AnyConnect 버전 4.0 및 NAC Posture 에이전트가 ISE 트러블슈팅 가이드에 팝업되지 않음

목차

소개

ISE(Identity Services Engine)는 NAC(Network Admission Control) 에이전트(Microsoft Windows, Macintosh 또는 웹 에이전트를 통해) 또는 AnyConnect 버전 4.0을 사용해야 하는 상태 조정 기능을 제공합니다. AnyConnect 버전 4.0 ISE 상태 모듈은 NAC 에이전트와 정확히 유사하며 따라서 이 문서에서 NAC 에이전트라고 합니다.클라이언트에 대한 상태 실패 의 가장 일반적인 증상은 작동 시나리오로 인해 항상 NAC 상담원 창이 PC를 팝업 및 분석하므로 NAC 상담원이 팝업되지 않는다는 것입니다.이 문서는 포스처가 실패할 수 있는 많은 원인을 좁히는 데 도움이 됩니다. 즉 NAC 에이전트가 팝업되지 않습니다.NAC Agent 로그는 Cisco TAC(Technical Assistance Center)에서만 디코딩할 수 있으며 가능한 근본 원인은 다양하기 때문에 철저한 분석이 아닙니다.그러나 단순히 "상담원이 포스처 분석을 팝업 표시하지 않음"보다 상황을 명확히 하고 문제를 더 정확히 찾아내는 것이 목적이며 가장 일반적인 원인을 해결하는 데 도움이 될 것입니다.

사전 요구 사항

요구 사항

이 문서에 나열된 시나리오, 증상 및 단계는 초기 설정이 이미 완료된 후 문제를 해결할 수 있도록 작성되었습니다.초기 컨피그레이션에 대해서는 Cisco.com의 Cisco ISE 컨피그레이션 가이드에서 포스처 서비스를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE 버전 1.2.x
- ISE용 NAC Agent 버전 4.9.x
- AnyConnect 버전 4.0

참고:릴리스 노트가 주요 동작 변화를 나타내지 않는 한 이 정보는 ISE의 다른 릴리스에도 적용되어야 합니다.

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

문제 해결 방법론

상담원이 팝업하는 이유는 무엇입니까?

ISE 노드를 검색하면 에이전트가 팝업됩니다.상담원이 전체 네트워크 액세스 권한이 없고 상태 리디렉션 시나리오에 있는 경우 ISE 노드를 계속 찾습니다.

상담원 검색 프로세스의 세부사항을 설명하는 Cisco.com 문서가 있습니다.ISE(Identity Services Engine)용 NAC(Network Admission Control) 에이전트 검색 프로세스.이 문서에서는 컨텐츠 중복을 방지하기 위해 핵심 사항만 설명합니다.

클라이언트가 연결되면 RADIUS 인증(MAC 필터링 또는 802.1x)을 거치게 되며, ISE는 리디렉션 ACL(Access Control List) 및 네트워크 장치(스위치, ASA(Adaptive Security Appliance) 또는 무선 컨트롤러)로의 리디렉션 URL을 반환하여 클라이언트 트래픽이 IP 주소 및 DNS(Domain Name Server) 해상도만 얻을 수 있도록 제한합니다.클라이언트에서 오는 모든 HTTP(S) 트래픽은 ISE 포털 자체로 향하는 트래픽을 제외하고 CPP(Client Posture and Provisioning)로 끝나는 ISE의 고유 URL로 리디렉션됩니다.NAC 에이전트는 기본 게이트웨이로 일반 HTTP GET 패킷을 전송합니다.상담원이 CPP 리디렉션 이외의 응답 또는 다른 응답을 받지 못한 경우, 상담원은 자신이 전체 연결을 가지고 있다고 간주하며 상태 확인을 진행하지 않습니다.특정 ISE 노드 끝에 CPP URL로 리디렉션되는 HTTP 응답을 수신하면 포스처 프로세스를 계속하고 해당 ISE 노드에 연결합니다.해당 ISE 노드에서 포스처 세부사항을 성공적으로 수신할 때만 팝업되고 분석을 시작합니다.

또한 NAC Agent는 구성된 검색 호스트 IP 주소에 도달합니다(둘 이상의 구성이 필요하지 않음). 세션 ID를 사용하여 리디렉션 URL을 가져오려면 또한 리디렉션되어야 합니다.검색 IP 주소가 ISE 노드인 경우 올바른 세션 ID를 얻기 위해 리디렉션되기를 기다리므로 해당 IP 주소는 추적하지 않습니다.따라서 일반적으로 검색 호스트는 필요하지 않지만 리디렉션을 트리거하기 위해 리디렉션 ACL 범위의 IP 주소로 설정할 때(예: VPN 시나리오) 유용합니다.

