了解身份服务引擎和Active Directory

目录

简介

先决条件

- 要求
- 使用的组件

AD协议

- Kerberos协议
- MS-RPC协议
  - ISE与Active Directory(AD)集成
- 将ISE加入AD
- 加入AD域
- 退出AD域
- DC故障转移
- 通过LDAP的ISE-AD通信
- 针对AD流进行用户身份验证：
- ISE搜索过滤器

简介

本文档介绍身份服务引擎(ISE)和Active Directory(AD)如何通信、使用的协议、AD过滤器和流程。

先决条件

要求

思科建议您掌握以下方面的基本知识：

- ISE上的外部身份身份验证
- ISE 2.x和Active Directory集成

使用的组件

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

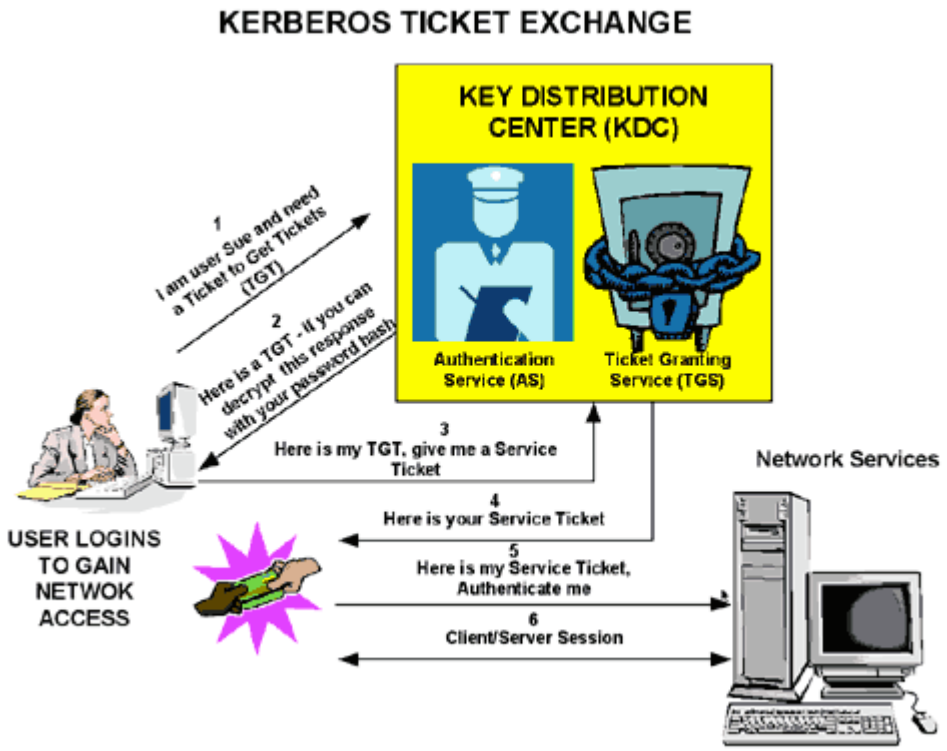
AD协议

Kerberos协议

Kerberos的三个头由密钥分发中心(KDC)、客户端用户和要访问的服务器组成。KDC作为域控制器(DC)的一部分进行安装，并执行以下两项服务功能：身份验证服务(AS)和票证授予服务(TGS)。

