AnyConnect Version 4.0 and NAC Posture Agent Does Not Pop Up on ISE Troubleshoot Guide

Contents

Introduction

Identity Services Engine (ISE) provides posturing capabilities that require the use of the Network Admission Control (NAC) agent (for Microsoft Windows, Macintosh, or via webagent) or AnyConnect Version 4.0. The AnyConnect Version 4.0 ISE posture module works exactly like the NAC agent and is therefore referred to as the NAC agent in this document. The most common symptom of posture failure for a client is that the NAC agent does not pop up since a working scenario always causes the NAC agent window to pop up and analyze your PC. This document helps you narrow down the many causes that can lead the posture to fail, which means the NAC agent does not pop up. It is not meant to be exhaustive because the NAC agent logs can only be decoded by the Cisco Technical Assistance Center (TAC) and the possible root causes are numerous; however it aims to clarify the situation and pinpoint the problem further than simply "the agent does not pop up with the posture analysis" and will probably help you solve the most common causes.

Prerequisites

Requirements

The scenarios, symptoms, and steps listed in this document are written for you to troubleshoot

issues after the initial setup is already completed. For the initial configuration, refer to Posture Services on the Cisco ISE Configuration Guide on Cisco.com.

Components Used

The information in this document is based on these software and hardware versions:

- ISE Version1.2.x
- NAC Agent for ISE Version 4.9.x
- AnyConnect Version 4.0

> **Note**: The information should also be applicable to other releases of ISE unless the release notes indicate major behavioral changes.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Troubleshooting Methodology

What makes the agent pop up?

The agent pops up when it discovers an ISE node. If the agent senses that it does not have full network access and is in a posture redirection scenario, it constantly looks for an ISE node.

There is a Cisco.com document that explains the details of the agent discovery process: Network Admission Control (NAC) Agent Discovery Process for Identity Services Engine. In order to avoid content duplication, this document only discusses the key point.

When a client connects, it undergoes a RADIUS authentication (MAC filtering or 802.1x) at the end of which, ISE returns the redirection Access Control List (ACL) and the redirection URL to the network device (switch, Adaptive Security Appliance (ASA), or Wireless controller) in order to restrict the client traffic to only allow it to obtain an IP address and Domain Name Server (DNS) resolutions. All HTTP(S) traffic that comes from the client is redirected to a unique URL on ISE that ends with CPP (Client Posture and Provisioning), except traffic destined to the ISE portal itself. The NAC agent sends a regular HTTP GET packet to the default gateway. If the agent receives no answer or any other answer than a CPP redirection, it considers itself to have full connectivity and does not proceed with posturing. If it receives an HTTP response that is a redirection to a CPP URL at the end of a specific ISE node, then it continues the posture process and contacts that ISE node. It only pops up and starts the analysis when it successfully receives the posture details from that ISE node.

The NAC agent also reaches out to the configured discovery host IP address (it does not expect more than one to be configured). It expects to be redirected there as well in order to get the redirection URL with the session ID. If the discovery IP address is an ISE node, then it does not pursue because it waits to be redirected in order to get the right session ID. So the discovery host is usually not needed, but can be useful when set as any IP address in the range of the redirect ACL in order to trigger a redirection (like in VPN scenarios, for example).

Possible Causes

Redirection Does Not Happen

This is the most common cause by far. In order to validate or invalidate, open a browser on the PC where the agent does not pop up and see if you are redirected to the posture agent download page when you type any URL. You can also type a random IP address such as **http://1.2.3.4** in order to avoid a possible DNS issue (if an IP address redirects but a website name does not, you can look at DNS).

If you get redirected, you should collect the agent logs and ISE support bundle (with the posture and swiss module to debug mode) and contact Cisco TAC. This indicates that the agent discovers an ISE node but something fails during the process to obtain the posture data.

If no redirection happens, you have your first cause, which still requires further investigation of the root cause. A good start is to check the configuration on the network access device (Wireless LAN Controller (WLC) or switch) and move to the next item in this document.

