瞭解身份服務引擎(ISE)和Active Directory(AD)

目錄

簡介

本文檔介紹身份服務引擎(ISE)和Active Directory(AD)如何通訊、使用的協定、AD過濾器和流。

必要條件

需求

思科建議瞭解以下方面的基本知識：

- ISE 2.x和Active Directory整合。
- ISE上的外部身份身份驗證。

採用元件

- ISE 2.x。
- Windows Server(Active Directory)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

AD通訊協定

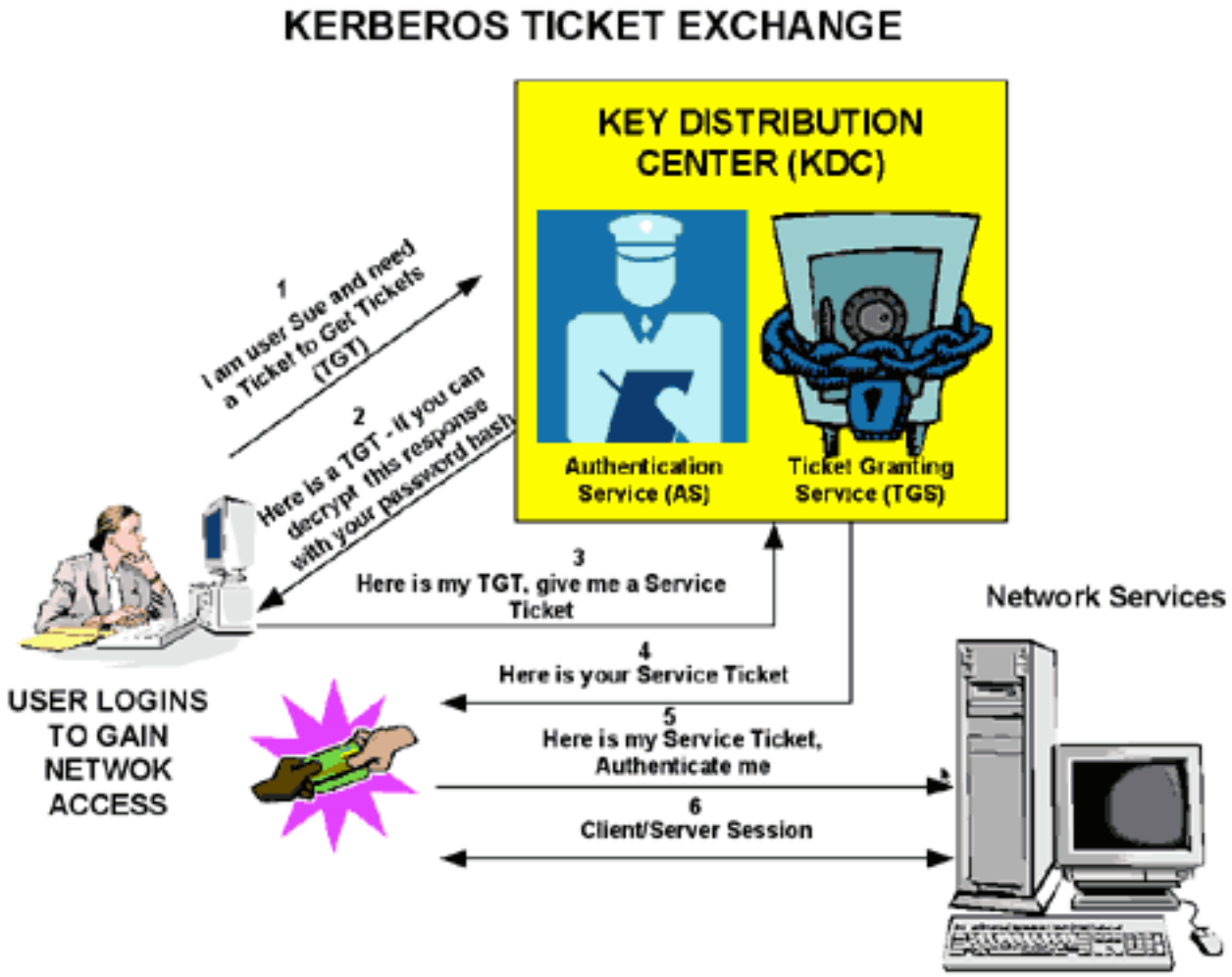
Kerberos通訊協定

Kerberos的三個頭包括金鑰分發中心(KDC)、客戶端使用者和要訪問的伺服器。

KDC作為域控制器(DC)的一部分安裝，並執行兩種服務功能：身份驗證服務(AS)和票證授予服務(TGS)。

客戶端最初訪問伺服器資源時，涉及三個交換：

1. 作為Exchange。
2. TGS交換。
3. 客戶端/伺服器(CS)交換。



- 域控制器= KDC(AS + TGS)。
- 使用您的密碼向AS（SSO門戶）進行身份驗證。
- 獲取票證授予票證(TGT)（會話cookie）。
- 請求登入服務(SRV01)。
- SRV01將您重定向到KDC。
- Show TGT to KDC —（我已經通過身份驗證）
- KDC為您提供SRV01的TGS。
- 重定向至SRV01。
- 顯示到SRV01的服務票證。
- SRV01驗證/信任服務票證。
- 服務票裡有我的所有資訊
- SRV01將我登入。

