Comprensión de Identity Service Engine (ISE) y Active Directory (AD)

Contenido

Introducción

Este documento describe cómo Identity Service Engine (ISE) y Active Directory (AD) se comunican, los protocolos que se utilizan, los filtros de AD y los flujos.

Prerequisites

Requirements

Cisco recomienda un conocimiento básico de:

- ISE 2.x e integración con Active Directory .
- Autenticación de identidad externa en ISE.

Componentes Utilizados

- 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Protocolos AD

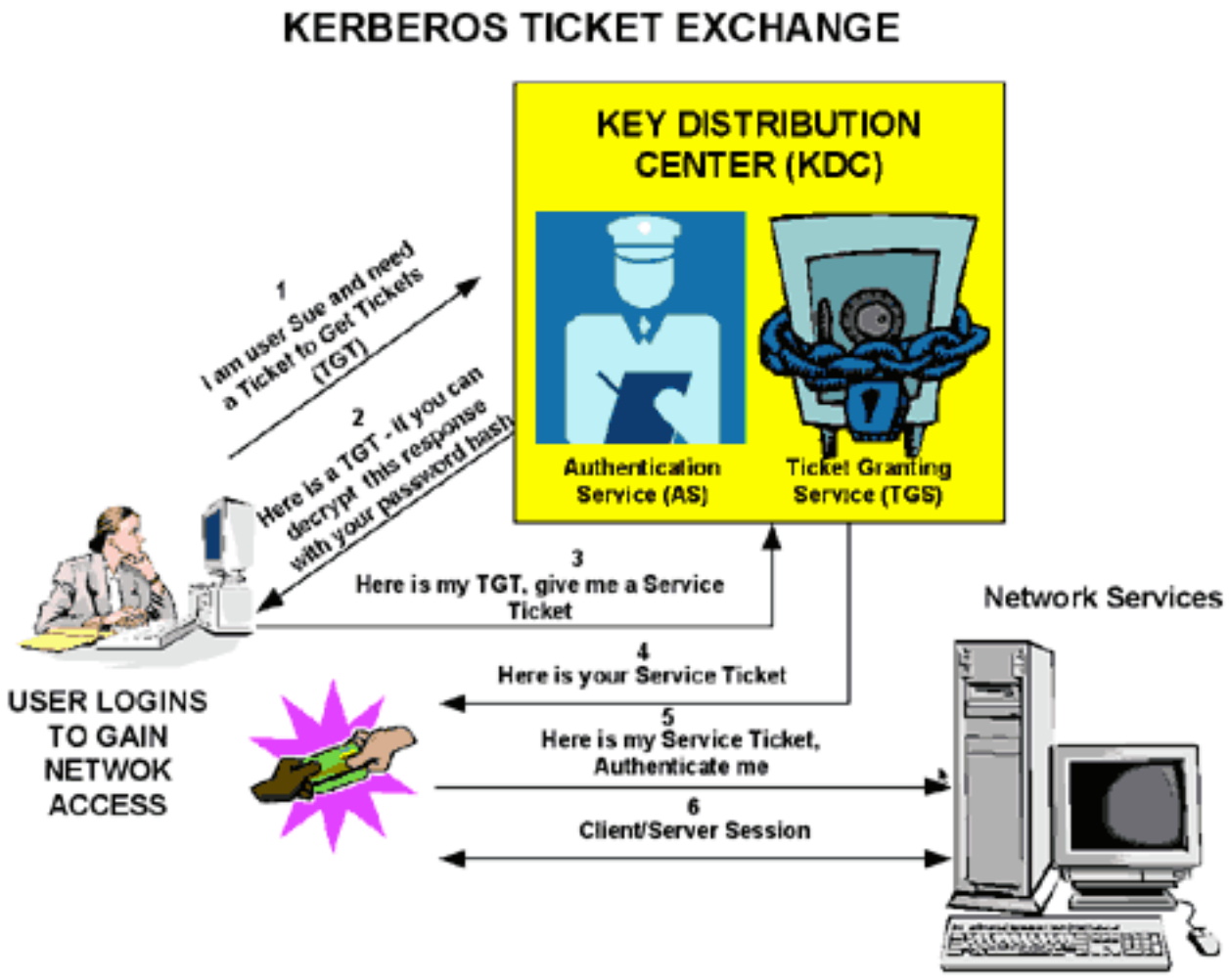
Protocolo Kerberos

Los tres jefes de Kerberos comprenden el Key Distribution Center (KDC), el usuario cliente y el servidor al que se debe acceder.

El KDC se instala como parte del controlador de dominio (DC) y realiza dos funciones de servicio: El Servicio de autenticación (AS) y el Servicio de concesión de notificaciones (TGS).

Cuando el cliente accede inicialmente a un recurso del servidor, se realizan tres intercambios:

1. AS Exchange.
2. Intercambio de TGS.
3. Intercambio cliente/servidor (CS).



- Controlador de dominio = KDC (AS + TGS).
- Autentique a AS (el portal de SSO) con su contraseña.
- Obtenga un Ticket Granting Ticket (TGT) (una cookie de sesión).
- Solicitud de conexión a un servicio (SRV01).
- SRV01 le redirige a KDC.
- Show TGT to KDC - (Ya estoy autenticado)
- KDC le proporciona TGS para SRV01.

- Redirigir a SRV01.
- Mostrar ticket de servicio para SRV01.
- SRV01 verifica/confía en el vale de servicio.
- El ticket de servicio tiene toda mi información.
- El SRV01 me conecta.