客户端最初访问服务器资源时，涉及三个交换：

1. AS交换
2. TGS交换
3. 客户端/服务器(CS)交换

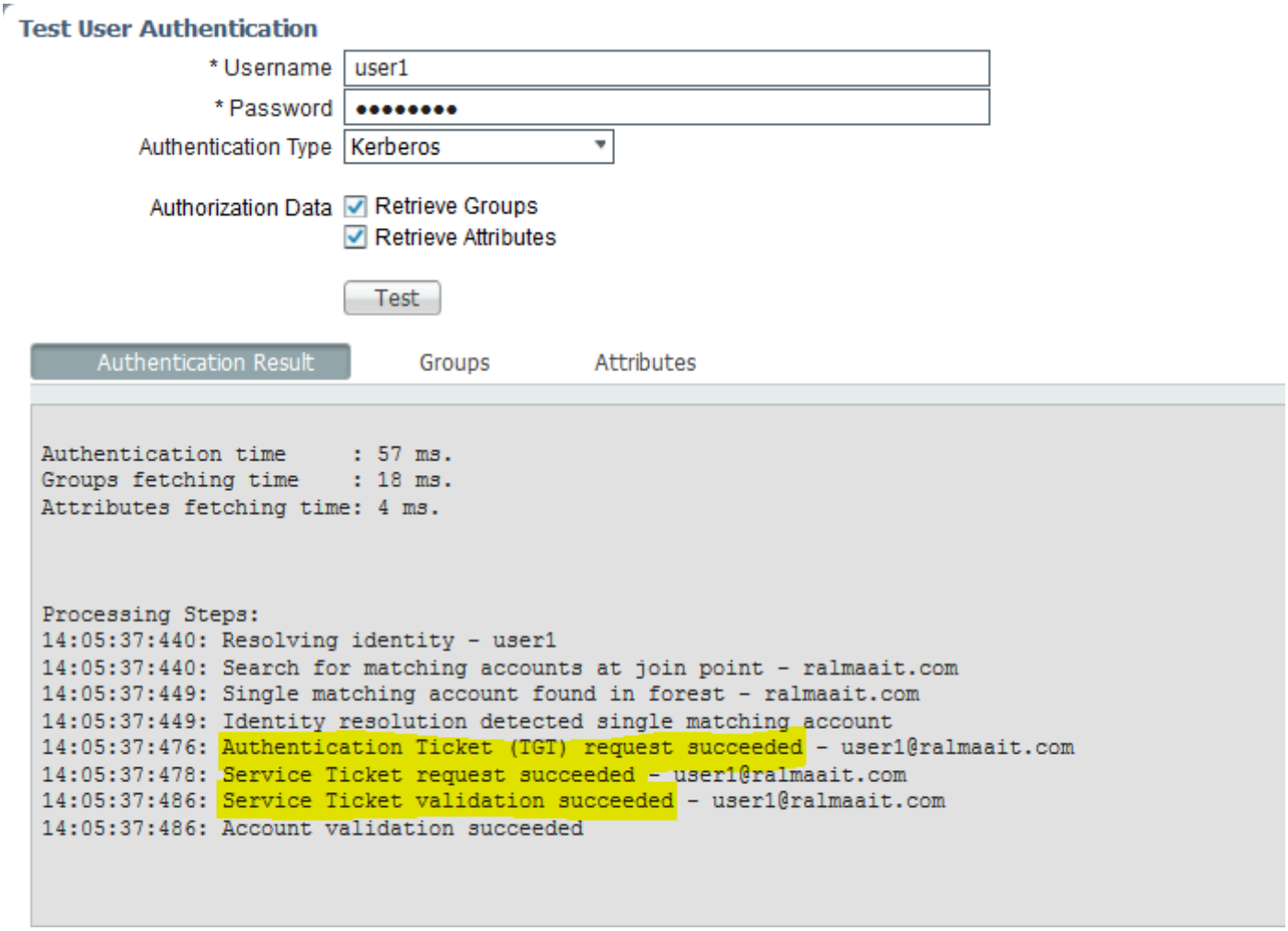


- 域控制器= KDC(AS + TGS)
- 使用您的密码向AS（SSO门户）进行身份验证
- 获取票证授予票证(TGT)（会话cookie）
- 请求登录服务(SRV01)
- SRV01将您重定向到KDC
- Show TGT to KDC —（我已经通过身份验证）
- KDC为您提供SRV01的TGS
- 重定向至SRV01
- 显示到SRV01的服务票证
- SRV01验证/信任服务票证
- 服务票证包含我的所有信息
- SRV01让我登录

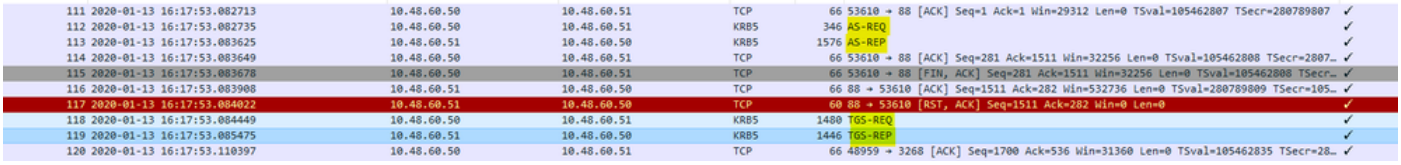
初次登录网络时，用户必须协商访问权限并提供登录名称和密码，以由其域内的KDC的AS部分进行验证。KDC有权访问Active Directory用户帐户信息。通过身份验证后，用户将被授予对本地域有效的票证授予票证(TGT)。TGT的默认有效期为10小时，在用户登录会话期间续订，无需用户重新输入密码。TGT缓存在易失性存储器空间中的本地计算机上，用于请求与整个网络中服务的会话。

当需要访问服务器服务时，用户向KDC的TGS部分提供TGT。KDC上的TGS对用户TGT进行身份验证，并为客户端和远程服务器创建票证和会话密钥。然后，此信息（服务票证）在客户端计算机上本地缓存。TGS接收客户端TGT并使用其自己的密钥进行读取。如果TGS批准客户端请求，将为客户端和目标服务器生成服务票证。客户端使用之前从AS应答检索的TGS会话密钥读取其部分。客户端在下一次客户端/服务器交换时向目标服务器提供TGS应答的服务器部分。

