Troubleshoot Umbrella Connector Blocking an Active Directory Service Account

Contents

Introduction

This document describes how to troubleshoot why an Active Directory Service Account is blocked by the Umbrella Connector.

Overview

The Umbrella Connector service makes WMI connections to the event logs of any registered domain controller (DC) that is part of the same Umbrella Site, in order to read logon event information. These logon events are then parsed and uploaded to all Virtual Appliances (VAs) at the same Umbrella Site. The VA then creates a temporary User-to-IP mapping for that username/source IP address. There are a couple of points worth noting:

- Umbrella Insights can only support one logged-on user per IP at a time
- The most recently processed logon event from a source IP 'wins'

As all logon events are equal, the connector has a hard coded list of common AD service accounts whose events are ignored. You can see logon events from these accounts picked up in the connector log file. For example:

> Event from blacklisted user ignored: OpenDNS_Connector

This is done to prevent service accounts, (which just like standard users generate logon events in the DC security event logs,) from overriding the User-to-IP mapping of the actual logged on user.

In large environments, depending on the process/application which a service account is used for, they can also generate thousands of logon events every minute. This is also additional load for the connector, which can manifest as a delay between user logon and the correct policy being applied, or a correct policy applied that is later lost.

List of Blocked Accounts

- _vmware_user_
- Administrator
- ANONYMOUS
- Anonymous Logon
- ASPNET
- Local Service

- McAfeeMVSUser
- MHControl
- Network Service
- netwrix
- OpenDNS_Connector
- peersyncsvc
- s-pcadmin
- SophosUpdateMgr
- SophosUpdMgr
- svc-altiris
- svc.iCreate

Further Information

You can also exclude any other AD account logon events from being processed by the connector. Please see this article for instructions:

https://support.umbrella.com/hc/en-us/articles/231266088

Additionally, there are AD groups that can be excluded from the connector's AD Sync, which is performed to populate the Dashboard policy area with a list of AD users, computers and groups. This can be found here:

https://support.umbrella.com/hc/en-us/articles/115005206526