Creazione di gruppi di criteri di accesso corrispondenti ai gruppi di Active Directory

Sommario

Domanda

Come creare gruppi di criteri di accesso corrispondenti ai gruppi di Active Directory (AD)

Il primo passaggio consiste nel configurare un realm di autenticazione (realm NT LAN Manager (NTLM)) e un'identità che utilizza il realm di autenticazione.

—

1. Creare un'area di autenticazione NTLM in Web Security Appliance (WSA) in **Rete > Autenticazione**.
2. Dopo aver configurato l'area di autenticazione NTLM, scegliere **Web Security Manager > Identità**, quindi fare clic su **Aggiungi identità**.
3. Per creare un'identità, eseguire la procedura seguente: Nome: ID autenticazioneInserisci sopra: 1Definisci membri per autenticazione: *<nome area autenticazione NTLM>*Schema: **Utilizzare Basic o NTLMSSP** o **NTLMSSP**Lasciare tutte le altre impostazioni come predefinite.
   Se si desidera verificare l'autenticazione rispetto ai client selezionati, utilizzare **Definisci membri per subnet** e specificare l'indirizzo IP del client richiedente. In questo modo, il server WSA può richiedere l'autenticazione solo per i client selezionati.Fare clic su **Invia**.

A questo punto è necessario avere solo due identità, **Auth.Id** e **Criteri di identità globali**, con l'autenticazione abilitata per **Auth.Id** Identity.

Il passaggio successivo consiste nell'utilizzare l'identità **Auth.Id** e creare criteri di accesso basati su tale identità. È possibile specificare gli utenti o i gruppi AD richiesti nei criteri di accesso.
—

1. Scegliere **GUI > Web Security Manager > Criteri di accesso**.
2. Fare clic su **Aggiungi criterio**.
3. Per creare un criterio di accesso, eseguire la procedura seguente: Nome criterio: Politica.VenditeInserisci sopra criterio: 1Criteri di identità: Auth.Id - **Specifica gruppi e utenti autorizzati**Immettere manualmente i nomi dei gruppi oppure fare clic su **Aggiorna directory** per ottenere l'elenco degli utenti esistenti in Active Directory. Dopo aver selezionato gli utenti, fare clic su **Add** (Aggiungi).Al termine, fare clic su **Submit** (Invia).

Se è necessario creare un altro criterio di accesso, fare clic su **Aggiungi criterio** e creare un altro criterio di accesso per il nuovo gruppo AD.

Non creare nuove identità per lo stesso realm di autenticazione. Riutilizzare l'identità esistente (Auth.Id) e creare nuovi criteri di accesso per gruppi AD diversi, purché l'identità non sia associata a **Porte proxy**, **Categorie URL**, **Agenti utente** o **Definisci membri per subnet**.

Per i criteri di accesso multipli che utilizzano gruppi AD diversi, l'impostazione dovrebbe essere simile alla seguente:
—

Identità

"Auth.Id"
"Criteri di identità globali"

Criteri di accesso

"Sales.Policy" con "Auth.Id"
"Support.Policy" con "Auth.Id"
"Manager.Policy" con "Auth.Id"
"Admin.Policy" con "Auth.Id"
"Criteri globali" con "Tutti"