

# Identity Service Engine(ISE)とActive Directory(AD)について

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ADプロトコル](#)

[Kerberosプロトコル](#)

[MS-RPCプロトコル](#)

[ISEとActive Directory\(AD\)の統合](#)

[ADへのISEの結合](#)

[ADドメインへの参加](#)

[ADドメインを離れる](#)

[DCフェールオーバー](#)

[LDAPによるISE-AD通信](#)

[ADフローに対するユーザ認証 :](#)

[ISE検索フィルタ](#)

## 概要

このドキュメントでは、Identity Service Engine(ISE)とActive Directory(AD)の通信方法、使用されるプロトコル、ADフィルタ、およびフローについて説明します。

## 前提条件

### 要件

シスコでは、次の基本知識を推奨しています。

- ISE 2.xとActive Directoryの統合 ( ISE 2.xとActive Directory Integration )
- ISEでの外部ID認証。

### 使用するコンポーネント

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

# ADプロトコル

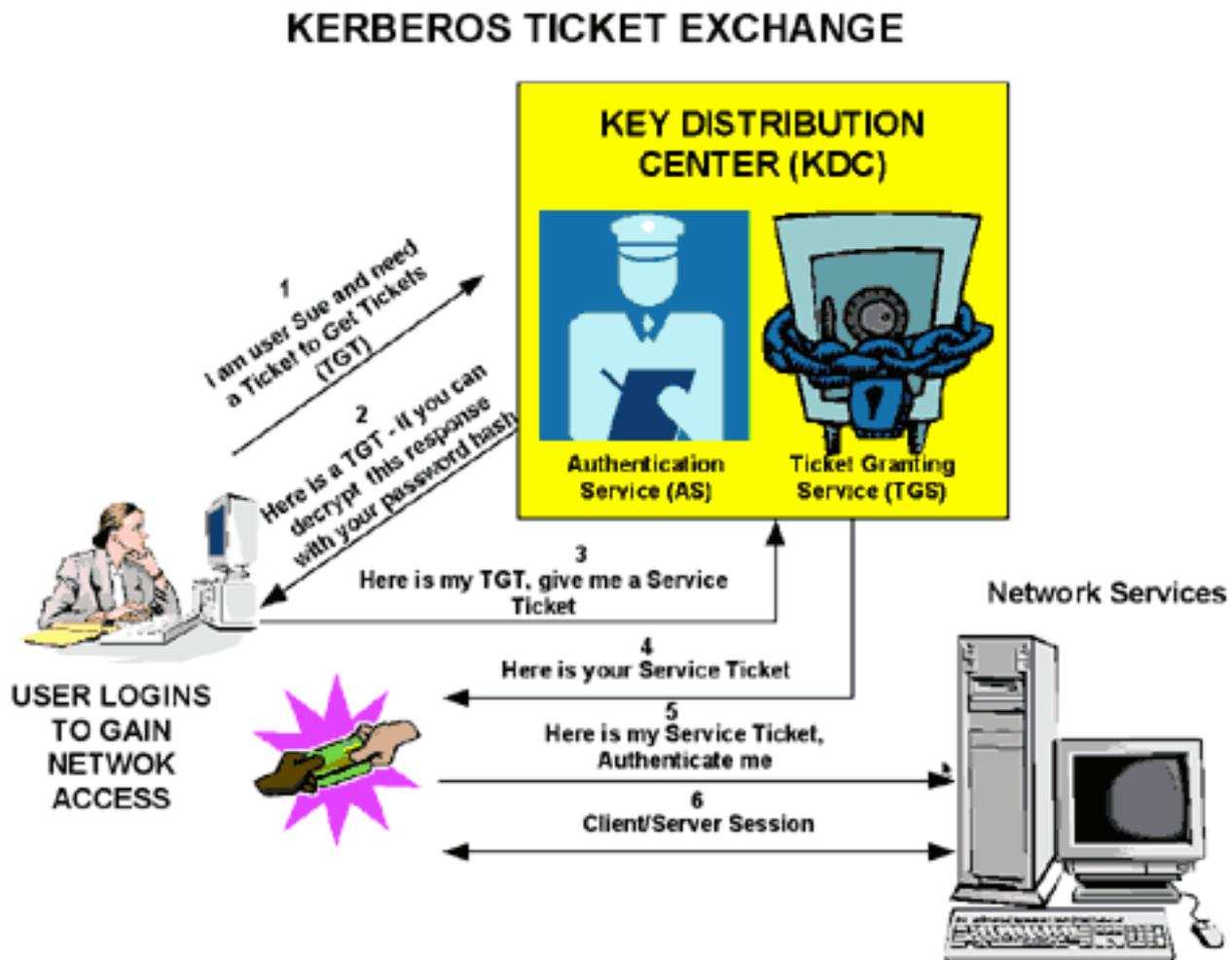
## Kerberosプロトコル

Kerberosの3つのヘッドは、キー配布センター(KDC)、クライアントユーザ、およびアクセスするサーバで構成されます。

KDCはドメインコントローラ(DC)の一部としてインストールされ、次の2つのサービス機能を実行します。認証サービス(AS)とチケット認可サービス(TGS)。

クライアントが最初にサーバリソースにアクセスするときは、次の3つの交換が関係します。

1. AS Exchange。
2. TGS交換。
3. クライアント/サーバ(CS)Exchange。



- ドメインコントローラ= KDC(AS + TGS)。
- パスワードを使用してAS ( SSOポータル ) に認証します。
- チケット認可チケット(TGT) ( セッションクッキー ) を取得します。
- サービス(SRV01)へのログインを要求します。
- SRV01がKDCにリダイレクトします。
- Show TGT to KDC: ( 認証済み )
- KDCはSRV01のTGSを提供します。

- SRV01にリダイレクトします。
- SRV01へのサービスチケットを表示します。
- SRV01はサービスチケットを確認し、信頼します。
- サービスチケットに私の情報がすべて含まれています。
- SRV01がログインします。

最初にネットワークにログオンしたユーザーは、ドメイン内のKDCのAS部分で確認するために、アクセスをネゴシエートし、ログイン名とパスワードを提供する必要があります。