Cuando iniciaron sesión inicialmente en una red, los usuarios deben negociar el acceso y proporcionar un nombre y una contraseña de inicio de sesión para que la parte AS de un KDC dentro de su dominio pueda verificarlos.

El KDC tiene acceso a la información de cuenta de usuario de Active Directory. Una vez autenticado, se concede al usuario un vale de concesión de vale (TGT) válido para el dominio local.

El TGT tiene una duración predeterminada de 10 horas y se renueva durante la sesión de inicio de sesión del usuario sin que este tenga que volver a introducir su contraseña.

El TGT se almacena en caché en el equipo local en el espacio de memoria volátil y se utiliza para solicitar sesiones con servicios en toda la red.

El usuario presenta el TGT a la parte TGS del KDC cuando se necesita acceso a un servicio de servidor.

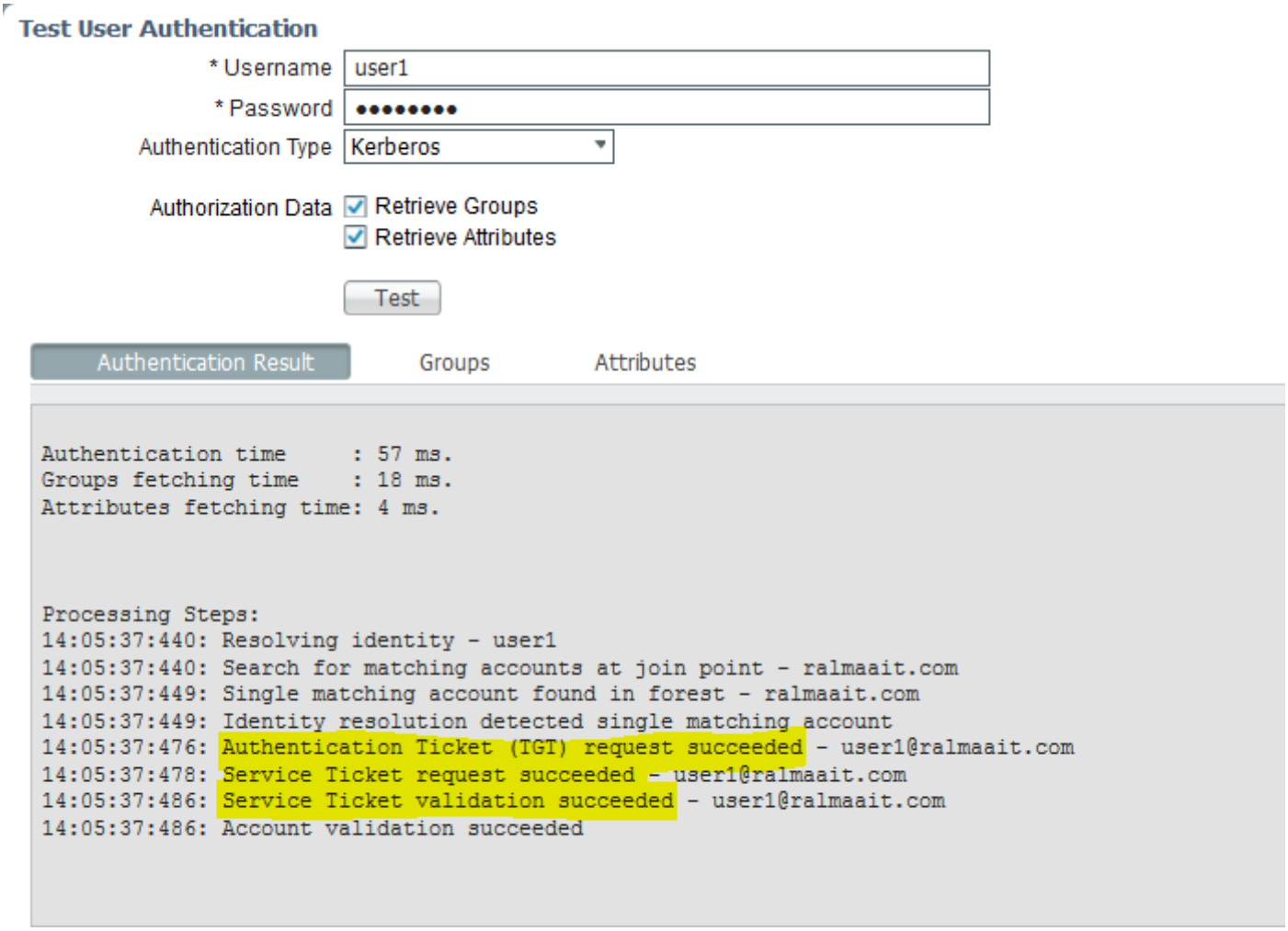
El TGS en el KDC autentica al usuario TGT y crea un ticket y una clave de sesión para el cliente y el servidor remoto. Esta información (el vale de servicio) se almacena localmente en la memoria caché del equipo cliente.

El TGS recibe el cliente TGT y lo lee con su propia clave. Si el TGS aprueba la solicitud del cliente, se genera un ticket de servicio tanto para el cliente como para el servidor de destino.

