SWG 모듈에 대한 최대 디버그 로깅 활성화

목차

소개

이 문서에서는 AnyConnect 및 CSC(Cisco Secure Client)에 대해 SWG(Secure Web Gateway) 모듈에서 최대 디버그 로깅을 활성화하는 방법에 대해 설명합니다.

최대 디버그 로깅을 활성화하는 활용 사례

다음과 같은 문제를 해결할 때 SWG 모듈에서 최대 디버그 로깅을 활성화합니다.

- 종속 포털을 통한 핫스팟 문제
- 외부 도메인 바이패스 목록이 적용되지 않음
- 간헐적인 DNS 또는 웹 성능 문제

AnyConnect 4.10 MR7, CSC 5.0 MR2 이상에서 최대 디버그 로깅 활성화

AnyConnect 4.10 MR7, CSC 5.0 MR2 또는 이전 버전을 사용하는 경우 다음 단계를 수행합니다. 기본적으로 최대 디버그 로깅은 활성화되지 않으며 Umbrella 대시보드 또는 ASA를 통해 구성할 수 없습니다. 파일의 개체에"logLevel": "1"수동으로orgConfig추가해야SWGConfig.json합니다. 최신 버전의

AnyConnect 또는 Cisco Secure Client를 사용 중인 경우 이 섹션을 건너뛰십시오.

SWGConfig.json의 위치

- Windows(AnyConnect):

```
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG\
```

- Windows(보안 클라이언트):

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
```

- macOS(AnyConnect):

```
/opt/cisco/anyconnect/umbrella/swg/
```

- macOS(보안 클라이언트):

```
/opt/cisco/secureclient/umbrella/swg/
```

디버그 로깅을 영구화하십시오.

수정된SWGConfig.json파일은 다음 API가 Cisco AnyConnect Umbrella 모듈에서 동기화될 때까지만 유지됩니다. 이 구성을 유지하고 API 동기화에서 덮어쓰지 않도록 하려면 폴더에swg_org_config.flag파일을Umbrella/data배포합니다.

1. 플래그 파일 생성

    - Umbrella Data 폴더에 이름이**swg_org_config.flag**지정된 새 파일을 생성합니다. 파일 확장명은 다음과 같아야 합니다. .flag.

    - Windows(AnyConnect):
    -

    ```
    C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\data\swg_org_config.fl
    ```

    - Windows(보안 클라이언트):
    -

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\swg_org_config.flag
```

- macOS(AnyConnect):
-

```
/opt/cisco/anyconnect/umbrella/data/swg_org_config.flag
```

- macOS(보안 클라이언트):
-

```
/opt/cisco/secureclient/umbrella/data/swg_org_config.flag
```

2. 내용 복사 및 수정

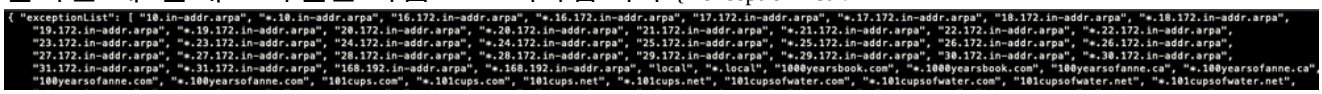
- 파일의**orgConfig**개체의 내용을SWGConfig.json파일에swg_org_config.flag복사합니다.
- 뒤에"logLevel": "1"첨부
- 예를 들면 다음과 같습니다.

```
{
"exceptionList": [
"www.example.com",
"smh.com.au",
"*.smh.com.au",
"www.blue.com",
"*.www.blue.com",
"146.112.133.72"
// ...additional entries...
],
"failOpen": 1,
"logLevel": "1",
"swgAnycast": "146.112.255.50",
"swgDomain": "swg-url-proxy-https.sigproxy.qq.opendns.com",
"swgEchoService": "http://www.msftconnecttest.com/connecttest.txt"
}
```

- 플래그 파일이 로 시작하고 로{ "exceptionList": [...]끝나는지 확인합니다**"SWGEchoService": "http://www.msftconecttest.com/connecttest.txt"}**.
- 개체 앞이나 뒤에 추가 줄을 복사하지 마십시오.
- identity, 또는deviceId과 같은 줄을 잘못 복사하면 SWG 기능이 중단될adUserID수 있습니다.

잘못된 예: 플래그 파일에는**identity**,deviceId또는 이전의 키dUserID 가 포함되어 있습니다.

올바른 예: 플래그 파일은 다음으로 시작합니다 { "exceptionList":



14970100184724

3. 서비스 다시 시작

    - Cisco AnyConnect Secure Mobility Agent/Secure Client 서비스를 다시 시작하거나 시스템을 재부팅하거나 VPN을 연결하고 연결을 끊습니다.

