota: è necessario eseguire il commit delle modifiche dopo aver modificato queste configurazioni.

```
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 rimuove tutti i record DNS memorizzati nella cache dalla tabella della cache DNS:

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

configurazione avanzata

```
 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]>
```

Il codice di stato HTTP 307 (reindirizzamento temporaneo) indica che la risorsa di destinazione risiede temporaneamente in un URI (Uniform Resource Identifier) diverso e che l'agente utente NON DEVE modificare il metodo di richiesta se esegue un reindirizzamento automatico a tale URI. Poiché il reindirizzamento può cambiare nel tempo, il client deve continuare a utilizzare l'URI della richiesta effettiva originale.

Ulteriori dettagli su : Qual è il codice di stato del reindirizzamento temporaneo HTTP 307 - Kinsta

Queste opzioni controllano il modo in cui SWA decide l'indirizzo IP a cui connettersi, quando valuta una richiesta client in una distribuzione proxy trasparente. Quando si riceve una richiesta, WSA visualizza un indirizzo IP di destinazione e un nome host. L'autorità di certificazione deve decidere se considerare attendibile l'indirizzo IP di destinazione originale per la connessione TCP o se eseguire la propria risoluzione DNS e utilizzare l'indirizzo risolto. Il valore predefinito è "0 = Usa sempre le risposte DNS in ordine", ovvero SWA non considera attendibile il client per fornire l'indirizzo IP.

Opzione 1: SWA prova l'indirizzo IP fornito dal client per la connessione, ma se l'operazione non riesce, torna all'indirizzo risolto. L'indirizzo risolto viene utilizzato per la valutazione dei criteri (categoria Web, reputazione Web e così via).

Opzione 2: SWA utilizza solo l'indirizzo fornito dal client per la connessione e non esegue il fallback. L'indirizzo risolto viene utilizzato per la valutazione dei criteri (categoria Web, reputazione Web e così via).

Opzione 3: SWA utilizza solo l'indirizzo fornito dal client per la connessione e non esegue il fallback. L'indirizzo IP fornito dal client viene utilizzato per la valutazione dei criteri (categoria Web, reputazione Web e così via).