KDCは、Active Directoryのユーザーアカウント情報にアクセスできます。認証されると、ユーザーにはローカルドメインで有効なチケット認可チケット(TGT)が付与されます。

TGTのデフォルトのライフタイムは10時間で、ユーザーがパスワードを再入力しなくても、ユーザーのログオンセッションを通じて更新されます。

TGTは、揮発性メモリ領域内のローカルマシンにキャッシュされ、ネットワーク全体のサービスとのセッションを要求するために使用されます。

ユーザーは、サーバー・サービスへのアクセスが必要な場合に、KDCのTGS部分にTGTを提示します。

KDC上のTGSはユーザーTGTを認証し、クライアントとリモートサーバの両方のチケットとセッションキーを作成します。この情報(サービスチケット)は、クライアントマシンにローカルにキャッシュされます。

TGSはクライアントTGTを受信し、自身のキーで読み取ります。TGSがクライアント要求を承認すると、クライアントとターゲットサーバの両方に対してサービスチケットが生成されます。

クライアントは、先にAS応答から取得したTGSセッションキーで自身の部分を読み取ります。

クライアントは、TGS応答のサーバ部分を、次のクライアント/サーバ交換のターゲットサーバに提示します。

例：

## Test User Authentication

\* Username

\* Password

Authentication Type

Authorization Data  Retrieve Groups  
 Retrieve Attributes

Authentication Result	Groups	Attributes
Authentication time : 57 ms. Groups fetching time : 18 ms. Attributes fetching time: 4 ms.		
Processing Steps: 14:05:37:440: Resolving identity - user1 14:05:37:440: Search for matching accounts at join point - ralmaait.com 14:05:37:449: Single matching account found in forest - ralmaait.com 14:05:37:449: Identity resolution detected single matching account 14:05:37:476: Authentication Ticket (TGT) request succeeded - user1@ralmaait.com 14:05:37:478: Service Ticket request succeeded - user1@ralmaait.com 14:05:37:486: Service Ticket validation succeeded - user1@ralmaait.com 14:05:37:486: Account validation succeeded		

