Understand Identity Service Engine and Active Directory

Contents

Introduction

Prerequisites

- Requirements
- Components Used

AD Protocols

- Kerberos Protocol
- MS-RPC Protocol
  - ISE Integration with Active Directory (AD)
- Join ISE to AD
- Join AD domain
- Leave AD domain
- DC Failover
- ISE-AD Communication through LDAP
- User Authentication Against AD Flow:
- ISE SearchFilters

Introduction

This document describes how Identity Service Engine (ISE) and Active Directory (AD) communicate, protocols that are used, AD filters, and flows.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of:

- External Identity Authentication on ISE
- ISE 2.x and Active Directory Integration

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

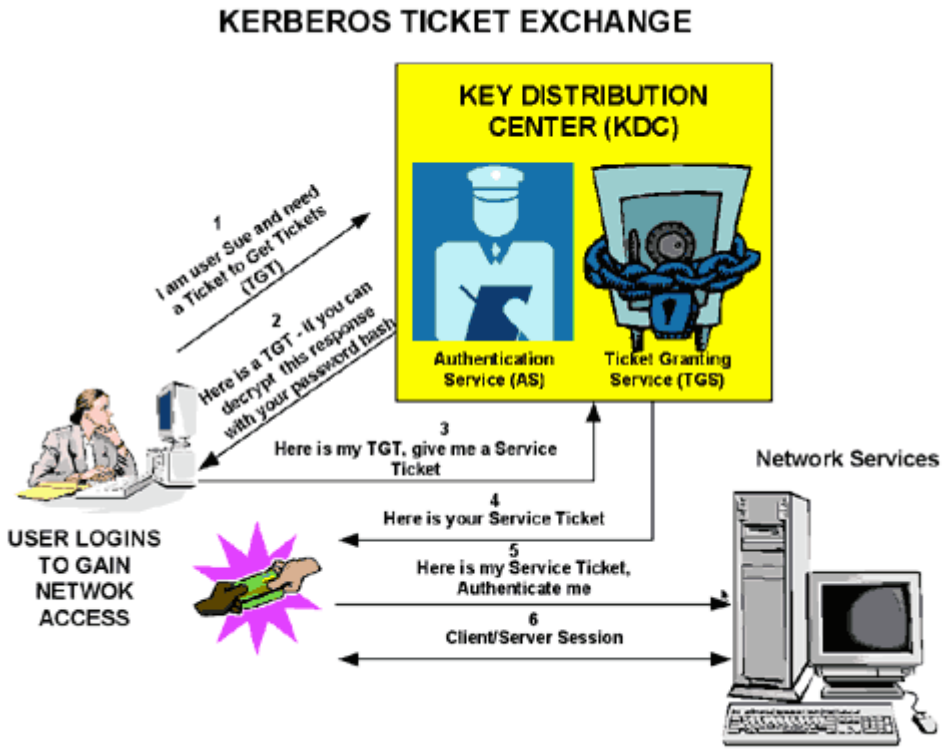
AD Protocols

Kerberos Protocol

The three heads of Kerberos comprise of the Key Distribution Center (KDC), the client user, and the server to access. The KDC is installed as part of the Domain Controller (DC) and performs two service functions: The Authentication Service (AS) and the Ticket-Granting Service (TGS).

Three exchanges are involved when the client initially accesses a server resource:

