Integration von Active Directory über VA oder CSC

Inhalt

Einleitung

In diesem Dokument werden zwei Methoden zur Integration von Active Directory (AD) in Umbrella beschrieben: Virtual Appliance (VA) oder Cisco Secure Client (CSC)

Voraussetzungen

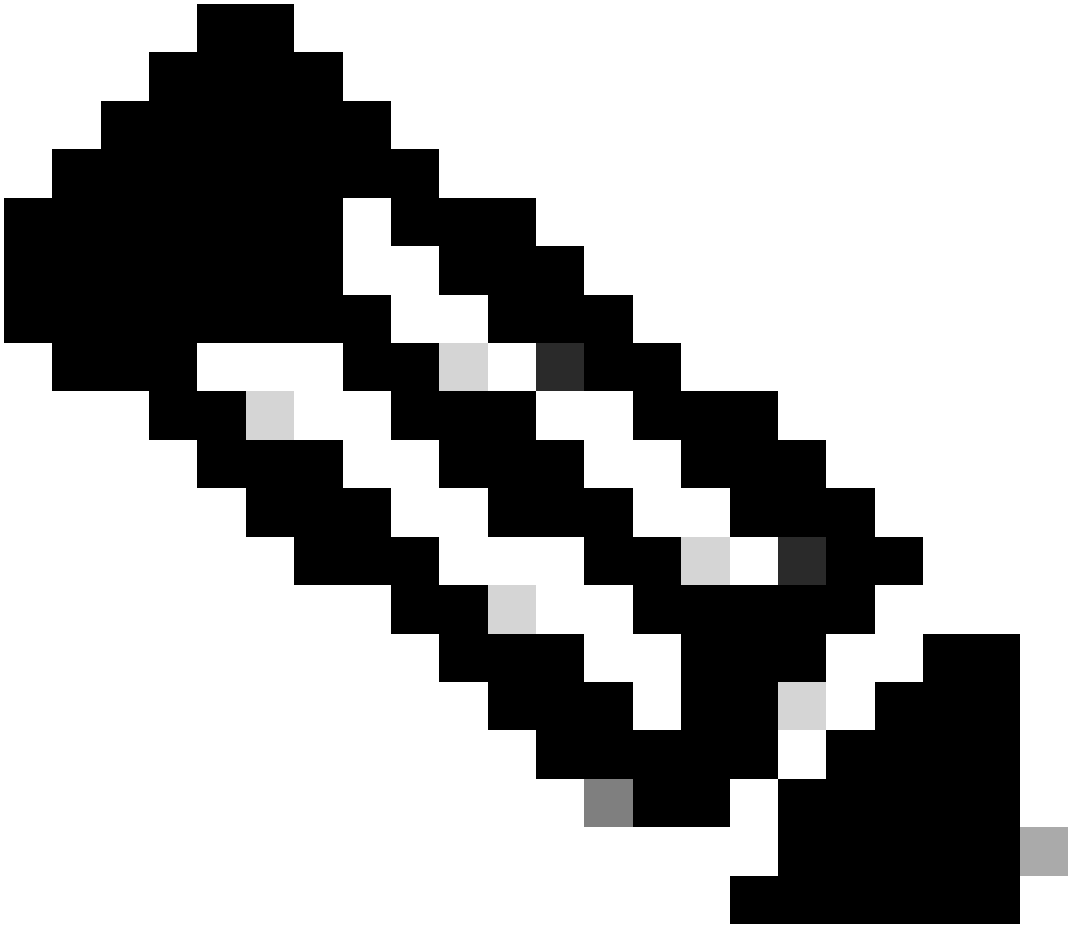
Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- AD-Anschluss: Synchronisiert die AD-Struktur einer einzelnen Active Directory-Domäne mit dem Dashboard. Für die VA-Implementierung werden außerdem die Anmeldeereignisse von den DCs am gleichen Umbrella-Standort aktiv mit den VAs synchronisiert. Der AD-Tree für die Organisation wird vom AD Connector mit der Umbrella-Cloud synchronisiert, wobei diese Daten aus dem registrierten DC abgerufen werden. Tree-Updates werden erkannt, und die Umbrella Cloud wird innerhalb weniger Stunden aktualisiert.
- Domänencontroller (AD-Server): Die DCs werden über das WSF-Skript für die Registrierungskonfiguration, das vom Dashboard heruntergeladen wird, im Dashboard registriert. Dadurch werden der Name, die Domäne und die interne IP dem Dashboard hinzugefügt, um dem Connector mitzuteilen, mit welchen IPs eine Synchronisierung erfolgen soll. Wenn Sie das Skript nicht ausführen können, ist auch eine manuelle Registrierung