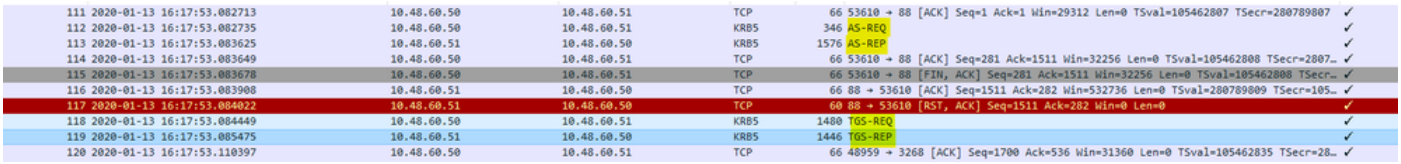
El cliente lee su parte con la clave de sesión TGS recuperada anteriormente de la respuesta AS.

El cliente presenta la parte del servidor de la respuesta TGS al servidor de destino en el siguiente intercambio cliente/servidor.

Ejemplo:



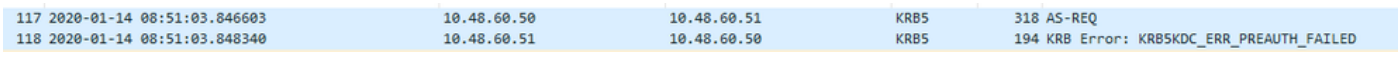
Capturas de paquetes de ISE para un usuario autenticado:



AS-REQ contiene el nombre de usuario. Si la contraseña es correcta, el servicio AS proporciona un TGT cifrado con la contraseña de usuario. El TGT se proporciona al servicio TGT para obtener un ticket de sesión.

La autenticación es correcta cuando se recibe un vale de sesión.

Este es un ejemplo donde la contraseña dada por el cliente es incorrecta:



