# 액세스 로그의 성능 매개변수 구성

## 목차



## 소개

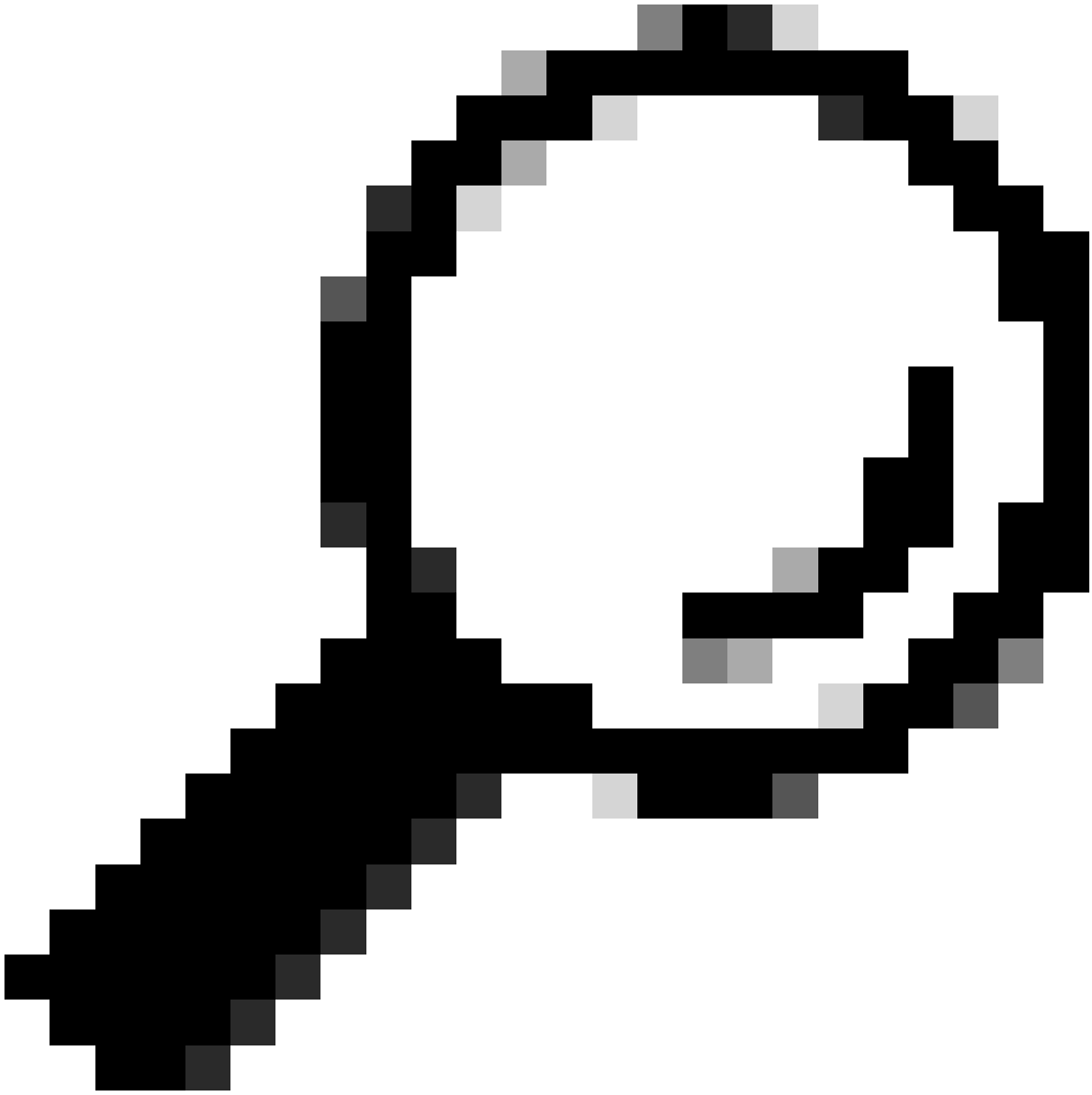
이 문서에서는 SWA(Secure Web Appliance) 액세스 로그에 성능 매개변수 사용자 정의 필드를 추가하는 단계에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA 관리 인터페이스에 대한 SSH(Secure Shell Protocol) 액세스
- SWA 관리 인터페이스에 대한 GUI(Graphical User Interface) 액세스



팁: SWA 데이터 파티션에 20% 이상의 사용 가능한 디스크 공간이 있는 것이 가장 좋습니다. status detail 명령의 출력에서 CLI(Command Line Interface)의 디스크 사용량을 확인할 수 있습니다.

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

대기 시간 문제가 있고 트래픽이 SWA를 통해 프록시되는 경우 액세스 로그는 대기 시간의 근본 원인을 해결하는 데 유용할 수 있습니다. 현재 액세스 로그 설정을 변경하거나 Custom(사용자 지정) 필드에 Performance Parameters(성능 매개변수)가 추가된 새 액세스 로그를 만들 수 있습니다.

