Integrare Active Directory utilizzando VA o CSC

Sommario

Introduzione

In questo documento vengono descritti due metodi per l'integrazione di Active Directory (AD) con Umbrella: Virtual Appliance (VA) o Cisco Secure Client (CSC).

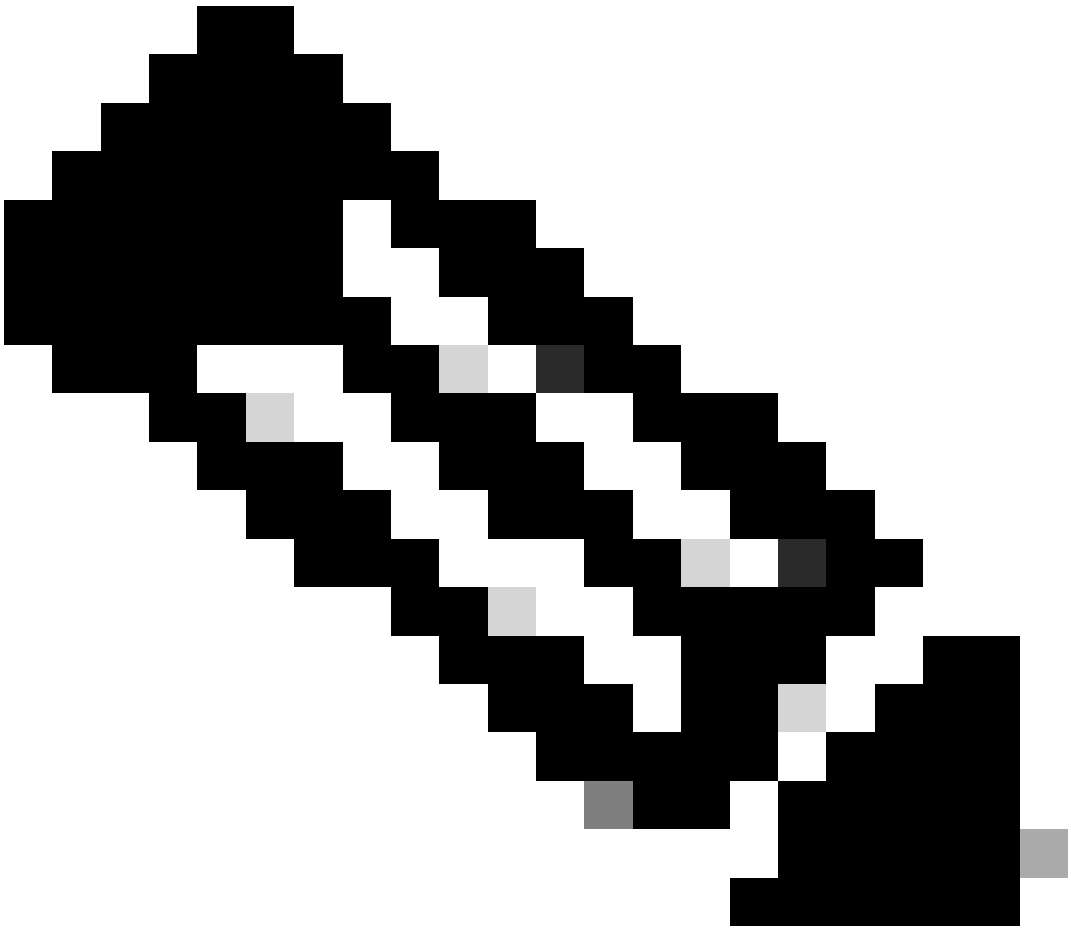
Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Connettore AD: Sincronizza l'albero AD di un singolo dominio Active Directory con il dashboard. Per l'implementazione VA, sincronizza anche attivamente gli eventi di accesso dai controller di dominio sullo stesso sito Umbrella ai controller di dominio di accesso. L'albero AD per l'organizzazione viene sincronizzato con il cloud Umbrella dal connettore AD, estraendo questi dati dal controller di dominio registrato. Vengono rilevati aggiornamenti della struttura e il cloud Umbrella viene aggiornato entro diverse ore.
- Controller di dominio (server AD): I controller di dominio vengono registrati nel dashboard tramite lo script wsf di configurazione della registrazione scaricato dal dashboard. Il nome, il dominio e l'indirizzo IP interno verranno aggiunti al dashboard per indicare al connettore con quali IP tentare di eseguire la sincronizzazione. Se non è possibile eseguire lo script, è possibile anche eseguire la registrazione manuale. Contatta il Supporto Umbrella per ulteriori informazioni e supporto.
- Appliance virtuale: Il server d'inoltro DNS locale Umbrella. Applica (facoltativo) l'identità AD

sulla rete e gli IP interni sui report. In questo modo tutti i client mobili sottostanti vengono attivati per disabilitare la protezione DNS e rimandare alla modalità "Dietro protezione VA".
- Cisco Secure Client: Il servizio software locale Umbrella che fornisce la crittografia DNS e l'identificazione utente a Windows e macOS. Inoltre, è fornito come modulo AnyConnect.



Nota: I prerequisiti differiscono in modo significativo tra le due implementazioni. Fare riferimento all'implementazione specifica per i prerequisiti completi.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

In questo articolo vengono illustrati ed esplorati i due diversi metodi di integrazione di Active Directory con Umbrella Dashboard. Al momento, gli utenti AD possono essere applicati ai criteri e ai report tramite le appliance virtuali Umbrella o Cisco Secure Client.