가능한 원인

리디렉션이 발생하지 않음

이것이 지금까지 가장 흔한 원인이다.유효성을 검사하거나 무효화하려면 에이전트가 팝업되지 않는 PC에서 브라우저를 열고 URL을 입력할 때 포스처 에이전트 다운로드 페이지로 리디렉션되는지 확인합니다.DNS 문제를 방지하기 위해 무작위 IP 주소(예: http://1.2.3.4)를 입력할 수도 있습니다(IP 주소가 리디렉션되지만 웹 사이트 이름이 리디렉션되지 않는 경우 DNS를 확인할 수 있음).

리디렉션되는 경우 에이전트 로그 및 ISE 지원 번들(포스처 및 디버그 모드로 향하는 스위스 모듈 포함)을 수집하고 Cisco TAC에 문의하십시오.이는 에이전트가 ISE 노드를 검색하지만 포스처 데이터를 가져오는 동안 오류가 발생했음을 나타냅니다.

리디렉션이 발생하지 않을 경우 첫 번째 원인을 가지며, 이 경우 근본 원인에 대한 추가 조사가 필요합니다.먼저 네트워크 액세스 디바이스(WLC(Wireless LAN Controller) 또는 스위치의 컨피그레이션을 확인하고 이 문서의 다음 항목으로 이동합니다.

특성이 네트워크 디바이스에 설치되지 않음

이 문제는 리디렉션이 발생하지 **않는** 시나리오**의** 하위 **사례입니다**.리디렉션이 수행되지 않으면 첫 번째 작업은 클라이언트가 스위치 또는 무선 액세스 레이어에서 올바른 상태에 있는지(지정된 클라이언트에서 문제가 발생할 때) 확인하는 것입니다.