4. 컨피그레이션 확인

    - SWGConfig.json다시 시작 또는 VPN 연결/연결 끊기 후 파일을 열어 SWG 최대 디버그 로그 레벨이 설정되었는지 확인합니다. 이 항목을 구성하면 파일에 다음과 같은 항목이 나타납니다.

```
"logLevel": "1"
```

최대 디버그 로그 확인 및 제공

Windows 확인

1. Windows 이벤트 뷰어를 엽니다.
2. 이 예와 유사한 로그 행을 찾습니다. 이는 최대 디버그 로깅이 활성화되었음을 나타냅니다.

    예 1:

```
BRIDGE | Thread 1d18 | Connection : Resolved IP from 'swg-url-proxy-https.sigproxy.qq.opendns.com'
THREAD | Thread 1d18 | SetGUID '959bfe4d6fba87a65b433321c6748d761d9492cb'
```

    예 2: 프록시되는 모든 웹 요청이 기록됩니다. 내부/외부 도메인 목록에 따라 AnyConnect SWG를 우회하는 웹 요청은 기록되지 않습니다.

```
LISTEN | Thread 1d18 | Connection : Hostnames from KDF are login.live.com
```

3. 최대 디버그 이벤트 로그(.evtx)를 txt로 변환하려면 PowerShell 명령을 사용합니다.

```
Get-WinEvent -Path C:\Desktop\Umbrella.evtx | Format-Table -AutoSize | Out-File C:\Desktop\Umbrell
```

macOS 확인

Mac OSX에서는 이 명령으로 디버그 로깅을 볼 수 있습니다(grep 또는 txt로 기록할 수 있음).

1. 다음 명령을 실행합니다.

```
>log show --predicate 'subsystem contains "com.cisco.anyconnect.swg" || senderImagePath endswith "
```

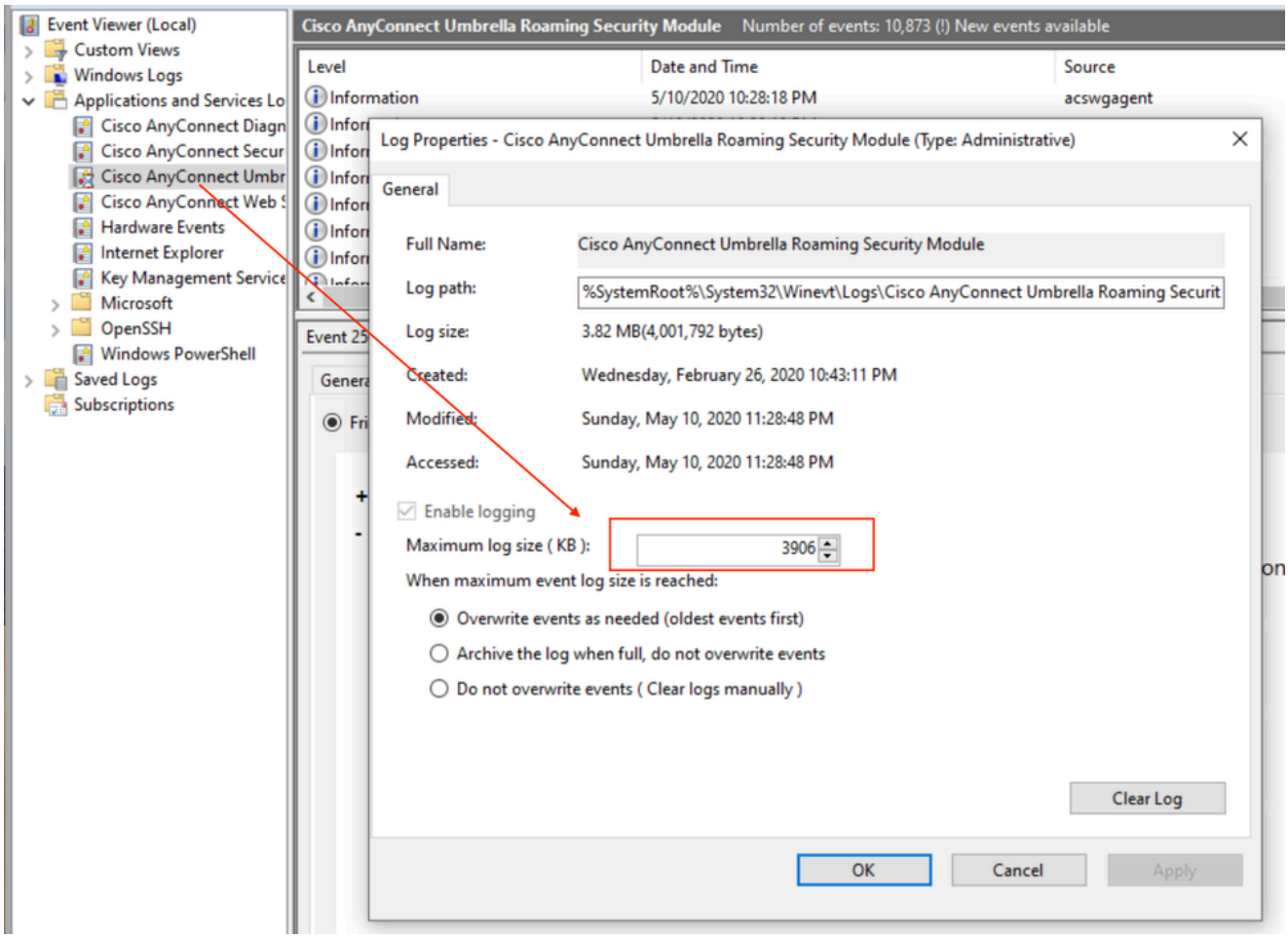
   - 최대 디버그 로깅이 활성화된 상태에서 purple.com을 탐색할 때의 출력 예:

```
2022-09-19 10:51:15.627229+1000 0x16b121 Default 0x0 98970 0 acswgagent: Connection : Hostna
```

