A versão 4.0 de AnyConnect e da postura NAC agente não estalam acima no ISE pesquisam defeitos o guia

Índice

Introdução

O Identity Services Engine (ISE) fornece as capacidades posturing que exigem o uso do agente do Network Admission Control (NAC) (para Microsoft Windows, Macintosh, ou através de webagent) ou da versão 4.0 de AnyConnect. O módulo da postura da versão 4.0 ISE de AnyConnect funciona exatamente como o agente NAC e é referido consequentemente como o agente NAC neste documento. A maioria de sintoma comum da falha da postura para um cliente é que o agente NAC não estala acima desde que uma encenação de trabalho faz com sempre que a janela de agente NAC estale acima e analise seu PC. Este documento ajuda-o a reduzir para baixo muitas causas que podem conduzir a postura para falhar, que significa que o agente NAC não estala acima. Não se significa ser exaustivo porque os logs do agente NAC podem somente ser descodificados pelo centro de assistência técnica da Cisco (TAC) e as causas de raiz possíveis são numerosas; contudo aponta esclarecer a situação e localizar mais o problema do que simplesmente “o agente não estala acima com a análise da postura” e o ajudará provavelmente a resolver a maioria de causas comum.

Pré-requisitos

Requisitos

As encenações, os sintomas, e as etapas alistadas neste documento estão escritos para que você pesquise defeitos edições depois que a instalação inicial é terminada já. Para a configuração inicial, refira serviços da postura no manual de configuração de Cisco ISE no cisco.com.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ISE Version1.2.x
- Agente NAC para a versão 4.9.x ISE
- Versão 4.0 de AnyConnect

> Nota: A informação deve igualmente ser aplicável a outras liberações do ISE a menos que os Release Note indicarem mudanças comportáveis principais.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Metodologia de Troubleshooting

Que faz o agente estalar acima?

O agente estala acima quando descobre um nó ISE. Se o agente detecta que não tem o acesso de rede completo e está em uma encenação da reorientação da postura, procura constantemente um nó ISE.

Há um documento do cisco.com que explique os detalhes do processo de descoberta do agente: Processo de descoberta do agente do Network Admission Control (NAC) para o Identity Services Engine. A fim evitar a duplicação satisfeita, este documento discute somente o ponto chave.

Quando um cliente conecta, submete-se a uma autenticação RADIUS (MAC que filtra ou 802.1x) na extremidade de que, ISE retorna o Access Control List da reorientação (ACL) e a reorientação URL ao dispositivo de rede (interruptor, ferramenta de segurança adaptável (ASA), ou controlador wireless) a fim restringir o tráfego do cliente para permitir somente que obtenha definições de um endereço IP de Um ou Mais Servidores Cisco ICM NT e do Domain Name Server (DNS). Todo o tráfego de HTTP que vem do cliente é reorientado a uma URL original no ISE que termina com CPP (postura e abastecimento do cliente), exceto o tráfego destinado ao portal próprio ISE. O agente NAC envia um pacote regular HTTP GET ao gateway padrão. Se o agente recebe a sem resposta ou a qualquer outro resposta do que uma reorientação CPP, considera-se ter a conectividade direta e não se continua com posturing. Se recebe uma resposta HTTP que seja uma reorientação a um CPP URL na extremidade de um nó específico ISE, a seguir continua o processo e os contatos da postura esse nó ISE. Estala somente acima e começa a análise quando recebe com sucesso os detalhes da postura desse nó ISE.

O agente NAC igualmente alcança para fora ao endereço IP de Um ou Mais Servidores Cisco ICM NT configurado do host da descoberta (não espera mais de um ser configurado). Espera ser reorientado lá também a fim obter a reorientação URL com o ID de sessão. Se o endereço IP de Um ou Mais Servidores Cisco ICM NT da descoberta é um nó ISE, a seguir não leva a cabo porque espera para ser reorientado a fim obter o ID de sessão direito. O host da descoberta não é

precisado assim geralmente, mas pode ser útil quando ajustado porque todo o endereço IP de Um ou Mais Servidores Cisco ICM NT na escala da reorientação ACL a fim provocar uma reorientação (como em cenários VPN, por exemplo).