示例：

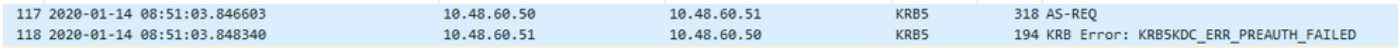


从ISE为经过身份验证的用户捕获的数据包：



AS-REQ包含用户名。如果密码正确，则AS服务提供使用用户密码加密的TGT。然后为TGT提供接收会话票证的TGT服务。当收到会话票证时，身份验证成功。

以下示例说明客户端提供的密码不正确：



如果密码不正确，则AS请求会失败，且不会收到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
```

在此下一个示例中，当密码不正确时，以下是ad_agent.log文件中的日志：

2020-01-14 13:36:05,442 DEBUG，140574072981248,krb5:将请求（276字节）发送到RALMAAIT.COM,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG，140574072981248,krb5:收到来自KDC的错误：-1765328360/预身份验证失败，LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG，140574072981248,krb5:预身份验证重试输入类型：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错误代码：-1765328360(消息：预身份验证失败),LwTranslateKrb5Error(),lwadvapi/threaded/lwkrb5.c:892

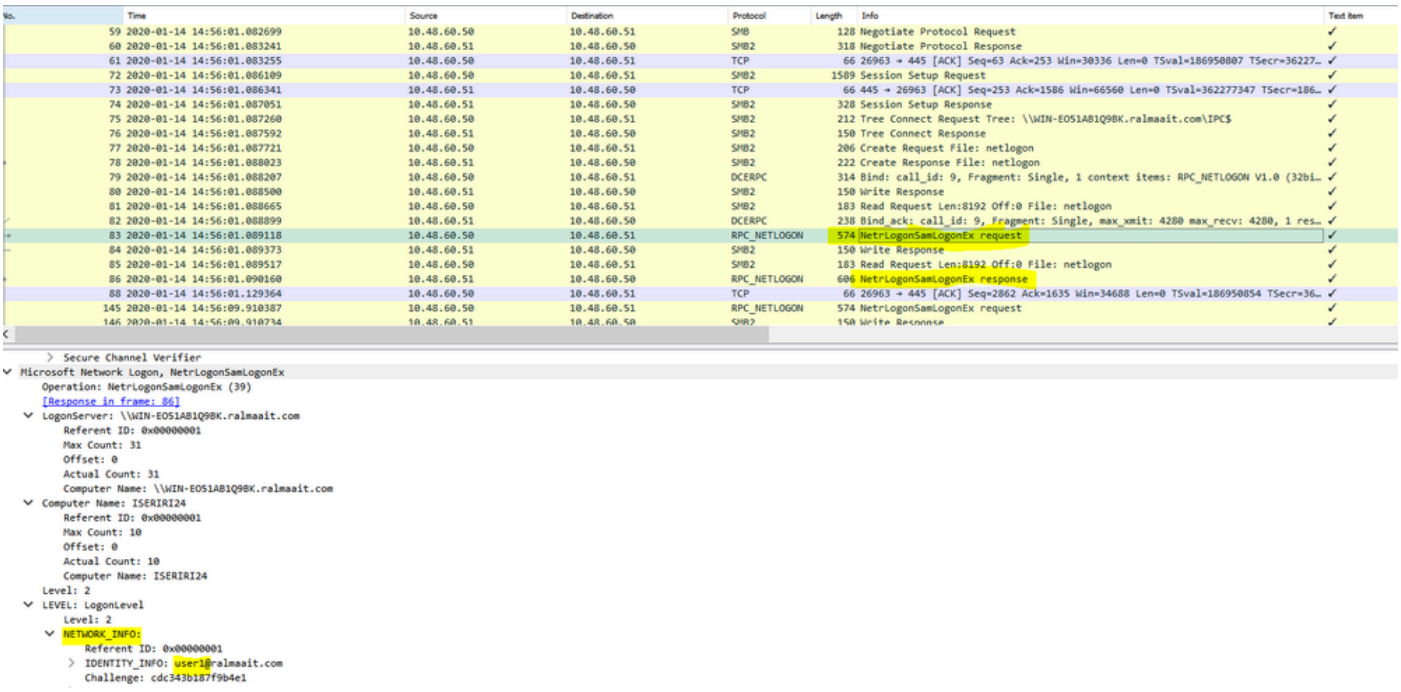
2020-01-14 13:36:05,444 DEBUG，140574072981248,[LwKrb5InitializeUserLoginCredentials()]错误代码：40022(符号：LW_ERROR_PASSWORD_MISMATCH),LwKrb5InitializeUserLoginCredentials(),lwadvapi/threaded/lwk

---

MS-RPC协议

ISE使用MS-RPC over SMB，而SMB提供身份验证，不需要单独的会话来查找给定RPC服务的位置。它使用名为“命名管道”的机制在客户端和服务器之间通信。