Si la contraseña es incorrecta, la solicitud de AS falla y no se recibe un 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
```

Registra en el archivo ad_agent.log cuando la contraseña es incorrecta:

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

2020-01-14 13:36:05,444 DEBUG ,140574072981248,krb5: Error recibido de KDC: -1765328360/Error de autenticación previa,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 ADVERTENCIA,140574072981248,[LwKrb5GetTgtImpl ../../lwadvapi/threaded/krbtgt.c:329] Código de error KRB5: -1765328360 (Mensaje: Error de autenticación previa),LwTranslateKrb5Error(),lwadvapi/threaded/lwkrb5.c:892

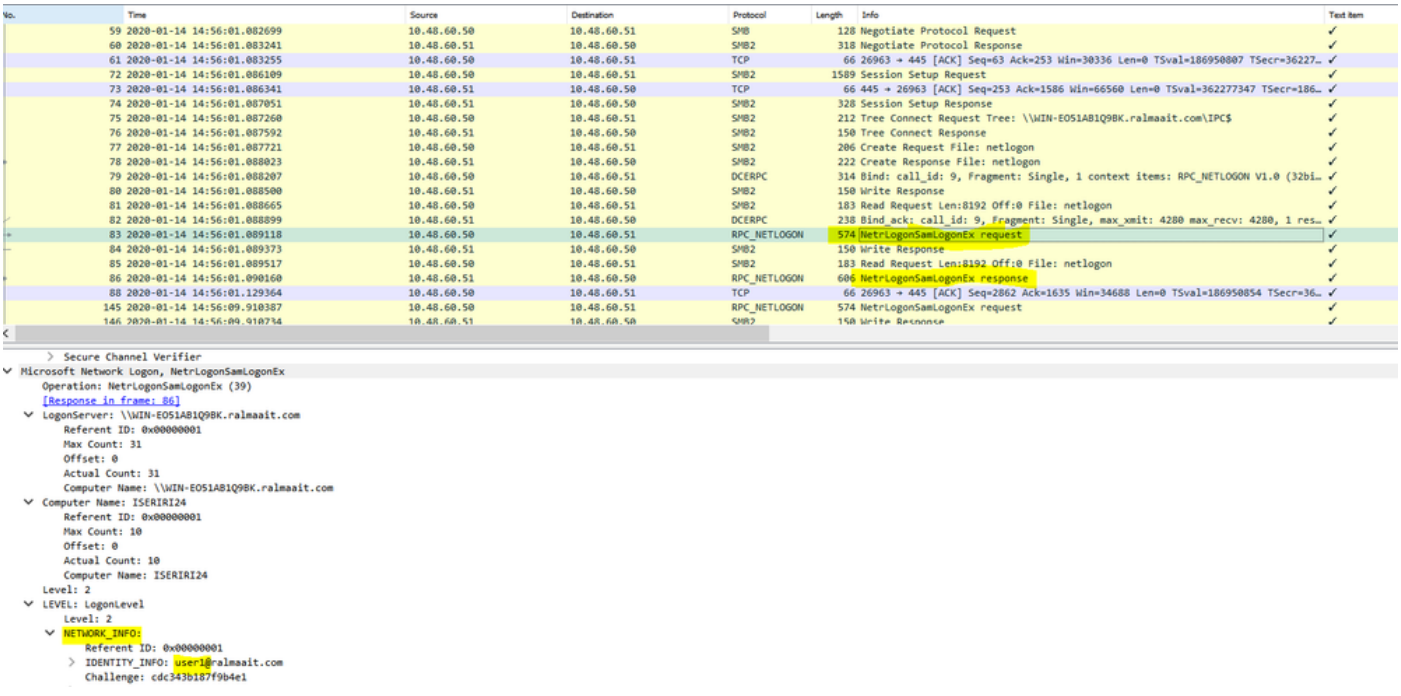
2020-01-14 13:36:05,444 DEBUG ,140574072981248,[LwKrb5InitializeUserLoginCredentials()] Código de error: 40022 (símbolo: LW_ERROR_PASSWORD_MISMATCH),LwKrb5InitializeUserLoginCredentials(),lwadvapi/threaded/lwkrb5.c:1453

Protocolo MS-RPC

ISE utiliza MS-RPC sobre SMB, SMB proporciona la autenticación y no requiere una sesión independiente para encontrar dónde se encuentra un servicio RPC determinado. Utiliza un mecanismo llamado "named pipe" para comunicarse entre el cliente y el servidor.

- Cree una conexión de sesión SMB.
- Transporte de mensajes RPC a través del puerto SMB/CIFS.TCP 445 como transporte
- La sesión SMB identifica qué puerto ejecuta un servicio RPC determinado y controla la autenticación de usuario.
- Conéctese a un recurso compartido oculto IPC$ para la comunicación entre procesos.
- Abra una canalización con nombre adecuada para el recurso/función RPC deseado.

Transaccionar el intercambio RPC sobre SMB.



negotiate protocol request/response negocia el dialecto de SMB. **session setup request/response** realiza la autenticación.

La solicitud y la respuesta de conexión de árbol se conectan al recurso solicitado. Está conectado a un recurso compartido especial IPC$.

Este recurso compartido de comunicación entre procesos proporciona los medios de comunicación entre hosts y también como transporte para las funciones de MSRPC.

En el paquete 77 es **Create Request File** y el nombre de archivo es el nombre del servicio conectado (el servicio netlogon en este ejemplo).

En los paquetes 83 y 86, la solicitud NetLogonSamLogonEX es donde se envía el nombre de usuario para la autenticación del cliente en ISE al AD en el campo Network_INFO.

El paquete de respuesta NetLogonSamLogonEX responde con los resultados.

Algunos valores de indicadores para la respuesta NetLogonSamLogonEX:
0xc000006a es STATUS_WRONG_PASSWORD
0x00000000 es STATUS_SUCCESS
0x00000103 es STATUS_PENDING

Integración de ISE con Active Directory (AD)

ISE utiliza LDAP, KRB y MSRBC para comunicarse con AD durante el proceso de unión/ausencia y autenticación.

Las siguientes secciones proporcionan los protocolos, el formato de búsqueda y los mecanismos utilizados para conectarse a un DC específico en AD y la autenticación de usuario en ese DC.

En caso de que el DC se desconecte por cualquier motivo, ISE conmutará por error al siguiente DC disponible y el proceso de autenticación no se verá afectado.