認証されたユーザのISEからのパケットキャプチャ：

Time	Source IP	Destination IP	Protocol	Details	Status	
111	2020-01-13 16:17:53.082713	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=105462807 TSecr=280789807	✓
112	2020-01-13 16:17:53.082735	10.48.60.50	10.48.60.51	KRB5	346 AS-REQ	✓
113	2020-01-13 16:17:53.083625	10.48.60.51	10.48.60.50	KRB5	1576 AS-REP	✓
114	2020-01-13 16:17:53.083649	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [ACK] Seq=281 Ack=1511 Win=32256 Len=0 TSval=105462808 TSecr=2807...	✓
115	2020-01-13 16:17:53.083678	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [FIN, ACK] Seq=281 Ack=1511 Win=32256 Len=0 TSval=105462808 TSecr=...	✓
116	2020-01-13 16:17:53.083908	10.48.60.51	10.48.60.50	TCP	66 88 → 53610 [ACK] Seq=1511 Ack=282 Win=532736 Len=0 TSval=280789809 TSecr=105...	✓
117	2020-01-13 16:17:53.084022	10.48.60.51	10.48.60.50	TCP	60 88 → 53610 [RST, ACK] Seq=1511 Ack=282 Win=0 Len=0	✓
118	2020-01-13 16:17:53.084449	10.48.60.50	10.48.60.51	KRB5	1480 TGS-REQ	✓
119	2020-01-13 16:17:53.085475	10.48.60.51	10.48.60.50	KRB5	1446 TGS-REP	✓
120	2020-01-13 16:17:53.110397	10.48.60.50	10.48.60.51	TCP	66 48959 → 3268 [ACK] Seq=1700 Ack=536 Win=31360 Len=0 TSval=105462835 TSecr=28...	✓

AS-REQにはユーザ名が含まれています。パスワードが正しければ、ASサービスはユーザパスワードで暗号化されたTGTを提供します。次に、TGTがTGTサービスに提供され、セッションチケットが取得されます。

セッションチケットを受信すると、認証が成功します。

次に、クライアントから与えられたパスワードが間違っている例を示します。

Time	Source IP	Destination IP	Protocol	Details	Status	
117	2020-01-14 08:51:03.846603	10.48.60.50	10.48.60.51	KRB5	318 AS-REQ	✓
118	2020-01-14 08:51:03.848340	10.48.60.51	10.48.60.50	KRB5	194 KRB Error: KRB5KDC_ERR_PREAUTH_FAILED	✗

パスワードが間違っていると、AS要求は失敗し、TGTは受信されません。

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

パスワードが間違っている場合にad\_agent.logファイルにログオンします。

2020-01-14 13:36:05,442

DEBUG,140574072981248,krb5:RALMAAIT.COM,LwKrb5TraceCallback(),lwadvapi/theaded/lwkrb5.c:1325に要求 ( 276バイト ) を送信

2020-01-14 13:36:05,444 DEBUG,140574072981248,krb5:KDCからエラーを受信しました : -1765328360/Preauthentication failed,LwKrb5TraceCallback(),lwadvapi/theaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG,140574072981248,krb5:Preauth tryagain入力タイプ : 16、14、19、2,LwKrb5TraceCallback(),lwadvapi/theaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 WARNING,140574072981248,[LwKrb5GetTgtImpl ../lwadvapi/theaded/krbtgt.c:329] KRB5エラーコード : -1765328360(メッセージ : 事前認証に失敗)、LwTranslateKrb5Error()、lwadvapi/theaded/lwkrb5.c:892