最初登入到網路時，使用者必須協商訪問並提供登入名稱和密碼，以便在其域內由KDC的AS部分進行驗證。

KDC可以訪問Active Directory使用者帳戶資訊。通過驗證後，使用者將被授予對本地域有效的票證授予票證(TGT)。

TGT的預設有效期為10小時，並在使用者登入會話期間續訂，而無需使用者重新輸入其密碼。

TGT快取在易失性儲存器空間的本地電腦上，用於請求與整個網路中服務的會話。

當需要訪問伺服器服務時，使用者向KDC的TGS部分顯示TGT。

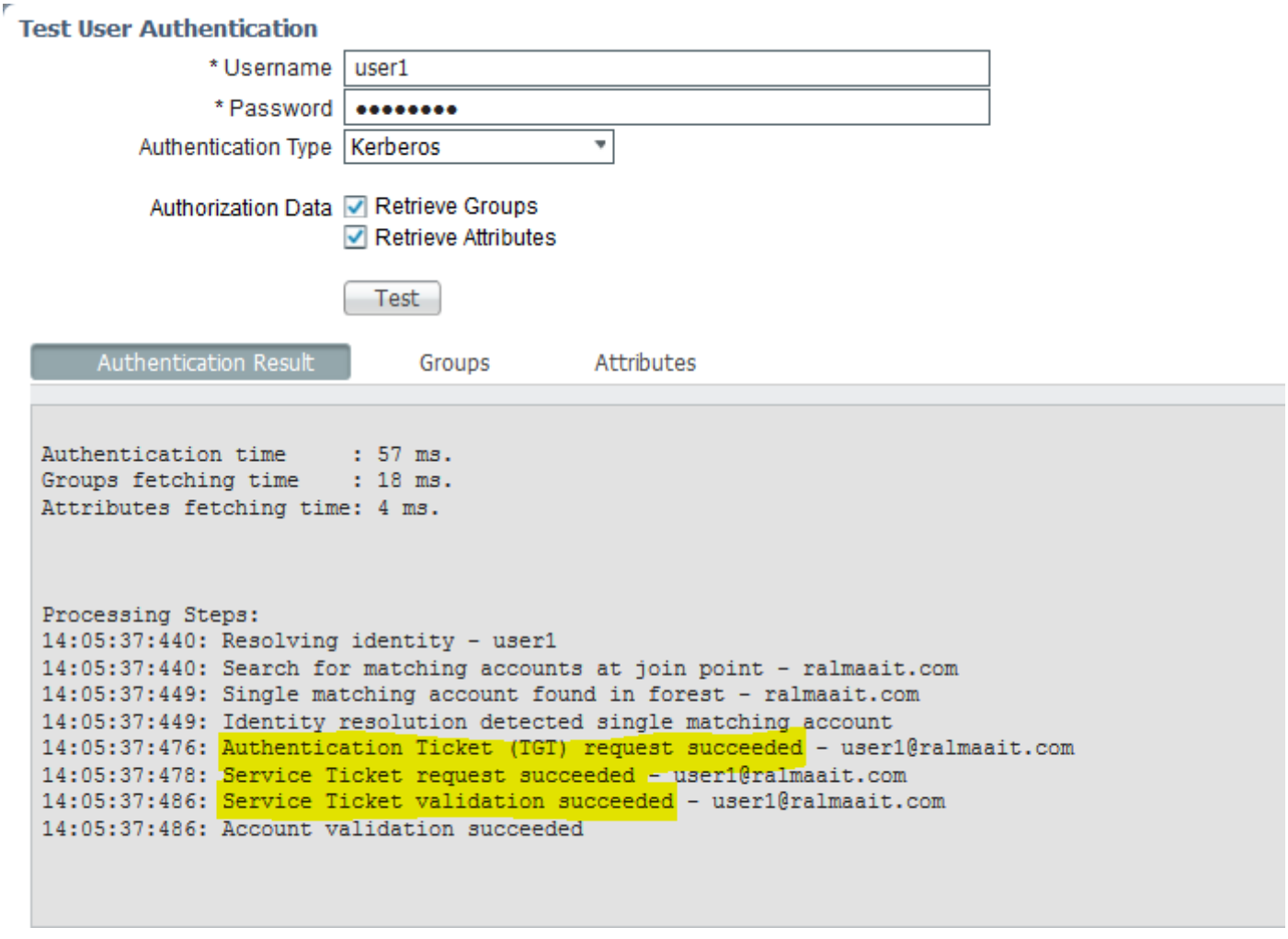
KDC上的TGS驗證使用者TGT並為客戶端和遠端伺服器建立票證和會話金鑰。然後，此資訊（服務票證）將在客戶端電腦上本地快取。