- 创建SMB会话连接
- 通过SMB/CIFS.TCP端口445传输RPC消息作为传输
- SMB会话标识特定RPC服务运行和处理用户身份验证的端口
- 连接到隐藏共享IPC$，进行进程间通信
- 为所需的RPC资源/功能打开相应的命名管道
- 通过SMB处理RPC交换



---

negotiate protocol request/response行协商SMB的方言，会话设置请求/响应执行身份验证。树连接请求和响应连接到请求的资源。您已连接到特殊共享IPC$。这种进程间通信共享提供了主机之间的通信方式，也作为MSRPC功能的传输方式。

Packet 77是Create Request File，文件名是连接的服务（本示例中为netlogon服务）的名称。

数据包83和86是NetrlogonSamLogonEX请求，在该请求中，您将ISE上客户端身份验证的用户名发送到AD的Network_INFO字段。NetrlogonSamLogonEX响应数据包回复结果。

NetrlogonSamLogonEX响应的某些标志值：

0xc000006a为STATUS_WRONG_PASSWORD
0x00000000为STATUS_SUCCESS
0x00000103为STATUS_PENDING

ISE与Active Directory(AD)集成

ISE使用LDAP、KRB和MSRBC在加入/退出和身份验证过程中与AD通信。以下各节提供了用于连接到AD上的特定DC以及针对该DC进行用户身份验证的协议、搜索格式和机制。如果DC因任何原因变为脱机，ISE会故障切换到下一个可用的DC，身份验证过程不受影响。

全局编录服务器(GC)是域控制器，用于存储林中所有Active Directory对象的副本。它存储域目录中所有对象的完整副本以及所有其他林域的所有对象的部分副本。全局编录允许用户和应用程序通过搜索包含在GC中的属性在当前林的任何域中查找对象。全局编录包含每个域中每个林对象的基本（但不完整）属性集（部分属性集、PAT）。

GC从林中的所有域目录分区接收数据，这些数据将使用标准AD复制服务进行复制。

将ISE加入AD

Active Directory和ISE集成的必备条件。

1. 在ISE中验证您具有超级管理员或系统管理员的权限。