Possíveis causas

A reorientação não acontece

Esta é a maioria de causa comum por muito. A fim validar ou invalidar, abrem um navegador no PC onde o agente não estala acima e vê se você está reorientado à página da transferência do agente da postura quando você datilografa toda a URL. Você pode igualmente datilografar um endereço IP de Um ou Mais Servidores Cisco ICM NT aleatório tal como http://1.2.3.4 a fim evitar uma edição possível DNS (se um endereço IP de Um ou Mais Servidores Cisco ICM NT reorienta mas um nome do Web site não faz, você pode olhar o DNS).

Se você obtém reorientado, você deve recolher o pacote dos logs do agente e do apoio ISE (com o módulo da postura e do suíço para debugar o modo) e contactar o tac Cisco. Isto indica que o agente descobre um nó ISE mas algo durante o processo não obtém os dados da postura.

Se nenhuma reorientação acontece, você tem sua primeira causa, que ainda exige investigações adicionais da causa de raiz. Um bom começo é verificar a configuração no dispositivo do acesso de rede (controlador do Wireless LAN (WLC) ou interruptor) e mover-se para o artigo seguinte neste documento.

Os atributos não são instalados no dispositivo de rede

Esta edição é um subcase da **reorientação não acontece** encenação. Se a reorientação não acontece, a primeira coisa é verificar (porque o problema ocorre em um cliente dado) que o cliente está colocado corretamente no estado direito pela camada do interruptor ou do acesso Wireless.

Estão aqui as saídas de exemplo do **comando detail do number> do <interface da relação da acesso-sessão da mostra** (você pôde ter que adicionar o **detalhe na** extremidade em algumas Plataformas) tomado no interruptor onde o cliente é conectado. Você deve verificar que o estado é de “sucesso Authz”, que a URL reorienta o ACL corretamente aponta ao pretendido reorientam o ACL, e que a URL reorienta pontos ao nó previsto ISE com o **CPP no** fim da URL. O campo ACS ACL não é imperativo porque mostra somente se você configurou uma lista de acessos carregável no perfil da autorização no ISE. É, contudo, importante olhá-lo e verificar que não há nenhum conflito com a reorientação ACL (veja documentos sobre a configuração da postura em caso da dúvida).

```
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
```

A fim pesquisar defeitos um WLC que execute AireOS, inscreva o **detalhe < MAC address > do cliente Wireless da mostra** e incorpore o **detalhe < do MAC address > do endereço MAC do cliente Wireless da mostra** a fim pesquisar defeitos um WLC que execute o Cisco IOS XE. As exibições de dados e você similares devem verificar a reorientação URL e ACL e se o cliente está no estado “POSTURE_REQD” ou similar (ele variam segundo a versão de software).

Se os atributos não estão atuais, você deve abrir os detalhes da autenticação no ISE do cliente que você pesquisava defeitos (navegue às **operações > às autenticações**) e verificar na seção do resultado que os atributos da reorientação estiveram enviados. Se não foram enviados, você deve rever a política da autorização a fim compreender porque os atributos não foram retornados para este cliente específico. Provavelmente uma das circunstâncias não combinou, assim que é uma boa ideia pesquisá-las defeitos um por um.

Recorde que, com respeito à reorientação ACL, o ® do Cisco IOS reorienta em indicações da licença (assim que nos endereços IP de Um ou Mais Servidores Cisco ICM NT ISE e DNS precise de ser negado) quando AireOS no WLC reorientar em instruções de negação (assim que nele está permitido para o ISE e o DNS).