1. AS Exchange
2. TGS Exchange
3. Client/Server (CS) Exchange

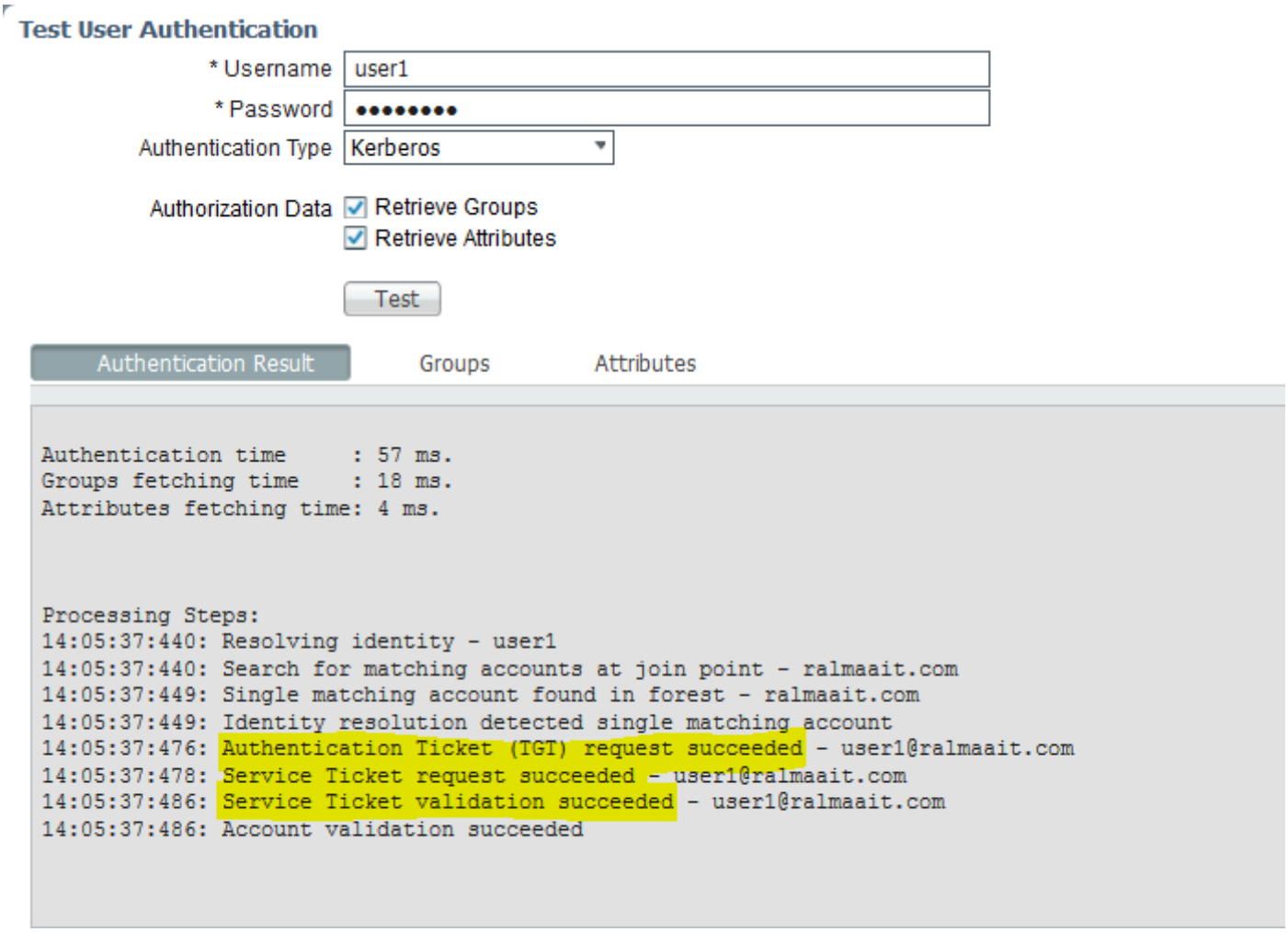


- Domain Controller = KDC (AS + TGS)
- Authenticate to AS (the SSO portal) with your password
- Obtain a Ticket Granting Ticket (TGT) (a session cookie)
- Request log in to a service (SRV01)
- SRV01 redirects you to KDC
- Show TGT to KDC – (I am already authenticated)
- KDC gives you TGS for SRV01
- Redirect to SRV01
- Shows service ticket to SRV01
- SRV01 verifies/trusts service ticket
- Service ticket has all my information
- SRV01 logs me in

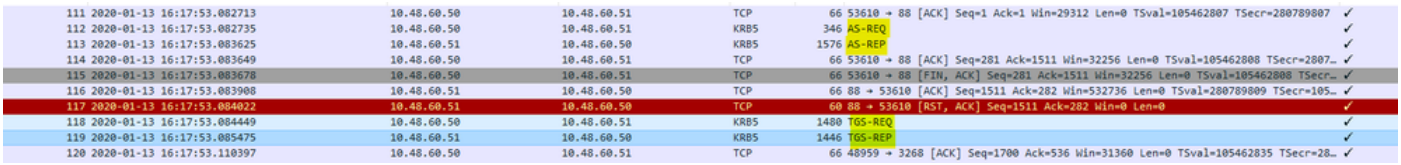
When initially logged onto a network, users must negotiate access and provide a log-in name and password to be verified by the AS portion of a KDC within their domain. The KDC has access to Active Directory user account information. Once authenticated, the user is granted a Ticket Granting Ticket (TGT) that is valid for the local domain. The TGT has a default lifetime of 10 hours and is renewed throughout the user log-on session without the requirement of the user to re-enter the password. The TGT is cached on the local machine in volatile memory space and is used to request sessions with services throughout the network.

The user presents the TGT to the TGS portion of the KDC when access to a server service is needed. The TGS on the KDC authenticates the user TGT and creates a ticket and session key for both the client and the remote server. This information (the service ticket) is then cached locally on the client machine. The TGS receives the client TGT and reads with its own key. If the TGS approves of the client request, a service ticket is generated for both the client and the target server. The client reads its portion with the TGS session key retrieved earlier from the AS reply. The client presents the server portion of the TGS reply to the target server in the next client/server exchange.