2. 使用网络时间协议(NTP)服务器设置同步Cisco服务器和Active Directory之间的时间。ISE和AD之间允许的最大时间差为5分钟。
3. 在ISE上配置的DNS必须对DC、GC和KDC的SRV查询进行应答，无论是否包含其他站点信息。
4. 确保所有DNS服务器都可以应答任何可能的Active Directory DNS域的前向和反向DNS查询。
5. 对于您计划与思科加入的域，AD必须至少有一个全局目录服务器可运行并可由思科访问。

加入AD域

ISE应用域发现以分三个阶段获取有关加入域的信息：

1. 查询加入的域 — 发现其林中的域和加入的域外部信任的域。
2. 查询其林中的根域 — 与林建立信任关系。
3. Queries root domains in trusted forest — 发现受信任林中的域。

此外，思科ISE发现DNS域名（UPN后缀）、备用UPN后缀和NTLM域名。

ISE应用DC发现以获取有关可用DC和GC的所有信息。

1. 加入过程以域本身存在的AD上超级管理员的输入凭证开始。如果用户名存在于不同的域或子域中，则必须使用UPN表示法(username@domain)记录用户名。
2. ISE发送针对所有DC、GC和KDC记录的DNS查询。如果DNS回复未收到应答，则集成失败，并出现DNS相关错误。
3. ISE使用CLDAP ping通过向DC发送的CLDAP请求来发现所有DC和GC，这些DC与SRV记录中的优先级相对应。使用第一个DC响应，并且ISE连接到该DC。

用于计算DC优先级的一个因素是DC响应CLDAP ping所用的时间；响应速度越快，优先级越高。



注意：CLDAP是ISE用来建立和维护与DC连接的机制。它测量第一个DC应答之前的响应时间。如果您没有看到来自DC的答案，它将失败。如果响应时间大于2.5秒，则发出警告。CLDAP ping站点上的所有DC（如果没有站点，则对域中的所有DC执行ping操作）。CLDAP响应包含DC站点和客户端站点（分配ISE计算机的站点。）

---

4. ISE接收具有“加入用户”凭证的TGT。
5. 使用MSRPC（SAM和SPN）生成ISE计算机帐户名称。
6. 如果ISE计算机帐户已存在，则按SPN搜索AD。如果ISE计算机不存在，ISE将创建一个新计算机。
7. 打开计算机帐户并设置ISE计算机帐户密码，并验证ISE计算机帐户是否可访问。
8. 设置ISE计算机帐户属性（SPN、dns主机名等）。