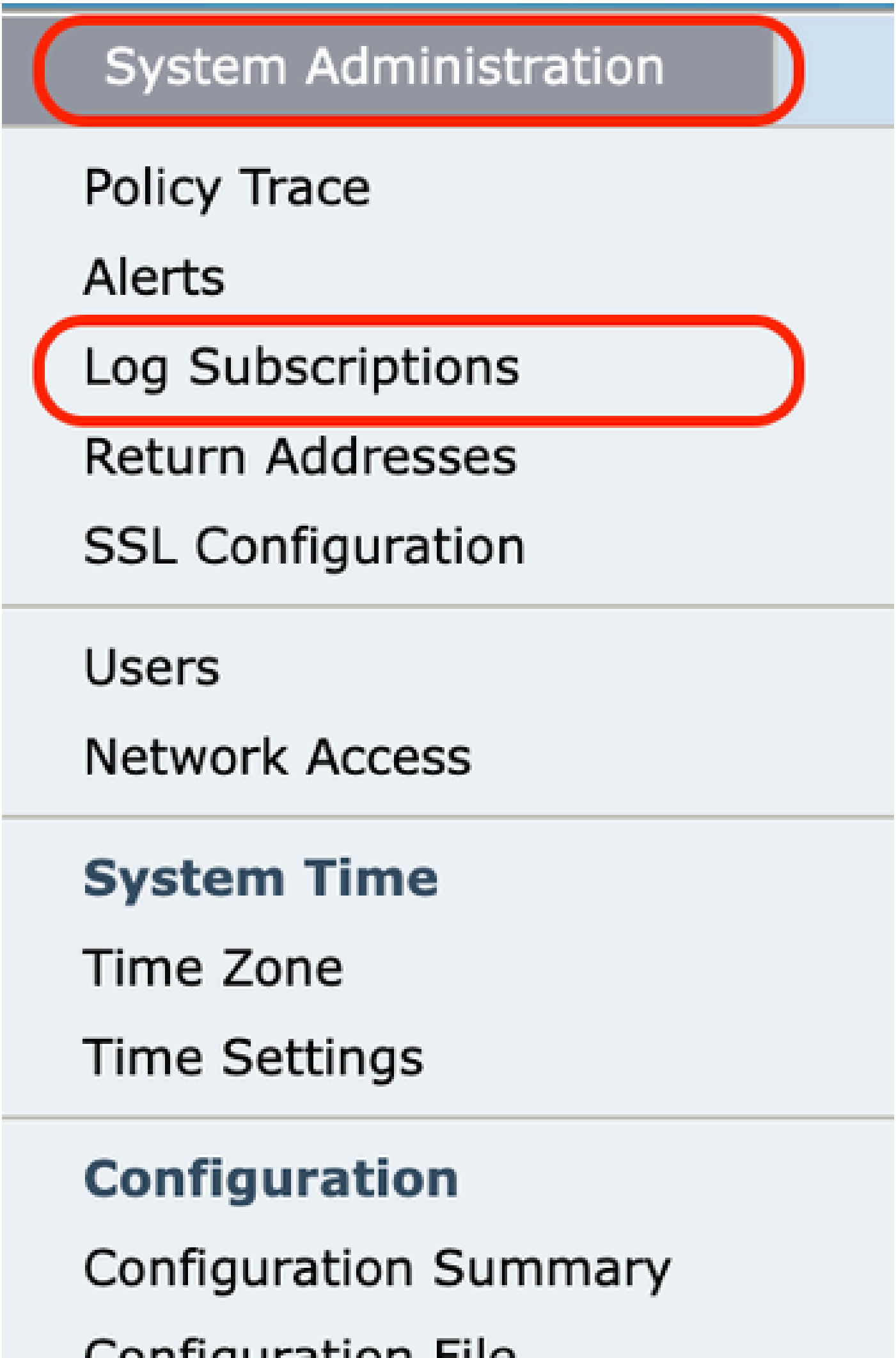
# 추가 액세스 로그 생성

일부 조건에서 내부 정책 또는 일부 다른 컨피그레이션으로 인해 현재 액세스 로그를 변경할 수 없습니다. 이 제한을 극복하기 위해 다른 액세스 로그를 만들고 새 액세스 로그에 사용자 지정 성능 매개변수를 추가할 수 있습니다.

## GUI에서 새 액세스 로그 생성

1단계. GUI에 로그인합니다.

2단계. System Administration(시스템 관리) 메뉴에서 Log Subscriptions(로그 서브스크립션)를 선택합니다.


System Administration
Policy Trace
Alerts
Log Subscriptions
Return Addresses
SSL Configuration
Users
Network Access
System Time
Time Zone
Time Settings
Configuration
Configuration Summary

