

如何配置WSA以執行LDAP身份驗證組策略？

目錄

[問題：](#)

問題：

環境：思科網路安全裝置(WSA),AsyncOS的所有版本

本知識庫文章所參考的軟體不是思科維護或支援的。 此資訊出於方便而提供。 如需更多幫助，請與軟體供應商聯絡。

要使「身份驗證組」起作用，首先需要在「GUI > 網路 > 身份驗證」下配置身份驗證領域。

1. 首先將「身份驗證協定」設定為「LDAP」，然後導航到「組授權」（其他部分配置正確）。
2. 指定您的「組名屬性」。此屬性用於儲存在「網路安全管理器」>「Web訪問策略」>「按一下新增組」>「選擇身份驗證組的組型別」>「目錄查詢」表中顯示的值。此屬性必須唯一，而且此屬性代表的葉節點需要包含其組中的使用者清單。
3. 接下來，指定「組過濾器查詢」。這是WSA用來查詢LDAP目錄中所有組的搜尋過濾器。
4. 現在，指定「組成員屬性」，這是葉節點中儲存成員唯一值的屬性。由於此屬性保留此組的成員，因此您會看到多個條目。請確保此屬性中包含的值與同一頁上的「使用者名稱屬性」中包含的值相對應。

以下是WSA如何使用LDAP領域配置來將使用者名稱與LDAP組進行匹配的示例：

1. 我們將「組過濾器查詢」設定為「objectClass=group」
2. WSA將首先使用此過濾器並搜尋LDAP目錄，然後查詢結果。
3. 然後，WSA將使用結果查詢「組成員屬性」中指定的屬性。假定這是一個名為「member」的屬性。
4. 現在，如果使用者通過WSA代理以「USERNAME_A」身份登入，則WSA將在LDAP伺服器中查詢該使用者的帳戶，如果存在匹配項，則將使用「使用者名稱屬性」中指定的屬性(示例：uid)並檢查「uid」是否與上面收集的「member」屬性中列出的使用者匹配。
5. 如果存在匹配，則使用者將使用配置的策略；如果沒有，則WSA將評估行中的下一個策略。

要檢視需要使用LDAP伺服器配置哪些屬性，請參閱「Softerra LDAP瀏覽器」

<http://www.ldapbrowser.com>