Un servidor de catálogo global (GC) es un controlador de dominio que almacena copias de todos los objetos de Active Directory del bosque.

Almacena una copia completa de todos los objetos del directorio del dominio y una copia parcial de todos los objetos de los demás dominios de bosque.

Por lo tanto, el Catálogo global permite a los usuarios y las aplicaciones buscar objetos en cualquier dominio del bosque actual con una búsqueda de atributos incluidos en GC.

El catálogo global contiene un conjunto básico (pero incompleto) de atributos para cada objeto de bosque de cada dominio (conjunto parcial de atributos, PAT).

GC recibe datos de todas las particiones de directorio de dominio del bosque. Se copian con el

servicio de replicación de AD estándar.

Incorporación de ISE a AD

Prerrequisitos de Active Directory e integración con ISE

1. Compruebe que dispone de los privilegios de un superadministrador o administrador del sistema en ISE.
2. Utilice la configuración del servidor de protocolo de tiempo de la red (NTP) para sincronizar la hora entre el servidor de Cisco y Active Directory. La diferencia de tiempo máxima permitida entre ISE y AD es de 5 minutos
3. El DNS configurado en ISE debe ser capaz de responder a consultas SRV de DC, GC y KDC con o sin información adicional del sitio.
4. Asegúrese de que todos los servidores DNS puedan responder a consultas DNS inversas y de reenvío para cualquier dominio DNS de Active Directory posible.
5. AD debe tener al menos un servidor de catálogo global operativo y accesible para Cisco, en el dominio al que se une Cisco.

Unirse al dominio AD

ISE aplica la detección de dominios para obtener información sobre el dominio de unión en tres fases:

1. Consulta dominios unidos: detecta dominios de su bosque y dominios de confianza externa para el dominio unido.
2. Consulta los dominios raíz de su bosque: establece confianza con el bosque.
3. Consulta dominios raíz en bosques de confianza: detecta dominios de los bosques de confianza.

Además, Cisco ISE detecta nombres de dominio DNS (sufijos UPN), sufijos UPN alternativos y nombres de dominio NTLM.

ISE aplica una detección de DC para obtener toda la información sobre los DC y GC disponibles.

1. El proceso de unión comienza con las credenciales de entrada de super admin en AD que existen en el dominio mismo. Si existe en un dominio o subdominio diferente, el nombre de usuario debe indicarse en una notación UPN (username@domain).
2. ISE envía una consulta DNS para todos los registros de DC, GC y KDC. Si la respuesta de DNS no tenía una de ellas en su respuesta, la integración falla con un error relacionado con DNS.
3. ISE utiliza el ping CLDAP para detectar todos los DC y GC a través de solicitudes CLDAP enviadas a los DC que corresponden a sus prioridades en el registro SRV. Se utiliza la primera respuesta de DC e ISE se conecta a ese DC.

Un factor que se utiliza para calcular la prioridad DC es el tiempo que tarda el DC en responder a los pings CLDAP; una respuesta más rápida recibe una prioridad más alta.