9. 使用KRB5接收ISE计算机凭证的TGT并发现所有受信任域。
10. 当加入完成时，ISE节点更新其AD组和关联的SID并自动开始SID更新过程。在AD端验证此过程是否可完成。

退出AD域

当ISE离开时，AD必须考虑：

1. 使用完整的AD管理员用户执行离开流程。这将验证ISE计算机帐户是否已从Active Directory数据库中删除。
2. 如果AD没有凭证，ISE帐户不会从AD中删除，必须手动删除。
3. 当从CLI重置ISE配置或在备份或升级后恢复配置时，它会执行离开操作并从Active Directory域断开ISE节点。但是，如果加入，ISE节点帐户不会从Active Directory域中删除。
4. 建议使用Active Directory凭证从管理员门户执行离开操作，因为它还会从Active Directory域中删除节点帐户。当您更改ISE主机名时，也建议这样做。

DC故障转移

当连接到ISE的DC因任何原因离线或不可访问时，DC故障切换在ISE上自动触发。DC故障切换可通过以下条件触发：

1. AD连接器检测到当前选定的DC在某些CLDAP、LDAP、RPC或Kerberos通信尝试期间变得不可用。在这种情况下，AD连接器将启动DC选择并故障切换到新选择的DC。

2. DC已启动并响应CLDAP ping，但是，由于某些原因，AD连接器无法与其通信（例如，RPC端口被阻塞，DC处于“中断复制”状态，DC未正确停用）。

在这种情况下，AD连接器启动带有阻止列表的DC选择（“不良”DC被置于阻止列表中），并尝试与选定的DC通信。阻止列表中选定的DC不会缓存。

AD连接器必须在合理的时间内完成故障切换（如果可能的话，请发生故障）。 因此，AD连接器在故障切换期间尝试有限数量的DC。如果存在无法恢复的网络或服务器错误，ISE会阻止AD域控制器，以防止ISE使用错误的DC。如果DC不响应CLDAP ping，则不会将其添加到阻止列表中。ISE只在DC不响应时降低其优先级。

通过LDAP的ISE-AD通信

ISE使用以下搜索格式之一在AD中搜索计算机或用户。如果搜索的是计算机，则ISE会在计算机名称末尾添加“$”。这是用于标识AD中用户的身份类型列表：

- SAM名称：用户名或计算机名，不带任何域标记，这是AD中的用户登录名。示例：Sajeda或sajeda$