L'opzione scelta dipende dal livello di attendibilità che l'amministratore deve porre nel client quando determina l'indirizzo risolto per un determinato nome host. Se il client è un proxy downstream, scegliere l'opzione 3 per evitare l'aggiunta della latenza di ricerche DNS non necessarie.

cache DNS

Per aumentare l'efficienza e le prestazioni, Cisco SWA archivia le voci DNS per i domini a cui si è

connessi di recente. La cache DNS consente a SWA di evitare ricerche DNS eccessive negli stessi domini. Le voci della cache DNS scadono a causa del valore TTL (Time to Live) del record.

Quando il valore TTL del record nel server DNS è maggiore del valore TTL della cache dnsconfig SWA, la cache dns utilizzerà il valore TTL del server DNS.

Quando il valore TTL del record nel server DNS è inferiore al tempo TTL della cache dnsconfig SWA, la cache dns utilizza l'impostazione TTL da dnsconfig WSA.

⚠ Attenzione: i file SWA dispongono di due cache DNS, una è progettata per il processo proxy e l'altra per il processo interno.

Per impostazione predefinita, i record DNS SWA sono stati memorizzati nella cache per almeno 30 minuti, indipendentemente dal valore TTL del record. I siti Web moderni che fanno un uso intensivo di Content Delivery Networks (CDN) avrebbero bassi record TTL in quanto i loro indirizzi IP cambiano frequentemente.

In questo modo, un client potrebbe memorizzare nella cache un indirizzo IP per un determinato server e SWA memorizzare nella cache un indirizzo diverso per lo stesso server. Per risolvere questo problema, è possibile ridurre il valore TTL predefinito SWA a cinque minuti dalla sezione SETUP del comando dsnconfig CLI.

Ad esempio, se il valore "TTL minimo in secondi per la cache DNS" nella configurazione DNS è stato impostato su 10 minuti e il valore TTL di un record è di 5 minuti, il valore TTL del record memorizzato nella cache viene aumentato a 10 minuti.

D'altra parte, se il valore TTL del record è impostato su 15 minuti, SWA memorizza il record per 15 minuti nella cache.

Tuttavia, talvolta è necessario cancellare la cache DNS delle voci. Voci della cache DNS danneggiate o scadute possono talvolta causare problemi di recapito a uno o più host remoti.

Questo problema si verifica in genere dopo che l'accessorio è stato disconnesso per uno spostamento di rete o in altre circostanze.

