SHD 로그로 Secure Web Appliance 성능 문제 해결

목차

소개

이 문서에서는 시스템 상태 데몬 로그(shd_logs) 및 이 로그를 사용하여 SWA(Secure Web Appliance) 성능 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 물리적 또는 가상 SWA(Secure Web Appliance)가 설치되었습니다.
- 라이센스가 활성화되었거나 설치되었습니다.
- SSH(Secure Shell) 클라이언트.
- 설치 마법사가 완료되었습니다.

- SWA에 대한 관리 액세스.

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.

SHD 로그란?

SHD 로그에는 1분마다 SWA의 성능 관련 프로세스 통계가 대부분 저장됩니다.

다음은 SHD 로그 라인의 예입니다.

```
Mon Jun 9 23:46:14 2022 Info: Status: CPULd 66.4 DskUtil 5.2 RAMUtil 11.3 Reqs 0 Band 0 Latency 0 Cache
SrvConn 0 MemBuf 0 SwpPgOut 0 ProxLd 0 Wbrs_WucLd 0.0 LogLd 0.0 RptLd 0.0 WebrootLd 0.0 SophosLd 0.0 Mc
```

SHD 로그는 CLI(Command Line Interface) 및 FTP(File Transfer Protocol)에서 허용됩니다. GUI(Graphical User Interface)에서 로그를 보는 옵션은 없습니다.

액세스 SHD 로그

CLI에서:

1. CLI에서 grep 또는 tail을 입력합니다.
2. 목록에서 "shd_logs Type: SHD Logs Retrieval: FTP Poll"을 찾고 관련 번호를 입력합니다.
3. grep할 정규식을 입력하십시오. 로그 내에서 검색할 정규식을 입력할 수 있습니다. 예를 들어, 날짜 및 시간을 입력할 수 있습니다.
4. 이 검색에서 대/소문자를 구분하지 않으시겠습니까? [Y]> SHD_Logs에서 이 옵션이 필요하지 않은 대/소문자를 구분하지 않는 경우 이 옵션을 기본값으로 둘 수 있습니다.
5. 일치하지 않는 행을 검색하시겠습니까? [N]> Grep 정규식을 제외한 모든 항목을 검색할 필요가 없는 경우 이 줄을 기본값으로 설정할 수 있습니다.
6. 로그를 추적하시겠습니까? [N]> 이 옵션은 grep의 출력에서만 사용할 수 있습니다. 이 옵션을 기본값(N)으로 설정하면 현재 파일의 첫 번째 행의 SHD 로그가 표시됩니다.
7. 출력 페이지를 매기시겠습니까? [N]> "Y"를 선택한 경우 출력이 적은 명령의 출력과 같으므로 행과 페이지 사이를 탐색할 수 있습니다. 또한 로그 내부를 검색하여(Type /then 키워드 및 enter 키) q 유형별로 로그 보기를 종료할 수 있습니다.

FTP에서:

1. GUI > Network > Interfaces에서 FTP가 활성화되었는지 확인합니다.
2. FTP를 통해 SWA에 연결합니다.
3. Shd_logs 폴더에는 로그가 포함되어 있습니다.

SHD 로그 필드

SHD의 필드에 대한 자세한 내용은 다음과 같습니다.

필드 번호	이름	식별자	설명
8	CPUL	백분율(%) 0 ~ 99	CPU 로드 OS에서 보고한 시스템에 사용된 총 CPU 비율
10	츠크우티	백분율(%)	디스크 사용률

		0 ~ 99	/data 파티션에서 스페이스드 사용
12	라무틸	백분율(%) 0 ~ 99	RAM 사용률 OS에서 보고된 사용 가능한 메모리의 비율
14	요구 사항	요청/초	요청 지난 1분 동안의 평균 트랜잭션(요청) 수
16	밴드	초 단위	대역폭 절약 지난 1분 동안 절약된 평균 대역폭입니다. - 지난 1분 동안 평균 저장된 SNMP 대역폭과 동일
18	레이턴시 [1]	밀리초(ms)	최근 1분 동안의 평균 레이턴시(응답 시간) 액세스 로그의 두 번째 필드 - TCP 연결이 최종 사용자로부터 WSA로 (또는 연결이 해독되지 않은 경우 최종 사용자로부터 웹 서버로) 소요되는 시간을 표시합니다. WSA는 마지막 분 동안 액세스 로그에 로깅된 각 요청에 대한 시간을 합산하여 이러한 요청 수로 나눈 후 SHD에 대한 평균 레이턴시를 가져옵니다.
20	캐시 적중	번호 #	지난 1분 동안의 캐시

