

Come configurare WSA per eseguire Criteri di gruppo di autenticazione LDAP?

Sommario

[Domanda:](#)

Domanda:

Ambiente: Cisco Web Security Appliance (WSA), tutte le versioni di AsyncOS

Questo articolo della Knowledge Base fa riferimento a software non gestito o supportato da Cisco. Le informazioni sono fornite a titolo di cortesia. Per ulteriore assistenza, contattare il fornitore del software.

Per il corretto funzionamento di "Authentication Group", è necessario innanzitutto configurare un realm di autenticazione in "GUI > Rete > Autenticazione".

1. Impostare innanzitutto "Authentication Protocol" (Protocollo di autenticazione) su "LDAP" e passare a "Group Authorization" (con altre sezioni configurate correttamente).
2. Specificare l'"Attributo nome gruppo". Questo è l'attributo che contiene il valore visualizzato in "Web Security Manager" > "Criteri di accesso Web" > "Fare clic su Aggiungi gruppo" > "Seleziona tipo di gruppo per gruppo di autenticazione" > tabella "Ricerca nelle directory". Questo attributo deve essere univoco e il nodo foglia rappresentato da questo attributo deve contenere un elenco di utenti nel relativo gruppo.
3. Specificare quindi la query del filtro di gruppo. Questo è il filtro di ricerca utilizzato da WSA per individuare tutti i gruppi nella directory LDAP.
4. A questo punto, specificare "Attributo appartenenza al gruppo", ovvero l'attributo nel nodo foglia che conterrà il valore univoco dei membri. Poiché questo attributo contiene il membro di questo GRUPPO, verrebbero visualizzate più voci. Verificare che il valore incluso in questo attributo corrisponda al valore incluso in "Attributo nome utente" nella stessa pagina.

Di seguito è riportato un esempio di come WSA utilizzerebbe la configurazione del realm LDAP per confrontare un nome utente con un gruppo LDAP:

1. Si supponga di impostare "Group Filter Query" su "objectClass=group"
2. WSA utilizzava prima questo filtro ed eseguiva una ricerca nella directory LDAP per trovare il risultato.
3. Quindi, utilizzando il risultato, WSA cercherà l'attributo specificato in "Group Membership Attribute". Si supponga che si tratti di un attributo denominato "member".
4. Ora, se un utente accede come 'USERNAME_A' tramite il proxy WSA, WSA cercherà l'account dell'utente nel server LDAP e, in caso di corrispondenza, utilizzerà l'attributo

specificato in "User Name Attribute" (esempio: uid) e verifica se "uid" corrisponde agli utenti elencati nell'attributo "member" raccolto in precedenza.

5. In caso di corrispondenza, l'utente utilizzerà il criterio configurato. In caso contrario, WSA valuterà il criterio successivo in linea.

Per informazioni sugli attributi da configurare utilizzando il server LDAP, vedere "Softerra LDAP Browser" <http://www.ldapbrowser.com>