- CN:这是AD上的用户显示名称，不能与SAM相同。示例：萨赫达·艾哈迈德
- 用户主体名称(UPN):这是SAM名称和域名(SAM_NAME@domian)的组合。 示例：或sajeda$@cisco.com
- 备用UPN:这是在AD中配置的除域名以外的其他/备用UPN后缀。此配置在AD中全局添加（未按用户配置），不需要为实际域名后缀。
    - 每个AD可以有多个UPN后缀（@alt1.com、@alt2.com等）。 例如，主UPN(sajeda@cisco.com)、备用UPN:sajeda@domain1、sajeda@domain2
- NetBIOS前缀名称：这是计算机名称的域名/用户名。例如，CISCO\sajeda或CISCO\machine$
- 具有不合格计算机的主机/前缀：当仅使用计算机名称且仅使用主机/计算机名称时，此命令用于计算机身份验证。例如，主机/计算机。
- 具有完全限定计算机的主机/前缀：当使用计算机FQDN时，这用于计算机身份验证，通常在证书身份验证的情况下。它是计算机的主机/FQDN。例如，host/machine.cisco.com。

- SPN名称：客户端的名称，用于唯一标识仅用于计算机的服务（例如，HTTP、LDAP、SSH）实例。

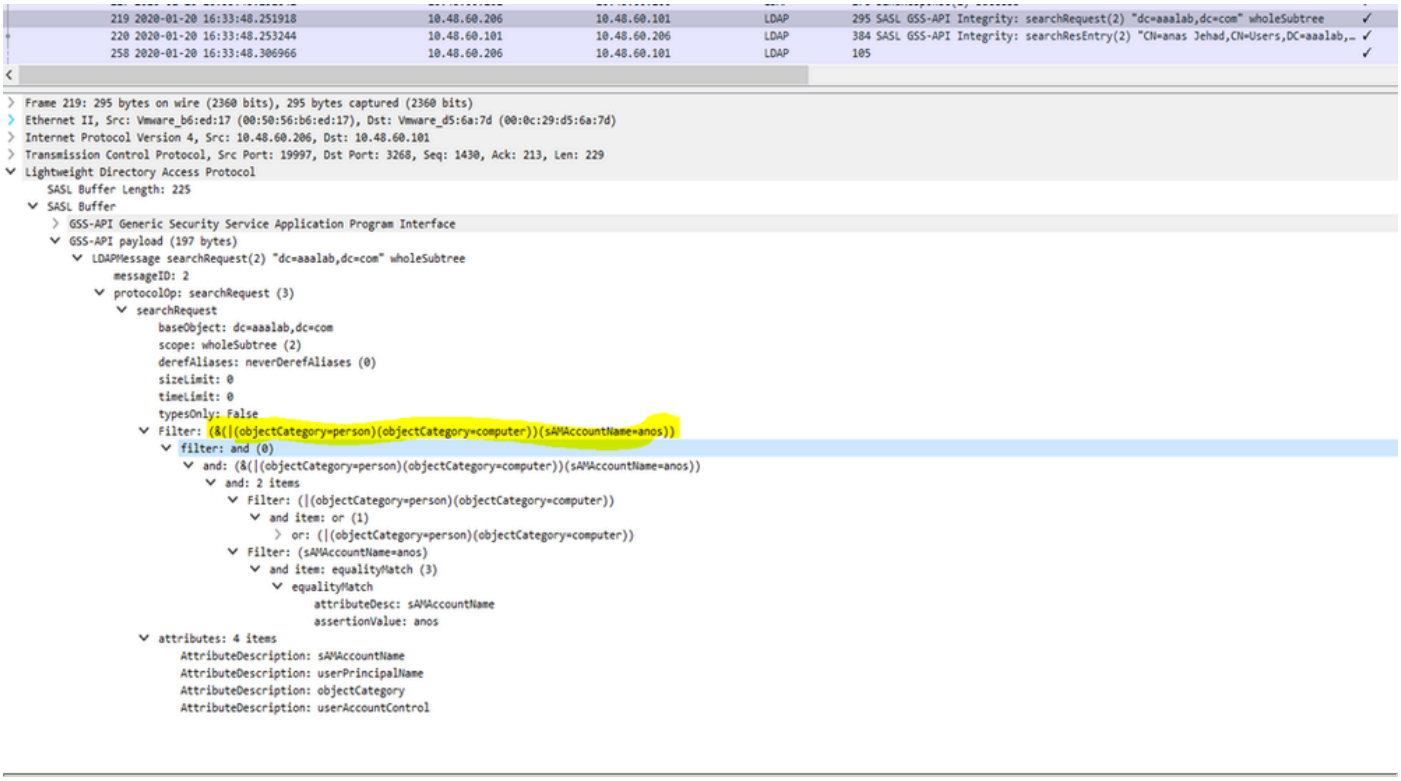
针对AD流进行用户身份验证：

1. 解析身份并确定身份类型 — SAM、UPN、SPN。如果ISE仅以用户名形式接收身份，则会在AD中搜索关联的SAM帐户。如果ISE收到身份为username@domain，它会在AD中搜索匹配的UPN或邮件。在这两种情况下，ISE对计算机或用户名使用其他过滤器。
2. 搜索域或林（取决于身份类型。）
3. 保留所有关联帐户（JP、DN、UPN、域）的信息。
4. 如果未找到关联帐户，则无法识别用户的AD回复。
5. 对每个关联帐户执行MS-RPC（或Kerberos）身份验证。
6. 如果只有一个帐户与输入身份和密码匹配，则身份验证成功。
7. 如果多个帐户与传入身份匹配，则ISE使用密码解决歧义，并且使用关联密码的帐户进行身份验证，而其他帐户将不正确的密码计数器增加1。
8. 如果没有帐户与传入的标识和密码匹配，则AD会使用错误的密码进行回复。

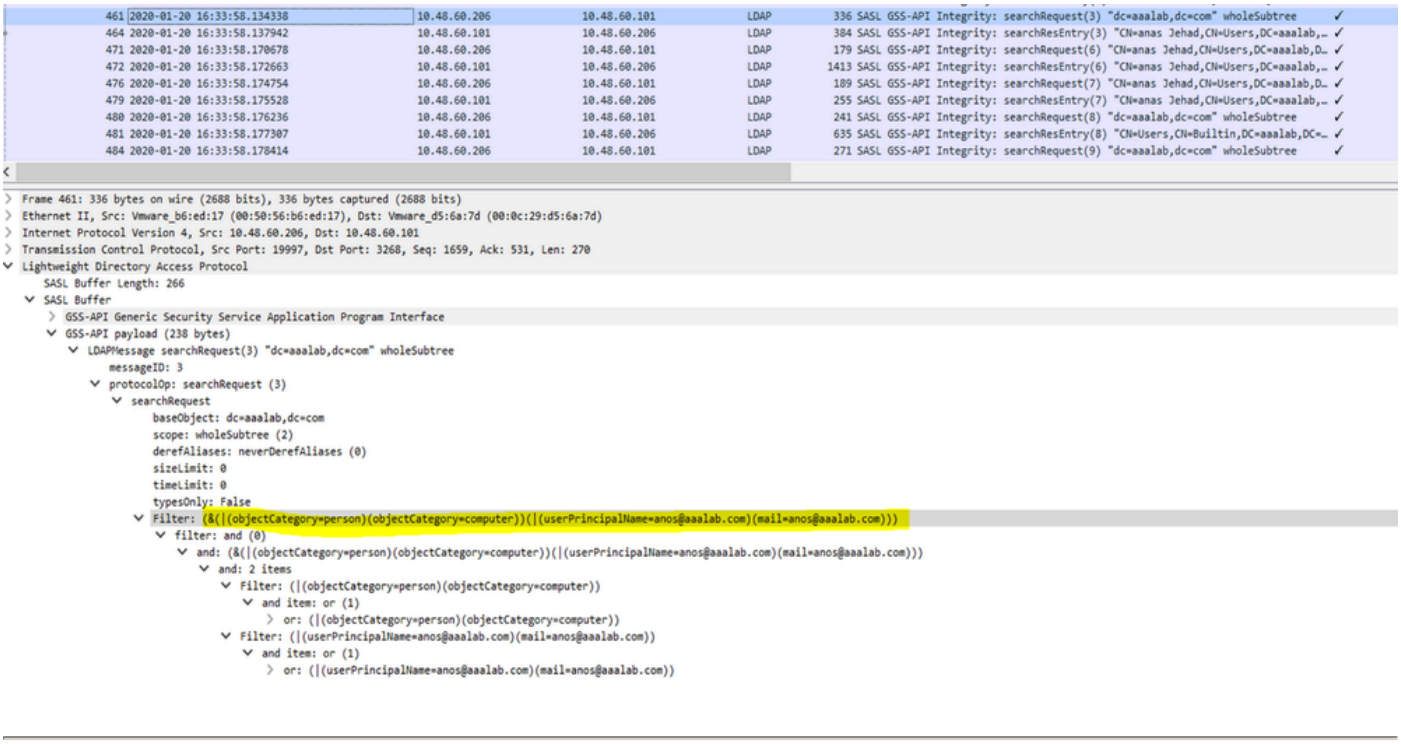