			적중 평균입니다. - 지난 1분 동안의 SNMP 캐시 적중 평균과 동일
22	CliConnection	번호 #	현재 클라이언트 연결의 총 수 클라이언트에서 WSA로 - SNMP 현재 총 클라이언트 연결과 동일
24	Srv 연결	번호 #	현재 서버 연결의 총 수 WSA에서 웹 서버로 - SNMP 현재 총 서버 연결과 같습니다.
26	MemBuf [2]	백분율(%) 0 ~ 99	메모리 버퍼 현재 사용 가능한 프록시 버퍼 메모리의 총량입니다.
28	SwpPgOut	번호 #	OS에서 보고한 스와핑된 페이지 수입니다. 페이지 파일 또는 페이징 파일은 RAM이 완전히 사용될 때 정보를 저장하는 임시 위치로 사용되는 하드 드라이브의 공간입니다.
30	ProxLd	백분율(%) 0 ~ 99	Prox 프로세스 로드 모든 수신 요청을 처리하는 프로세스 (HTTP/HTTPS/FTP/SOCKS)

32	Wbrs_WucLd	백분율(%) 0 ~ 99	웹 평판 코어링 로드 실제 WBRS 스캔 엔진에 사용되는 프로세스입니다. 프록시 프로세스는 reqscand 프로세스와 상호 작용하여 WBRS 스캔을 수행합니다.
34	로그Ld	백분율(%) 0 ~ 99	프록시 로그 로드
36	RptLd	백분율(%) 0 ~ 99	보고서 엔진 로드 보고 데이터베이스를 만드는 프로세스입니다. 'reportd'는 'haystackd'와 상호 작용하여 웹 추적 데이터베이스를 만듭니다.
38	WebrootLd	백분율(%) 0 ~ 99	Webroot 안티멀웨어 로드
40	SophosLd	백분율(%) 0 ~ 99	Sophos 안티바이러스 로드

42	McafeeLd	백분율(%) 0 ~ 99	Mcafee Antivirus 로드
44	WTTLd	백분율(%) 0 ~ 99	웹 트래픽 탭
46	AMPLd	백분율(%) 0 ~ 99	AMP(Advanced Malware Protection)

1. WSA에 요청이 많지 않고 어떤 시점에 긴 기간 연결이 완료된 경우(예: 며칠) SHD 로그에서 레이턴시가 최고조에 달할 수도 있습니다. 그러면 이 단일 요청은 완료되고 액세스 로그에 로그인했을 때 해당 분 동안 레이턴시를 늘릴 수 있습니다.

2. 다음 각목의 1에 해당하는 것

"시스템의 RAM 사용량 working 시스템에서 사용하지 않는 RAM은 웹 개체 캐시에서 사용되므로 효율성이 90%보다 높을 수 있습니다. 시스템이 experiencing 심각한 성능 문제가 있으며 이 값은 100%에 머물지 않습니다. operating 보통."

참고: 프록시 버퍼 메모리는 이 RAM을 사용하는 구성 요소 중 하나입니다

SHD 로그 문제 해결

기타 프로세스 고부하

다른 공정의 부하가 높으면 이 글에서 표-1을 확인하고 그 공정과 관련된 로그를 읽는다.

높은 레이턴시

SHD 로그에서 대기 시간이 높은 경우 Proxy_track logs in/data/pub/track_stats/를 확인해야 합니다. 레이턴시가 높은 기간을 찾습니다. 프록시 트랙에는 레이턴시와 관련된 레코드가 몇 개 있습니다. 각 섹션의 앞에 있는 숫자는 마지막 재부팅 이후 발생한 총 횟수입니다. 예를 들어, 이 코드에서 다음을 수행합니다.

```
Current Date: Wed, 11 Jun 2022 20:03:32 CEST
...
   Client Time    6309.6 ms    109902
...
Current Date: Wed, 11 Jun 2022 20:08:32 CEST
...
   Client Time    6309.6 ms    109982
```

5분 안에 6309.6ms 이상이 걸린 클라이언트 요청 수는 80건입니다. 따라서 각 시간대의 숫자를 빼야 정확한 값을 얻을 수 있으므로 다음 항목을 고려해야 합니다.

클라이언트 시간: 클라이언트에서 SWA로 걸리는 시간입니다.

적중 시간: 캐시 적중: 요청된 데이터가 캐시에 있으며 클라이언트에 전달될 수 있습니다.

Miss Time: 캐시 누락: 요청한 데이터가 캐시에 없거나 최신 상태가 아니며 클라이언트에 배달될 수 없습니다.

서버 트랜잭션 시간: SWA에서 웹 서버까지 걸리는 시간입니다.

또한 성능 확인 과정에서 다음 값을 고려해야 합니다.

사용자 시간: 160.852(53.33%)
시스템 시간: 9.768(3.256%)

Track Stat(추적 상태) 로그에서 정보는 5분(300초)마다 로깅됩니다. 이 예에서 사용자 시간 160.852는 CPU에서 사용자 요청을 처리하기 위한 작업으로 로드한 시간(초)입니다. 시스템 시간은 SWA가 네트워크 이벤트(예: 라우팅 결정 등)를 처리한 시간입니다. 이 두 백분율의 합계가 해당 시간의 총 CPU 로드입니다. 사용자 시간이 많은 경우 복잡도가 높은 구성을 고려해야 합니다.

관련 정보

- WSA AsyncOS 릴리스 정보
- Cisco Secure Email and Web Manager용 호환성 매트릭스
- 업그레이드 및 업데이트 연결 확인
- Cisco 기술 지원 및 다운로드

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.