möglich. Wenden Sie sich für weitere Informationen und Unterstützung an den Umbrella Support.

- Virtuelle Appliance: Der Umbrella DNS Forwarder vor Ort. Wendet (optional) AD-Identität im Netzwerk sowie interne IPs in Berichten an. Dadurch werden alle Roaming-Clients dahinter veranlasst, den DNS-Schutz zu deaktivieren und den Modus "Behind VA protection" (hinter VA-Schutz) zurückzustellen.
- Cisco Secure Client: Der Umbrella-Software-Service vor Ort, der DNS-Verschlüsselung sowie Benutzeridentifizierung für Windows und MacOS bietet. Wird auch als AnyConnect-Modul geliefert.



Anmerkung: Die Voraussetzungen für diese beiden Implementierungen sind sehr unterschiedlich. Vollständige Voraussetzungen finden Sie in der jeweiligen Implementierung.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

In diesem Artikel werden die beiden verschiedenen Methoden zur Integration von Active Directory in das Umbrella Dashboard erläutert und erläutert. Derzeit können AD-Benutzer über die Umbrella Virtual Appliances oder den Cisco Secure Client auf Richtlinien und Berichte angewendet werden.

Sichere Client-Implementierung

Anforderungen

- Ein AD-Anschluss
- Ein Rechenzentrum auf dem Dashboard
- Der Benutzer OpenDNS_Connector muss über die Berechtigung Schreibschutz für den Domänencontroller verfügen.
- Mindestversionen des Secure Client für den Standalone-Client (AnyConnect-Modul):
    - Windows: 2,1,0 (4,5,01044)
    - OSX: 2,0,39 (4,5,02033)

So funktioniert es

- Der aktuell angemeldete AD-Benutzer wird direkt am lokalen Computer durch den Roaming-Client ermittelt, der die lokale Registrierung liest.
- Unterstützt maximal einen gleichzeitig angemeldeten Benutzer auf der Workstation.
- Zwei gleichzeitige Benutzer können dazu führen, dass kein AD-Benutzer angewendet wird.
- Die AD-Benutzer-GUID und die interne IP-Adresse werden über EDNS0 im DNS-Proxy des Roaming-Clients an die DNS-Abfrage angefügt, die an die Umbrella-Resolver gesendet wird und den AD-Benutzer eindeutig identifiziert.
- Alle Richtlinien werden auf die Resolverseite angewendet.
- Es ist kein aktiver Anschluss erforderlich. Die AD-Benutzer- und Gruppenrichtlinienanwendung kann jedoch die letzte erfolgreiche AD-Baumsynchronisierung wiedergeben.

Einsatzbereiche

- Jedes Netzwerk weltweit.
- Funktioniert nicht hinter einer virtuellen Umbrella-Appliance, da die DNS-Ebene deaktiviert ist, um sich auf die lokalen VAs zu verschieben.

Einschränkungen

- Erfordert aktiven und aktivierten Endpunkt-Agent auf der Workstation.
- Keine Unterstützung für Server-Betriebssysteme.
- Die Richtlinie kann nicht basierend auf der internen Netzwerk-IP angewendet werden.
- Die Richtlinie oder die Berichterstellung kann für den AD-Computer nicht angewendet werden (verwenden Sie stattdessen den Roaming-Hostnamen).