TGS接收客戶端TGT並使用其自己的金鑰讀取它。如果TGS批准客戶端請求，將為客戶端和目標伺服器生成服務票證。

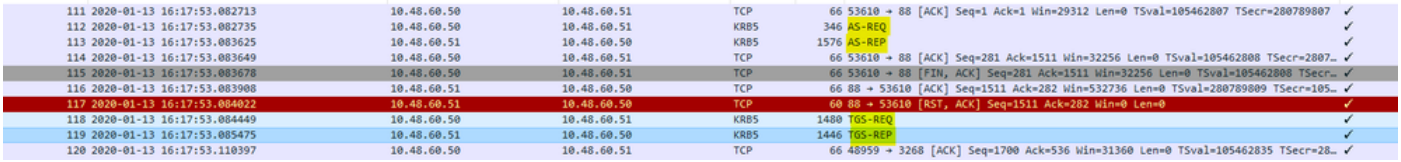
客戶端使用之前從AS回覆中檢索的TGS會話金鑰讀取其部分。

客戶端在下一客戶端/伺服器交換中向目標伺服器顯示TGS回覆的伺服器部分。

範例：



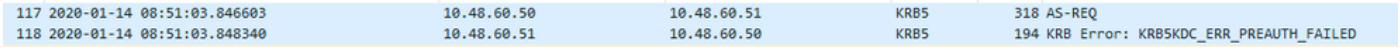
通過身份驗證的使用者從ISE捕獲資料包：



AS-REQ包含使用者名稱。如果密碼正確，則AS服務會提供一個使用使用者密碼加密的TGT。然後將TGT提供給TGT服務以獲得會話票證。

收到會話票證時，身份驗證成功。

以下是使用者端提供的密碼錯誤的範例：



如果密碼錯誤，則AS請求失敗且未收到TGT:

```
Processing Steps:
13:19:55:837:   Resolving Identity - User1
13:19:55:837:   Search For Matching Accounts At Join Point - Ralmaait.com
13:19:55:843:   Single Matching Account Found In Forest - Ralmaait.com
13:19:55:843:   Identity Resolution Detected Single Matching Account
13:19:55:856:   Authentication Ticket (TGT) Request Failed - User1@ralmaait.com,ERROR_PASSWORD_MISMATCH
```

密碼錯誤時登入ad_agent.log檔案：

2020-01-14 13:36:05,442 DEBUG，140574072981248,krb5:將請求（276位元組）傳送到RALMAAIT.COM,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG，140574072981248,krb5:從KDC收到錯誤：-1765328360/預身份驗證失敗，LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG，140574072981248,krb5:Preauth重試輸入型別：16, 14, 19, 2,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 WARNING，140574072981248,[LwKrb5GetTgtImpl ../../lwadvapi/threaded/krbtgt.c:329] KRB5錯誤代碼：-1765328360(消息：預身份驗證失敗),LwTranslateKrb5Error(),lwadvapi/threaded/lwkrb5.c:892

2020-01-14 13:36:05,444 DEBUG，140574072981248,[LwKrb5InitializeUserLoginCredentials()]錯誤代碼：40022(符號：LW_ERROR_PASSWORD_MISMATCH),LwKrb5InitializeUserLoginCredentials(),lwadvapi/threaded/lwkrb5.c:1453