Os atributos são no lugar mas o dispositivo de rede não reorienta

A causa principal é neste caso um problema de configuração. Você deve rever a configuração do dispositivo de rede contra o manual de configuração e os exemplos de configuração no cisco.com. Se este é o caso, o problema existe tipicamente durante todo todas as portas ou Access point (AP) do dispositivo de rede. Se não, o problema pôde somente ocorrer em alguns switchports ou em alguns AP. Se este é o caso, você deve comparar a configuração daqueles onde o problema ocorre comparado às portas ou aos AP onde a postura trabalha muito bem.

FlexConnect AP é sensível porque podem cada um ter uma configuração exclusiva e é fácil fazer um erro em um ACL ou em um VLAN em alguns AP e não outro.

Um outro problema comum é que o cliente VLAN não tem um SVI. Isto aplica-se somente ao Switches e é discutido em detalhe na reorientação do tráfego ISE no Catalyst 3750 Series Switch. Tudo pôde olhar bom da perspectiva dos atributos.

Lista de acesso carregável de interferência (DACL)

Se, ao mesmo tempo que os atributos da reorientação, você empurram um DACL de volta ao interruptor (ou o Airespace-ACL para um controlador wireless), a seguir poderia obstruir sua reorientação. O DACL é aplicado primeiramente e determina o que são deixadas cair completamente e o que vai sobre ser processado. Então a reorientação ACL é aplicada e

determina o que é reorientado.

O que isto significa concretamente é aquele na maioria das vezes, você quererá permitir todo o tráfego HTTP e HTTPS em seu DACL. Se você o obstrui, não estará reorientado desde que será deixado cair antes isso. Não é um interesse de segurança, porque esse tráfego será reorientado na maior parte na reorientação ACL após, assim que não é permitido realmente na rede; contudo, você precisa de permitir aqueles dois tipos de tráfego no DACL para que tenha uma possibilidade bater a reorientação ACL mesmo após.

Versão de agente ruim NAC

Éfácil esquecer que as versões de agente específicas NAC estão validadas contra versões específicas do ISE. Muitos administradores promovem seu conjunto ISE e esquecem-no transferir arquivos pela rede a versão de agente relacionada NAC no base de dados dos resultados do abastecimento do cliente.

Se você usa uma versão de agente antiquada NAC para seu código ISE, esteja ciente que pôde trabalhar mas igualmente não pôde. Assim não é nenhuma surpresa que alguns clientes trabalham e outro não fazem. Uma maneira de verificar é ir à seção da transferência do cisco.com de sua versão ISE e a verificação que as versões de agente NAC são lá. Tipicamente há diversos apoiados para cada versão ISE. Este página da web recolhe todas as matrizes: Informação de compatibilidade de Cisco ISE.

O proxy da Web HTTP está no uso por clientes

O conceito de um proxy da Web HTTP é que os clientes não resolvem os endereços IP de Um ou Mais Servidores Cisco ICM NT eles mesmos do Web site DNS nem contactam os Web site diretamente; um pouco, enviam simplesmente seu pedido ao servidor proxy, que toma dele. O problema típico com uma configuração comum é que o cliente resolve um Web site (tal como www.cisco.com) diretamente enviando o HTTP GET para ele ao proxy, que obtém interceptado e reorientado legalmente ao portal ISE. Contudo, em vez então de enviar o HTTP seguinte GET ao endereço IP de Um ou Mais Servidores Cisco ICM NT portal ISE, o cliente continua a enviar esse pedido ao proxy.

Caso que você decide não reorientar o tráfego de HTTP destinado ao proxy, seus usuários têm de acesso direto aos Internet inteira (desde que todo o tráfego atravessa o proxy) sem autenticar ou posturing. A solução é alterar as configurações do navegador dos clientes e adicionar realmente uma exceção para o endereço IP de Um ou Mais Servidores Cisco ICM NT ISE nos ajustes do proxy. Esta maneira, quando o cliente tem que alcançar o ISE, envia o pedido diretamente ao ISE e não ao proxy. Isto evita o loop infinito aonde o cliente obtém constantemente reorientado mas nunca vê a página de login.