Cancellazione della cache DNS dalla GUI

Passaggio 1. Scegli rete dal menu in alto

Passaggio 2. Scegli DNS

Passaggio 3. Scegliere Cancella cache DNS

⚠ Attenzione: questo comando può causare un calo temporaneo delle prestazioni durante il ripopolamento della cache

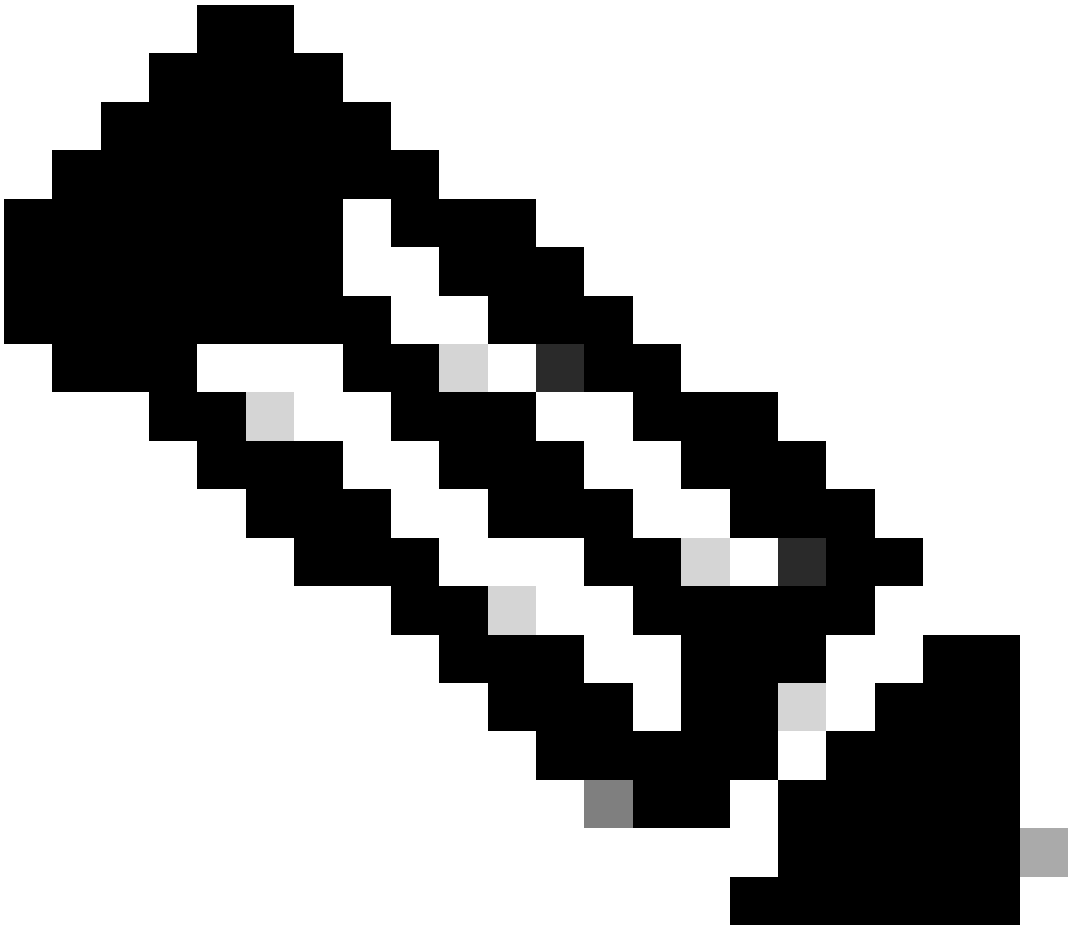
---

Cancellazione della cache DNS dalla CLI

La cache DNS in Cisco WSA può essere cancellata dalla CLI tramite dnsflushcommand.

Visualizza cache DNS

Non è possibile visualizzare i record DNS memorizzati nella cache in SWA dalla CLI o dalla GUI.



Nota: non è possibile eseguire query nella cache DNS tramite nslookup.

Risoluzione dei problemi relativi a DNS

Visualizza registri DNS

Alcuni tipi di log correlati al componente proxy Web non sono abilitati. Il tipo di registro del proxy Web principale, denominato "Registro proxy predefinito", è attivato per impostazione predefinita e

acquisisce le informazioni di base su tutti i moduli Proxy Web.

Ogni modulo Proxy Web dispone inoltre di un proprio tipo di registro che è possibile attivare manualmente in base alle esigenze.

Registri di sistema, registra DNS, errori e attività di commit. attivata per impostazione predefinita

---

 Suggerimento: se si modifica il livello di log per i log di sistema in DEBUG, è possibile visualizzare le query e le risposte DNS. È possibile modificare il livello di log da GUI e CLI.

Modifica del livello di log dei log di sistema dalla GUI

Passaggio 1. Scegliere Amministrazioni di sistema dal menu principale

Passaggio 2. Scegli sottoscrizioni log

Passaggio 3. Scegli registri di sistema

Passaggio 4. Scegliere DEBUG nella sezione Log Level

Passaggio 5. Invia

Passaggio 6. Conferma modifiche

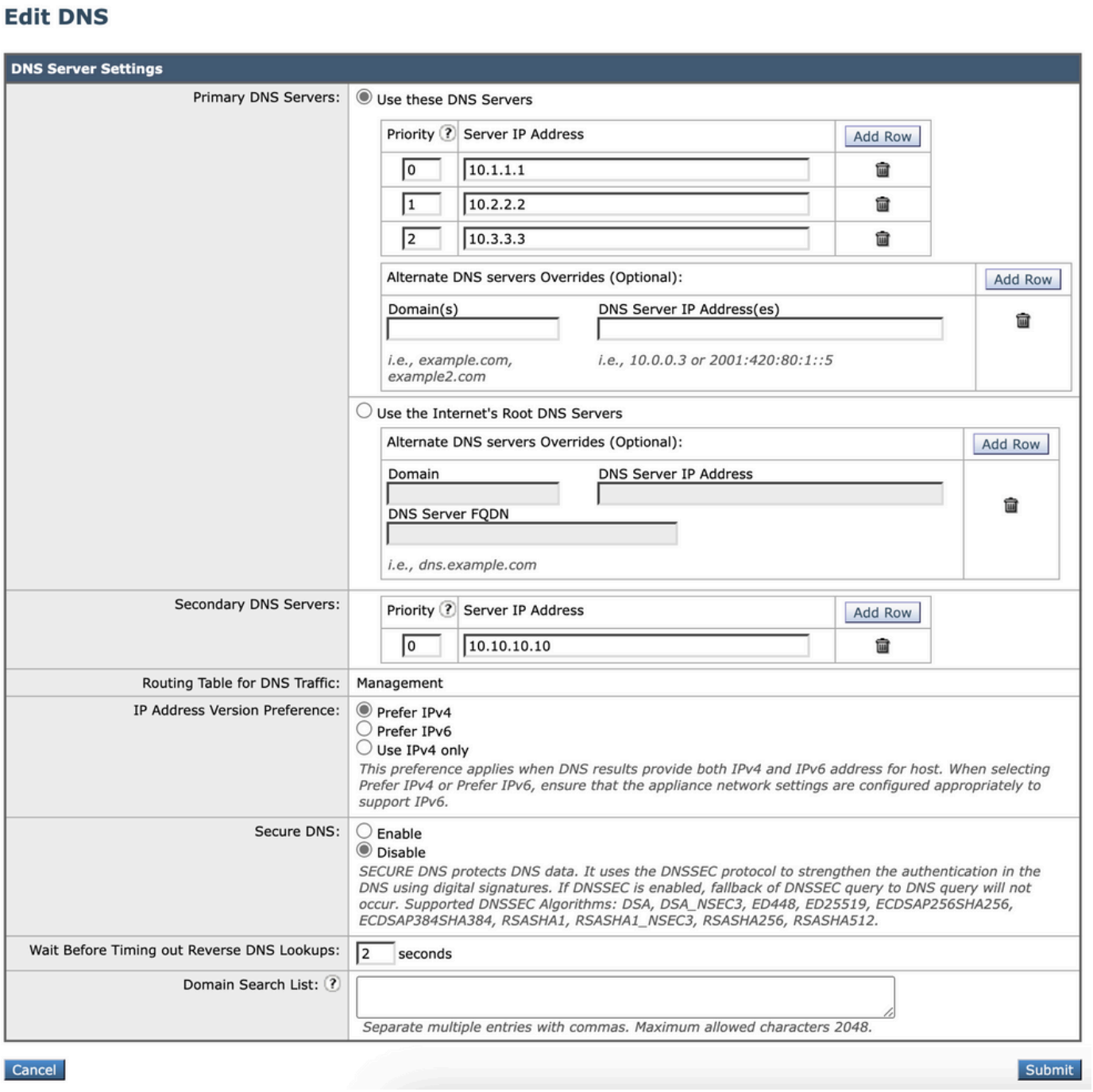


Immagine - Modifica log di sistema, livello log

Modifica del livello di log dei log di sistema dalla CLI

Passaggio 1. Log in to CLI

Passaggio 2. Digitare logconfig

Passaggio 3. Scegliere MODIFICA

Passaggio 4. Immettere il numero associato a System_Logs

Passaggio 5. Premere Invio finché non si raggiunge il livello Log

Passaggio 6. Scegliere il numero 4 per Debug

Passaggio 7. Premere Invio fino a uscire dalla procedura guidata

Passaggio 8. Per salvare le modifiche, digitare 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
```