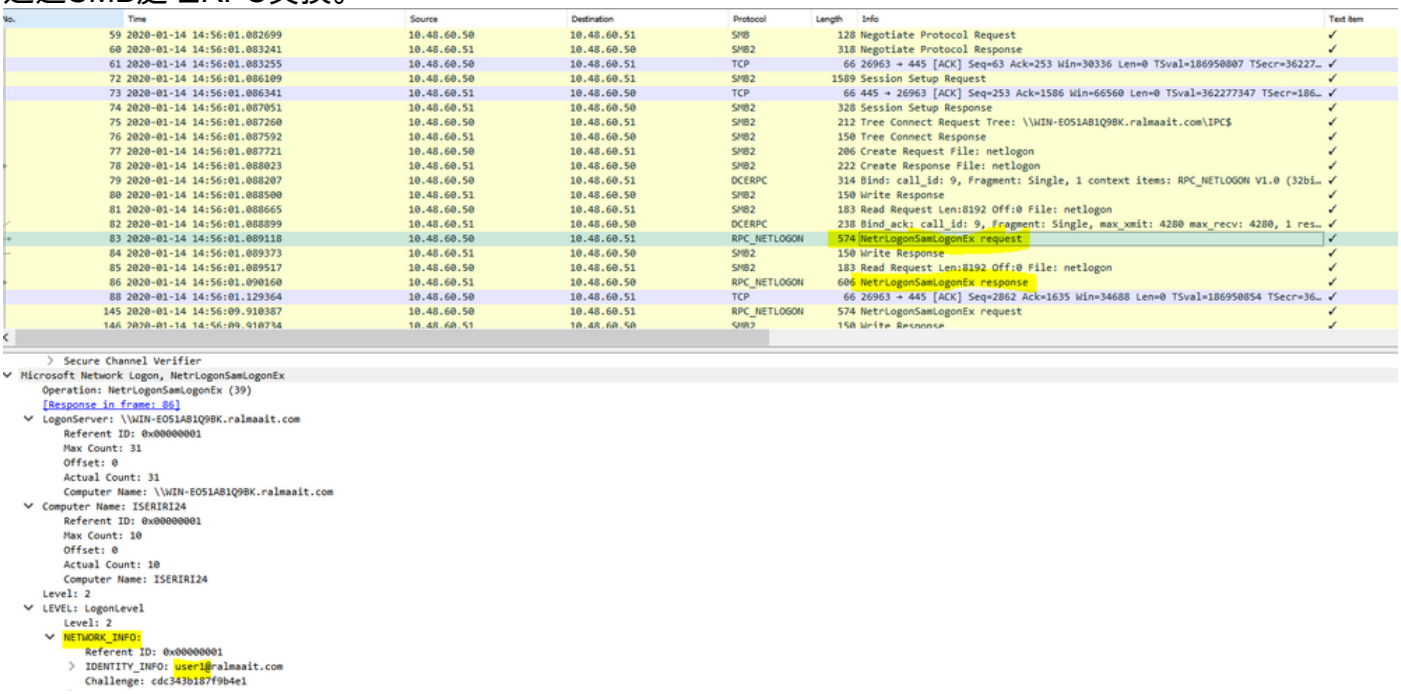
MS-RPC通訊協定

ISE使用MS-RPC over SMB，SMB提供身份驗證並且不需要單獨的會話來查詢給定RPC服務的位置。它使用名為「命名管道」的機制，在客戶端和伺服器之間進行通訊。

- 建立SMB會話連線。
- 通過SMB/CIFS.TCP埠445傳輸RPC消息作為傳輸
- SMB會話標識特定RPC服務運行的埠並處理使用者身份驗證。
- 連線到隱藏共用IPC$以進行進程間通訊。

- 為所需的RPC資源/函式開啟相應的命名管道。

通過SMB處理RPC交換。



其 **negotiate protocol request/response** line會協商SMB的方言。其 **session setup request/response** 執行身份驗證。

樹連線請求和響應連線到請求的資源。您已連線到一個特殊共用IPC$。

這種進程間通訊共用提供了主機之間的通訊方式，同時也作為MSRPC功能的傳輸。

資料包77是 **Create Request File** 檔名是連線的服務（本例中為netlogon服務）的名稱。

在資料包83和86上，NetrlogonSamLogonEX請求是將客戶端身份驗證的使用者名稱傳送到AD的欄位Network_INFO的位置。

NetrlogonSamLogonEX響應資料包將回覆結果。

NetrlogonSamLogonEX響應的某些標誌值：
0xc000006a是STATUS_WRONG_PASSWORD
0x00000000為STATUS_SUCCESS
0x00000103為STATUS_PENDING

ISE與Active Directory(AD)整合

ISE使用LDAP、KRB和MSRBC在加入/離開和身份驗證過程中與AD通訊。

接下來的部分提供了用於連線到AD上的特定DC的協定、搜尋格式和機制，以及針對該DC的使用者身份驗證。

如果DC由於任何原因而離線，ISE會故障切換到下一個可用的DC，身份驗證過程不會受到影響。

全域性目錄伺服器(GC)是儲存林中所有Active Directory對象的副本的域控制器。

它儲存域目錄中所有對象的完整副本，以及所有其他林域的所有對象的部分副本。

因此，全域性目錄允許使用者和應用程式在當前林的任何域中查詢對象，並搜尋包含在GC中的屬性。

全域性目錄包含每個域中每個林對象的基本屬性集（但不完整）（部分屬性集、PAT）。

GC從林中的所有域目錄分割槽接收資料。它們使用標準AD復制服務進行複製。

將ISE加入AD

Active Directory與ISE整合的先決條件

1. 驗證您在ISE中擁有超級管理員或系統管理員的許可權。
2. 使用網路時間協定(NTP)伺服器設定同步Cisco伺服器和Active Directory之間的時間。ISE和AD之間允許的最大時間差為5分鐘
3. 在ISE上配置的DNS必須能夠回答DC、GC和KDC的SRV查詢，包括或不包括其他站點資訊。
4. 確保所有DNS伺服器都能響應任何可能的Active Directory DNS域的前向和反向DNS查詢。
5. 在您加入思科的域中，AD至少必須有一個全域性目錄伺服器可以運行並可由思科訪問。

加入AD域

ISE應用域發現以三個階段獲取有關加入域的資訊：

1. 查詢加入的域 — 發現其林中的域以及外部信任加入的域的域。
2. 查詢其林中的根域 — 與林建立信任。
3. Queries root domains in trusted forest — 從受信任的林中發現域。

此外，思科ISE發現DNS域名（UPN字尾）、備用UPN字尾和NTLM域名。

ISE應用DC發現以獲取有關可用DC和GC的所有資訊。

1. 加入過程以域本身存在的AD上的super admin輸入憑據開始。如果使用者名稱存在於不同的域或子域中，則必須使用UPN表示法(username@domain)標籤使用者名稱。
2. ISE傳送所有DC、GC和KDC記錄的DNS查詢。如果DNS應答中沒有其中一個應答，則整合將失敗，並出現DNS相關錯誤。
3. ISE使用CLDAP ping通過向DC傳送的CLDAP請求來發現所有DC和GC，這些請求與SRV記錄中的優先順序相對應。使用第一個DC響應，然後ISE連線到該DC。