2. AnyConnect DART 번들에는 최대 디버그 로그가 포함되어 있습니다. 지원 여부를 확인한 후 문제를 재현하고 타임스탬프, 사용자 환경, 문제의 도메인을 기록한 다음 이 정보를 DART 번들과 함께 제공합니다.

추가 참고 사항

- 최대 디버그 로깅은 자세한 로그를 생성합니다. 특히 간헐적인 문제의 경우 대용량 로그를 수용하도록 Windows 이벤트 뷰어에서 Umbrella Roaming Security Module 로그 크기를 구성합니다.



360056784112

- 문제 해결이 완료되면 최대 디버그 로깅을 비활성화하려면 파일을 제거하거나 swg_org_config.flag이름을 변경합니다.

CSC 5.0 MR3 및 AC 4.10 MR8 이상에서 최대 디버그 로깅 활성화

개요

CSC 5.0 MR3 및 AC 4.10 MR8부터 디버그 로깅 활성화는 더 간단한 프로세스를 사용합니다.

변경 사항

- 디버그 로깅을SWGConfigOverride.json활성화하려면 파일(정적 콘텐츠 포함)을 SWG 폴더에 복사합니다.
- 를 복사하거나 수정할 필요가orgConfig없습니다SWGConfig.json. 이 파일의 내용은 조직을 조직으로 변경하지 않습니다.
- DNS 모듈에서 컨피그레이션 동기화를 수행하거나 플래그 파일에서 읽는 종속성이 없습니다. 파일은SWGConfig.json그대로 유지됩니다.

디버그 로깅 사용

SWGConfigOverride.json 의 컨피그레이션 값은 의 값(있는 경우)보다 우선하며, logLevel(디버그 로깅을 활성화/비활성화하기 위해) 및 autotuning(전송 버퍼 자동 튜닝을 활성화/비활성화하기 위해) 두 개의 컨피그레이션만 포함할SWGConfig.json. The **SWGConfigOverride.json** 수 있습니다.

1. 디버그 로깅을 활성화하려면 내용SWGConfigOverride.json과 함께 복사합니다.

```
{"logLevel": "1"}
```

   - 디버그 로깅 및 자동 조정을 모두 활성화하려면 다음을 사용합니다.

```
{"logLevel": "1", "autotuning": "1"}
```

2. SWG 폴더**SWGConfigOverride.json**에 배치:

- Windows(AnyConnect):
  `C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG\`
- Windows(보안 클라이언트):
  `C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\`
- macOS(AnyConnect):
  `/opt/cisco/anyconnect/umbrella/swg/`
- macOS(보안 클라이언트):
  `/opt/cisco/secureclient/umbrella/swg/`

3. SWG 또는 Umbrella 서비스를 다시 시작하거나 시스템을 다시 시작합니다.

- macOS: AnyConnect 또는 보안 클라이언트 에이전트를 중지하고 시작합니다.
- 창: 서비스 MMC 스냅인을 통해 보안 웹 게이트웨이(4.10.x의 acswgagent 빌드 /5.x 빌드의 csc_swgagent 빌드) 서비스를 다시 시작하거나 중지/시작합니다(시작 > 실행 > Services.msc).

참고: 디버그 로깅을 활성화하는 이전 방법은 계속 지원되며 계속 따를 수 있으며 5.0 MR3

또는 4.10 MR8 이전 클라이언트의 유일한 옵션입니다.

컨피그레이션 및 운영 메모

- 파일SWGConfig.json은 대/소문자를 구분합니다. 큰따옴표와 함께 사용합니다"logLevel": "1".
- 값logLevel은 정수가 아닌 문자열 1이므로 큰따옴표가 있는 "1"이어야 합니다.
- 파일swg_org_config.flag확장명은 .flag 아니어야 .txt합니다.
- 최대 디버그 로깅은 매우 자세한 로그를 생성합니다. Umbrella 지원 엔지니어가 요청하는 경우에만 최대 디버그 로깅을 활성화합니다.
- 이swg_org_config.flag파일에는 바이패스된 도메인의 정적 목록이 포함되어 있으며 Dashboard(대시보드) > Deployments(구축) > Domain Management(도메인 관리)에 나열된 External Domains(외부 도메인)와 동기화되지 않습니다.

관련 정보

- Cisco 기술 지원 및 다운로드
- Cisco Secure Access Help Center
- Cisco ISE 설계 가이드

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.