Suggerimento: una volta completata la risoluzione dei problemi, accertarsi di modificare il livello di log in Informazioni, altrimenti si verificherebbe un carico eccessivo sul disco Input/Output (I/O) e il file di log verrebbe popolato in modo rapido.

nslookup

Utilizzare il comando nslookup per visualizzare la risposta di risoluzione dei nomi in SWA per FQDN diversi.

In questo esempio, nel primo tentativo di risolvere il nome, il valore TTL è impostato su 30 minuti.

Al secondo tentativo, è possibile vedere che il valore TTL è inferiore a 30 minuti, il che indica che il record è stato risolto dalla cache.

```
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
```

scavare

dig è un altro comando utile per eseguire query sui record DNS. Con dig è possibile specificare l'interfaccia di origine o il server DNS in cui si desidera eseguire la query:

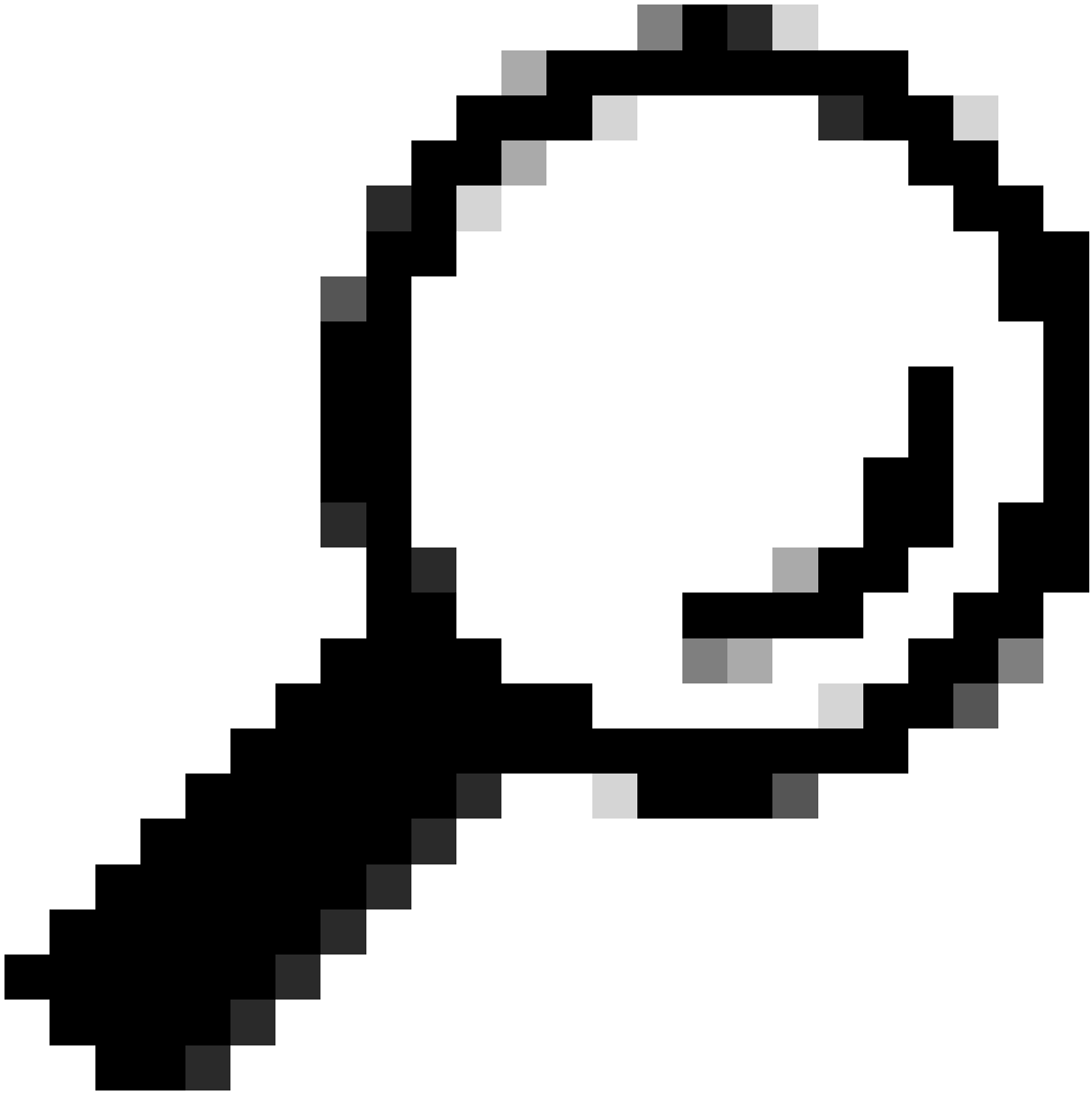
In questo esempio, viene riportata la query per A-Record dal server 10.1.1.1

```
 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
```