Example:

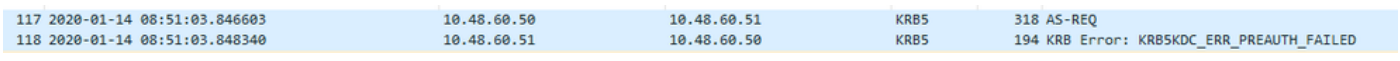


Packet captures from ISE for an authenticated user:



The AS-REQ contains the username. If the password is correct, the AS service provides a TGT encrypted with the users password. The TGT is then provided the TGT service to receive a session ticket. Authentication is successful when a session ticket is received.

This is an example where the password given by the client is incorrect:



If the password is incorrect, the AS request fails and the TGT is not received:

```
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
```

In this next example, these are logs on the ad_agent.log file when the password is incorrect:

2020-01-14 13:36:05,442 DEBUG ,140574072981248,krb5: Sent request (276 bytes) to RALMAAIT.COM,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG ,140574072981248,krb5: Received error from KDC: -1765328360/Preauthentication failed,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG ,140574072981248,krb5: Preauth tryagain input types: 16, 14, 19, 2,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

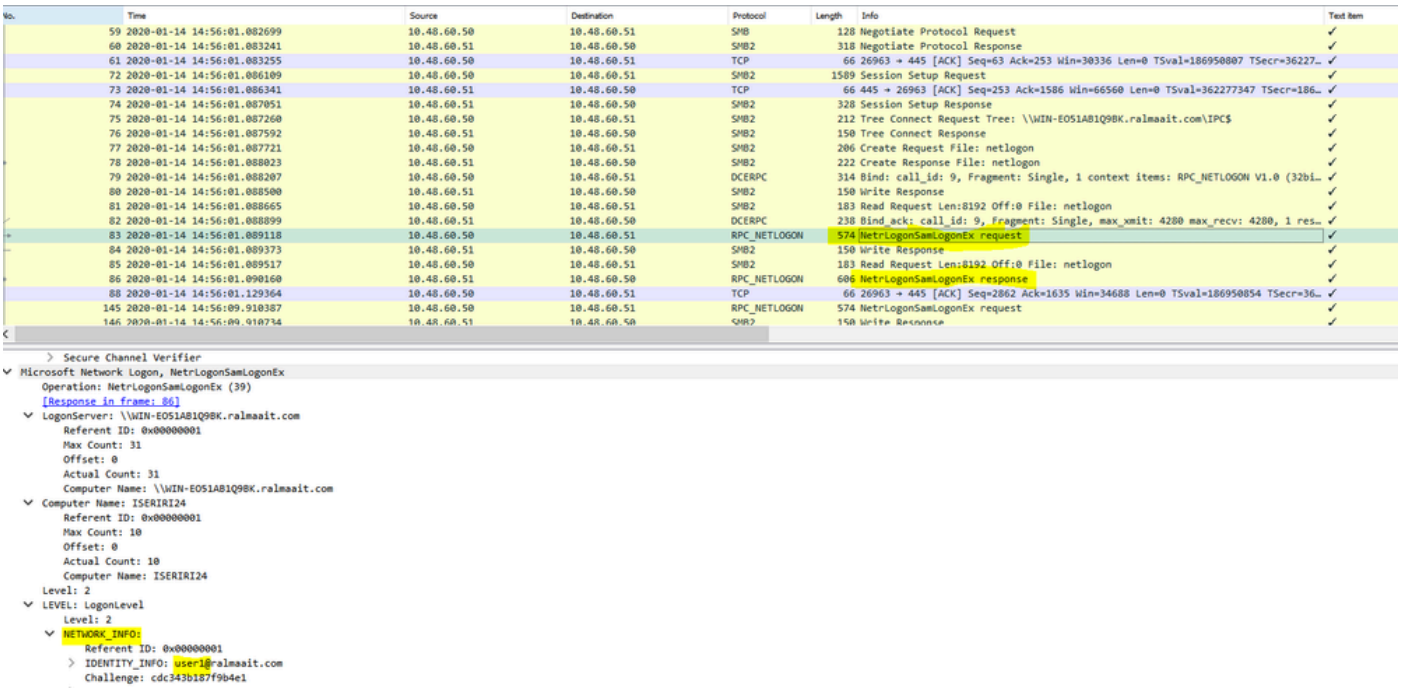
2020-01-14 13:36:05,444 WARNING,140574072981248,[LwKrb5GetTgtImpl ../../lwadvapi/threaded/krbtgt.c:329] KRB5 Error code: -1765328360 (Message: Preauthentication failed),LwTranslateKrb5Error(),lwadvapi/threaded/lwkrb5.c:892

2020-01-14 13:36:05,444 DEBUG ,140574072981248,[LwKrb5InitializeUserLoginCredentials()] Error code: 40022 (symbol: LW_ERROR_PASSWORD_MISMATCH),LwKrb5InitializeUserLoginCredentials(),lwadvapi/threaded/lwkrb5.c:14

MS-RPC Protocol

ISE uses MS-RPC over SMB, and SMB provides the authentication and does not require a separate session to find where a given RPC service is located. It uses a mechanism called “named pipe” to communicate between the client and server.

