Troubleshoot Umbrella Insights AD Integration Not Detecting User Traffic

Contents

[Introduction](#)

[Overview](#)

[Explanation](#)

[Resolution](#)

Introduction

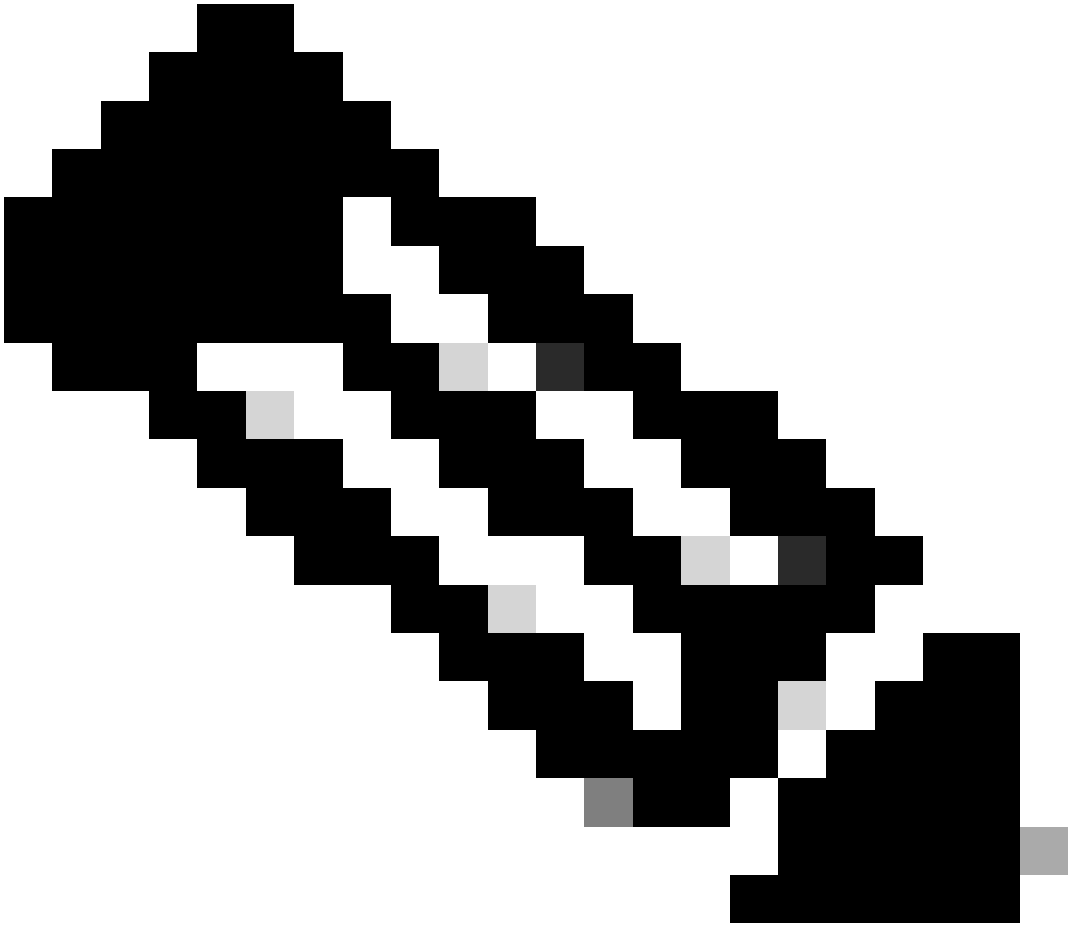
This document describes how to troubleshoot Umbrella Insights AD integration not detecting user traffic.

Overview

You have installed Umbrella Insights, Set up a connector and Virtual Appliances and registered your domain controllers. All your components are displayed as green and working in the dashboard under `deployments --> Sites and Active Directory` however, You have a policy configured to use AD users or group objects, but you are still not seeing user activity reported in the dashboard or policy being applied correctly.

You might also notice in this entry repeats in the file **OpenDNSAuditClient.log**

> `Last Event Received at 1970-01-01 00:00:00`



Note: The log file is located in *C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>*
VERSION = the actual installed version of the Connector service, such as *v1.1.22*

Explanation

The main reason why this happens is because audit logon events might not be configured in your Active Directory domain. The log message indicates that the connector has not seen one single user event since it was installed. Currently this is not something that generates an error in the dashboard.