用於計算DC優先順序的一個因素是DC響應CLDAP ping所用的時間；更快的響應獲得更高的優先順序。

> **附註**：CLDAP是ISE用來建立和維護與DC連線的機制。 它測量第一個DC應答之前的響應時間。如果您未從DC看到任何響應，則它將失敗。如果響應時間大於2.5秒則發出警告。CLDAP ping站點中的所有DC（如果沒有站點，則表示域中的所有DC）。 CLDAP響應包含DC站點和客戶端站點（ISE電腦分配到的站點）。

4. 然後ISE接收具有「加入使用者」憑據的TGT。
5. 使用MSRPC生成ISE電腦帳戶名稱。（SAM和SPN）
6. 如果ISE電腦帳戶已存在，則按SPN搜尋AD。如果ISE電腦不存在，ISE會建立一個新電腦。
7. 開啟電腦帳戶、設定ISE電腦帳戶密碼並驗證ISE電腦帳戶是否可訪問。
8. 設定ISE電腦帳戶屬性（SPN、dns主機名等）。
9. 使用KRB5獲取ISE電腦憑證的TGT並發現所有受信任域。
10. 當連線完成時，ISE節點更新其AD組和關聯的SID並自動啟動SID更新過程。驗證此過程是否可在AD端完成。

離開AD域

當ISE離開時，AD必須考慮：

1. 使用完整的AD管理員使用者執行離開過程。這將驗證ISE電腦帳戶是否已從Active Directory資料庫中刪除。
2. 如果AD沒有憑據，則不會從AD中刪除ISE帳戶，必須手動刪除。
3. 當您從CLI重置ISE配置或在備份或升級後恢復配置時，它會執行離開操作並斷開ISE節點與Active Directory域的連線。（如果加入）。 但是，ISE節點帳戶不會從Active Directory域中刪除。
4. 建議使用Active Directory憑據從管理員門戶執行離開操作，因為它還會從Active Directory域中刪除節點帳戶。當您更改ISE主機名時，也建議這樣做。

DC故障轉移

當連線到ISE的DC由於任何原因變得離線或不可訪問時，ISE會自動觸發DC故障切換。DC故障切換可通過以下條件觸發：

1. AD聯結器檢測到當前選定的DC在某些CLDAP、LDAP、RPC或Kerberos通訊嘗試期間變得不可用。在這種情況下，AD聯結器將啟動DC選擇並故障切換到新選擇的DC。
2. DC已啟動並響應CLDAP ping，但AD聯結器由於某種原因無法與其通訊(例如：RPC埠被阻止，DC處於「中斷複製」狀態，DC尚未正確停用)。

在這些情況下，AD聯結器用阻止清單啟動DC選擇（阻止清單中有「不良」DC），並嘗試與選定的DC通訊。阻止清單中選定的DC不會快取。

AD聯結器必須在合理的時間內完成故障轉移（如果無法成功則失敗）。 因此，AD聯結器在故障轉移期間嘗試有限數量的DC。

如果存在不可恢復的網路或伺服器錯誤，ISE會阻止AD域控制器，以防止ISE使用錯誤的DC。如果DC不響應CLDAP ping，則不會將其新增到阻止清單中。ISE只降低不響應的DC的優先順序。

通過LDAP的ISE-AD通訊

ISE使用下列搜尋格式之一在AD中搜尋電腦或使用者。如果搜尋的是電腦，則ISE會在電腦名稱末尾新增「$」。這是一個身份型別清單，用於在AD中標識使用者：

- SAM名稱：使用者名稱或電腦名（不含任何域標籤），這是AD中的使用者登入名。**範例：早枝或早枝**
- CN:是AD上的使用者顯示名稱，不能與SAM相同。**範例：薩吉達·艾哈邁德。**

- 使用者主體名稱(UPN):是SAM名稱和域名(SAM_NAME@domian)的組合。 **範例：sajeda@cisco.com或sajeda$@cisco.com**

- 其他UPN:是在AD中配置的不是域名的附加/備用UPN字尾。此配置將全域性新增到AD中（未按使用者配置），並且不需要為真正的域名字尾。

每個AD可以具有多個UPN字尾(@alt1.com、@alt2.com、...等)。 **範例：主UPN(sajeda@cisco.com)，備用UPN:sajeda@domain1, sajeda@domain2**

- NetBIOS字首名稱：電腦名稱的域名\使用者名稱。**範例：CISCO\sajeda或CISCO\machine$**

- 主機/字首與不合格的電腦：當僅使用電腦名稱時，此名稱用於電腦身份驗證，它僅是主機/電腦名稱。**範例：主機/機器**

- 具有完全限定電腦的主機/字首：當使用電腦FQDN時（通常在證書身份驗證時，這是電腦的主機/FQDN），此命令用於電腦身份驗證。 **範例：host/machine.cisco.com**

