Fehlerbehebung: Umbrella Insights AD-Integration erkennt Benutzerdatenverkehr nicht

Inhalt

Einleitung

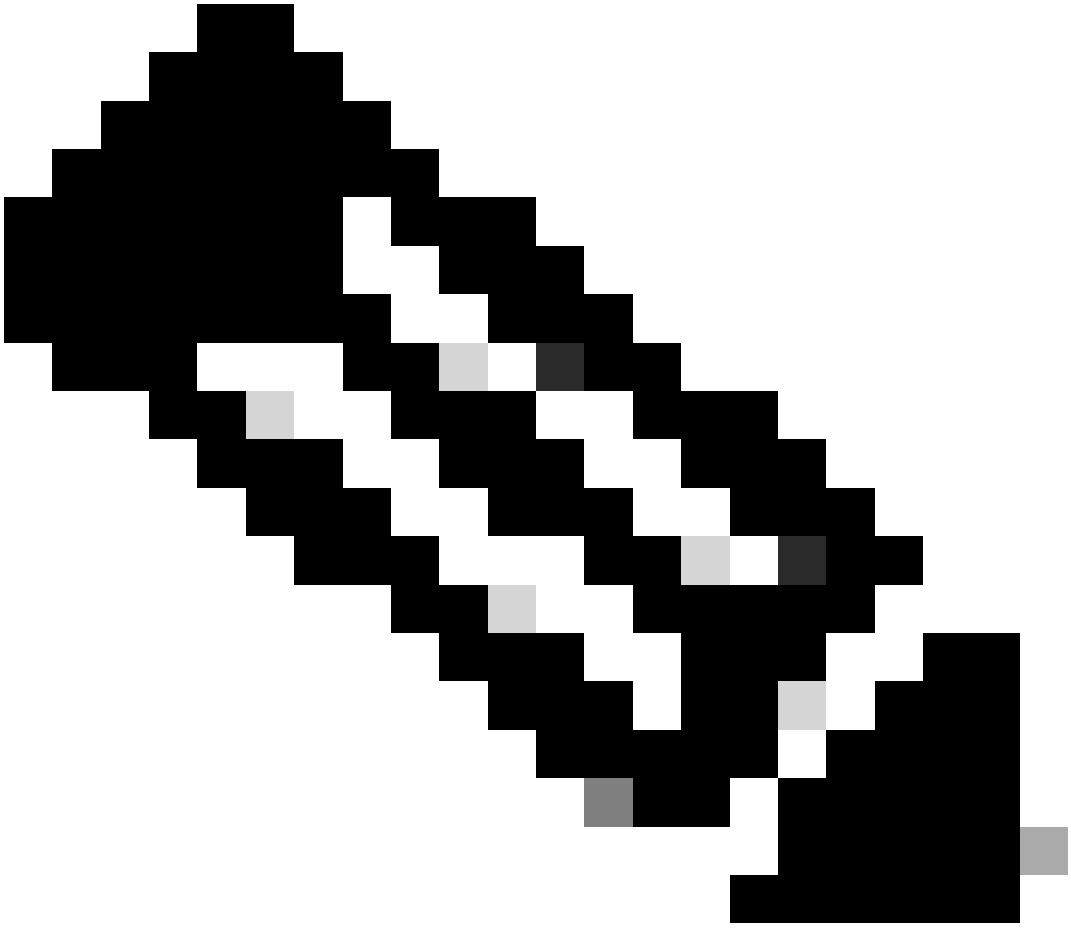
In diesem Dokument wird die Fehlerbehebung bei der AD-Integration von Umbrella Insights beschrieben, die Benutzerdatenverkehr nicht erkennt.

Überblick

Sie haben Umbrella Insights installiert, einen Connector und virtuelle Appliances eingerichtet und Ihre Domain-Controller registriert. Alle Komponenten werden grün dargestellt und funktionieren im Dashboard unter `Bereitstellungen -> Standorte und Active Directory`. Sie verfügen jedoch über eine Richtlinie, die für die Verwendung von AD-Benutzern oder Gruppenobjekten konfiguriert ist, sehen jedoch immer noch keine Benutzeraktivitäten, die im Dashboard oder in der Richtlinie richtig angewendet werden.

Sie können in diesem Eintrag auch in der Datei OpenDNSAuditClient.log Wiederholungen feststellen

`Letzte um 1970-01-01 00:00:00 Uhr empfangene Veranstaltung`



Anmerkung: Die Protokolldatei befindet sich unter C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\
VERSION = die tatsächlich installierte Version des Connector-Diensts, z. B. v1.1.22

Erläuterung

Der Hauptgrund dafür ist, dass Anmeldeversuche in der Active Directory-Domäne möglicherweise nicht konfiguriert sind. Die Protokollmeldung zeigt an, dass seit der Installation des Connectors kein einziges Benutzerereignis aufgetreten ist. Derzeit wird dadurch kein Fehler im Dashboard generiert.