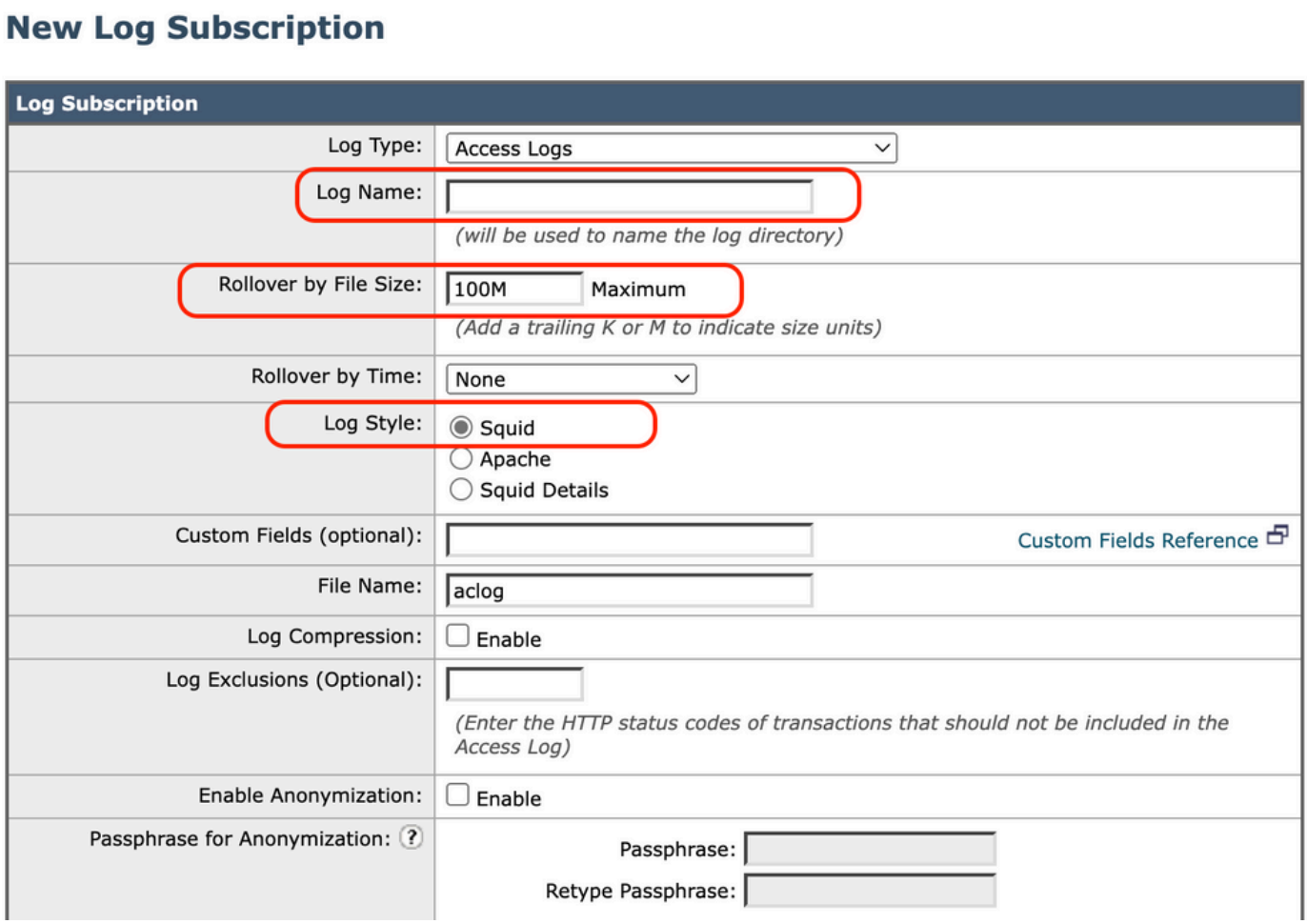
는 현재 로그 파일이 사용자가 지정한 최대 파일 크기 제한 또는 마지막 롤오버 이후의 최대 시간에 도달하면 로그 서브스크립션을 보관(롤오버)합니다.

7단계. 로그 스타일로 Squid를 선택합니다.

8단계. 파일 이름은 이 새 로그에 대한 폴더 이름 및 로그 파일 이름을 정의하는 것입니다. 이 예에서는 TAC_access_logs인 로그 이름과 동일한 것이 좋습니다.

9단계. 로그 압축을 활성화하여 로그 파일을 압축하거나 로그를 텍스트 파일로 유지할 수 있습니다.

10단계. 로그 제외는 HTTP(Hypertext Transfer Protocol) 응답 코드를 필터링하는 것입니다. HTTP 상태 코드를 필터링하지 마십시오.




필수 필드 입력

11단계. SWA에서 로그를 유지하려면 FTP 폴링을 선택합니다. 1을 입력하고 Enter 키를 누릅니다.

12단계. 변경 사항을 제출하고 커밋합니다.

## CLI에서 새 액세스 로그 구성

1단계. CLI에 로그인합니다.

2단계. logconfig를 실행합니다.

3단계. 새 로그를 생성하려면 New를 입력하고 Enter 키를 누릅니다.

4단계. 목록에서 Access Logs(액세스 로그)를 찾아 연결된 번호를 입력하고 Enter를 누릅니다.

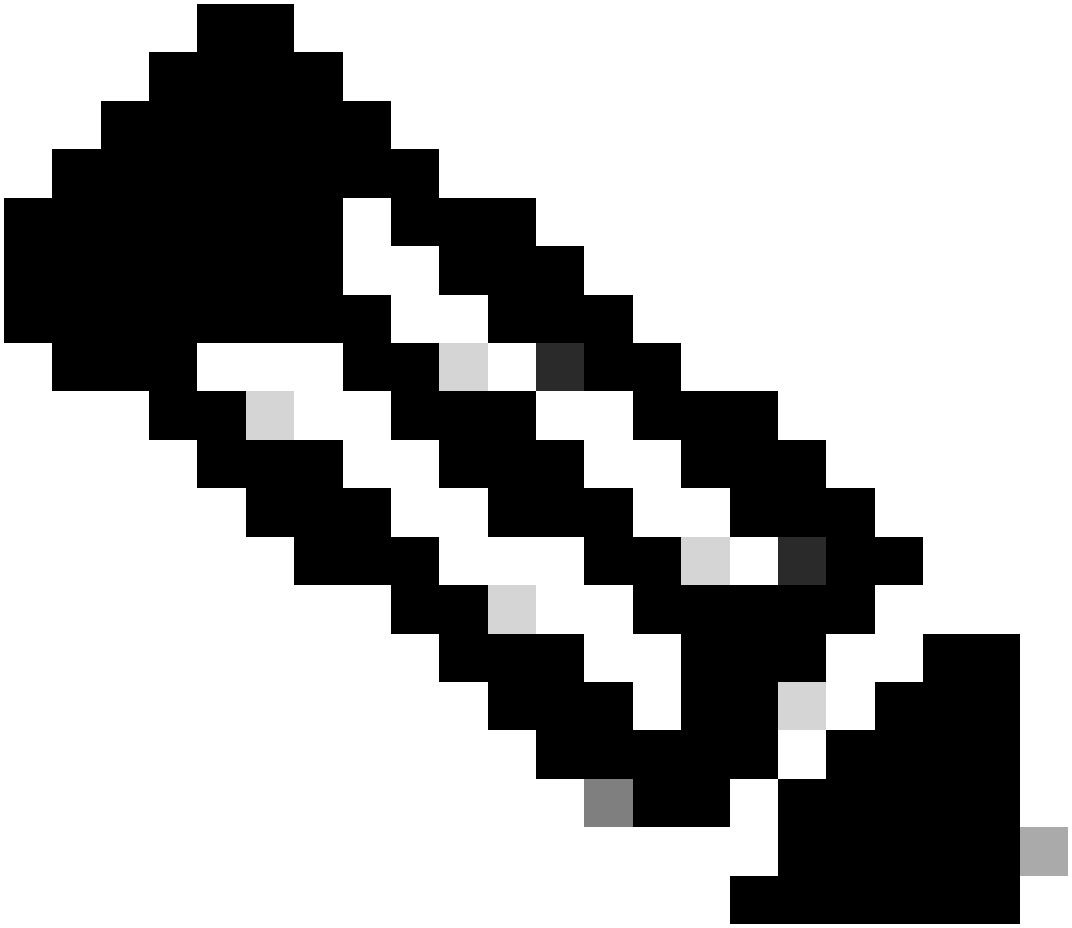
5단계. 새 로그의 이름을 입력합니다.