- Create an SMB session connection
- Transport RPC messages over SMB/CIFS.TCP port 445 as a transport
- SMB session identifies which port a particular RPC service runs and handles user authentication
- Connect to hidden share IPC$ for inter-process communication
- Open an appropriate named pipe for the desired RPC resource/function
- Transact the RPC exchange over SMB



The **negotiate protocol request/response** line negotiates the dialect of SMB and the **session setup request/response** performs the authentication. Tree Connect Request and Response connect to the requested resource. You are connected to a special share IPC$. This inter-process communication share provides the means of communication between hosts and also as a transport for MSRPC functions.

Packet 77 is the **Create Request File** and the file name is the name of the connected service (the netlogon service in this example).

Packets 83 and 86 are the NetrlogonSamLogonEX request, which is where you send the username for the client authentication on ISE to the AD at the field Network_INFO. The NetrlogonSamLogonEX response packet replies with the results.

Some flags values for the NetrlogonSamLogonEX response:

0xc000006a is STATUS_WRONG_PASSWORD
0x00000000 is STATUS_SUCCESS
0x00000103 is STATUS_PENDING

ISE Integration with Active Directory (AD)

ISE uses LDAP, KRB, and MSRBC to communicate with AD during the join/leave and authentication process. The next sections provide the protocols, search format, and mechanisms used to connect to a specific DC on AD and user authentication against that DC. If the DC becomes offline for any reason, ISE

fails over to the next available DC and the authentication process is not affected.

A Global Catalog server (GC) is a domain controller that stores copies of all Active Directory objects in the forest. It stores a complete copy of all objects in the directory of your domain and a partial copy of all objects of all other forest domains. The Global Catalog allows users and applications to find objects in any domain of the current forest with a search for attributes included to the GC. The Global Catalog contains a basic (but incomplete) set of attributes for each forest object in each domain (Partial Attribute Set, PAT).

The GC receives data from all domain directory partitions in the forest and they are copied with the standard AD replication service.

Join ISE to AD

Prerequisites for Active Directory and ISE integrations.

1. Verify you have privileges of a Super Admin or System Admin in ISE.
2. Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco server and Active Directory. The maximum allowed time difference between ISE and AD is 5 minutes.
3. The configured DNS on ISE must answer SRV queries for DCs, GCs, and KDCs with or without additional site information.
4. Ensure all DNS servers can answer forward and reverse DNS queries for any possible Active Directory DNS domain(s).
5. AD must have at least one global catalog server operational and accessible by Cisco, for the domain you plan to join with Cisco.

Join AD domain

ISE applies Domain Discovery to get information about the join domain in three phases:

1. Queries joined domains—Discovers domains from its forest and domains externally trusted to the joined domain.
2. Queries root domains in its forest—Establishes trust with the forest.
3. Queries root domains in trusted forests—Discovers domains from the trusted forests.

Additionally, Cisco ISE discovers DNS domain names (UPN suffixes), alternative UPN suffixes and NTLM domain names.

ISE applies a DC discovery to obtain all information on the available DCs and GCs.

1. The join process starts with the input credentials of a super admin on AD that exist in the domain

itself. If it exists in a different domain or subdomain, the username must be noted in a UPN notation (username@domain).
2. ISE sends a DNS query for all DCs, GCs, and KDCs records. If the DNS reply does not receive an answer, the integration fails with a DNS related error.
3. ISE uses the CLDAP ping to discover all DCs and GCs through the sent CLDAP requests to the DCs that correspond to their priorities in the SRV record. The first DC response is used, and ISE is connected to that DC.

One factor used to calculate the DC priority is the time taken by the DC to respond to CLDAP pings; a faster response receives a higher priority.



Note: CLDAP is the mechanism that ISE uses to establish and maintain connectivity with the DCs. It measures the response time until the first DC answer. It fails if you do not see an answer from DC. Warn if the response time is larger than 2.5 seconds. CLDAP pings all DCs on site (if no site, then all DCs in the domain). The CLDAP response contains DC site and Client site (the site where the ISE machine is assigned.)

---

4. ISE receives TGT with the 'join user' credentials.
5. Generate the ISE machine account name with the MSRPC (SAM and SPN.)
6. Search AD by SPN if the ISE machine account already exists. If the ISE machine does not exist, ISE creates a new one.
7. Open the Machine account and set the ISE machine account password, and verify the ISE machine account is accessible.
8. Set the ISE machine account attributes (SPN, dnsHostname, and so on).
9. Receive TGT with ISE machine credentials with KRB5 and discover all trusted domains.
10. When the join is complete, ISE node updates its AD groups and associated SIDS and automatically begins the SID update process. Verify this process can complete on the AD side.

