Informazioni su Umbrella Encryption per AD Sync

Sommario

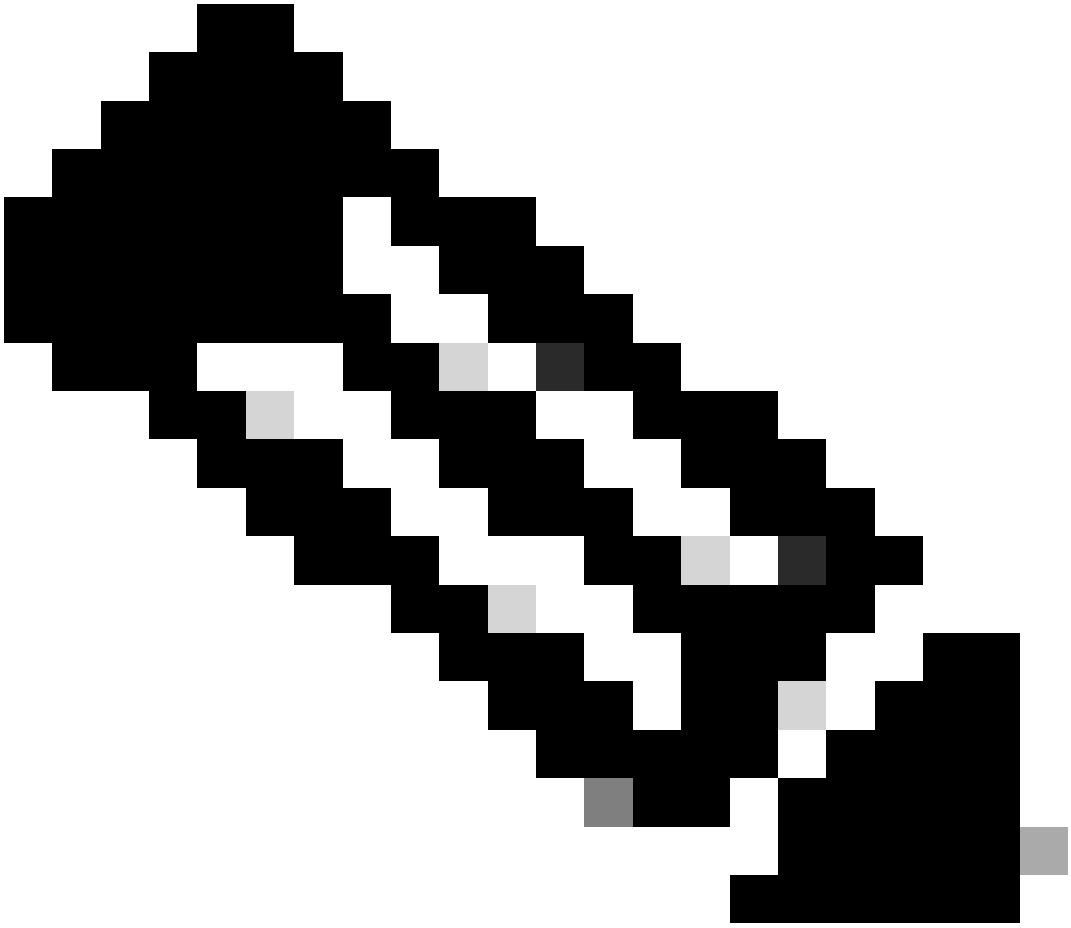
Introduzione

In questo documento viene descritta la crittografia Umbrella per la sincronizzazione di Active Directory, ad esempio come viene crittografato il trasferimento di dati.

Premesse

Il software Umbrella AD Connector recupera i dettagli delle informazioni su utenti, computer e gruppi dal controller di dominio Active Directory utilizzando LDAP. Da ogni oggetto vengono memorizzati solo gli attributi necessari, inclusi sAMAccountName, dn, userPrincipalName, memberOf, objectGUID, primaryGroupId (per utenti e computer) e primaryGroupToken (per gruppi).

Questi dati vengono quindi caricati in Umbrella per l'utilizzo nella configurazione dei criteri e nel reporting. Questi dati sono inoltre necessari per il filtro per utente o per computer.



Nota: objectGUID inviato sotto forma di hash.

Per sapere esattamente cosa viene sincronizzato, è possibile esaminare i file con estensione ldif contenuti in:

```
C:\Program Files\OpenDNS\OpenDNS Connector\ADSync\*.ldif
```

In questo articolo viene descritto come crittografare il trasferimento di dati.