다음은 **show access-session interface <interface number> detail** 명령의 출력 예입니다(일부 플랫폼의 끝에 **세부** 정보를 추가해야 할 수 있음).상태가 "Authz success(인증 성공)"인지, URL 리디렉션 ACL이 의도된 리디렉션 ACL을 올바르게 가리키는지, URL 리디렉션이 URL 끝에 CPP가 있는 예상 ISE 노드를 가리키는지 확인해야 합니다.ACS ACL 필드는 ISE의 권한 부여 프로파일에 다운로드 가능한 액세스 목록을 구성한 경우에만 표시되므로 필수 필드가 아닙니다.그러나 이를 살펴보고 리디렉션 ACL과 충돌이 없는지 확인하는 것이 중요합니다(확실하지 않은 경우 상태 컨피그레이션에 대한 문서 참조).

```
01-SW3750-access#show access-sess gi1/0/12 det
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cpp
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

AireOS를 실행하는 WLC의 문제를 해결하려면 **show wireless client detail <mac address>**를 입력하고 Cisco IOS-XE를 실행하는 WLC의 문제를 해결하려면 show wireless client mac-address <mac address> detail을 입력합니다.유사한 데이터가 표시되고 리디렉션 URL 및 ACL을 확인해야 하며 클라이언트가 "POSTURE_REQD" 상태 또는 유사한지(소프트웨어 버전에 따라 다름) 확인해야 합니다.

특성이 없는 경우 문제 해결 중인 클라이언트의 ISE에서 인증 세부 정보를 열고(**Operations(작업) >**

Authentications(인증)로 이동) Result(결과) 섹션에서 리디렉션 특성이 전송되었는지 확인해야 합니다.전송되지 않은 경우 이 특정 클라이언트에 대해 특성이 반환되지 않은 이유를 알아보려면 권한 부여 정책을 검토해야 합니다.조건 중 하나가 일치하지 않을 수 있으므로 하나씩 문제를 해결하는 것이 좋습니다.

리디렉션 ACL과 관련하여 Cisco IOS®는 허용 명령문을 재전송하므로 WLC의 AireOS는 거부 명령문을 재전송하므로 ISE와 DNS는 거부됩니다.

특성이 제자리에 있지만 네트워크 디바이스가 리디렉션되지 않음

이 경우 주요 원인은 구성 문제입니다.Cisco.com의 컨피그레이션 가이드 및 컨피그레이션 예에 따라 네트워크 디바이스의 컨피그레이션을 검토해야 합니다.이 경우 일반적으로 네트워크 디바이스의 모든 포트 또는 액세스 포인트(AP) 전체에 문제가 발생합니다.그렇지 않으면 일부 스위치 포트 또는 일부 AP에서만 문제가 발생할 수 있습니다.이 경우 문제가 발생한 포트의 컨피그레이션을 포스처가 제대로 작동하는 포트 또는 AP와 비교해야 합니다.

FlexConnect AP는 각각 고유한 컨피그레이션을 가질 수 있으며, 일부 AP에서 ACL 또는 VLAN을 실수하는 것은 쉬우며 다른 AP는 그렇지 않기 때문에 민감합니다.

또 다른 일반적인 문제는 클라이언트 VLAN에 SVI가 없다는 것입니다.이는 스위치에만 적용되며 Catalyst 3750 Series 스위치의 ISE 트래픽 리디렉션에서 자세히 설명합니다.속성 관점에서 모든 것이 좋게 보일 수 있습니다.

DACL(Downloadable Access-list) 간섭

리디렉션 특성과 동시에 DACL을 스위치(또는 무선 컨트롤러의 Airespace-ACL)로 다시 푸시하면 리디렉션을 차단할 수 있습니다.DACL이 먼저 적용되고 완전히 삭제되는 항목과 처리될 내용을 결정합니다.그런 다음 리디렉션 ACL이 적용되고 리디렉션되는 항목을 결정합니다.

이것이 구체적으로 의미하는 것은 대부분의 경우 DACL에서 모든 HTTP 및 HTTPS 트래픽을 허용해야 한다는 것입니다.차단하면 이전 삭제되므로 리디렉션되지 않습니다.트래픽은 대개 이후에 리디렉션 ACL에서 리디렉션되므로 네트워크에서 실제로 허용되지 않기 때문에 보안 문제가 아닙니다.그러나 DACL에서 이러한 두 유형의 트래픽을 허용해야 리디렉션 ACL에 바로 도달할 수 있습니다.

잘못된 NAC Agent 버전

특정 NAC Agent 버전이 특정 버전의 ISE에 대해 검증된다는 사실을 잊기 쉽습니다.많은 관리자가 ISE 클러스터를 업그레이드하고 클라이언트 프로비저닝 결과 데이터베이스에 관련 NAC 에이전트 버전을 업로드하는 것을 잊습니다.

ISE 코드에 오래된 NAC Agent 버전을 사용하는 경우 이 버전이 작동할 수도 있지만 작동하지 않을 수도 있습니다.그래서 어떤 고객들은 일을 하고 다른 사람들은 그렇지 않다는 것은 놀랄 일이 아니다.확인할 수 있는 한 가지 방법은 ISE 버전의 Cisco.com 다운로드 섹션으로 이동하여 어떤 NAC 에이전트 버전이 있는지 확인하는 것입니다.일반적으로 각 ISE 버전에 대해 여러 가지가 지원됩니다.이 웹 페이지는 모든 행렬을 수집합니다.Cisco ISE 호환성 정보.