6단계. 1을 입력하여 이 서브스크립션의 로그 스타일로 Squid를 선택하고 Enter 키를 누릅니다.

7단계. HTTP 오류 상태 코드를 필터링하지 않습니다. 다음 단계로 이동하려면 Enter를 누릅니다.

8단계. FTP 폴링을 선택하여 SWA의 로그를 유지합니다. 1을 입력하고 Enter 키를 누릅니다.

---



참고: 로그를 FTP(File Transfer Protocol) 서버, SCP(Secure Copy Protocol) 서버 또는 Syslog 서버로 푸시합니다. 관련 옵션을 선택할 수 있습니다.

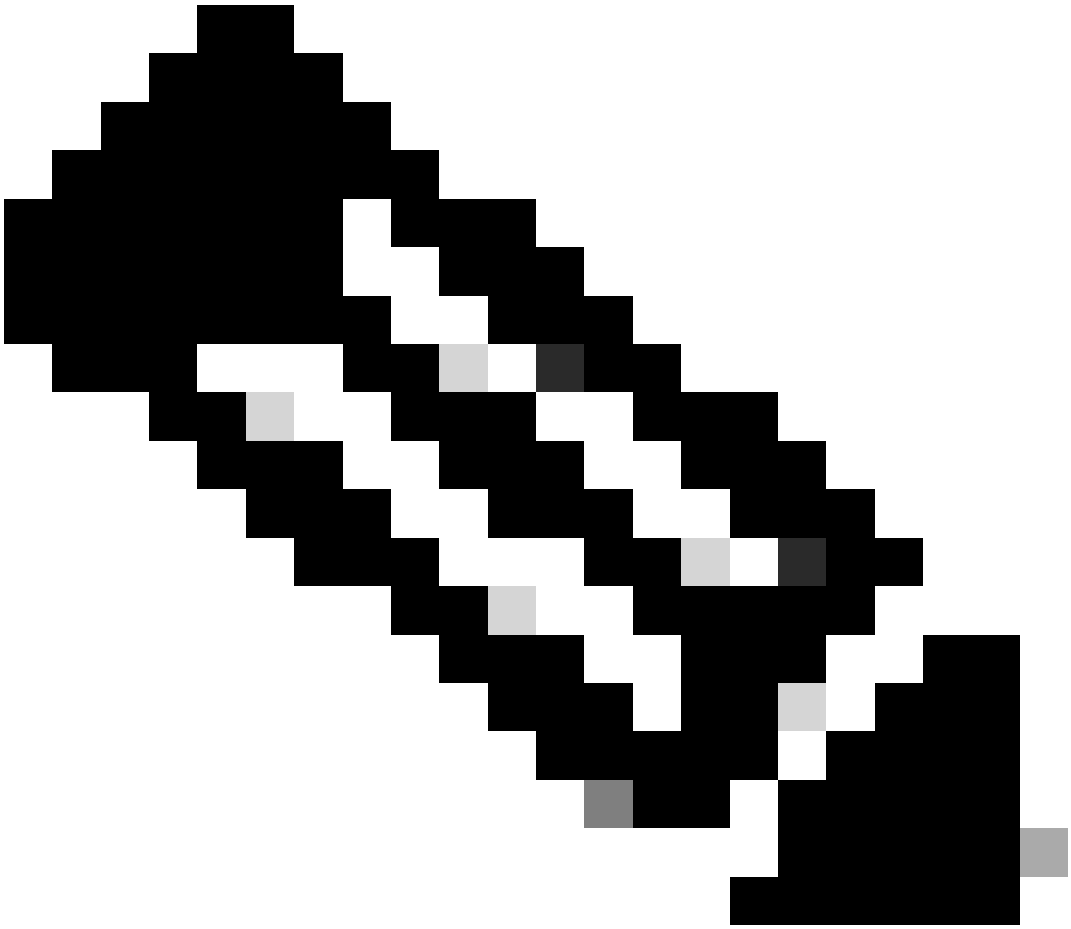
---

9단계. 이 단계는 새 로그의 폴더 이름 및 파일 이름을 정의하는 것입니다. 로그 이름과 같으면 더 좋

으며 Enter 키를 누릅니다.

10단계. 로그를 새 파일에 SWA 역할을 적용하기 전에 파일 크기(바이트)에 대해 102400(100KB)에서 10737418240(10GB) 사이의 값을 입력합니다.