Utilizzo di 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.
```



Suggerimento: è possibile scegliere l'indirizzo IP di origine da cui eseguire la query per la risoluzione dei nomi.

Risposta DNS lenta

Se il caricamento di tutti o di alcuni URL richiede un tempo maggiore rispetto a quando si aggiorna la stessa pagina, è preferibile controllare il tempo di risposta DNS. Per controllare il tempo di risposta DNS in SWA sono disponibili due opzioni:

- Configurare il campo personalizzato AccessLogs.
- Registri di Trackstat.

Modifica i log degli accessi per visualizzare le statistiche DNS

È possibile modificare i log degli accessi per visualizzare l'ora DNS per ogni richiesta Web.

Passaggio 1. Accedere alla GUI.

Passaggio 2. Dal menu Amministrazione di sistema, scegliere Registra sottoscrizioni.

Passaggio 3. Dalla colonna Nome log, fare clic su accesslogs o sul nome della nuova cartella creata. Nell'esempio, TAC_access_logs.

Passaggio 4.Nella sezione Custom Fields, incollare la seguente stringa:

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

Passaggio 5.Inviare ed eseguire il commit delle modifiche.

Nome campo personalizzato	Campo personalizzato	Registri W3C	Descrizione
risposta DNS	%:<d	tempo di attesa x-p2p-dns	Tempo impiegato dal proxy Web per inviare la richiesta DNS (Domain Name Request) al processo DNS del proxy Web.
Totale DNS	%:>d	x-p2p-dns-svc-time	Tempo impiegato dal processo DNS del proxy Web per restituire un risultato DNS al proxy Web.

Per ulteriori informazioni su come modificare i campi personalizzati nei log degli accessi, visitare il collegamento: Configure Performance Parameter in Access Logs - Cisco

Tempo di risposta DNS complessivo nei registri Trackstat

È possibile visualizzare le statistiche del servizio DNS e di altri servizi interni nei registri trackstat. È possibile accedere ai log di trackstats collegandosi al proprio SWA tramite FTP.

In questo esempio è possibile visualizzare le statistiche della cache e il numero di risposte DNS, suddivise in categorie in base al tempo trascorso dal server DNS dall'ultimo riavvio dell'applicazione SWA.

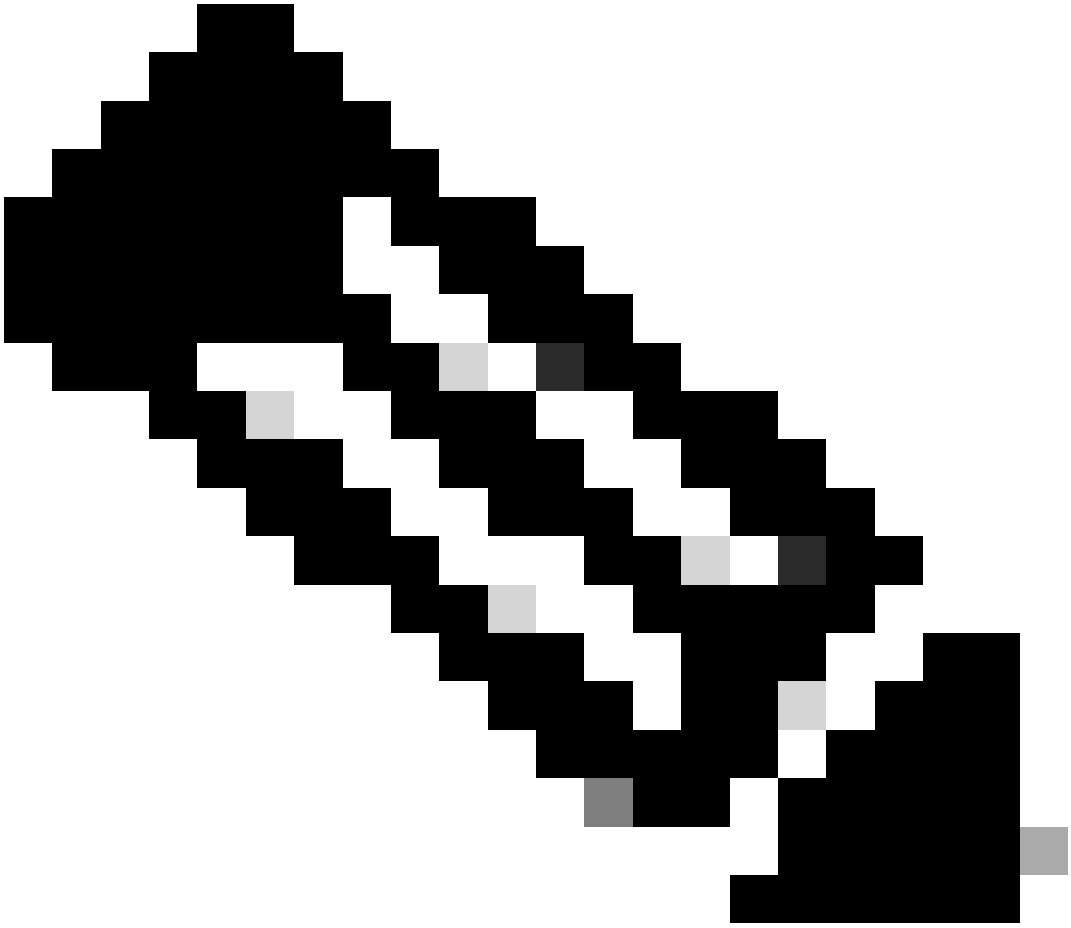
```
...
INFO: DNS Cache Stats: Entries 662, Expire 1697, Hits 88739, Misses 664, Reclaims 0
...
       DNS Time       1.0 ms    349
       DNS Time       1.6 ms    550
       DNS Time       2.5 ms    374
       DNS Time       4.0 ms    32
       DNS Time       6.3 ms    35
       DNS Time      10.0 ms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