Leave AD domain

When ISE leaves, the AD must consider:

1. Use a full AD admin user to perform the leave processes. This verifies the ISE machine account is removed from the Active Directory database.
2. If the AD is left without credentials, the ISE account is not removed from AD and must be deleted manually.
3. When resetting the ISE configuration from the CLI or restoring configuration after a backup or upgrade, it performs a leave operation and disconnects the ISE node from the Active Directory domain. If joined, however, the ISE node account is not removed from the Active Directory domain.
4. It is recommended to perform a leave operation from the admin portal with the Active Directory credentials as it also removes the node account from the Active Directory domain. This is also recommended when you change the ISE hostname.

DC Failover

When the DC connected to the ISE become offline or unreachable for any reason, DC failover is triggered automatically on ISE. DC failover can be triggered by the these conditions:

1. AD connector detects that the currently selected DC became unavailable during some CLDAP, LDAP, RPC or Kerberos communication attempt. In such cases, the AD connector initiates DC selection and fails over to the newly selected DC.
2. DC is up and responds to CLDAP ping, however, the AD Connector cannot communicate with it for some reason (for example, the RPC port is blocked, DC is in ‘broken replication' state, DC has not been properly decommissioned.)

In such cases, the AD connector initiates DC selection with a blocked list (“bad” DC is placed in the blocked list) and tries to communicate with the selected DC. The DC selected in the blocked list is not cached.

The AD connector must complete failover within a reasonable amount of time (or fail if not possible). For this reason, the AD connector tries a limited number of DCs during failover. The ISE blocks AD Domain Controllers if there is an unrecoverable network or server error to prevent the ISE from the use of a bad DC. The DC is not added to the blocked list if it does not respond to CLDAP pings. ISE only lowers the priority of the DC if it does not respond.

ISE-AD Communication through LDAP

ISE searches for a machine or user in AD with one of the these search formats. If the search was for a machine, then ISE adds “$” at the end of the machine name. This is a list of Identity types which is used to identify a user in AD:

- SAM Name: Username or machine name without any domain markup, this is the User Log on Name in AD. Example: sajeda or sajeda$
- CN: This is the user display name on AD, it must not be same as the SAM. Example: sajeda Ahmed
- User Principal Name (UPN): This is a combination of the SAM name and domain name (SAM_NAME@domian). Example: sajeda@cisco.com or sajeda$@cisco.com
- Alternative UPN: This is an additional/alternative UPN suffixes that configured in the AD other than domain name. This configuration is added globally in AD (not configured per user) and is not necessary to be a real domain name suffix.
    - Each AD can have multiple UPN suffix (@alt1.com,@alt2.com, and so on). For example, main UPN (sajeda@cisco.com), alternative UPN :sajeda@domain1, sajeda@domain2

- NetBIOS Prefixed Name: This is the domain name/username of the machine name. For example, CISCO\sajeda or CISCO\machine$

- Host/Prefix with an Unqualified Machine: This is used for machine authentication when the machine name is only used and it is the host/machine name only. For example, host/machine.

- Host/Prefix with Fully Qualified Machine: This is used for machine authentication when the Machine FQDN is used, usually in case of certificate authentication. It is the host/FQDN of the machine. For example, host/machine.cisco.com.

- SPN Name: The name a client uniquely identifies an instance of a service, (for example, HTTP, LDAP, SSH) used for machine only.