---

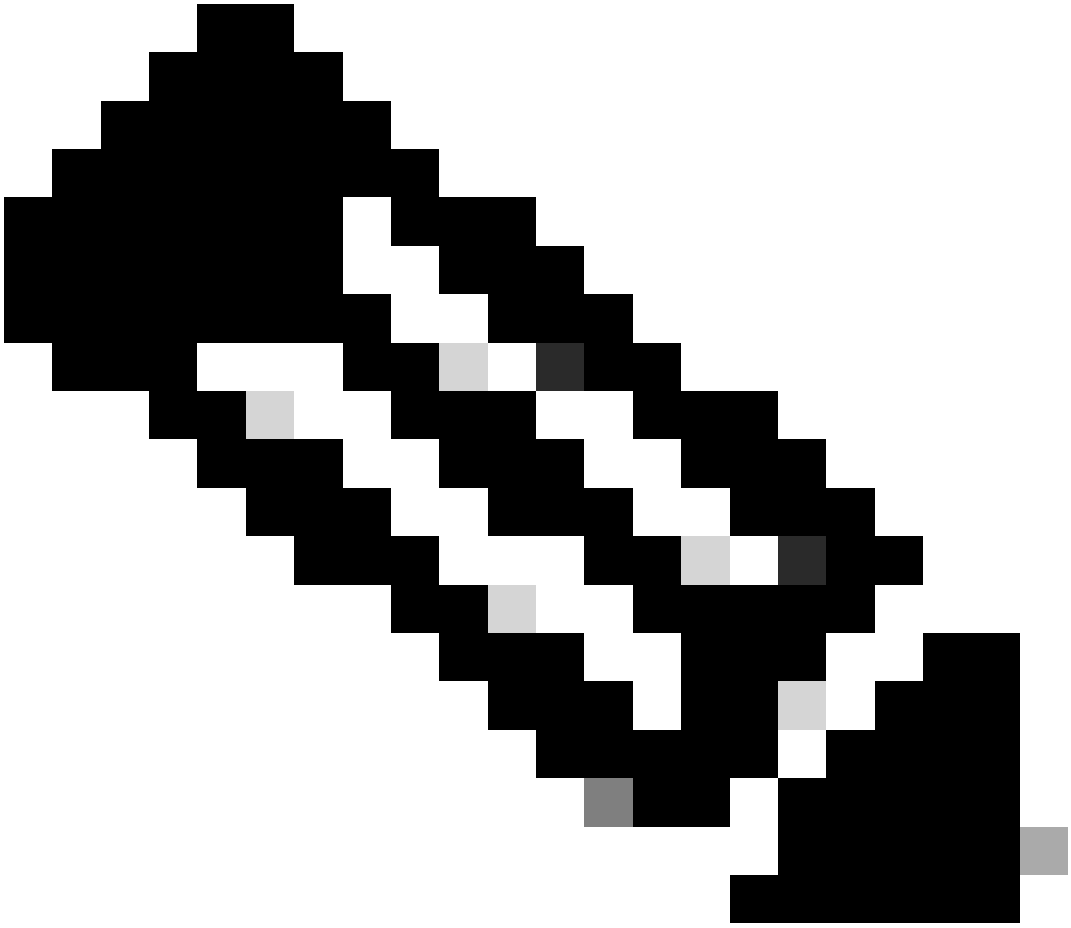


참고: SWA는 현재 로그 파일이 사용자가 지정한 최대 파일 크기 제한 또는 마지막 롤오버 이후의 최대 시간에 도달하면 로그 서브스크립션을 보관(롤오버)합니다.

---

11단계. 최대 파일 수는 디바이스에 저장된 로그 파일 수를 나타냅니다. 총 로그 파일 수가 이 값에 도달하면 이전 로그가 SWA에서 삭제됩니다. 기본값은 파일 10개이며 사용 가능한 디스크 공간 및 기타 로그 컨피그레이션으로 인해 로그 수를 입력하고 Enter를 누를 수 있습니다.

12단계. 이 단계에서는 로그를 압축하거나 텍스트 파일로 유지할 수 있습니다. Yes에 Y를 입력하고 No에 N을 입력하고 Enter 키를 누릅니다.



참고: 파일 크기가 최대 파일 크기에 도달하면 압축됩니다. 압축 비율은 네트워크 트래픽 동작에 따라 다르며 로그 파일 간에 다를 수 있습니다.

---

13단계. Enter를 눌러 로그 구성 마법사를 종료합니다.

14단계. commit을 입력하여 변경 사항을 저장합니다.

```
SWA_CLI> logconfig
...
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.
[]> NEW

Choose the log file type for this subscription:
1. AVC Engine Framework Logs
2. AVC Engine Logs
```

```
3. Access Control Engine Logs
4. Access Logs
....
58. Webroot Logs
59. Welcome Page Acknowledgement Logs
[1]> <=== type the number assosiated with Access Logs and press Enter

Please enter the name for the log:
[]> <=== Chose desiered name, in this example, TAC_access_logs

Choose the log style for this subscription:
1. Squid
2. Apache
3. Squid Details
[1]> <=== Press Enter to keep the default value

Enter the HTTP Error Status codes (comma separated list of 4xx and 5xx codes) you want to filter out fr
[]> <=== Press Enter to keep the default value

Choose the method to retrieve the logs:
1. FTP Poll
2. FTP Push
3. SCP Push
4. Syslog Push
[1]> <=== Choose FTP poll to keep the logs in the SWA

Filename to use for log files:
[aclog]> <=== It is better to have teh same file name as the log, in this example, TAC_access_logs

Do you want to configure time-based log files rollover? [N]> <=== Enter the desiered answer

Please enter the maximum file size:
[104857600]> <=== Enter the desiered answer, or you can leave as default

Please enter the maximum number of files:
[100]> <=== Enter the desiered answer, it depends on free disk space and log file size

Should an alert be sent when files are removed due to the maximum number of files allowed? [N]> <=== En

Do you want to compress logs (yes/no)
[n]> <=== Enter the desiered answer

Currently configured logs:
1. "Splunk Logs" Type: "Access Logs" Retrieval: FTP Push - Host 10.0.0.1
2. "TAC_access_logs" Type: "Access Logs" Retrieval: FTP Poll
3. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
....
40. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
41. "welcomeack_logs" Type: "Welcome Page Acknowledgement 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.
[]> <=== Press Enter to exit the log configuration wizard

SWA_CLI> commit
Please enter some comments describing your changes:
[]> <=== Type the change description and press Enter
```

# 액세스 로그에 성능 매개 변수에 대한 사용자 지정 필드 추가

1단계. GUI에 로그인합니다.