ISE搜索过滤器

过滤器用于标识要与AD通信的实体。ISE始终搜索用户和计算机组中的实体。搜索过滤器的示例：

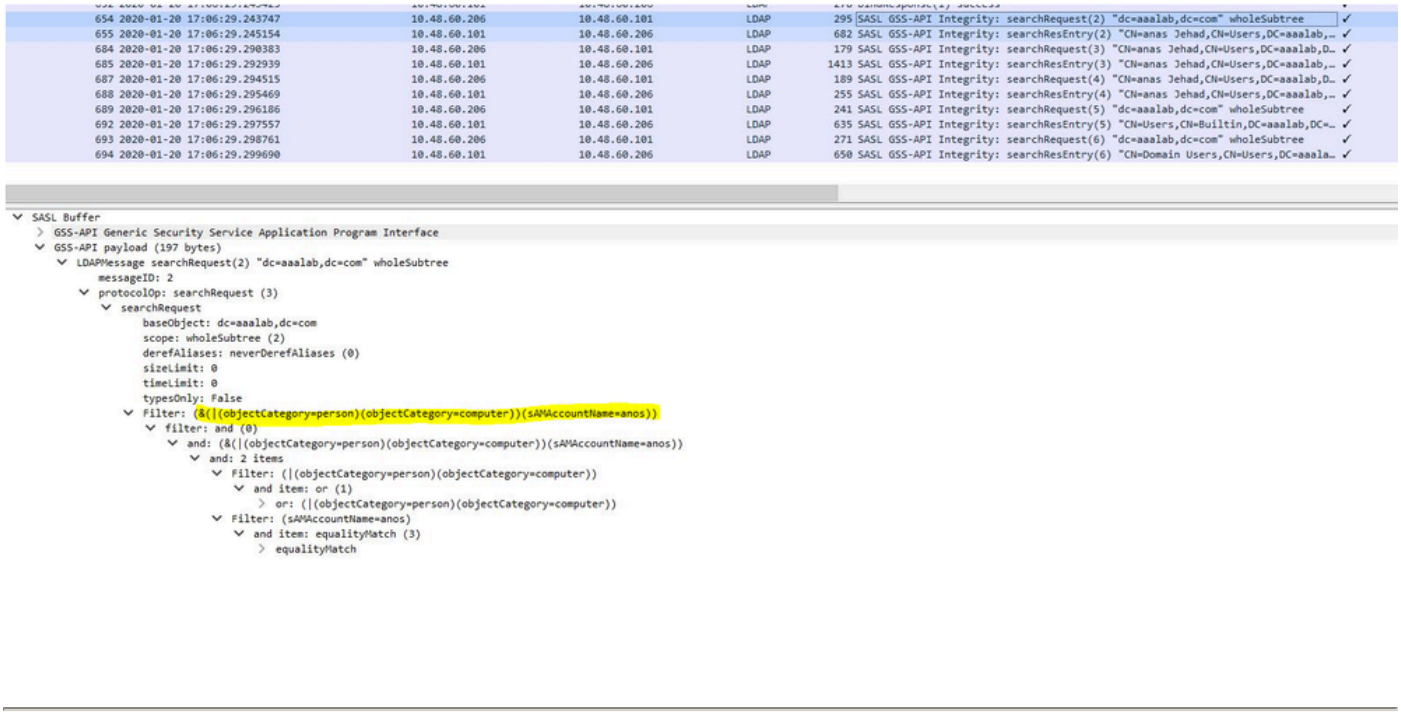
1. SAM搜索：如果ISE仅收到作为用户名的身份而不使用任何域标记，则ISE将用户名视为SAM并在AD中搜索所有具有身份为SAM名称的计算机用户或计算机。
2. 如果SAM名称不唯一，ISE使用密码区分用户，并且ISE配置为使用无密码协议，例如EAP-TLS。
3. 没有其他条件可以定位正确的用户，因此ISE身份验证失败并出现“模糊身份”错误。但是，如果用户证书存在于Active Directory中，思科ISE使用二进制比较解析身份。



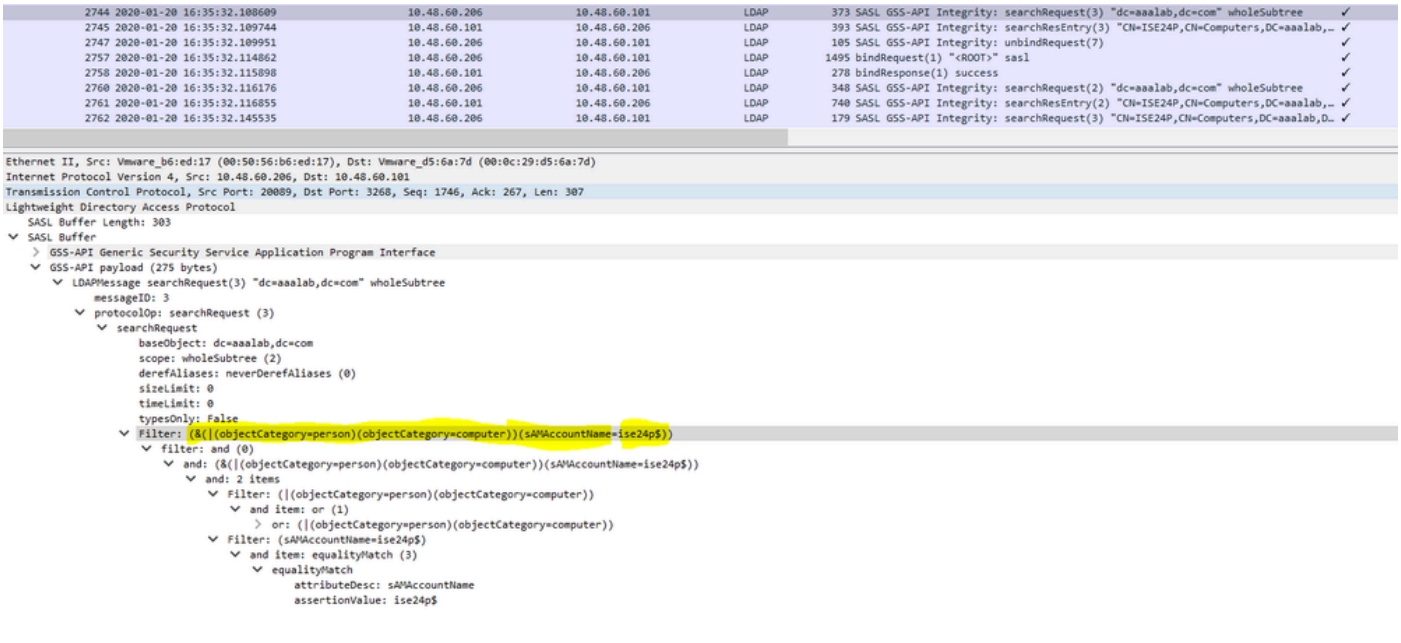
2. UPN或邮件搜索:如果ISE收到身份为username@domain的身份，ISE会搜索林全局目录以查找与UPN身份或邮件身份“身份=匹配的UPN或邮件”的匹配项。如果存在唯一匹配，思科ISE继续执行AAA流。如果有多个具有相同UPN和密码的加入点，或相同UPN和邮件，思科ISE会由于“模糊身份”错误而无法进行身份验证。



3. NetBIOS搜索:如果ISE收到带有NetBIOS域前缀的身份（例如，CISCO\sajedah），则ISE搜索NetBIOS域的林。找到后，它会查找提供的SAM名称（例如sajeda）。



4. 计算机基础搜索:如果ISE收到具有主机/前缀标识的计算机身份验证，则ISE会在林中搜索匹配的servicePrincipalName属性。如果在标识中指定了完全限定域后缀，例如host/machine.domain.com。思科ISE搜索域所在的林。如果身份采用主机/计算机形式，思科ISE会搜索所有林的服务主体名称。如果存在多个匹配项，思科ISE会由于“模糊身份”错误而无法进行身份验证。



注意：在ISE ad-agent.log文件中可以看到相同的过滤器。

注意：ISE 2.2补丁4、2.3补丁、1和先前识别的用户属性SAM、CN或两者。思科ISE版本

2.2补丁5及更高版本和2.3补丁2及更高版本仅使用sAMAccountName属性作为默认属性。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。