> **Nota:** CLDAP es el mecanismo que ISE utiliza para establecer y mantener la conectividad con los DC. Mide el tiempo de respuesta hasta la primera respuesta del DC. Si no ve ninguna respuesta del DC, se produce un error. Avisar si el tiempo de respuesta es superior

a 2,5 segundos. CLDAP hace ping a todos los DC del sitio (si no hay ningún sitio, todos los DC del dominio). La respuesta CLDAP contiene el sitio DC y el sitio Cliente (el sitio al que está asignado el equipo ISE).

4. A continuación, ISE recibe TGT con las credenciales de 'usuario de conexión'.
5. Generar nombre de cuenta de equipo ISE con MSRPC. (SAM y SPN)
6. Busque AD por SPN si la cuenta de la máquina ISE ya existe. Si el equipo ISE no existe, ISE crea uno nuevo.
7. Abra la cuenta del equipo, establezca la contraseña de la cuenta del equipo ISE y compruebe que la cuenta del equipo ISE está accesible.
8. Establezca los atributos de cuenta de equipo de ISE (SPN, dnsHostname y similares).
9. Obtenga TGT con credenciales de equipos ISE con KRB5 y descubra todos los dominios de confianza.
10. Una vez completada la unión, el nodo ISE actualiza sus grupos AD y los SID asociados e inicia automáticamente el proceso de actualización de SID. Verifique que este proceso pueda completarse en el lado AD.

Abandonar dominio AD

Cuando ISE abandone, AD debe tener en cuenta lo siguiente:

1. Utilice un usuario administrador de AD completo para realizar los procesos de abandono. Esto verifica que la cuenta del equipo ISE se elimina de la base de datos de Active Directory.
2. Si el AD se ha quedado sin credenciales, la cuenta de ISE no se elimina del AD y debe eliminarse manualmente.
3. Al restablecer la configuración de ISE desde la CLI o restaurar la configuración después de una copia de seguridad o actualización, se realiza una operación de ausencia y se desconecta el nodo de ISE del dominio de Active Directory. (si está unido). Sin embargo, la cuenta de nodo de ISE no se elimina del dominio de Active Directory.
4. Se recomienda realizar una operación de ausencia desde el portal de administración con las credenciales de Active Directory porque también quita la cuenta de nodo del dominio de Active Directory. Esto también se recomienda cuando cambia el nombre de host de ISE.

falla de DC

Cuando el DC conectado a ISE se desconecta o se vuelve inalcanzable por cualquier motivo, la conmutación por fallo del DC se activa automáticamente en ISE. La conmutación por fallo del DC se puede activar en las siguientes condiciones:

1. El conector AD detecta que el DC seleccionado actualmente no estaba disponible durante algún intento de comunicación CLDAP, LDAP, RPC o Kerberos. En estos casos, el conector AD inicia la selección de DC y conmuta por error al DC recién seleccionado.
2. DC está activo y responde al ping CLDAP, pero AD Connector no puede comunicarse con él por alguna razón (ejemplos: El puerto RPC está bloqueado, el DC está en estado de "replicación interrumpida", el DC no se ha retirado correctamente).

En estos casos, el conector de AD inicia la selección de DC con una lista bloqueada ("malo" DC se coloca en la lista bloqueada) e intenta comunicarse con el DC seleccionado. El DC seleccionado en la lista de bloqueados no se almacena en caché.