2단계. System Administration(시스템 관리) 메뉴에서 Log Subscriptions(로그 서브스크립션)를 선택합니다.

3단계. Log Name(로그 이름) 열에서 accesslogs(액세스 로그) 또는 새로 생성된 이름을 클릭합니다. 이 예에서는 TAC_access_logs입니다.

4단계. Custom Fields(맞춤형 필드) 섹션에서 다음 문자열을 붙여넣습니다.

```
[ Request Details: ID = %I, User Agent = %u, AD Group Memberships = ( %m ) %g ] [ Tx Wait Times (in ms)

       , Response Header = %:h>, Client Body = %:b> ] [ Rx Wait Times (in ms): 1st request byte = %:1<,

        a; DNS response = %:

         d, WBRS response = %:

           r, AVC response = %:A>, AVC total = %:A<, DCA response = %:C>, DCA total = %:C<, McAfee respo

            s; AMP response = %:e>, AMP total = %:e<; Latency = %x; %L ] [Client Port = %F, Server IP = %
```

5단계. 변경 사항을 제출하고 커밋합니다.

## 변경 사항 확인

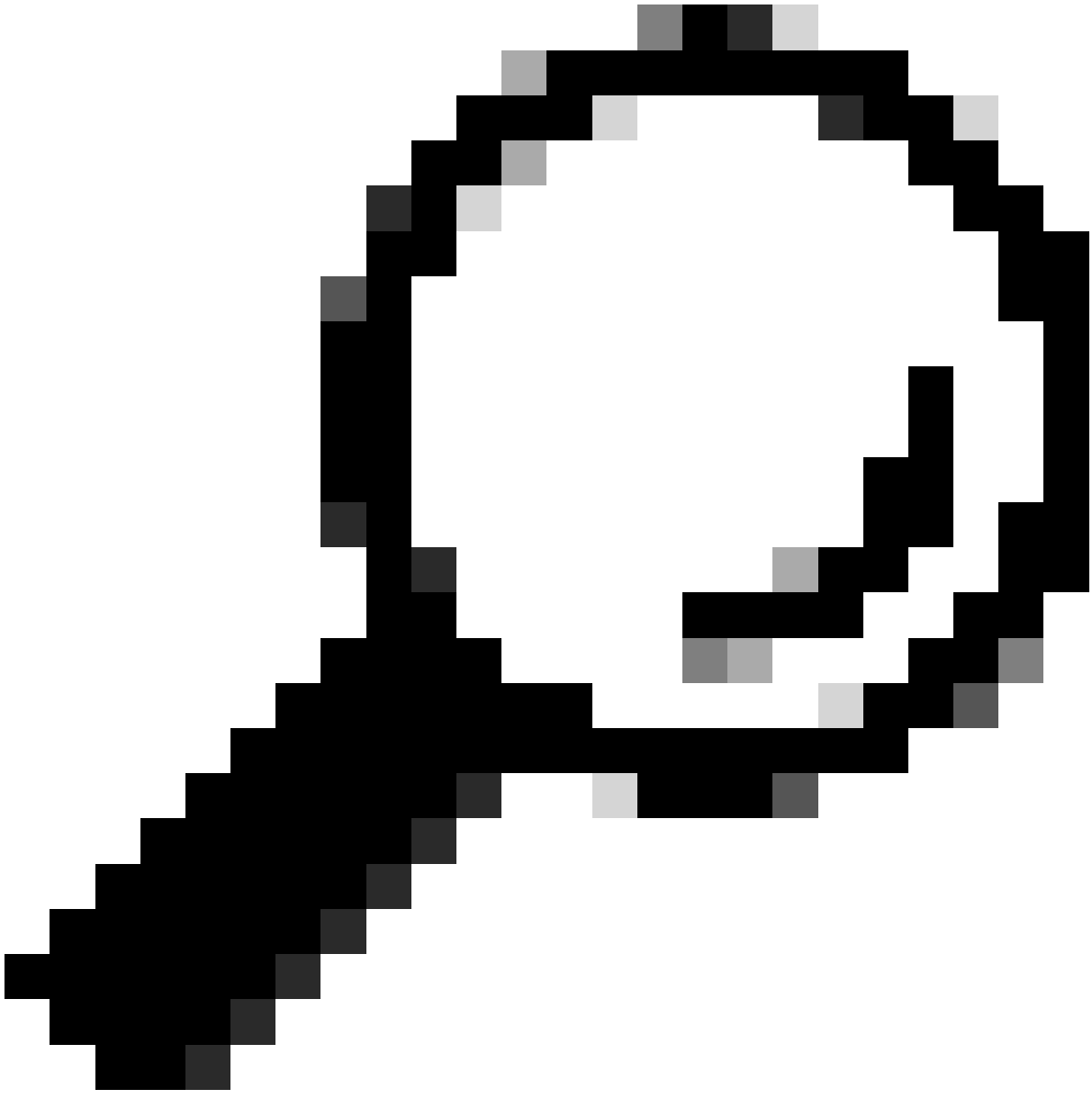
1단계. CLI에 로그인합니다.