Der Connector kann weiterhin versuchen, AD-Anmeldeereignisse aus dem registrierten Rechenzentrum abzurufen. Dies kann zu einem Dashboard-Fehler führen, der für die Roaming-Client-basierte AD-Integration nicht relevant ist. Um Fehler mit Berechtigungen zu entfernen, die sich auf das Abrufen von Anmeldeereignissen beziehen, ohne tatsächlich Ereignisse zu verzeichnen, deaktivieren Sie die Überwachung von Anmeldeereignissen (falls nicht anders verwendet) auf der Rückseite der Überwachungsanweisungen von hier.

Implementierung der virtuellen Appliance

Anforderungen

- Zwei VAs pro Umbrella-Standort
- Ein AD-Connector (redundanter zweiter optional) pro Umbrella-Standort
- Alle Rechenzentren (die keine schreibgeschützten Rechenzentren sind) müssen im Dashboard registriert werden.
- OpenDNS_Connector-Benutzer müssen über alle erforderlichen Berechtigungen verfügen.
- Anmeldeereignisse müssen aktiviert sein, um 4624 Sicherheitsereignisprotokolle auf allen DCs zu protokollieren. Vollständige Tipps zur Fehlerbehebung.

So funktioniert es

- Die VAs empfangen AD-Benutzerzuordnungen, die auf den Ereignisprotokollen der Windows-Domänencontroller für Sicherheitsanmeldungen basieren.
- Jede Workstation-Anmeldung wird im Sicherheitsereignisprotokoll des Anmeldeservers protokolliert, und zwar als eindeutiges Anmeldeereignis mit dem AD-Benutzernamen oder dem AD-Computernamen und der internen IP-Adresse der Workstation.
- Der Connector analysiert diese Ereignisse in Echtzeit über ein WMI-Abonnement und synchronisiert sie über TCP 443 mit jeder VA der Umbrella-Site.
- Die VA erstellt eine Live-Benutzerzuordnung zwischen der internen IP-Adresse eines AD-Benutzers/Computers und dem Benutzernamen des AD-Benutzers/Computers.
- Die VA hat nur Einblick in die interne Quell-IP einer DNS-Abfrage und nutzt die zuvor erwähnte Zuordnungsdatei, die durch die vom Connector synchronisierten Ereignisse erstellt wurde. Die VA hat keine direkte Übersicht darüber, wer derzeit bei einem Computer angemeldet ist. Dadurch werden die AD-Benutzer-GUID und die interne IP über EDNS0 an die DNS-Abfrage angefügt, die von der VA an die Umbrella Resolver gesendet wird, und der AD-Benutzer wird eindeutig identifiziert.
- Der AD-Computer-Hash wird auf die gleiche Weise angewendet.
- Alle Richtlinien werden auf die Resolverseite angewendet.

- Ein Connector muss in der Organisation funktionsfähig und aktiv sein, um einen AD-Benutzer zu empfangen, und Anmeldeereignisse müssen aktuell sein.
- Der Benutzer muss der letzte AD-Benutzer sein, der sich auf diesem Computer authentifiziert, wie in den Ereignisprotokollen zu sehen ist.

Einsatzbereiche

Im lokalen Unternehmensnetzwerk, in dem alle DNS auf eine virtuelle Umbrella-Appliance verweist, die zu demselben Umbrella-Standort gehört wie das Rechenzentrum, bei dem sich der Benutzer authentifiziert hat.

Einschränkungen

- Der Computer kann nicht auf eine VA verweisen, die zu einer anderen AD-Domäne oder einem Umbrella-Standort gehört (bei großen Bereitstellungen auf mehreren Domänen wird die AD-Anwendung nicht vom Basisnetzwerk erkannt).
- Bei großen Bereitstellungen kann eine Unterteilung in Umbrella-Standorte mit separaten VAs erforderlich sein.
- AD-Benutzerausnahmen können für AD-Dienstbenutzer erforderlich sein.
- Für den zuvor erwähnten Connector existiert ein maximaler Durchsatz von Anmeldeereignissen pro Sekunde, wodurch die Benutzeranwendung verzögert werden kann. Dies ist ein Faktor für die Netzwerklatenz und die Anzahl der VAs.

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.