- SPN名稱：客戶端唯一標識服務的例項所使用的名稱（例如：HTTP、LDAP、SSH），僅用於電腦。

針對AD流的使用者身份驗證：

1. 解析身份並確定身份型別 — SAM、UPN、SPN。如果ISE僅將身份作為使用者名稱接收，則它在AD中搜尋關聯的SAM帳戶。如果ISE接收身份為username@domain，則在AD中搜尋匹配的UPN或郵件。在這兩種情況下，ISE都使用額外的過濾器作為電腦或使用者名稱。
2. 搜尋域或林（取決於標識型別）
3. 保留有關所有關聯帳戶的資訊（JP、DN、UPN、域）
4. 如果未找到關聯帳戶，則無法識別使用者的AD回覆。
5. 對每個關聯帳戶執行MS-RPC（或Kerberos）身份驗證
6. 如果只有一個帳戶與輸入身份和密碼匹配，則身份驗證成功
7. 如果多個帳戶與傳入身份匹配，則ISE使用密碼來解決歧義性，以便具有關聯密碼的帳戶通過身份驗證，而其他帳戶將錯誤的密碼計數器增加1。
8. 如果沒有帳戶與傳入身份和密碼匹配，則AD會使用錯誤的密碼進行回覆。

ISE 搜尋篩選條件

過濾器用於標識要與AD通訊的實體。 ISE始終在使用者和電腦組中搜尋該實體。

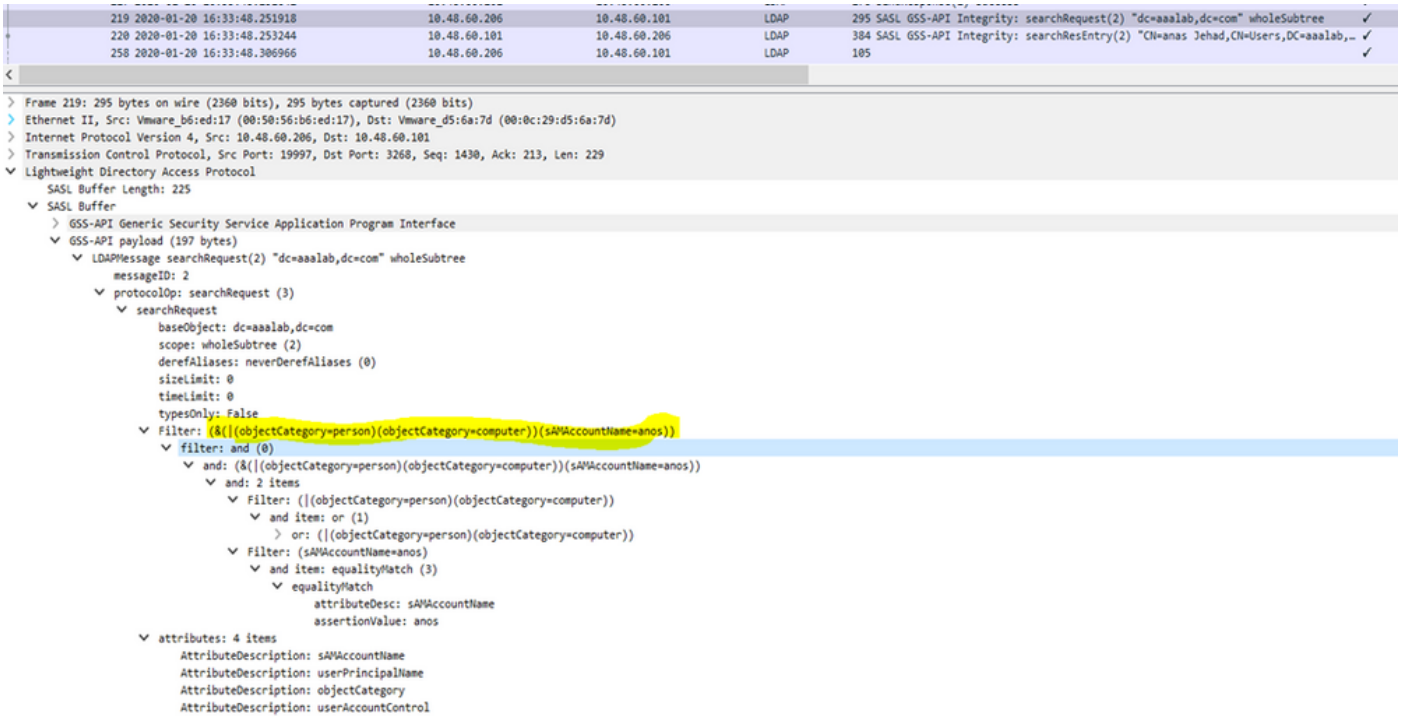
搜尋過濾器示例：

1. **SAM搜尋**：如果ISE只收到一個使用者名稱的身份，而沒有任何域標籤，則ISE將此使用者名稱視為SAM，並在AD中搜尋所有具有該身份為SAM名稱的電腦使用者或電腦。