Nell'ultima riga, ad esempio, indica che per 190 query DNS sono stati necessari più di 6.309 millisecondi (circa 6 secondi) dall'ultimo riavvio di SWA.

Per trovare il numero esatto in un periodo di tempo, sottrarre questi valori per l'ora di inizio e di fine.

Ad esempio, per identificare il tempo di risposta DNS dalle 10.00 alle 11.00, raccogliere le statistiche relative alle 11.00 e sottrarle dalle statistiche relative alle 10.00.

Il risultato è il tempo di risposta DNS dalle 10.00 alle 11.00 per la data desiderata.



Nota: i registri di stato dei brani vengono raccolti ogni 5 minuti.

Acquisizione pacchetti

È possibile acquisire pacchetti per visualizzare le richieste e le risposte DNS, per filtrare solo i pacchetti DNS utilizzabili: porta 53 .

Per avviare l'acquisizione dei pacchetti dalla GUI:

Passaggio 1. Scegliere Supporto e Guida dall'alto a destra

Passaggio 2. Scegli acquisizione pacchetto

Passaggio 3. (Facoltativo) Scegliere Modifica impostazioni per aggiungere il filtro

Passaggio 4. (Facoltativo) Selezionare le interfacce e immettere la porta 53 nella sezione Filtro personalizzato

