Informazioni sul supporto Umbrella per l'importazione delle identità di utenti e gruppi da Azure AD e Okta

Sommario

Introduzione

Questo documento descrive Umbrella che ora supporta il provisioning delle identità di utenti e gruppi da Azure Active Directory e Okta, in base allo standard SCIM.

Casi di utilizzo supportati

Umbrella SWG:

- Importa le identità di utenti e gruppi da Azure AD/Okta insieme all'impostazione dell'autenticazione SAML in Azure AD/Okta per gli utenti finali che si connettono a SWG tramite un tunnel IPSec, file PAC o concatenamento proxy.
- Importare le identità di utenti e gruppi da Azure AD per abilitare l'identificazione utente per il modulo SWG AnyConnect nei dispositivi che eseguono l'autenticazione in locale di AD o Azure AD.
- Importare le identità di utenti e gruppi da Okta per abilitare l'identificazione utente per il modulo SWG AnyConnect sui dispositivi che eseguono l'autenticazione in Active Directory locale.

DNS Umbrella:

- Importa le identità di utenti e gruppi da Azure AD per abilitare l'identificazione utente per il modulo DNS AnyConnect/client roaming nei dispositivi che eseguono l'autenticazione in locale ad Active Directory o Azure AD.
- Importare le identità di utenti e gruppi da Okta per abilitare l'identificazione utente per il modulo DNS AnyConnect o il client roaming sui dispositivi che eseguono l'autenticazione in Active Directory locale.

Vincoli

- Azure AD/Okta non è in grado di fornire l'integrazione dell'identità utente per le appliance

virtuali Umbrella (VA). Questo problema si verifica perché Azure AD/Okta non dispone della visibilità dei mapping utente - IP privati richiesti dai VA. Le distribuzioni VA continuano a richiedere l'installazione di un connettore Umbrella AD in sede per facilitare l'integrazione di AD.

- La distribuzione simultanea delle stesse identità utente/gruppo da AD e Azure AD/Okta locali non è supportata. Se in precedenza è stato distribuito un connettore AD locale per effettuare il provisioning di utenti e gruppi e ora si sta cercando di effettuare il provisioning delle stesse identità di utenti e gruppi da Azure AD/Okta, è necessario arrestare obbligatoriamente il connettore AD prima di attivare il provisioning di Azure AD/Okta.
- Non esiste alcun limite al numero di utenti di cui è possibile eseguire il provisioning da Azure AD/Okta. Per i gruppi, è possibile eseguire il provisioning di un massimo di 200 gruppi da Azure AD/Okta a un'organizzazione Umbrella. Azure AD supporta i gruppi dinamici, pertanto è possibile creare un gruppo 'Tutti gli utenti' ed eseguire il provisioning di questo gruppo insieme a un massimo di 199 altri gruppi in cui definire i criteri Umbrella. Okta ha un gruppo Everyone incorporato, quindi è possibile effettuare il provisioning di questo gruppo insieme ad altri 199 gruppi sui quali desiderano definire le regole.
- AnyConnect SWG non supporta l'autenticazione SAML in Azure AD. Si basa sullo stesso meccanismo di autenticazione passiva utilizzato con l'AD locale.

Assegnazione di identità

Per assegnare le identità a uno di questi provider di identità, è possibile utilizzare le istruzioni documentate nei seguenti link:

- Eseguire il provisioning delle identità da Azure AD: https://docs.umbrella.com/umbrella-user-guide/docs/microsoft-azure-ad-integration
- Specificare le identità da Okta: https://docs.umbrella.com/umbrella-user-guide/docs/okta-integration

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).