2020-01-14 13:36:05,444 DEBUG ,140574072981248,[LwKrb5InitializeUserLoginCredentials()]エラーコード : 40022(記号 : LW\_ERROR\_PASSWORD\_MISMATCH),LwKrb5InitializeUserLoginCredentials(),lwadvapi/theaded/lwkrb5.c:1453

## MS-RPCプロトコル

ISEはSMB上でMS-RPCを使用します。SMBは認証を提供し、特定のRPCサービスが存在する場所を見つけるために個別のセッションを必要としません。クライアントとサーバ間の通信には、「名前付きパイプ」と呼ばれるメカニズムを使用します。

- SMBセッション接続を作成します。
- RPCメッセージをトランスポートとしてSMB/CIFS.TCPポート445経由で転送する
- SMBセッションは、特定のRPCサービスが実行するポートを識別し、ユーザー認証を処理します。
- プロセス間通信の隠し共有IPC \$に接続します。
- 目的のRPCリソース/関数の適切な名前付きパイプを開きます。

SMB上でRPC交換を処理します。

No.	Time	Source	Destination	Protocol	Length	Info	Text Item
59	2020-01-14 14:56:01.082699	10.48.60.50	10.48.60.51	SMB	128	Negotiate Protocol Request	✓
60	2020-01-14 14:56:01.083241	10.48.60.51	10.48.60.50	SMB2	318	Negotiate Protocol Response	✓
61	2020-01-14 14:56:01.083255	10.48.60.50	10.48.60.51	TCP	66	26963 → 445 [ACK] Seq=63 Ack=253 Min=30336 Len=0 TSval=186950807 TSecr=36227...	✓
72	2020-01-14 14:56:01.086109	10.48.60.50	10.48.60.51	SMB2	1589	Session Setup Request	✓
73	2020-01-14 14:56:01.086341	10.48.60.51	10.48.60.50	TCP	66	445 → 26963 [ACK] Seq=253 Ack=1588 Min=66560 Len=0 TSval=362277347 TSecr=186...	✓
74	2020-01-14 14:56:01.087951	10.48.60.51	10.48.60.50	SMB2	328	Session Setup Response	✓
75	2020-01-14 14:56:01.087260	10.48.60.50	10.48.60.51	SMB2	212	Tree Connect Request Tree: \\WIN-E051AB1Q9BK.raimaait.com\IPC\$	✓
76	2020-01-14 14:56:01.087592	10.48.60.51	10.48.60.50	SMB2	150	Tree Connect Response	✓
77	2020-01-14 14:56:01.087721	10.48.60.50	10.48.60.51	SMB2	206	Create Request File: netlogon	✓
78	2020-01-14 14:56:01.088023	10.48.60.51	10.48.60.50	SMB2	222	Create Response File: netlogon	✓
79	2020-01-14 14:56:01.088207	10.48.60.50	10.48.60.51	DCERPC	314	Bind: call_id: 9, Fragment: Single, 1 context items: RPC_NETLOGON V1.0 (32bi...	✓
80	2020-01-14 14:56:01.088500	10.48.60.51	10.48.60.50	SMB2	150	Write Response	✓
81	2020-01-14 14:56:01.088665	10.48.60.50	10.48.60.51	SMB2	183	Read Request Len:8192 Off:0 File: netlogon	✓
82	2020-01-14 14:56:01.088899	10.48.60.51	10.48.60.50	DCERPC	238	Bind ack: call_id: 9, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 res...	✓
83	2020-01-14 14:56:01.089118	10.48.60.50	10.48.60.51	RPC_NETLOGON	574	NetLogonSamLogonEx request	✓
84	2020-01-14 14:56:01.089373	10.48.60.51	10.48.60.50	SMB2	150	Write Response	✓
85	2020-01-14 14:56:01.089517	10.48.60.50	10.48.60.51	SMB2	183	Read Request Len:8192 Off:0 File: netlogon	✓
86	2020-01-14 14:56:01.090160	10.48.60.51	10.48.60.50	RPC_NETLOGON	606	NetLogonSamLogonEx response	✓
88	2020-01-14 14:56:01.129364	10.48.60.50	10.48.60.51	TCP	66	26963 → 445 [ACK] Seq=2862 Ack=1635 Min=34688 Len=0 TSval=186950854 TSecr=36...	✓
145	2020-01-14 14:56:09.910387	10.48.60.50	10.48.60.51	RPC_NETLOGON	574	NetLogonSamLogonEx request	✓
146	2020-01-14 14:56:09.910734	10.48.60.51	10.48.60.50	SMB2	150	Write Response	✓