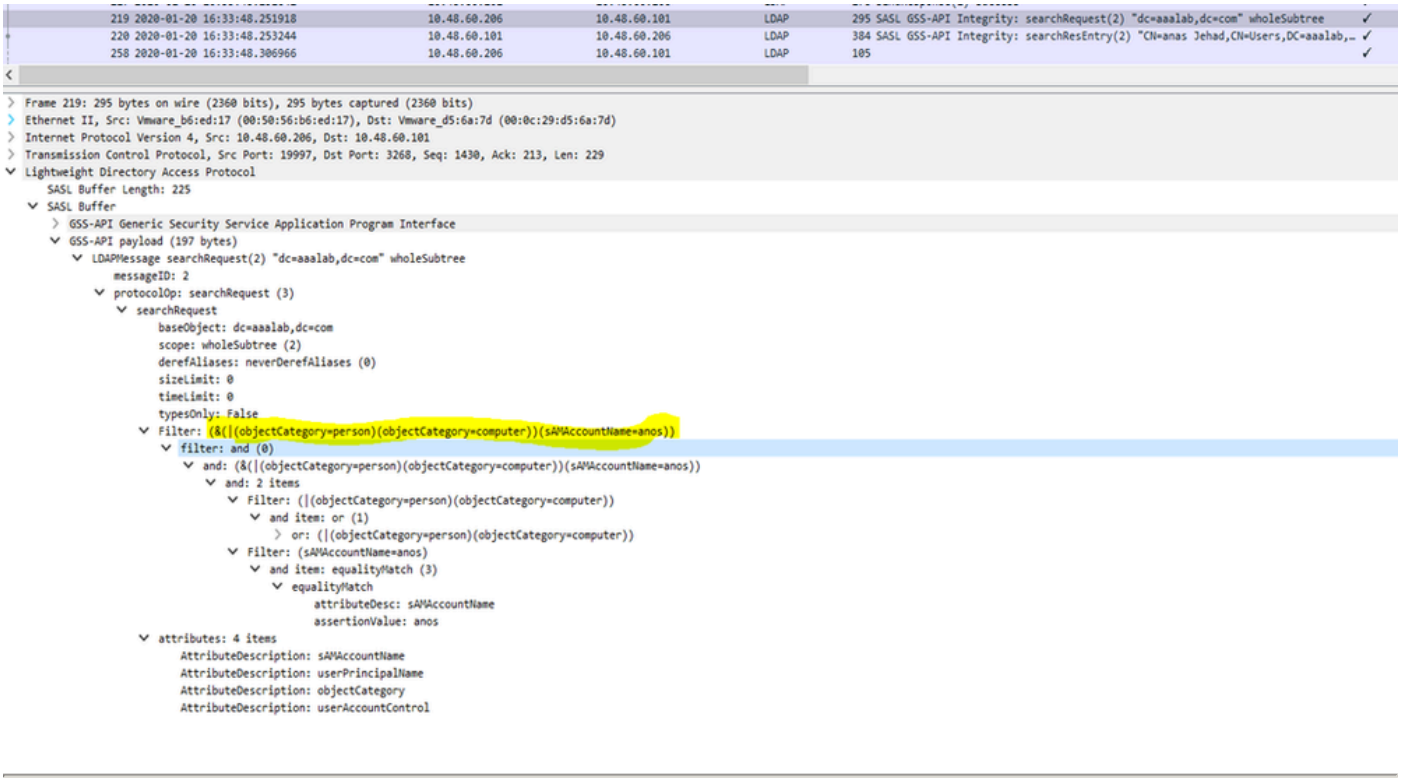
User Authentication Against AD Flow:

1. Resolve Identity and determine identity type - SAM, UPN, SPN. If ISE receives the identity as a username only, it searches for an associated SAM account in AD. If ISE receives the identity as a username@domain, it searches for a matched UPN or mail in AD. In both scenarios, ISE uses additional filters for machine or a username.
2. Search the domain or forest (depending on identity type.)
3. Keep information on all associated accounts (JP, DN, UPN, Domain.)
4. If no associated account is found, AD replies with user is unknown.
5. Perform MS-RPC (or Kerberos) authentication for each associated account.
6. If only a single account matches to input identity and password, authentication is successful.
7. If multiple accounts match the incoming identity, ISE uses the password to solve the ambiguity, and the account with an associated password is authenticated while the other accounts increase the incorrect password counter by 1.
8. If no account matches the incoming identity and password, AD replies with wrong password.

