Troubleshoot Active Directory Users Missing from the Activity Search Report in Umbrella

Contents

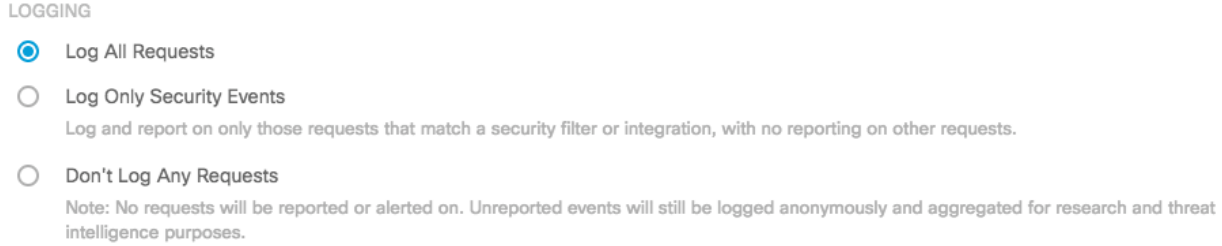
Introduction

This document describes the Activity Search Report in Cisco Umbrella. The Activity Search Report is a nearly live report of all the DNS queries your users are making. If you have set up the Cisco Umbrella Active Directory (AD) integration, you can expect to see your AD users populating the Identity column in your Activity Search. However, there are situations where the users are missing from the Identity column.

Resolution

If you think you should be seeing AD users directly in the Identity column in the Activity Search, but are not seeing them, or are seeing a few, but not as many as you expected, here are a few things to check:

1. Sites and Active Directory
    - Check all of your AD Components to make sure that there are no reported errors or issues. If you see any grey, orange, or red status indicators on any of the components, obtain these details and open a support ticket (umbrella-support@cisco.com).
        - Diagnostic Test from an affected user (a user that is not showing up in the Activity Search)
        - Screenshot of the Virtual Appliance (VA) Console, with any error messages expanded
        - AD Connector Audit Logs
2. Logging settings
    - In the Advanced Settings of every policy, there is a section at the bottom that concerns how much to log. You can set it to:
        - Log All Requests
        - Log Only Security Events
        - Do not Log Any Requests
    - If your policy is currently set to "Log Only Security Events", that can explain why you are not seeing as many queries as you expect, or no results at all from some users.



3. Correct policy precedence
    - If you have a policy applying to a Network Identity that is higher in the list of policies than your

AD user policy, the Network Identity policy is likely going to apply. This in turn means that on the Activity Search, you are going to see the Network as the reported Identity. Please check the Cisco Umbrella documentation on Best Practices and Policy Precedence as well.

Cause

Where does the Activity Search get the "Identity"?

When a DNS query comes into Umbrella, assuming your AD Integration is working as expected, this information is passed along in the query:

- Internal IP address
- AD Identity hash (user, host, or both)
- Egress IP
- Domain being queried

The AD Identity Hash is added to the query by the Virtual Appliance, who is passed that information, and the corresponding Internal IP address for the logon event from the AD Connector.

Cisco Umbrella then uses this information to find the organization and to determine which policy to apply. If you have no policies specifically applied to your AD users, but do have one for your Networks or Sites, then Cisco Umbrella applies the policy using that Identity. This means that when the query, identity, and response are reported in the Activity Search, **the Identity that triggered the policy that is reported.** The other information is still tagged in the request, so you can still search for an AD user and get the activity that reports a network as the Identity. Additionally, if you export the Activity Search data to a CSV file, it shows you all the identity information that is associated with the query.

Additional Information

If you are still not seeing any AD users, please reach out to Support (umbrella-support@cisco.com), with a diagnostic test result, and any AD Connector Audit Logs that are relevant.