如果SAM名稱不唯一，ISE使用密碼區分使用者，ISE配置為使用無密碼協定，例如EAP-TLS。

沒有其他條件來定位正確的使用者，因此ISE身份驗證失敗，出現「模糊身份」錯誤。

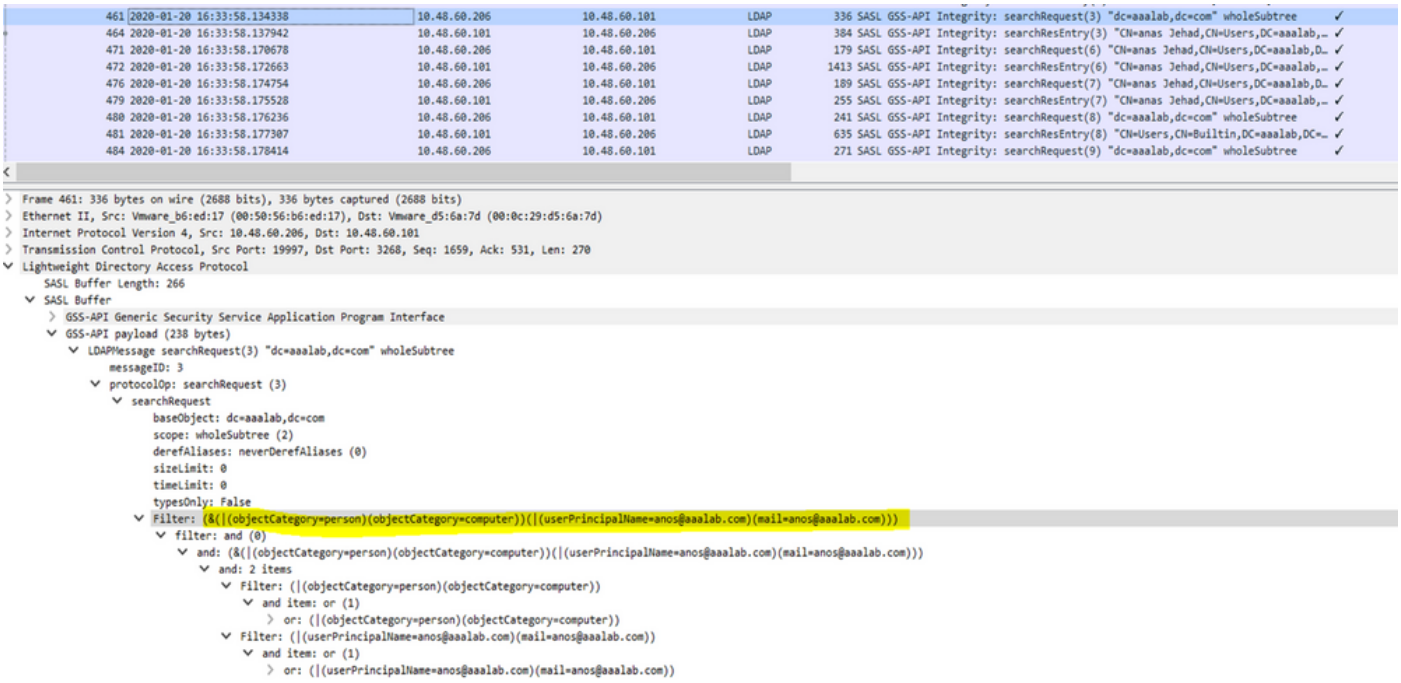
但是，如果使用者證書存在於Active Directory中，思科ISE使用二進位制比較解析身份。



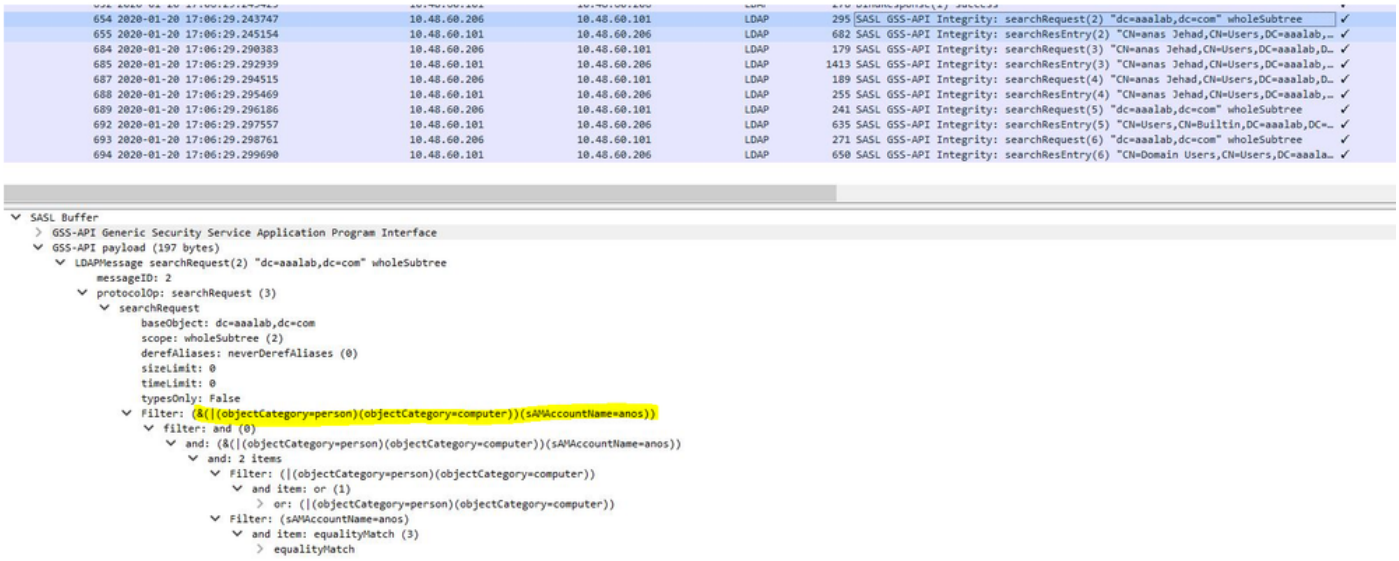
2. **UPN或MAIL搜尋**：如果ISE收到身份為username@domain，則ISE搜尋每個林全域性目錄以查詢與該UPN身份或郵件身份「身份=匹配的UPN或電子郵件」的匹配項。