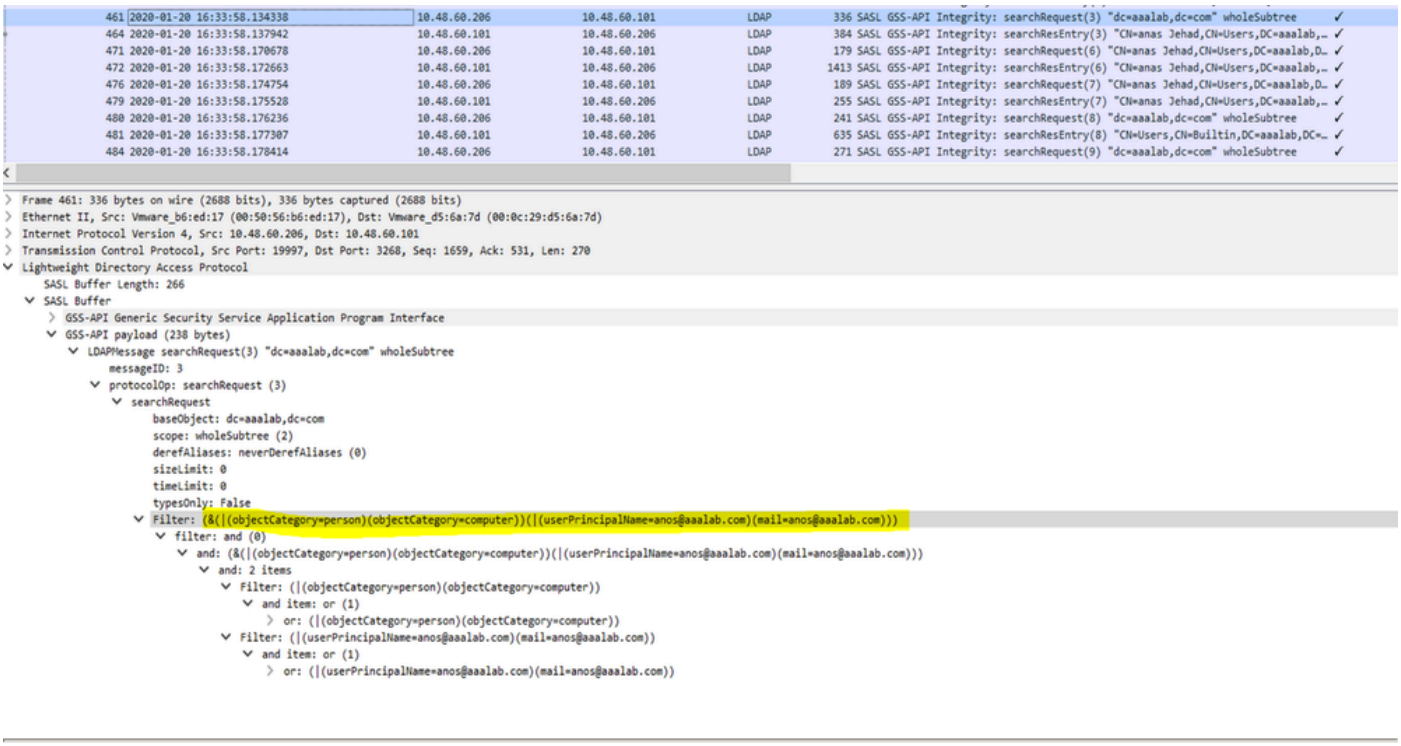
ISE Search Filters

Filters are used to identify an entity to communicate with AD. ISE always searches for an entity in the users and machines group. Examples of search filters:

1. **SAM search:** If the ISE receives an identity as a username only without any domain markup, ISE treats the username as a SAM and searches in AD for all machine users or machines that have the identity as a SAM name.
2. If the SAM name is not unique, ISE uses the password to differentiate between users and ISE is configured to use a passwordless protocol such as EAP-TLS.
3. There are no other criteria to locate the correct user, so, ISE fails the authentication with an “Ambiguous Identity” error. However, if the user certificate is present in Active Directory, Cisco ISE uses a binary comparison to resolve the identity.