Auflösung

Die Hauptaufgabe besteht darin, die AD-Gruppenrichtlinie auf die richtige Überwachungsrichtlinienkonfiguration zu überprüfen:

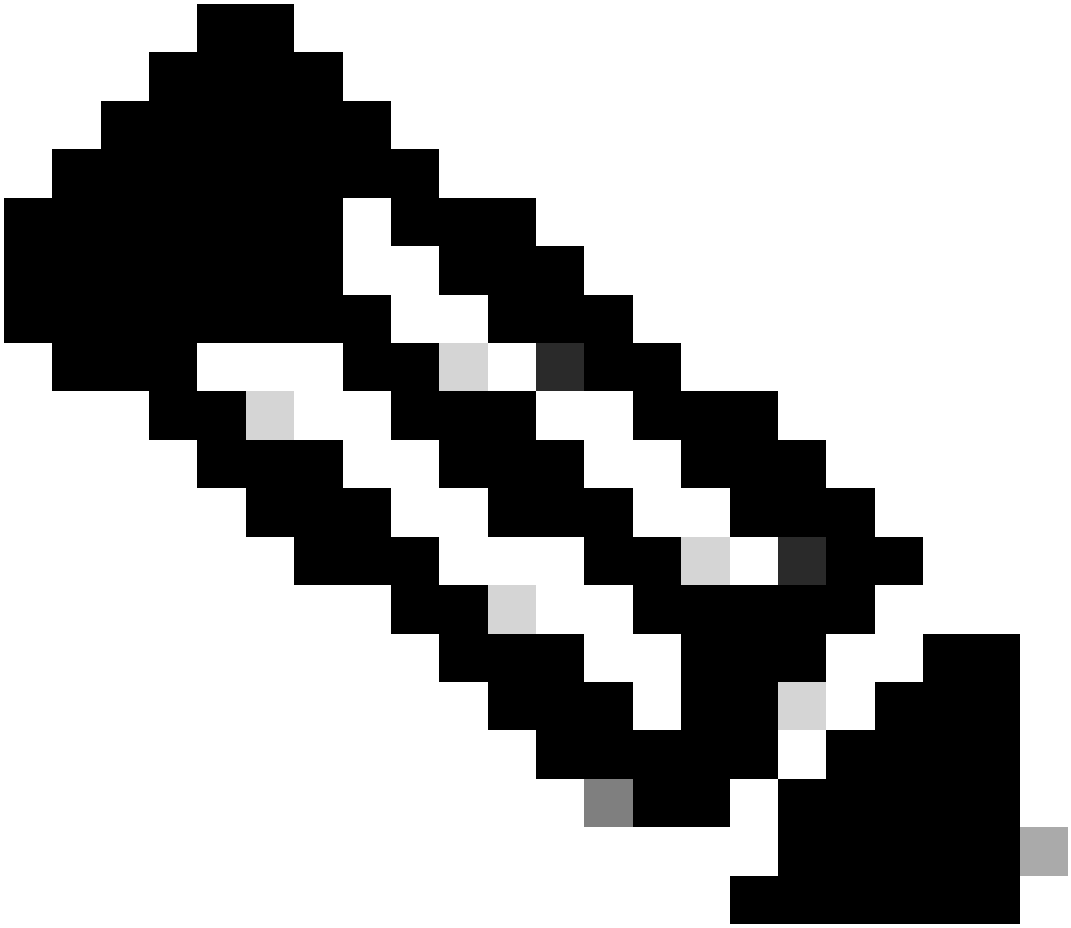
1. Öffnen Sie auf dem Domänencontroller den `Bereich Gruppenrichtlinienverwaltung unter Verwaltung,` und wählen Sie eine Richtlinie aus, die für Domänencontroller gilt (wahrscheinlich ist die Standard-Domänencontrollerrichtlinie).

2. Klicken Sie mit der rechten Maustaste auf diese Richtlinie, und wählen Sie Bearbeiten aus, um den `Gruppenrichtlinienverwaltungs-Editor` aufzurufen.

3. Navigieren Sie zum Ordner `"Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Überwachungsrichtlinie"`, und wählen Sie Anmeldeereignisse überwachen aus, um die Eigenschaften anzuzeigen.

4. Diese Richtlinie muss so ausgelegt sein, dass Erfolgsversuche überwacht werden.

5. Führen Sie den Befehl gpupdate aus, um die Richtlinie anzuwenden.



Anmerkung: Es gibt Fälle, in denen diese Einstellung sowohl für die Standard-Domänencontroller als auch für die Standard-Domänenrichtlinie konfiguriert werden muss.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.