如果存在唯一匹配，思科ISE繼續處理AAA流。

如果存在多個具有相同UPN和密碼或相同UPN和郵件的加入點，思科ISE會以「模糊身份」錯誤來失敗身份驗證。



3. **NetBIOS搜尋**：如果ISE收到帶有NetBIOS域字首的標識（例如：CISCO\sajedah），則ISE在林中搜尋NetBIOS域。找到後，它會查詢提供的SAM名稱（在我們的示例中為sajeda）

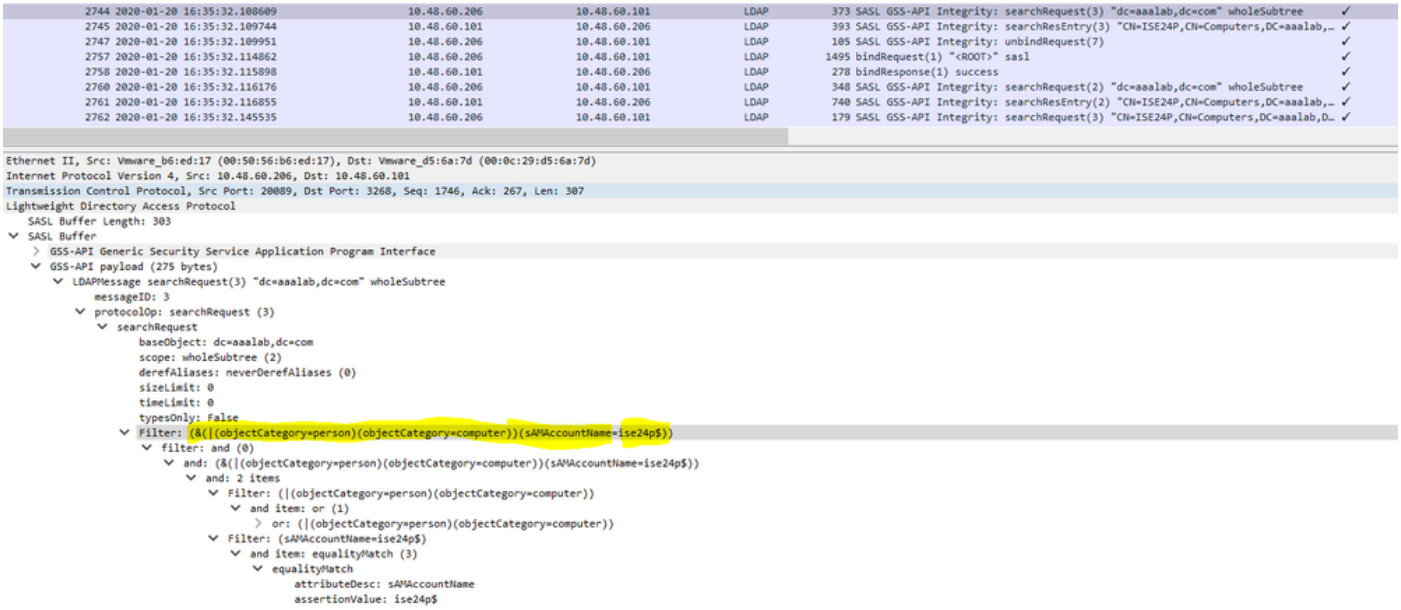


4. **基於電腦的搜尋**：如果ISE收到具有主機/字首標識的電腦身份驗證，則ISE在林中搜尋匹配的servicePrincipalName屬性。

如果在身份中指定了完全限定域字尾(例如host/machine.domain.com)，思科ISE會搜尋該域所在的林。

如果身份採用主機/電腦形式，思科ISE會搜尋所有林中的服務主體名稱。

如果存在多個匹配項，思科ISE會因「模糊身份」錯誤而身份驗證失敗。



附註：在ISE ad-agent.log檔案中看到相同的過濾器

附註：ISE 2.2補丁4和之前的補丁1和之前的補丁1和之前的已識別使用者，屬性為SAM、CN或兩者。Cisco ISE版本2.2補丁5和更高版本以及2.3補丁2和更高版本僅使用sAMAccountName屬性作為預設屬性。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。