Resolution

The main thing to to is check AD group policy for the correct Audit policy configuration:

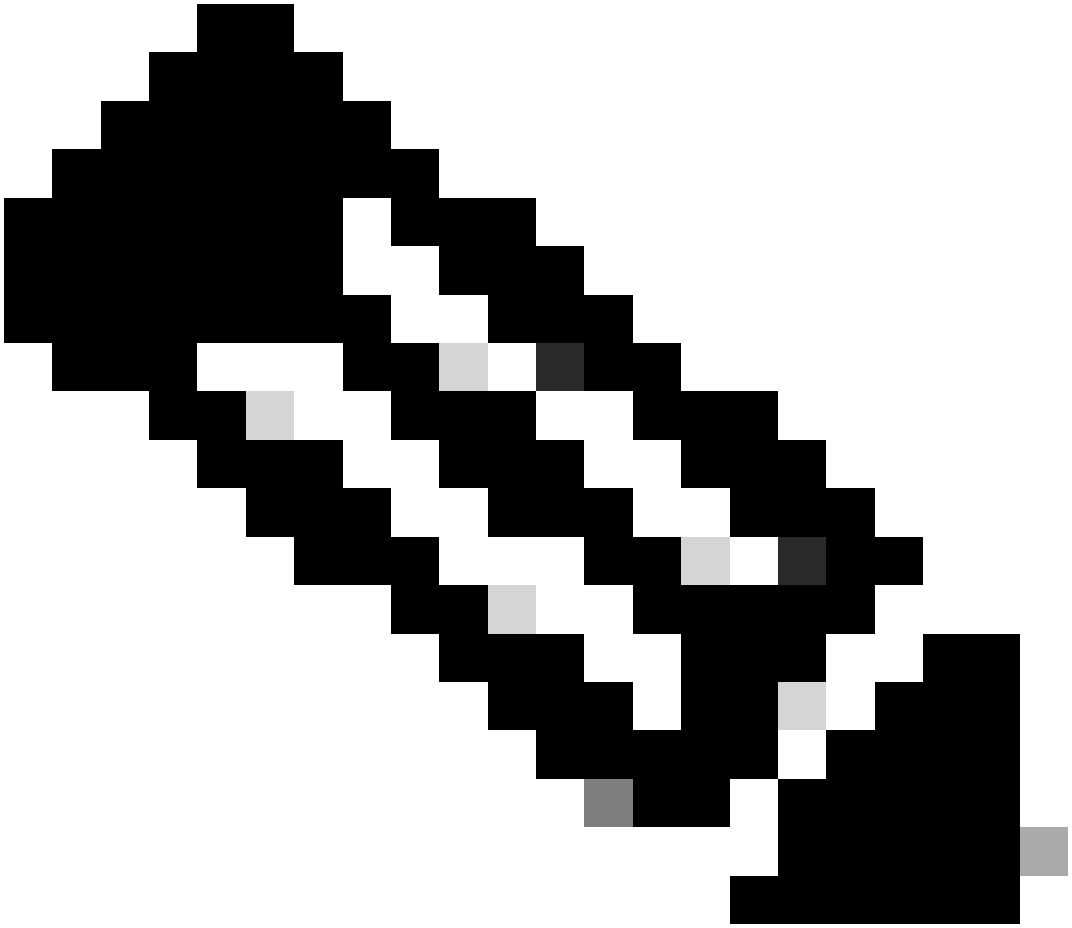
1. On the Domain Controller, open the `Group Policy Management panel located within *Administrative Tools*` and select a policy that applies to Domain Controllers (the Default Domain Controller Policy would be the likely candidate).

2. **Right-click** that policy and select **Edit** to bring up the `Group Policy Management Editor`.

3. Browse to the "`Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy`" folder and select **Audit logon events** to view its properties.

4. This policy must be to audit **Success** attempts.

5. Run the **gpupdate** command to apply the policy.



Note: There are cases where both the "Default Domain Controllers and the Default Domain Policy" might need to have that setting configured.