Attributes Are Not Installed on the Network Device

This issue is a subcase of the **Redirection Does Not Happen** scenario. If the redirection does not happen, the first thing is to verify (as the problem occurs on a given client) that the client is correctly placed in the right status by the switch or wireless access layer.

Here is example output of the **show access-session interface <interface number> detail** command (you might have to add **detail** at the end on some platforms) taken on the switch where the client is connected. You must verify that the status is "Authz success", that the URL redirect ACL correctly points to the intended redirect ACL, and that the URL redirect points to the expected ISE node with **CPP** at the end of the URL. The ACS ACL field is not mandatory because it only shows if you configured a downloadable access list on the authorization profile on ISE. It is, however, important to look at it and verify that there is no conflict with the redirect ACL (see documents about posture configuration in case of doubt).

```
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
```

In order to troubleshoot a WLC that runs AireOS, enter **show wireless client detail <mac address>** and enter **show wireless client mac-address <mac address> detail** in order to troubleshoot a WLC that runs Cisco IOS-XE. Similar data displays and you must verify the redirect URL and ACL and if the client is in "POSTURE_REQD" state or similar (it varies depending on the software version).

If attributes are not present, you must open the authentication details in the ISE of the client you were troubleshooting (navigate to **Operations > Authentications**) and verify in the Result section that the redirection attributes were sent. If they were not sent, you should review the authorization policy in order to understand why the attributes were not returned for this particular client. Probably one of the conditions did not match, so it is a good idea to troubleshoot them one by one.

Remember that, in regards to the redirect ACL, Cisco IOS® redirects on permit statements (so the ISE and DNS IP addresses need to be denied) while AireOS on the WLC redirects on deny statements (so it is permitted for ISE and DNS).

Attributes Are in Place But Network Device Does Not Redirect

The major cause in this case is a configuration issue. You should review the configuration of the network device against the configuration guide and configuration examples on Cisco.com. If this is the case, the problem typically exists throughout all ports or access points (APs) of the network device. If not, the problem might only occur on some switchports or some APs. If this is the case, you should compare the configuration of those where the problem occurs compared to the ports or APs where the posture works fine.

FlexConnect APs are sensitive because they can each have a unique configuration and it is easy to make a mistake in an ACL or a VLAN in some APs and not others.

Another common problem is that the client VLAN does not have an SVI. This only applies to switches and is discussed in detail in ISE Traffic Redirection on the Catalyst 3750 Series Switch. Everything might look good from the attributes perspective.

Interfering Downloadable Access-list (DACL)

If, at the same time as redirection attributes, you push a DACL back to the switch (or Airespace-ACL for a wireless controller), then it could block your redirection. The DACL is applied first and determines what is completely dropped and what goes on to be processed. Then the redirect ACL is applied and determines what is redirected.

What this concretely means is that most of the time, you will want to permit all HTTP and HTTPS traffic in your DACL. If you block it, it will not be redirected since it will be dropped before that. It is not a security concern, because that traffic will be redirected mostly on the redirect ACL after, so it is not really allowed on the network; however, you need to permit those two types of traffic in the DACL in order for them to have a chance to hit the redirect ACL right after.

Bad NAC Agent Version

It is easy to forget that specific NAC agent versions are validated against specific versions of ISE. Many administrators upgrade their ISE cluster and forget to upload the related NAC agent version

in the client provisioning results database.

If you use an outdated NAC agent version for your ISE code, be aware that it might work but it also might not. So it is no surprise that some clients work and others do not. One way to verify is to go to the Cisco.com download section of your ISE version and check which NAC agent versions are there. Typically there are several supported for each ISE version. This web page gathers all matrixes: Cisco ISE Compatibility Information.