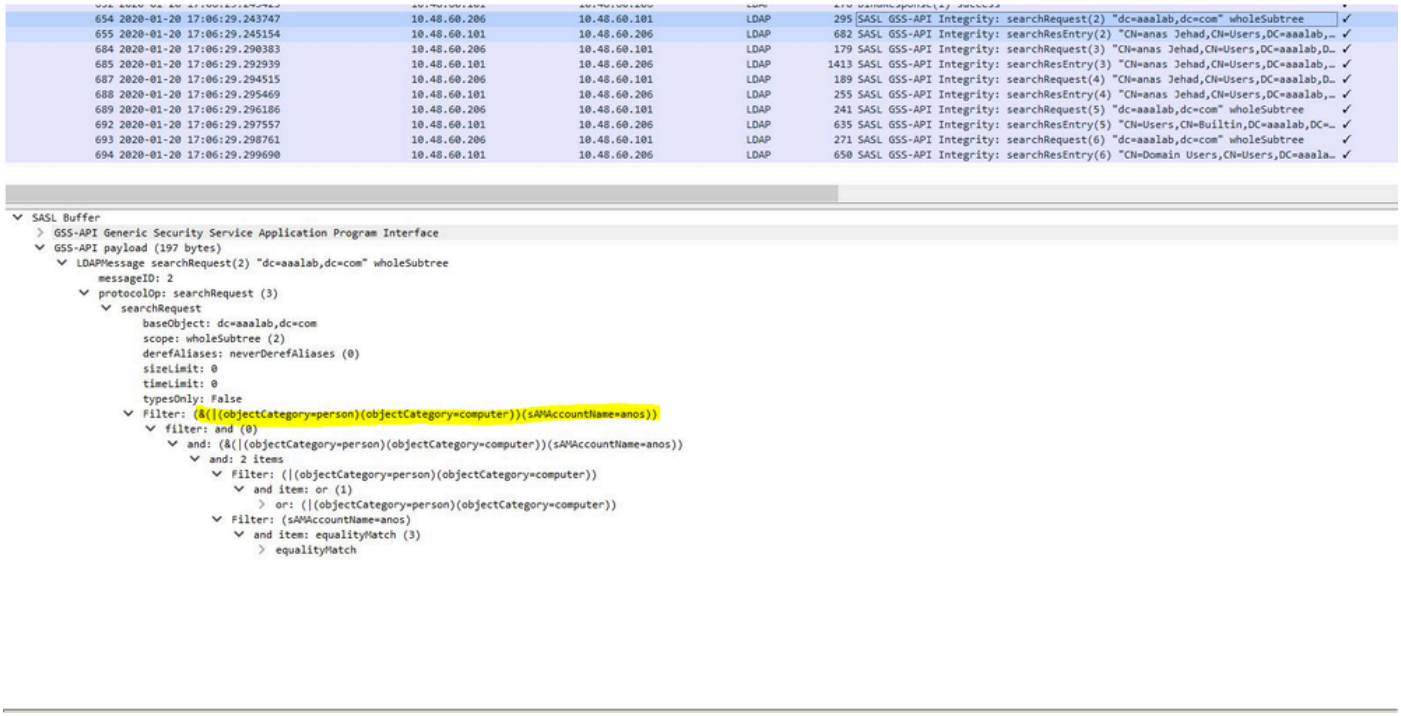


2. **UPN or MAIL Search**: If ISE receives an identity as username@domain, ISE searches the forest global catalog for a match to the UPN identity or Mail identity “identity=matched UPN or email”. If there is a unique match, Cisco ISE proceeds with the AAA flow. If there are multiple join points with the same UPN and a password, or the same UPN and Mail, Cisco ISE fails the authentication with an “Ambiguous Identity” error.

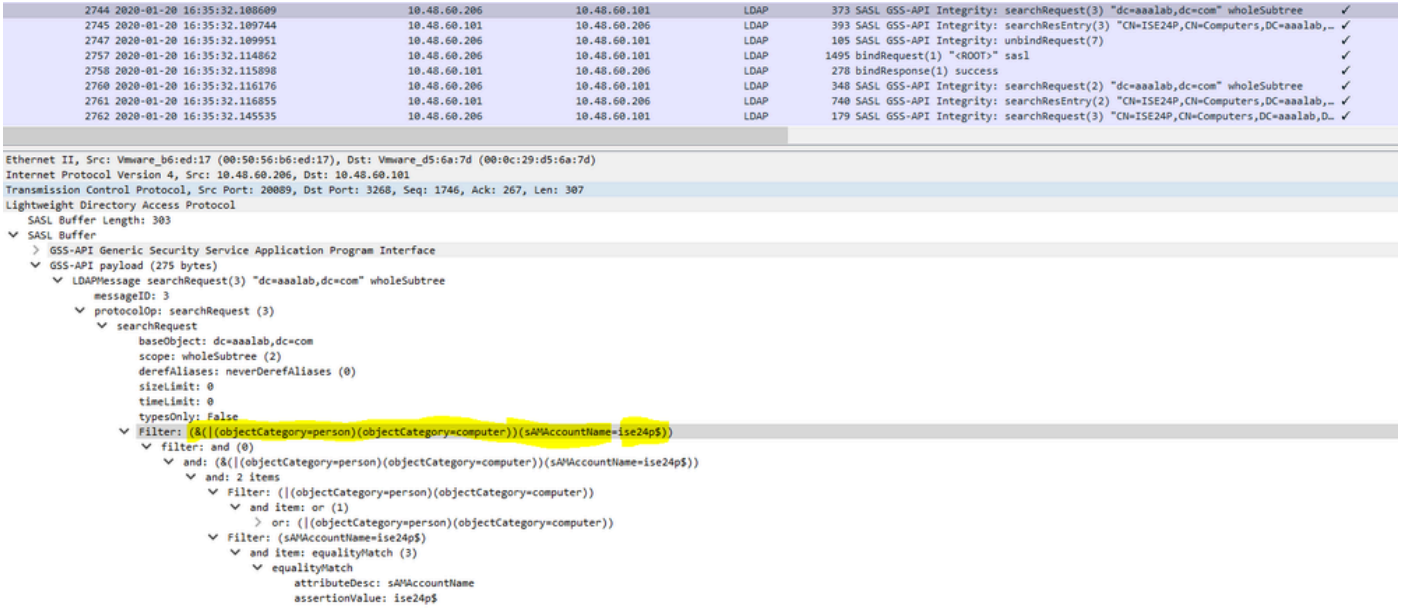


3. **NetBIOS Search**: If ISE receives an identity with a NetBIOS domain prefix (for example, CISCO\sajedah), ISE searches the forests for the NetBIOS domain. Once found, it looks for the

supplied SAM name (sajeda for example).



4. **Machine Base Search**: If ISE receives a machine authentication with a host/prefix identity, ISE searches the forest for a matched servicePrincipalName attribute. If a fully-qualified domain suffix was specified in the identity, like host/machine.domain.com. Cisco ISE searches the forest where the domain exists. If the identity is in the form of host/machine, Cisco ISE searches all forests for the service principal name. If there is more than one match, Cisco ISE fails the authentication with an “Ambiguous Identity” error.



Note: Same filters are seen in the ISE ad-agent.log files.

Note: ISE 2.2 patch 4, 2.3 patch, 1, and prior identified users with the attributes SAM, CN, or both. Cisco ISE, release 2.2 Patch 5 and above, and 2.3 Patch 2 and higher, use only sAMAccountName attribute as the default attribute.