Implementazione client sicura

Requisiti

- Un connettore AD
- Un controller di dominio nel dashboard
- L'utente OpenDNS_Connector deve disporre dell'autorizzazione Controller di dominio di sola lettura.
- Versioni minime Secure Client per il client standalone (modulo AnyConnect):
  - Windows: 2.1.0 (4.5.01044)
  - OSX: 2.0.39 (4.5.2033).

Come funziona

- L'utente AD attualmente connesso viene determinato direttamente nel computer locale dal client mobile che legge il Registro di sistema locale.
- Supporta un massimo di un utente connesso contemporaneamente alla workstation.
- Due utenti simultanei possono impedire l'applicazione di utenti AD.
- Il GUID utente di Active Directory e l'indirizzo IP interno vengono collegati tramite EDNS0 nel proxy DNS del client mobile alla query DNS inviata ai resolver Umbrella, identificando in modo univoco l'utente di Active Directory.
- Tutti i criteri vengono applicati sul lato del sistema di risoluzione.
- Non è richiesto alcun connettore attivo. L'applicazione di Criteri di gruppo e utente AD può tuttavia riflettere la sincronizzazione dell'albero di Active Directory più recente completata.

Dove funziona

- Qualsiasi rete a livello globale.
- Non funziona dietro un'appliance virtuale Umbrella poiché il livello DNS è disattivato per rimandare ai VA locali.

Limitazioni

- Richiede che l'agente endpoint sia attivo e abilitato sulla workstation.
- Non supporta i sistemi operativi server.
- Impossibile applicare il criterio basato sull'IP della rete interna.
- Impossibile applicare criteri o rapporti per il computer AD (utilizzare il nome host comune).

Il connettore può ancora tentare di eseguire il pull degli eventi di accesso di Active Directory da un

controller di dominio registrato. Ciò può causare un errore del dashboard che non è rilevante per l'integrazione di Active Directory basata su client mobili. Per rimuovere gli errori relativi alle autorizzazioni per il pulling degli eventi di login senza eseguire il pulling di alcun evento, disattivare il controllo degli eventi di login (se non altrimenti utilizzato) tramite le istruzioni di controllo riportate di seguito.

Implementazione dell'appliance virtuale

Requisiti

- Due VA per sito Umbrella
- Un connettore AD (ridondante secondo opzionale) per sito Umbrella
- Ogni controller di dominio (che non è un controller di dominio di sola lettura) deve essere registrato nel dashboard.
- L'utente OpenDNS_Connector deve disporre dell'insieme completo di autorizzazioni dei prerequisiti.
- È necessario abilitare gli eventi di accesso per registrare i registri eventi di protezione 4624 in tutti i controller di dominio. Vedere i suggerimenti completi per la risoluzione dei problemi.

Come funziona

- I VA ricevono i mapping degli utenti AD in base ai registri eventi di accesso di protezione dei controller di dominio Windows.
- Ogni accesso alla workstation viene registrato nel registro eventi di protezione del controller di dominio del server di accesso come evento di accesso univoco, con il nome utente o il nome del computer AD e l'indirizzo IP interno della workstation.
- Il connettore analizza questi eventi in tempo reale tramite una sottoscrizione WMI e li sincronizza con ogni VA sul sito Umbrella tramite TCP 443.
- VA crea un mapping utente attivo tra l'indirizzo IP interno di un utente/computer AD e il nome utente dell'utente/computer AD.
- Il VA ha visibilità solo sull'IP di origine interno di una query DNS e utilizza il file di mapping precedentemente menzionato creato dagli eventi sincronizzati del connettore. L'amministratore di sistema non ha alcuna visibilità diretta su chi è attualmente connesso a una macchina. In questo modo il GUID utente di Active Directory e l'indirizzo IP interno tramite EDNS0 vengono associati alla query DNS inviata ai resolver Umbrella da VA, che identifica in modo univoco l'utente di Active Directory.
- L'hash del computer AD viene applicato nello stesso modo.
- Tutti i criteri vengono applicati sul lato del sistema di risoluzione.
- Un connettore deve essere funzionale e attivo nell'organizzazione per ricevere un utente AD e gli eventi di accesso devono essere correnti.
- L'utente deve essere l'ultimo utente AD a eseguire l'autenticazione a questo computer come indicato nei registri eventi.

Dove funziona

Sulla rete aziendale locale in cui tutti i DNS puntano a un dispositivo virtuale Umbrella

appartenente allo stesso sito Umbrella del controller di dominio a cui l'utente ha eseguito l'autenticazione.

Limitazioni

- Il computer non può puntare a un VA appartenente a un dominio Active Directory o a un sito Umbrella diverso (le distribuzioni di grandi dimensioni su più domini non possono vedere l'applicazione Active Directory fuori dalla rete di base).
- Le installazioni di grandi dimensioni possono richiedere la suddivisione in siti Umbrella con VA separati.
- Le eccezioni degli utenti AD possono essere necessarie per gli utenti AD del servizio.
- Esiste un throughput massimo di eventi di accesso al secondo per il connettore menzionato in precedenza che può ritardare l'applicazione utente. Questo è un fattore della latenza di rete e del numero di VA.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).