2단계. tail을 입력하고 enter 키를 누릅니다.

3단계. Performance Parameter(성능 매개변수)를 추가한 액세스 로그와 관련된 번호를 찾습니다. 번호를 입력하고 Enter 키를 누릅니다.

이 샘플과 마찬가지로 액세스 로그에 추가 정보가 추가되어 있습니다.

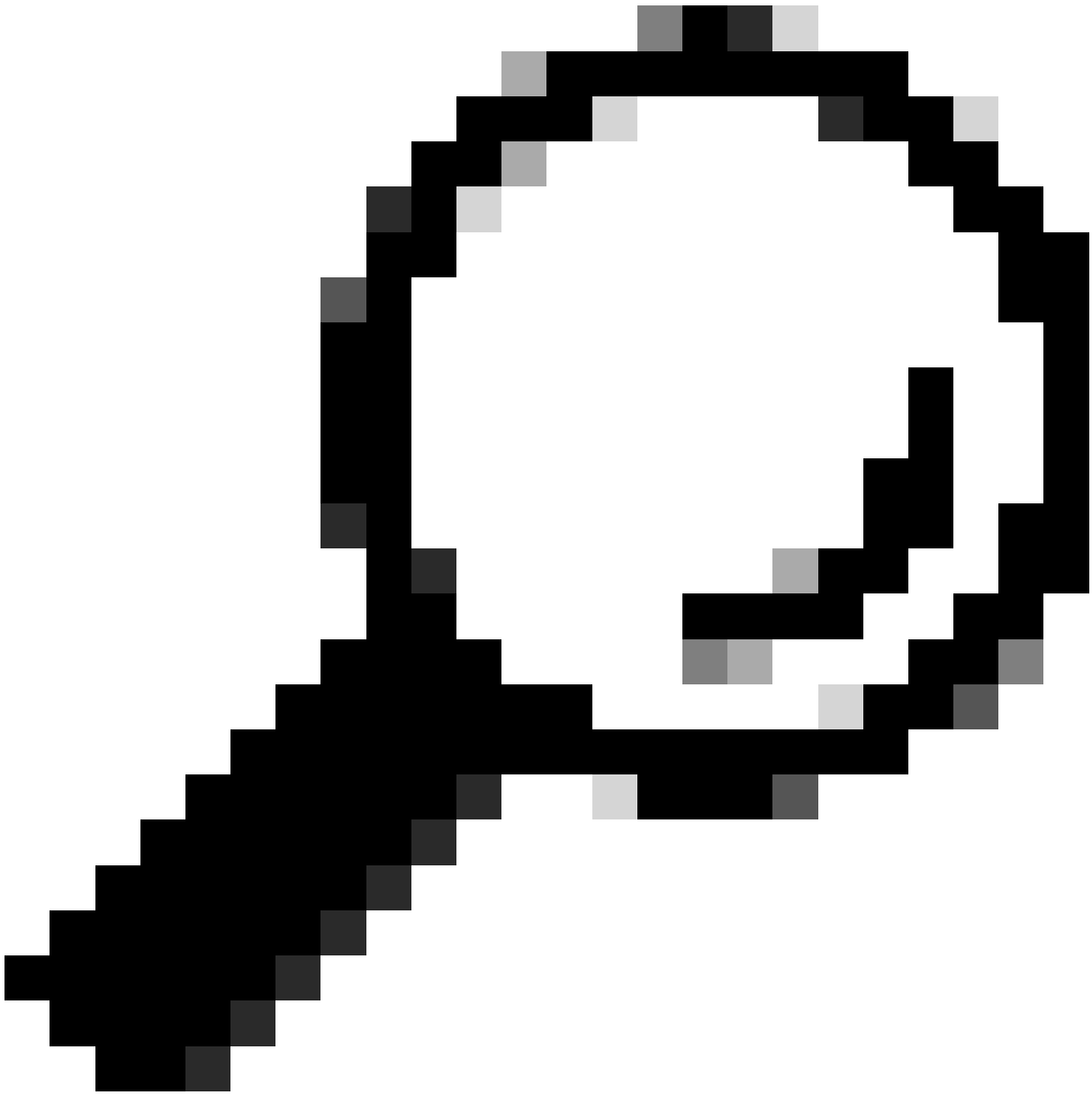
```
1680893872.492 1131 172.18.122.156 TCP_MISS/200 379725 GET http://www.cisco.com/en/US/docs/security/wsa/

        - " [ Request Details: ID = 104, User Agent = "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gec
```



팁: Control 키를 누르고 C를 누르면 tail 명령을 종료할 수 있습니다. tail 명령이 종료되지 않으면 q를 입력합니다C를 누릅니다.

## 사용자 정의 필드의 필드 설명

Custom Performance Parameter Field(맞춤형 성능 매개변수 필드)에 사용되는 값은 다음 정보에 매핑됩니다.