Note que o agente NAC não está afetado pelos ajustes do proxy incorporados ao sistema e continua a atuar normalmente. Isto significa que se você usa um proxy da Web, você não pode ter o funcionamento da descoberta do agente NAC (porque usa a porta 80) e para mandar usuários auto-instalar o agente estão reorientados uma vez que à página da postura quando consultam (desde que esse usa a porta de proxy e o Switches típico não pode reorientar em portas múltiplas).

Os anfitriões da descoberta são configurados no agente NAC

Especialmente após a versão 1.2 ISE, recomenda-se não configurar nenhum host da descoberta no agente NAC a menos que você tiver a experiência no que faz e não faz. O agente NAC é suposto descobrir o nó ISE que autenticou o dispositivo do cliente com a descoberta HTTP. Se você confia em anfitriões da descoberta, você pôde mandar o agente NAC contactar um outro nó ISE do que esse que autenticaram o dispositivo e que não trabalha. A versão 1.2 ISE rejeita um agente que descubra o nó com o processo do host da descoberta porque quer o agente NAC obter o ID de sessão da reorientação URL, assim que este método é desanimado.

Em alguns casos, você pôde querer configurar um host da descoberta. Então deve ser configurado com todo o endereço IP de Um ou Mais Servidores Cisco ICM NT (mesmo se não-existente) que seja reorientado pela reorientação ACL, e não deve idealmente estar na mesma sub-rede como o cliente (se não o cliente ARP indefinidamente para ele e para enviar nunca o pacote de descoberta HTTP).

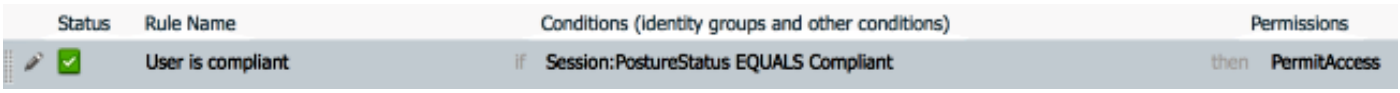
O agente NAC não estala acima às vezes

Quando a edição é mais intermitente e as ações tais como a desconexão/que replugging a Conectividade do cabo/wifi a fazem trabalhar, é um problema mais sutil. Poderia ser um problema com os ID de sessão do RAIO onde o ID de sessão é suprimido no ISE pela contabilidade do RAIO (desabilitação que explica para ver se muda algo).

Se você usa ISE Version1.2, uma outra possibilidade é que o cliente envia muitos pacotes de HTTP de modo que nenhuns venham de um navegador ou do agente NAC. A versão 1.2 ISE faz a varredura do campo do agente de usuário em uns pacotes de HTTP para considerar se vem do agente NAC ou de um navegador, mas muitos outros aplicativos enviam o tráfego de HTTP com um campo do agente de usuário e não mencionam nenhuma sistema operacional ou informação util. A versão 1.2 ISE envia então uma mudança da autorização desligar o cliente. A versão 1.3 ISE não é afetada por este beause que da edição trabalha em uma maneira diferente. A solução é promover à versão 1.3 ou permitir todos os aplicativos detectados na reorientação ACL de modo que não sejam reorientados para o ISE.

Inverta o problema: O agente estala acima repetidamente

O problema oposto pode elevarar onde o agente estala acima, faz a análise da postura, valida o cliente, e estala então acima outra vez shortly after em vez de permitir a conectividade de rede e de ficar silencioso. Isto acontece porque, mesmo depois uma postura bem sucedida, o tráfego de HTTP é reorientado ainda ao portal CPP no ISE. É uma boa ideia atravessar a política da autorização ISE e certificar-se de então você tenha uma regra que envie um acesso da licença (ou a regra similar com ACL e os VLAN possíveis) quando considera um cliente complacente e NÃO uma reorientação CPP outra vez.



Informações Relacionadas

- Serviços da postura no manual de configuração de Cisco ISE
- Processo de descoberta do agente NAC para o ISE
- Reorientação do tráfego ISE no Catalyst 3750 Series Switch
- Suporte Técnico e Documentação - Cisco Systems