

ESA에서 메일 로그를 검색하고 보려면 어떻게 해야 합니까?



문서 ID:118552

업데이트 날짜:2014년 10월 10일

기고자: Cisco TAC 엔지니어

 [PDF 다운로드](#)

 [인쇄](#)

[피드백](#)

관련 제품

- [Cisco Email Security Appliance](#)

목차

[소개](#)

[ESA에서 메일 로그를 검색하고 보려면 어떻게 해야 합니까?](#)

[관련 Cisco 지원 커뮤니티 토론](#)

소개

이 문서에서는 ESA(Email Security Appliance)에서 메시지를 처리한 방법을 보여 주는 로그 항목을 검색하는 방법에 대해 설명합니다.

ESA에서 메일 로그를 검색하고 보려면 어떻게 해야 합니까?

로그를 검색하여 관심이 있는 IP 주소에서 수신되는 이메일의 *From*, *To*, *Subject*에 대한 자세한 정보를 수집할 수 있습니다.

로그 이름은 `mail_logs`입니다. System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션) > `mail_logs(mail_logs)`에서 이 정보를 확인할 수 있습니다.

이러한 로그에 액세스하는 방법에는 여러 가지가 있습니다.

1. 웹 브라우저를 통해 System Administration(시스템 관리) > Log Subscription(로그 서브스크립션)으로 이동합니다. `mail_logs`의 경우 `mail_logs` 오른쪽에 있는 `ftp` 링크를 클릭합니다. 오류가

발생하면 **Network(네트워크) > IP 인터페이스**로 이동하여 ESA에 일반적으로 액세스하는 인터페이스를 선택하고 FTP/port 21 서비스를 활성화합니다.

2. 명령줄에서 Putty와 같은 ssh 클라이언트를 사용하여 포트 22/ssh를 통해 ESA 어플라이언스의 CLI에 로그인합니다. 명령줄에서 grep를 사용하여 IP를 검색합니다. 어플라이언스의 mail_logs에 연결된 #을 입력한 다음 검색할 패턴(예:192.168.1.1 또는 joe@example.com). 다음 세 가지 질문에 대해 Enter 키를 누르고 기본값을 유지합니다. 검색을 완료하는 데 시간이 다소 걸릴 수 있습니다. 출력이 돌아오면 ICID 또는 MID를 검색할 수 있습니다.

```
grep "ICID 123456" mail_logs
```

출력이 돌아오면 MID를 검색할 수 있습니다

```
grep "MID 78901234" mail_logs
```

MID의 *From, To, Subject*를 볼 수 있어야 합니다. ICID의 IP 주소와 HAT Sender Group이 표시되어야 합니다.

3. 또 다른 옵션은 mail_logs를 로컬 시스템(데스크톱)에 ftp하고 자체 파일/텍스트 편집기를 사용하여 IP 주소를 검색하는 것입니다.

이 문서가 도움이 되었습니까? [예 아니요](#)

피드백을 주셔서 감사합니다.

[지원 케이스 열기 \(Cisco 서비스 계약 필요\)](#)

관련 Cisco 지원 커뮤니티 토론

[Cisco Support Community](#)는 질문하고 답변하고 제안을 공유하고 동료와 협업할 수 있는 포럼입니다.

이 문서에 사용된 [표기 규칙에](#) 대한 자세한 내용은 [Cisco](#) 기술 팁 표기 규칙을 참조하십시오.

업데이트 날짜:2014년 10월 10일

문서 ID:118552