Esaminare il flusso di integrazione di Umbrella Active Directory

Sommario

Introduzione

Questo documento descrive il flusso di comunicazione tra i componenti operativi in un'integrazione con Cisco Umbrella Active Directory (AD).

Premesse

La comprensione del flusso di comunicazione di Active Directory può essere utile per la risoluzione dei problemi e per garantire la corretta configurazione dell'ambiente prima della distribuzione.

Flusso di comunicazione con l'implementazione di Umbrella Active Directory

Quando lo script del connettore AD viene eseguito in un controller di dominio

Lo script di Windows esegue una connessione unica dal controller di dominio al cloud sulla porta TCP/443 utilizzando HTTPS per registrare il controller di dominio nel dashboard. Questa registrazione consente al connettore di riconoscere il DC. Viene effettuata una chiamata a **https://api.opendns.com** con parametri specifici. Una volta che lo script ha registrato correttamente il controller di dominio, viene visualizzato nel dashboard.

A volte i problemi possono essere correlati agli aggiornamenti dei certificati radice in Windows. Per determinare rapidamente il problema, passare a Internet Explorer e puntare il browser su: https://api.opendns.com/v2/OnPrem.Asset. Questa azione consente di stampare un messaggio simile al

seguente: **1005 Missing API key**. Se nella pagina vengono visualizzati errori o avvisi relativi ai certificati, verificare che sia installato l'ultimo aggiornamento dei certificati radice di Microsoft.

Modalità di comunicazione del connettore AD

Il connettore AD comunica con il servizio Umbrella Cloud o con un'appliance virtuale come segue:

- Connector to Cloud

  Il connettore carica tutti i dati di Active Directory (AD) ogni cinque minuti in caso di modifiche, utilizzando una connessione HTTPS sulla porta 443 TCP. Vengono caricate solo le informazioni relative a gruppi, utenti e computer. Non viene caricata alcuna password e tutte le informazioni utente vengono sottoposte a hashing localmente, rendendo i dati univoci.

- Connettore per appliance virtuali

  Il connettore invia costantemente eventi AD alle appliance virtuali utilizzando la porta 443 TCP (non crittografata). Questa è una comunicazione a senso unico; gli accessori non comunicano con i connettori. È necessario che il connettore e l'appliance virtuale (VA) comunichino su una rete attendibile.

- Connettore a controller di dominio

  Il connettore comunica con tutti i controller di dominio situati nello stesso sito utilizzando le porte 389 TCP e 3268 TCP/UDP per la sincronizzazione LDAP. Il connettore comunica inoltre con i controller di dominio tramite WMI/RPC. La porta 135 TCP è la porta standard per RPC e WMI. WMI utilizza inoltre una porta assegnata in modo casuale tra 1024 TCP e 65535 TCP per Windows 2003 e versioni precedenti o tra 49152 TCP e 65535 TCP per Windows 2008 e versioni successive. A partire dalla versione 1.1.24, il connettore comunica anche con il controller di dominio utilizzando LDAPS (LDAP su SSL) sulle porte 636 TCP e 3269 TCP.

Se vengono rilevati problemi di comunicazione, verificare la presenza di eventuali proxy di applicazione di livello 7 che potrebbero bloccare o eliminare i dati. Un caso comune è la funzione di ispezione sui dispositivi Cisco che agiscono su protocolli come DNS, HTTP o HTTPS. Per ulteriori informazioni, consultare la documentazione di Dell sull'applicazione dell'ispezione del protocollo a livello di applicazione.

Appliance virtuale (VA) - Cloud

Le appliance virtuali comunicano frequentemente sulla porta 443 TCP a **api.opendns.com**e a 53 TCP/UDP per query o richieste DNS e a 22, 25, 53, 80, 443 o 4766 TCP per stabilire il tunnel di supporto. Le appliance virtuali comunicano con il cloud utilizzando le porte 53 UDP/TCP, 443 TCP, 123 TCP e 80 TCP. Ricevono i dati dai connettori sulla porta 443 TCP (non una connessione HTTPS) ma non richiedono la comunicazione con essi.

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).