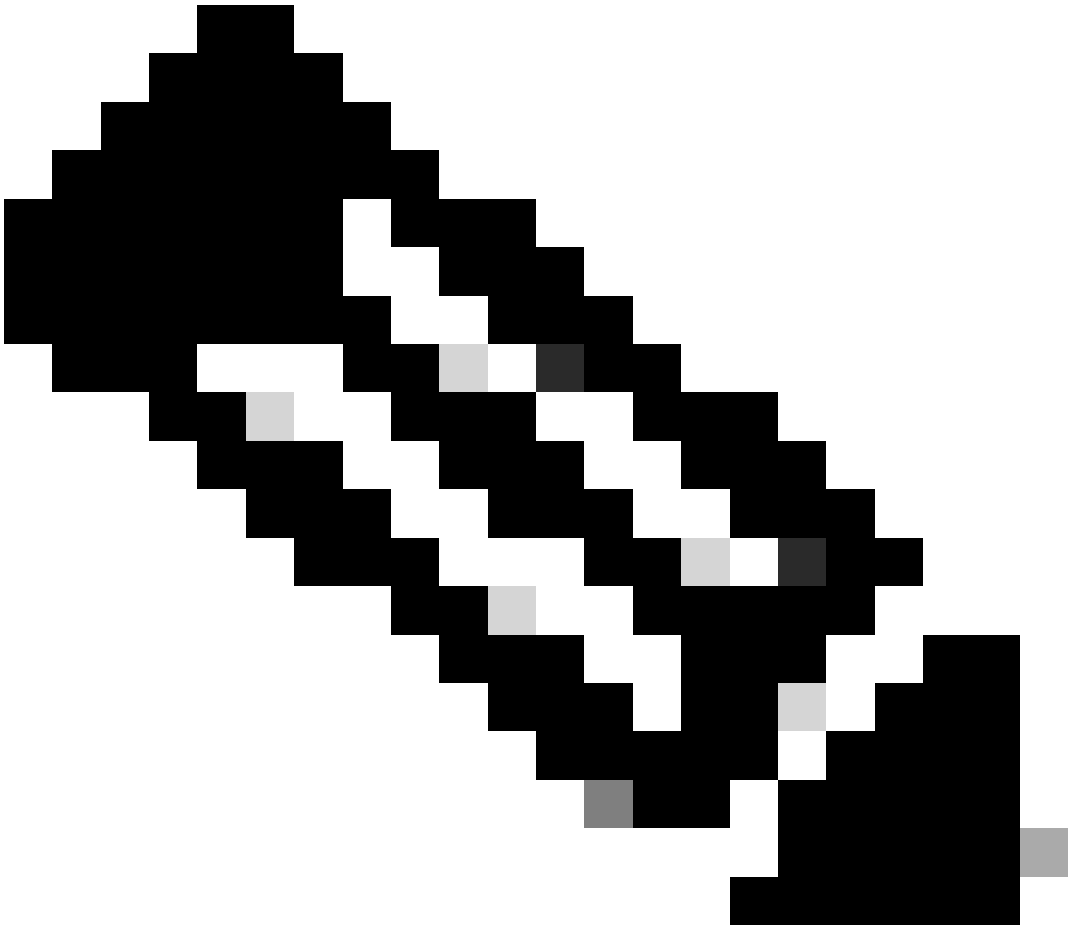
Crittografia per il caricamento dei dati di Active Directory

Umbrella AD Connector carica le informazioni di Active Directory in Umbrella utilizzando una connessione HTTPS sicura. Il caricamento tra il cloud Connector <>Umbrella è sempre crittografato.

Crittografia per il recupero dei dati di Active Directory

A partire dalla versione 1.1.22, il connettore tenta ora di recuperare i dettagli dell'utente tramite crittografia tra il connettore del controller di dominio <>. Si tentano due metodi:

- LDAPS. I dati vengono trasmessi su un tunnel protetto.
- LDAP con autenticazione Kerberos. Fornisce la crittografia a livello di pacchetto.



> Nota: LDAPS non viene utilizzato quando il software Connettore è in esecuzione sullo stesso server del controller di dominio utilizzato per ADsync.

Se il tentativo non riesce per qualsiasi motivo, viene ripristinato il meccanismo seguente:

- LDAP con autenticazione NTLM. In questo modo l'autenticazione è sicura, ma il trasferimento dei dati tra il DC > Connector avviene senza crittografia.

Per garantire la possibilità di eseguire la crittografia, si consiglia di:

- Abilitare LDAPS nei controller di dominio. Ciò esula dall'ambito del supporto Umbrella, ma può essere abilitato con la documentazione Microsoft.
- Verificare che il nome host dei controller di dominio sia configurato correttamente in 'Distribuzioni > Siti e Active Directory'. Per entrambi i metodi di crittografia è necessario il nome host corretto. Se il nome host non è corretto, è consigliabile registrare nuovamente il controller di dominio utilizzando lo script di configurazione oppure contattare il supporto tecnico Umbrella.

Per confermare che la crittografia è in corso. È possibile controllare il file di registro qui:

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\OpenDNSAuditClient.log
```

Durante la sincronizzazione di Active Directory, vengono visualizzate voci di registro quali:

Connessione LDAPS riuscita:
Utilizzo di SSL per la comunicazione <SERVER> per recuperare il DN.

Autenticazione Kerberos riuscita:
Utilizzo di Kerberos per la comunicazione <SERVER> per recuperare il DN.

Meccanismo di failback NTLM in uso:
Kerberos non riuscito per l'host controller di dominio <SERVER>. Il nome host non può essere valido. Fallback alla query NTLM.

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).