Passaggio 5. (Facoltativo) Scegliere Sottometti

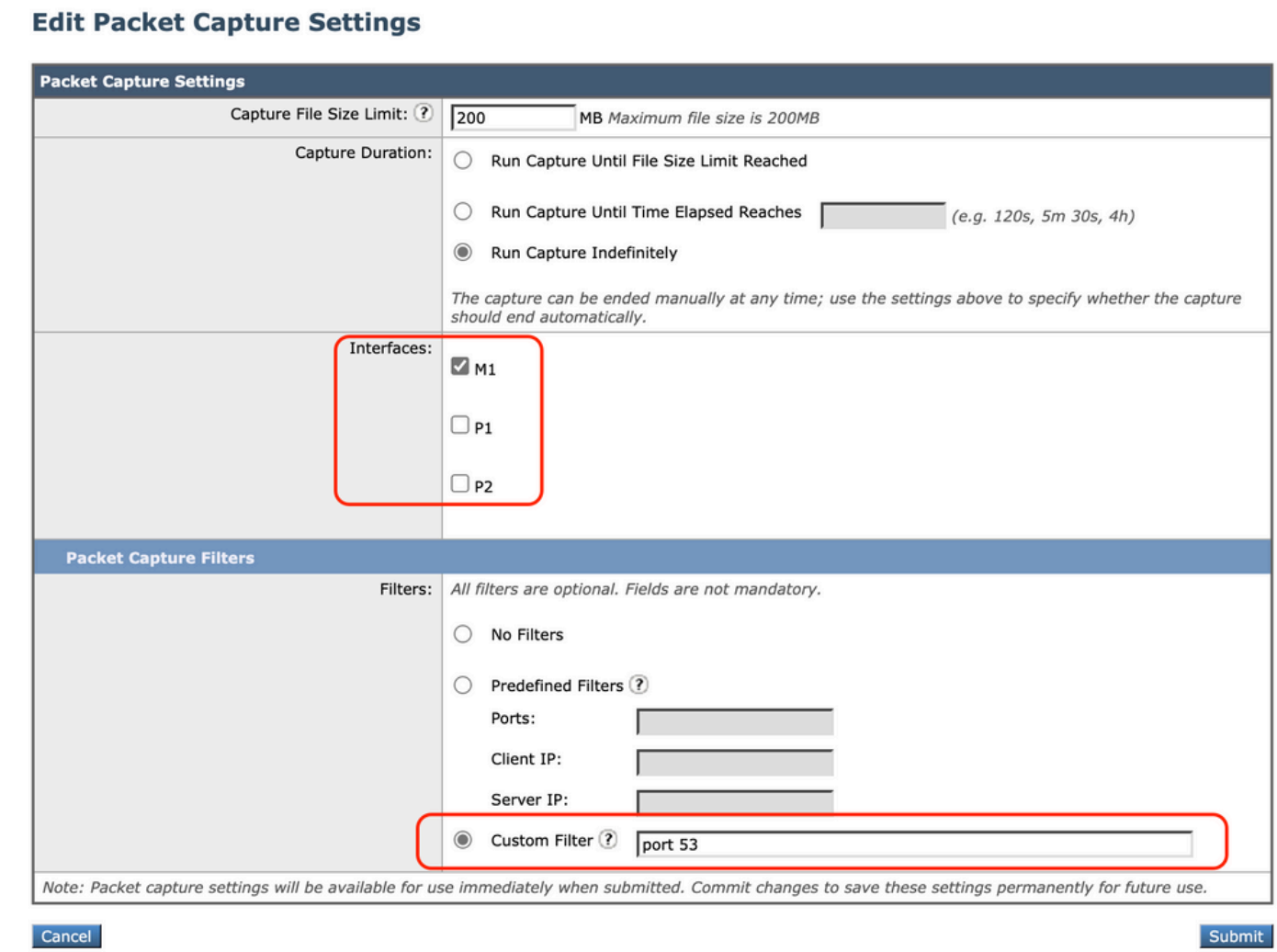
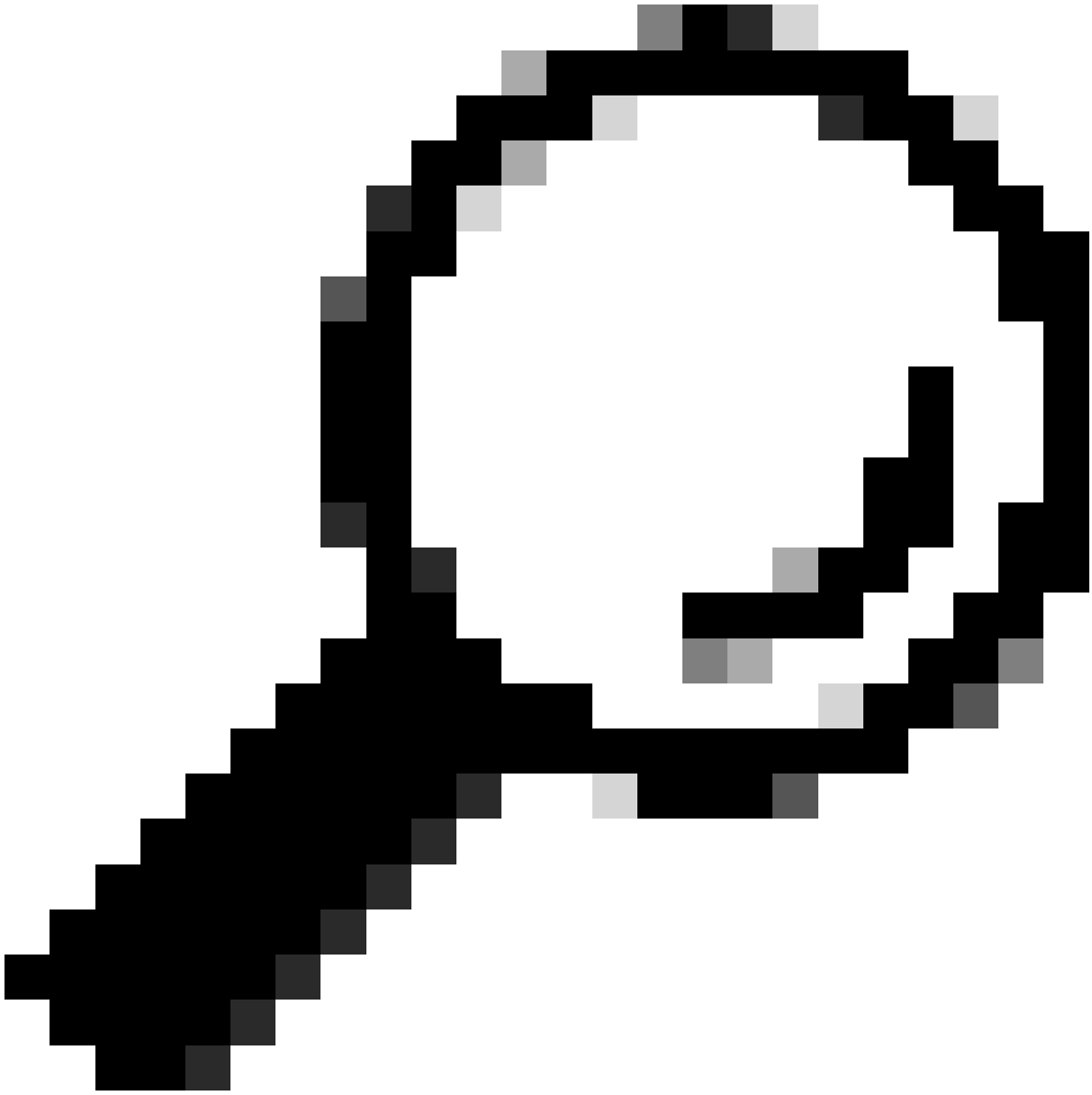


Immagine - Aggiungi filtro per acquisire pacchetti DNS



Suggerimento: le impostazioni di acquisizione del pacchetto possono essere utilizzate immediatamente dopo l'invio. Eseguire il commit delle modifiche per salvare definitivamente queste impostazioni per un utilizzo futuro.

