

如何使用LDAP接受查詢驗證中繼郵件的發件人？

目錄

[問題](#)

[日誌中顯示的內容](#)

問題

如何使用LDAP接受查詢驗證中繼郵件的發件人？

警告：僅當郵件到達公共偵聽程式時，才能對信封「郵件來自」地址執行LDAP接受查詢。專用偵聽程式不允許使用LDAP接受查詢。LDAP接受查詢僅應用於入站連線。因此，郵件流策略的「連線行為」不能設定為「中繼」，此設定才能正常工作。

以下是設定LDAP接受查詢發件人驗證所需的步驟：

1. 要允許/拒絕內部發件人向Internet中繼（具體取決於其在LDAP中的郵件地址），必須用公共偵聽程式替換專用偵聽程式。在此示例中，新的公共偵聽程式將命名為「Outbound_Sender_Validation」。
2. 建立新的LDAP伺服器配置檔案並為該配置檔案設定LDAP接受查詢。要獲取LDAP接受查詢以驗證信封郵件發件人地址，您需要將{a}替換為查詢字串中的{f}。有關如何配置和使用LDAP的詳細資訊，請參閱《高級使用手冊》。

範例：(郵件={a}) => (郵件={f})

3. 在「Outbound_Sender_Validation」偵聽器上啟用配置的LDAP接受查詢。
4. 轉到「Mail Policies > Recipient Access Table(RAT)」，然後切換到新的公共偵聽程式「Outbound_Sender_Validation」。要允許中繼，請將「所有其他收件人」設定為「接受」，並確保這是RAT中的唯一條目。
5. 轉到「HAT概述」並切換到「Outbound_Sender_Validation」監聽程式。在這裡，您只需要一個發件人組。為避免郵件轉發被開啟的風險，建議將此發件人組設定為僅與允許中繼的MTA的IP地址匹配。
重要的一點是，分配的郵件流策略的「連線行為」未設定為「中繼」，否則將禁用LDAP接受查詢。為確保沒有其他MTA可以通過「Outbound_Sender_Validation」進行連線，請將預設「ALL」發件人組的策略設定為BLOCKED。

日誌中顯示的內容

警告：基於此設定，在收到信封Rcpt To地址之前不會執行拒絕。這是因為LDAP接受查詢最初用於收件人而不是發件人驗證。這也會顯示在郵件日誌中，其中LDAP拒絕與收件人地址在同一日誌行

中宣告：

```
Wed Feb 18 16:16:19 2009 Info: New SMTP ICID 2643 interface Management
(10.0.0.100) address 10.0.0.200 reverse dns host unknown verified no
Wed Feb 18 16:16:19 2009 Info: ICID 2643 ACCEPT SG RELAY_HOSTS match 10.0.0.200
rfc1918
Wed Feb 18 16:16:32 2009 Info: Start MID 2554 ICID 2643
Wed Feb 18 16:16:32 2009 Info: MID 2554 ICID 2643
From: <do_not_exist@example.test>
Wed Feb 18 16:16:39 2009 Info: MID 2554 ICID 2643 To: <good_user@example.com>
Rejected by LDAPACCEPT
Wed Feb 18 16:17:14 2009 Info: ICID 2643 close
```

檢視此日誌條目會使您認為被拒絕的地址是「good_user@example.com」，即使它實際上是「do_not_exist@example.test」被拒絕。