팁: 지연 시간 = AMP total + Anti-Spyware total + Webroot total + Sophos total + McAfee total + AVC total + WBRS total + Auth total

| 사용자 지정 필드 이름 | 사용자 지 | 설명 |
| --- | --- | --- |

| | 정 필드 | |
|---|---|---|
| 요청 헤더 | %:<h | 첫 번째 바이트 이후 요청 헤더를 서버에 쓰는 데 걸리는 대기 시간입니다. |
| 서버에 요청 | %:<b | 헤더 후 요청 본문을 서버에 쓰기 위해 기다리는 시간. |
| 클라이언트에 첫 번째 바이트 | %:1> | 클라이언트에 쓴 첫 번째 바이트의 대기 시간입니다. |
| 클라이언트 본문 | %:b> | 클라이언트에 전체 본문이 작성될 때까지 기다리는 시간입니다. |
| Rx 대기 시간(밀리초): 첫 번째 요청 바이트 | %:1< | 웹 프록시가 서버에 연결하기 시작한 시점부터 서버에 처음으로 쓸 수 있는 시점까지 걸리는 시간입니다. 웹 프록시가 트랜잭션을 완료하기 위해 여러 서버에 연결해야 하는 경우 이 시간의 합입니다. |
| 요청 헤더 | %:h< | 첫 번째 바이트 이후 전체 클라이언트 헤더에 대한 대기 시간입니다. |
| 클라이언트 본문 | %:b< | 전체 클라이언트 본문을 기다리는 시간입니다. |
| 첫 번째 응답 바이트 | %:>1 | 서버의 첫 번째 응답 바이트에 대한 대기 시간입니다. |
| 응답 헤더 | %:>h | 첫 번째 응답 바이트 이후 서버 헤더의 대기 시간입니다. |
| 서버 응답 | %:>b | 이는 기본적으로 SWA가 서버에서 HTTP 헤더를 가져왔지만, SWA는 그 이후에 서버의 실제 콘텐츠가 될 응답 바이트를 기다린다는 것을 의미합니다. |
| 디스크 캐시 | %:>c | 웹 프록시가 디스크 캐시에서 응답을 읽는 데 필요한 시간입니다. |
| 인증 응답 | %:<a | 웹 프록시가 요청을 전송한 후 웹 프록시 인증 프로세스에서 응답을 수신할 때까지 대기하는 시간. |
| 총 인증 | %:>a | 웹 프록시 인증 프로세스로부터 응답을 수신하는 대기 시간에는 웹 프록시가 요청을 전송하는 데 필요한 시간이 포함됩니다. |

| | | |
|---|---|---|
| DNS 응답 | %:<d | 웹 프록시에서 DNS(Domain Name Request) 요청을 웹 프록시 DNS 프로세스로 보내는 데 걸린 시간입니다. |
| DNS 합계 | %:>d | 웹 프록시 DNS 프로세스가 DNS 결과를 웹 프록시로 다시 전송하는 데 걸린 시간입니다. |
| WBRS 응답 | %:<r | 웹 프록시가 요청을 전송한 후 웹 평판 필터에서 응답을 수신할 때까지 대기하는 시간. |
| WBRS 합계 | %:>r | 웹 평판 필터에서 판정을 수신할 때까지 대기하는 시간에는 웹 프록시에서 요청을 전송하는 데 필요한 시간이 포함됩니다. |
| AVC 응답 | %:A> | 웹 프록시에서 요청을 전송한 후 AVC(Application Visibility and Control) 프로세스에서 응답을 수신할 때까지 대기하는 시간. |
| AVC 합계 | %:A< | AVC 프로세스에서 응답을 수신할 때까지 대기하는 시간에는 웹 프록시에서 요청을 전송하는 데 필요한 시간이 포함됩니다. |
| DCA 응답 | %:C> | 웹 프록시가 요청을 전송한 후 DCA(Dynamic Content Analysis) 엔진에서 응답을 수신할 때까지 대기하는 시간. |
| DCA 합계 | %:C< | DCA(Dynamic Content Analysis) 엔진에서 판정을 수신할 때까지 대기하는 시간에는 웹 프록시에서 요청을 전송하는 데 필요한 시간이 포함됩니다. |
| McAfee 응답 | %:m> | 웹 프록시에서 요청을 전송한 후 McAfee 스캐닝 엔진에서 응답을 수신할 때까지 대기하는 시간. |
| McAfee 합계 | %:m< | McAfee 스캐닝 엔진에서 판정을 수신할 때까지 대기하는 시간에는 웹 프록시에서 요청을 전송하는 데 필요한 시간이 포함됩니다. |
| Sophos 응답 | %:p> | 웹 프록시에서 요청을 전송한 후 Sophos 스캐닝 엔진에서 응답을 수신할 때까지 대기하는 시간. |
| Sophos 합계 | %:p< | Sophos 스캐닝 엔진에서 판정을 수신할 때까지 대기하는 시간에는 웹 프록시에서 요청을 전송하는 데 필요한 시간이 포함됩니다. |
| AMP 응답 | %:e> | 웹 프록시에서 요청을 전송한 후 AMP 엔진에서 응답을 수신할 때까지 대 |

| | | |
|---|---|---|
| | | 기하는 시간. |
| AMP 합계 | %:e< | AMP 엔진에서 판정을 수신할 때까지 대기하는 시간에는 웹 프록시에서 요청을 전송하는 데 필요한 시간이 포함됩니다. |
| 대기 시간 | %x;<br>%L | 사람이 읽을 수 있는 형식의 대기 시간 및 요청 로컬 시간: DD/MMM/YYYY: hh:mm:ss +nnnn. 이 필드는 액세스 로그에 큰따옴표와 함께 기록됩니다.<br><br>이 필드를 사용하면 각 로그 항목에 대한 시간대 시간의 로컬 시간을 계산할 필요 없이 로그를 문제와 상호 연결할 수 있습니다. |
| 클라이언트 포트 | %F | 클라이언트측에서 사용된 포트 번호입니다. |
| 서버 IP 주소 | %k | 웹 서버 IP 주소입니다. |
| 서버 포트 번호 | %p | 웹 서버 포트 번호입니다. |

## 관련 정보

- AsyncOS 14.5 for Cisco Secure Web Appliance 사용 설명서 - GD(일반 배포) - Cisco
- Cisco Web Security Appliance 모범 사례 지침 - Cisco

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.