HTTP Web Proxy Is in Use by Clients

The concept of an HTTP web proxy is that clients do not resolve website DNS IP addresses themselves nor contact the websites directly; rather, they simply send their request to the proxy server, which takes care of it. The typical problem with a usual configuration is that the client resolves a website (such as www.cisco.com) by directly sending the HTTP GET for it to the proxy, which gets intercepted and rightfully redirected to the ISE portal. However, instead of then sending the next HTTP GET to the ISE portal IP address, the client continues to send that request to the proxy.

In case you decide to not redirect HTTP traffic destined to the proxy, your users have direct access to the whole Internet (since all traffic goes through the proxy) without authenticating or posturing. The solution is to actually modify the clients' browser settings and to add an exception for the ISE IP address in the proxy settings. This way, when the client has to reach ISE, it sends the request directly to the ISE and not to the proxy. This avoids the infinite loop where the client constantly gets redirected but never sees the login page.

Note that the NAC agent is not affected by the proxy settings entered in the system and it continues to act normally. This means that if you use a web proxy, you cannot both have the NAC agent discovery working (because it uses port 80) and have users self-install the agent once they are redirected to the posture page when they browse (since that uses the proxy port and typical switches cannot redirect on multiple ports).

Discovery Hosts Are Configured in the NAC Agent

Especially after ISE Version 1.2, it is recommended to not configure any discovery host on the NAC agent unless you have expertise on what it does and does not do. The NAC agent is supposed to discover the ISE node that authenticated the client device through HTTP discovery. If you rely on discovery hosts, you might have the NAC agent contact another ISE node than the one that authenticated the device and that does not work. ISE Version 1.2 rejects an agent that discovers the node through the discovery host process because it wants the NAC agent to get the session ID from the redirect URL, so this method is discouraged.

In some cases, you might want to configure a discovery host. Then it should be configured with any IP address (even if non-existing) that will be redirected by the redirect ACL, and it should ideally not be in the same subnet as the client (otherwise the client will ARP indefinitely for it and never send the HTTP discovery packet).

NAC Agent Does Not Pop Up Sometimes

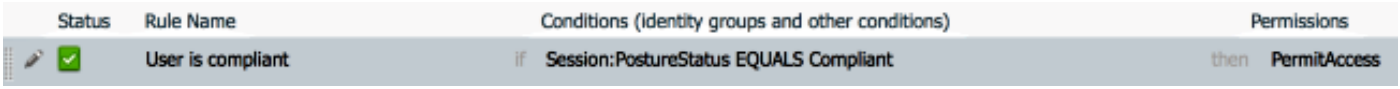
When the issue is more intermittent and actions such as unplugging/replugging the cable/wifi connectivity make it work, it is a more subtle problem. It could be a problem with the RADIUS session IDs where the session ID is deleted on the ISE by RADIUS accounting (disable

accounting to see if it changes something).

If you use ISE Version1.2, another possibility is that the client sends many HTTP packets so that none come from a browser or the NAC agent. ISE Version 1.2 scans the user-agent field in HTTP packets to see if it comes from the NAC agent or a browser, but many other applications send HTTP traffic with a user-agent field and do not mention any operating system or useful information. ISE Version 1.2 then sends a Change of Authorization to disconnect the client. ISE Version 1.3 is not affected by this issue beause it works in a different manner. The solution is either to upgrade to Version 1.3 or to allow all detected applications in the redirect ACL so that they are not redirected towards ISE.

Reverse Problem: Agent Pops Up Repeatedly

The opposite problem can arise where the agent pops up, does the posture analysis, validates the client, and then pops up again shortly after instead of allowing network connectivity and staying silent. This happens because, even after a successful posture, the HTTP traffic is still redirected to the CPP portal on ISE. It is a good idea to then go through the ISE authorization policy and check that you have a rule that sends a permit access (or similar rule with possible ACLs and VLANs) when it sees a compliant client and NOT a CPP redirection again.



Related Information

- **Posture Services on the Cisco ISE Configuration Guide**
- **NAC Agent Discovery Process for ISE**
- **ISE Traffic Redirection on the Catalyst 3750 Series Switch**
- **Technical Support & Documentation - Cisco Systems**