El conector AD debe completar la conmutación por error en un tiempo razonable (o fallar si no es posible). Por esta razón, el conector AD intenta un número limitado de DC durante la conmutación por error.

ISE bloquea los controladores de dominio de AD si hay un error irrecuperable de red o de servidor para evitar que ISE use un DC incorrecto. DC no se agrega a la lista de bloqueados si no responde a los pings CLDAP. ISE solo reduce la prioridad del DC que no responde.

Comunicación ISE-AD a través de LDAP

ISE busca equipo o usuario en AD con uno de estos formatos de búsqueda. Si la búsqueda fue para un equipo, ISE agrega "$" al final del nombre del equipo. Esta es una lista de tipos de identidad que se utiliza para identificar a un usuario en AD:

- Nombre SAM: nombre de usuario o nombre de equipo sin ninguna marca de dominio, es el nombre de inicio de sesión del usuario en AD. **Ejemplo: sajeda o sajeda$**
- CN: es el nombre para mostrar del usuario en AD; no debe ser igual que el SAM. **Ejemplo: sajeda Ahmed.**
- Nombre principal de usuario (UPN): es una combinación del nombre SAM y el nombre de dominio (SAM_NAME@domian). **Ejemplo: sajeda@cisco.com o sajeda$@cisco.com**
- UPN alternativo: es un sufijo UPN adicional o alternativo configurado en AD distinto del nombre de dominio. Esta configuración se agrega globalmente en AD (no se configura por usuario) y no es necesario ser un sufijo de nombre de dominio real.

Cada AD puede tener varios sufijos UPN (@alt1.com,@alt2.com,..., etc.). **Ejemplo: UPN principal (sajeda@cisco.com), UPN alternativo :sajeda@domain1 , sajeda@domain2**

- Nombre con prefijo NetBIOS: es el nombre de dominio\nombre de usuario del nombre del equipo. **Ejemplo: CISCO\sajeda o CISCO\machine$**
- Host/prefijo con máquina no calificada: se utiliza para la autenticación de equipo cuando sólo se utiliza el nombre de equipo, es sólo el nombre de host/equipo. **Ejemplo: host/máquina**
- Host/ prefijo con máquina completamente calificada: se utiliza para la autenticación de equipo cuando se utiliza el FQDN de equipo, normalmente en el caso de la autenticación de certificado, es el FQDN/host del equipo. **Ejemplo: host/machine.cisco.com**
- Nombre de SPN: Nombre con el que un cliente identifica de forma exclusiva una instancia de un servicio (ejemplos: HTTP, LDAP, SSH) utilizado sólo para el equipo.

Autenticación de usuario contra flujo AD:

1. Resolver identidad y determinar tipo de identidad: SAM, UPN, SPN. Si ISE recibe la identidad solo como nombre de usuario, busca una cuenta SAM asociada en AD. Si ISE recibe la identidad como un username@domain, busca un UPN o correo coincidente en AD. En ambos casos, ISE utiliza filtros adicionales para el equipo o el nombre de usuario.
2. Buscar dominio o bosque (depende del tipo de identidad)
3. Mantener información sobre todas las cuentas asociadas (JP, DN, UPN, dominio)

4. Si no se encuentra ninguna cuenta asociada, AD responde con un usuario desconocido.
5. Realizar autenticación MS-RPC (o Kerberos) para cada cuenta asociada
6. Si sólo una cuenta coincide con la identidad y la contraseña introducidas, la autenticación es correcta