Passaggio 6. Scegliere Avvia acquisizione.

Passaggio 7. (Facoltativo) Generare traffico, se si desidera risolvere problemi relativi all'accesso a un sito o a un URL specifico.

Passaggio 8. Interrompi acquisizione

Passaggio 9. Attendere l'aggiornamento della pagina, quindi scegliere la prima acquisizione di pacchetto dall'elenco "Gestisci file di acquisizione pacchetto"

Passaggio 10. Scegli il file da scaricare

L4TM

Il monitoraggio del traffico di layer 4 è in ascolto del traffico di rete che arriva su tutte le porte di ogni appliance Web protetta e confronta i nomi di dominio e gli indirizzi IP con le voci delle proprie tabelle di database per determinare se consentire il traffico in entrata e in uscita.

Quando i client interni vengono infettati da malware e tentano di telefonare a casa attraverso porte e protocolli non standard, L4 Traffic Monitor impedisce l'attività di phone-home per uscire dalla rete aziendale.

Per impostazione predefinita, Monitoraggio traffico L4 è abilitato e impostato per monitorare il traffico su tutte le porte, inclusi DNS e altri servizi.

Per ulteriori informazioni sul monitoraggio del traffico di layer 4, fare riferimento alla guida per l'utente.

Errori

Pagina Notifica

Per impostazione predefinita, SWA visualizza una pagina di notifica per informare gli utenti che sono stati bloccati e il motivo del blocco

Nome file e titolo notifica: ERR_DNS_FAIL (errore DNS)

Descrizione: pagina di errore visualizzata quando l'URL richiesto contiene un nome di dominio non valido.

Testo di notifica: risoluzione del nome host (ricerca DNS) per il nome host <hostname > non riuscita.

È possibile che l'indirizzo Internet sia stato digitato in modo errato o sia obsoleto, che l'host <hostname > sia temporaneamente non disponibile o che il server DNS non risponda.

Controlla l'ortografia dell'indirizzo Internet immesso. Se è corretto, provare la richiesta più tardi.

Immagine - Errore DNS FAIL

Codice risultato Accesslog NONE

I codici dei risultati delle transazioni nel file di log degli accessi descrivono il modo in cui l'accessorio risolve le richieste dei client. Se nel log degli accessi il codice risultato è NONE, significa che si è verificato un errore nella transazione. Ad esempio, un errore DNS o un timeout del gateway.

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

Impossibile avviare la cache DNS

Se al riavvio di un accessorio viene generato un avviso con il messaggio "Failed to bootstrap the DNS cache" (Impossibile avviare la cache DNS), significa che il sistema non è in grado di contattare i server DNS primari.

Questa situazione può verificarsi all'avvio se il sottosistema DNS viene connesso prima che venga stabilita la connettività di rete. Se questo messaggio viene visualizzato in altri momenti, potrebbe indicare problemi di rete o che la configurazione DNS non è impostata su un server valido

Raggiunto il numero massimo di errori durante l'esecuzione di query sul server DNS

Se uno o alcuni server DNS configurati in SWA non rispondono alle query DNS, SWA le considera

non in linea e non le invia per un periodo di tempo predefinito. Per ulteriori informazioni, leggere "Configurare DNS da CLI" in questo articolo.

DNS_FAIL

Quando SWA riceve una richiesta HTTP e non riesce a risolvere il nome host, per impostazione predefinita SWA restituisce una risposta simile alla seguente:

```
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
```

Questa funzione è denominata "espansione nome server".
WSA esegue questa operazione in tentativi che il reindirizzamento del nome host risolverebbe la pagina prevista per il client.

È possibile modificare "Formato URL per il reindirizzamento HTTP 307 in caso di errore di ricerca DNS", per ulteriori informazioni vedere la sezione advanceproxyconfig in questo articolo.

WSA considera la richiesta DNS che restituisce ServFail come un errore.
Ad esempio, NXDOMAIN restituirà "DNS_FAIL" anziché "SERVER_NAME_EXPANSION"

Informazioni correlate

Guida per l'utente di AsyncOS 15.0 per Cisco Secure Web Appliance

Uso delle best practice di Secure Web Appliance - Cisco

Cisco Content Hub - Introduzione al Domain Name System

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).