클라이언트에서 HTTP 웹 프록시를 사용 중입니다.

HTTP 웹 프록시의 개념은 클라이언트가 웹 사이트 DNS IP 주소를 직접 확인하지 않고 웹 사이트에 직접 연결하지 않는다는 것입니다.대신 프록시 서버에 요청을 보내면 됩니다. 프록시 서버에서 요

청을 처리합니다.일반적인 컨피그레이션의 일반적인 문제는 클라이언트가 웹 사이트(예: www.cisco.com)에 대한 HTTP GET을 프록시에 직접 전송하여 이를 해결한다는 것입니다. 그러면 가로채기가 되고 ISE 포털로 올바르게 리디렉션됩니다.그러나 다음 HTTP GET을 ISE 포털 IP 주소로 보내는 대신 클라이언트는 계속해서 프록시에 요청을 보냅니다.

프록시로 향하는 HTTP 트래픽을 리디렉션하지 않을 경우, 사용자는 인증 또는 상태 유지 없이 전체 인터넷(모든 트래픽은 프록시를 통과하므로)에 직접 액세스할 수 있습니다.이 솔루션은 실제로 클라이언트의 브라우저 설정을 수정하고 프록시 설정에서 ISE IP 주소에 대한 예외를 추가하는 것입니다.이렇게 하면 클라이언트가 ISE에 도달해야 할 경우 프록시가 아닌 ISE로 요청을 직접 보냅니다.이렇게 하면 클라이언트가 계속 리디렉션되지만 로그인 페이지가 표시되지 않는 무한 루프가 방지됩니다.

NAC Agent는 시스템에 입력된 프록시 설정의 영향을 받지 않으며 정상적으로 계속 작동합니다.즉, 웹 프록시를 사용할 경우 NAC Agent 검색 작업(포트 80을 사용하기 때문에) 둘 다 할 수 없으며, 사용자가 검색할 때 포스처 페이지로 리디렉션되면 에이전트가 자동으로 설치되도록 할 수 없습니다(프록시 포트를 사용하며 일반 스위치는 여러 포트에서 리디렉션할 수 없음).

NAC Agent에서 검색 호스트 구성

특히 ISE 버전 1.2 이후에는 NAC Agent에서 수행하는 작업과 수행하지 않는 작업에 대한 전문 지식이 없는 경우 NAC Agent에서 검색 호스트를 구성하지 않는 것이 좋습니다.NAC 에이전트는 HTTP 검색을 통해 클라이언트 디바이스를 인증한 ISE 노드를 검색해야 합니다.검색 호스트에 의존하는 경우, NAC Agent가 디바이스를 인증한 노드 이외의 다른 ISE 노드에 연결하도록 할 수 있으며 이는 작동하지 않습니다.ISE 버전 1.2는 NAC 에이전트가 리디렉션 URL에서 세션 ID를 가져오도록 하기 때문에 검색 호스트 프로세스를 통해 노드를 검색하는 에이전트를 거부하므로 이 방법은 사용하지 않습니다.

경우에 따라 검색 호스트를 구성할 수도 있습니다.그런 다음 리디렉션 ACL에 의해 리디렉션되는 IP 주소(존재하지 않는 경우에도)로 구성해야 하며 클라이언트와 동일한 서브넷에 있으면 안 됩니다(그렇지 않으면 클라이언트가 ARP를 무기한 수행하고 HTTP 검색 패킷을 전송하지 않음).

NAC Agent가 때때로 팝업되지 않음

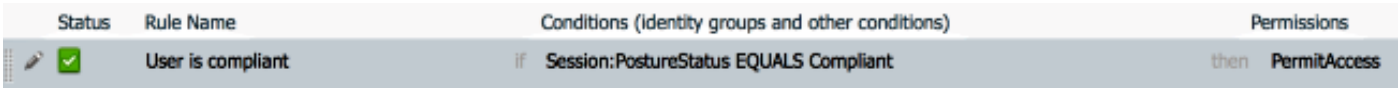
문제가 더 간헐적으로 발생하고 케이블/wifi 연결을 분리/재생하는 등의 작업이 작동하게 되면 더 미묘한 문제가 됩니다.RADIUS 어카운팅에 의해 세션 ID가 ISE에서 삭제되는 RADIUS 세션 ID에 문제가 있을 수 있습니다(변경 사항이 있는지 확인하기 위해 어카운팅 비활성화).

ISE 버전 1.2를 사용하는 경우, 클라이언트가 브라우저 또는 NAC 에이전트에서 나오지 않도록 많은 HTTP 패킷을 전송할 수도 있습니다.ISE 버전 1.2는 HTTP 패킷의 사용자 에이전트 필드를 스캔하여 NAC 에이전트나 브라우저에서 오는지 확인하지만, 다른 많은 애플리케이션은 사용자 에이전트 필드로 HTTP 트래픽을 전송하며 운영 체제나 유용한 정보는 언급하지 않습니다.그런 다음 ISE 버전 1.2에서 Change of Authorization(권한 부여 변경)을 보내 클라이언트 연결을 끊습니다.ISE 버전 1.3은 다른 방식으로 작동하므로 이 문제의 영향을 받지 않습니다.이 솔루션은 버전 1.3으로 업그레이드하거나 리디렉션 ACL에서 탐지된 모든 애플리케이션이 ISE로 리디렉션되지 않도록 하는 것입니다.

역방향 문제:상담원이 반복적으로 팝업됨

반대 문제가 발생할 수 있습니다. 상담원이 팝업하고 상태 분석을 수행하고 클라이언트를 검증한 다음 네트워크 연결을 허용하고 무음 상태를 유지하는 대신 잠시 후에 다시 팝업됩니다.이는 포스처가 성공한 후에도 HTTP 트래픽이 ISE의 CPP 포털로 여전히 리디렉션되기 때문에 발생합니다

.그런 다음 ISE 권한 부여 정책을 통해 CPP 리디렉션이 아닌 호환 클라이언트를 볼 때 허용 액세스(또는 가능한 ACL 및 VLAN이 있는 유사 규칙)를 전송하는 규칙이 있는지 확인하는 것이 좋습니다.



관련 정보

- Cisco ISE 컨피그레이션 가이드의 포스처 서비스
- ISE용 NAC Agent 검색 프로세스
- Catalyst 3750 Series 스위치의 ISE 트래픽 리디렉션
- 기술 지원 및 문서 – Cisco Systems