7. Si varias cuentas coinciden con la identidad entrante, ISE utiliza la contraseña para resolver la ambigüedad, de modo que la cuenta con una contraseña asociada se autentica y las demás cuentas aumentan el contador de contraseñas incorrectas en 1.
8. Si ninguna cuenta coincide con la identidad y la contraseña entrantes, AD responde con una contraseña incorrecta.

ISE Filtros de búsqueda

Los filtros se utilizan para identificar una entidad que desea comunicarse con AD. ISE siempre busca esa entidad en los grupos de usuarios y equipos.

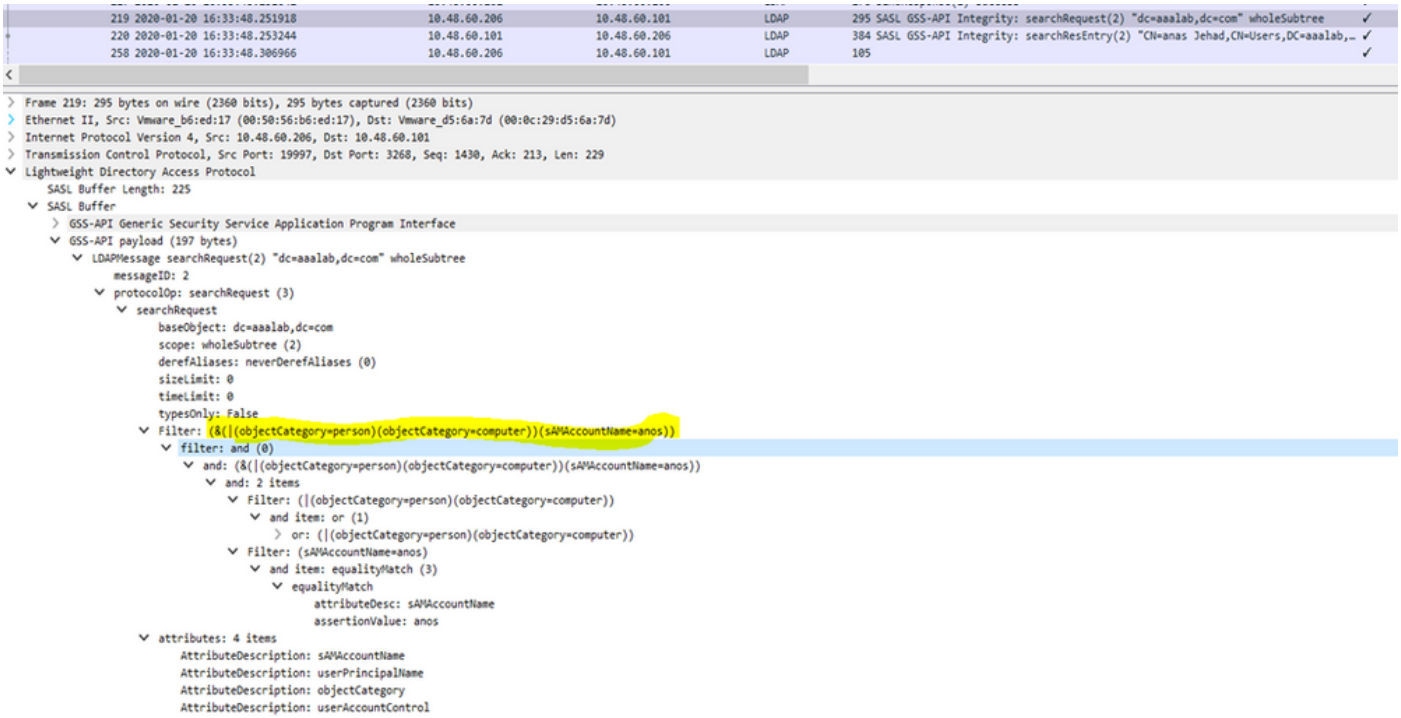
Ejemplos de filtros de búsqueda:

1. **Búsqueda SAM:** Si ISE recibe una identidad como un nombre de usuario solamente sin ningún marcado de dominio, ISE trata este nombre de usuario como un SAM y busca en AD a todos los usuarios o equipos que tengan esa identidad como un nombre SAM.

Si el nombre SAM no es único, ISE utiliza la contraseña para diferenciar entre usuarios e ISE está configurado para utilizar un protocolo sin contraseña como EAP-TLS.

No existen otros criterios para localizar al usuario adecuado, por lo que ISE falla la autenticación con un error de "identidad ambigua".

Sin embargo, si el certificado de usuario está presente en Active Directory, Cisco ISE utiliza la comparación binaria para resolver la identidad.

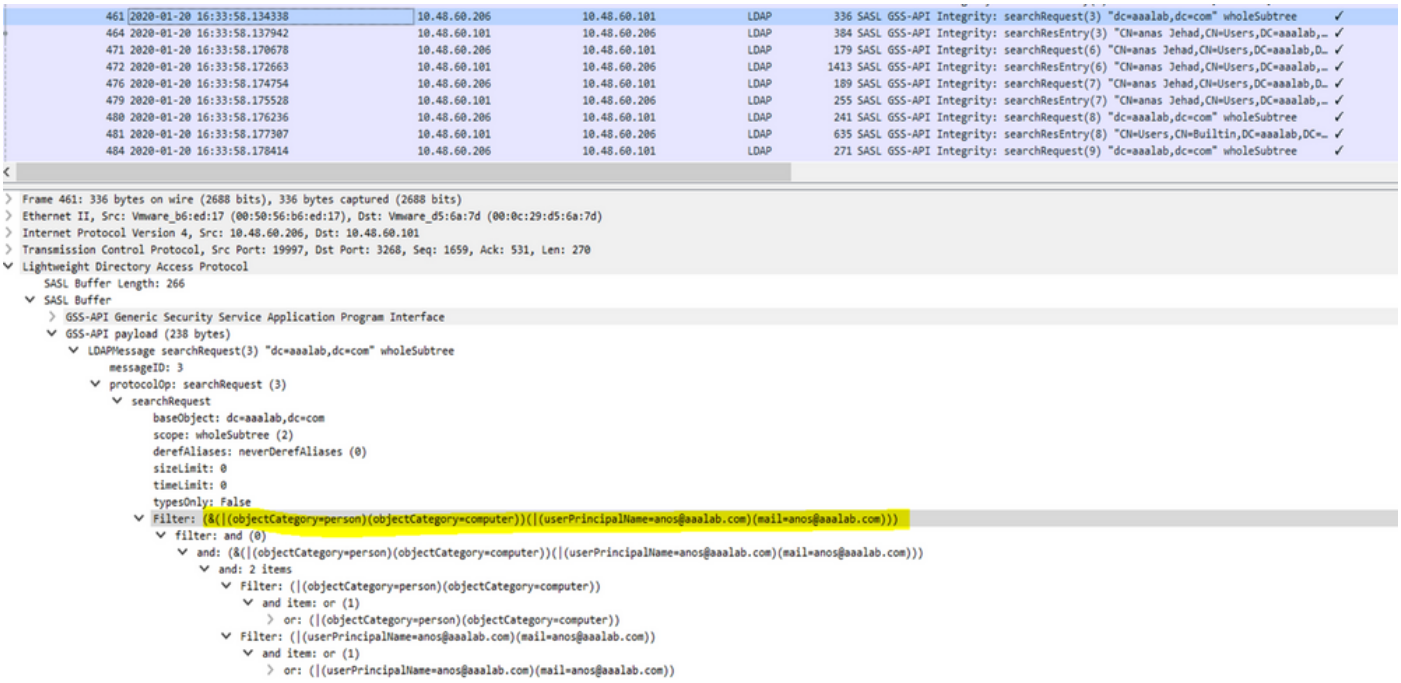


2. **Búsqueda de UPN o MAIL:** Si ISE recibe una identidad como username@domain, busca en los catálogos globales de cada bosque una coincidencia con esa identidad UPN o la

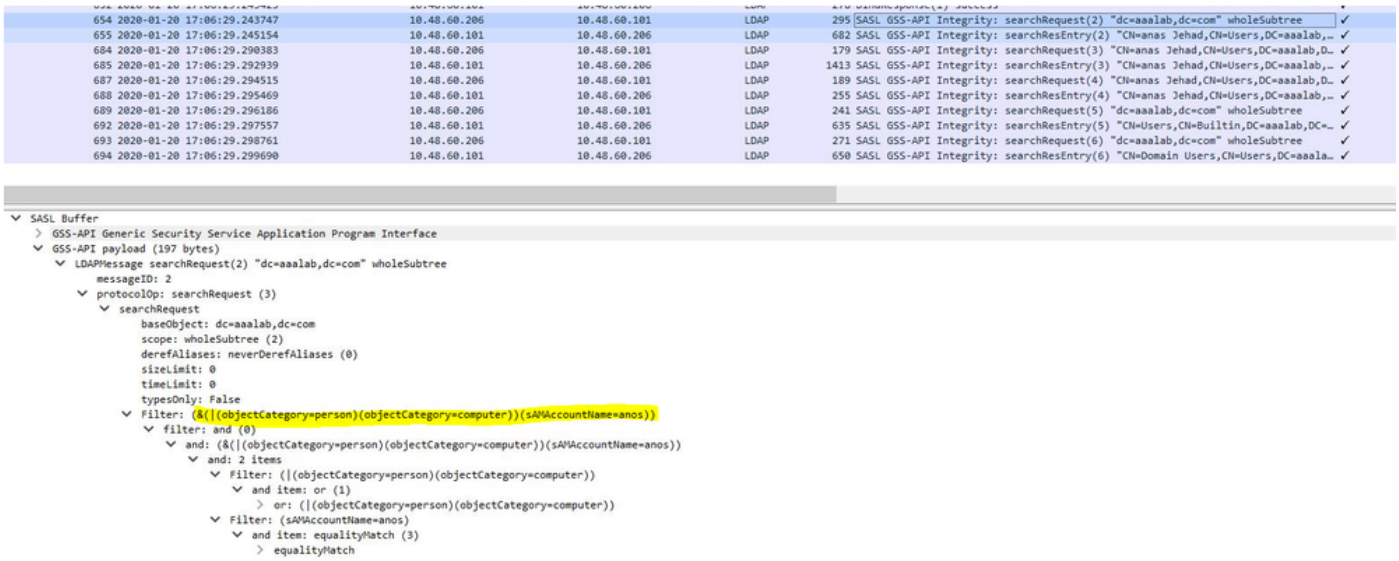
identidad de correo "identity=match UPN or email".

Si existe una coincidencia única, Cisco ISE continúa con el flujo AAA.

Si hay varios puntos de unión con el mismo UPN y una contraseña o con el mismo UPN y correo, Cisco ISE falla la autenticación con un error de "identidad ambigua".



3. **Búsqueda de NetBIOS:** Si ISE recibe una identidad con un prefijo de dominio NetBIOS (por ejemplo: CISCO\sajedah), busca el dominio NetBIOS en los bosques. Una vez encontrado, busca el nombre SAM proporcionado (sajeda en nuestro ejemplo)



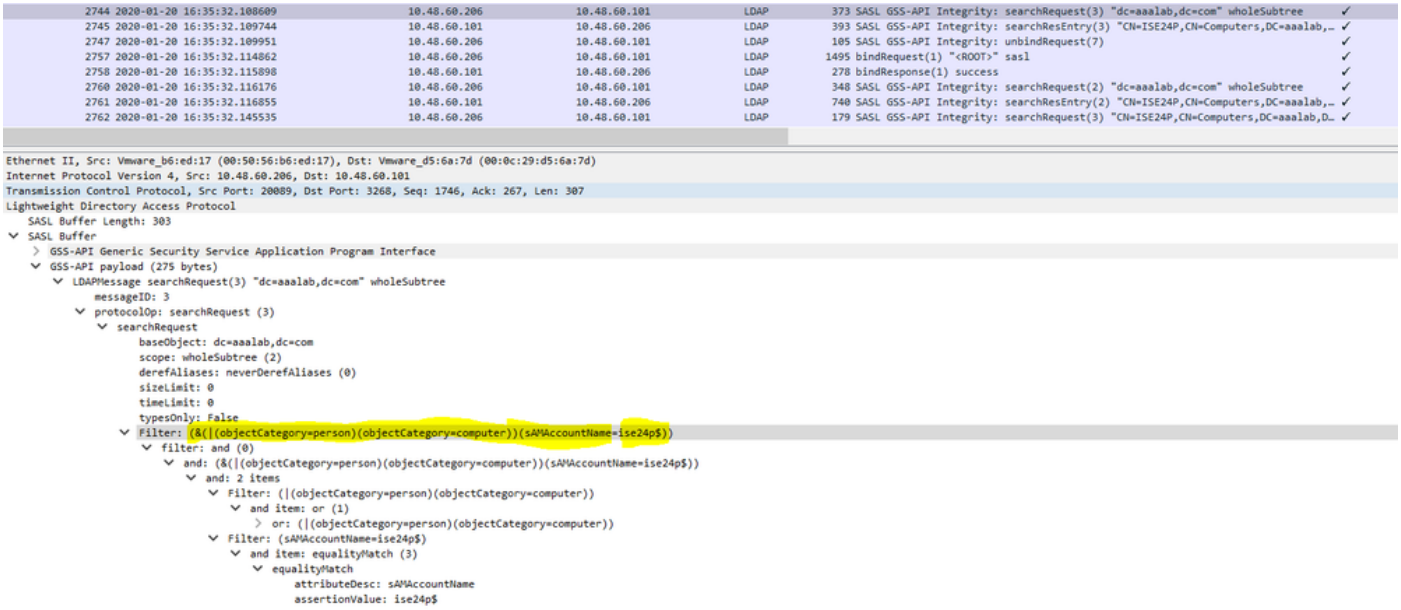
4. **Búsqueda por máquina:** Si ISE recibe una autenticación de equipo, con una identidad de host/prefijo, busca en el bosque un atributo servicePrincipalName coincidente.

Si se ha especificado un sufijo de dominio completo en la identidad, por ejemplo, host/machine.domain.com, Cisco ISE busca en el bosque en el que existe dicho dominio.

Si la identidad se encuentra en forma de host/máquina, Cisco ISE busca el nombre principal del

servicio en todos los bosques.

Si hay más de una coincidencia, Cisco ISE falla la autenticación con un error de "identidad ambigua".



Nota: Se ven los mismos filtros en los archivos ad-agent.log de ISE

Nota: El parche 4 de ISE 2.2 y los parches 1 y 2.3 anteriores y los usuarios identificados anteriormente con los atributos SAM, CN o ambos. Cisco ISE, versión 2.2 Parche 5 y posterior, y 2.3 Parche 2 y posterior, utilizan únicamente el atributo sAMAccountName como atributo predeterminado.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).