> Secure Channel Verifier

Microsoft Network Logon, NetLogonSamLogonEx  
Operation: NetLogonSamLogonEx (39)  
[Response in frame: 86]

LogonServer: \\WIN-E051AB1Q9BK.raimaait.com  
Referent ID: 0x00000001  
Max Count: 31  
Offset: 0  
Actual Count: 31  
Computer Name: \\WIN-E051AB1Q9BK.raimaait.com

Computer Name: ISERIRI24  
Referent ID: 0x00000001  
Max Count: 10  
Offset: 0  
Actual Count: 10  
Computer Name: ISERIRI24

Level: 2

LEVEL: LogonLevel  
Level: 2

NETWORK\_INFO:  
Referent ID: 0x00000001  
> IDENTITY\_INFO: User:lg@raimaait.com  
Challenge: cdc343b187f9b4e1

「 negotiate protocol request/response lineはSMBの方言をネゴシエートします。 「 session setup request/response 認証を実行します。

ツリー接続要求と応答は、要求されたリソースに接続します。特別な共有IPC \$に接続されていません。

このプロセス間通信シェアは、ホスト間の通信手段を提供し、MSRPC機能のトランスポートとしても使用できます。

パケット77は Create Request File ファイル名は、接続されているサービス ( この例ではnetlogonサービス ) の名前です。

パケット83および86では、NetrlogonSamLogonEX要求は、ISE上のクライアント認証用のユーザー名をNetwork\_INFOフィールドのADに送信する場所です。

NetrlogonSamLogonEX応答パッケージが結果を返します。

NetrlogonSamLogonEX応答の一部のフラグ値：  
0xc000006a is STATUS\_WRONG\_PASSWORD  
0x00000000:STATUS\_SUCCESS  
0x00000103:STATUS\_PENDING

## ISEとActive Directory(AD)の統合

ISEはLDAP、KRB、およびMSRBCを使用して、参加/脱退および認証プロセス中にADと通信します。

次のセクションでは、ADで特定のDCに接続し、そのDCに対するユーザー認証に使用するプロトコル、検索形式、およびメカニズムについて説明します。

何らかの理由でDCがオフラインになった場合、ISEは次に使用可能なDCにフェールオーバーし、認証プロセスは影響を受けません。

グローバルカタログサーバー(GC)は、フォレスト内のすべてのActive Directoryオブジェクトのコピーを格納するドメインコントローラーです。

ドメインのディレクトリにあるすべてのオブジェクトの完全なコピーと、他のすべてのフォレストドメインのすべてのオブジェクトの部分的なコピーが保存されます。

したがって、グローバルカタログを使用すると、ユーザーとアプリケーションは、GCに含まれる属性を検索して、現在のフォレストの任意のドメイン内のオブジェクトを検索できます。

グローバルカタログには、各ドメインの各フォレストオブジェクトの基本的な ( 不完全な ) 属性セット ( 部分属性セット、PAT ) が含まれています。

GCは、フォレスト内のすべてのドメインディレクトリパーティションからデータを受信します。

標準のADレプリケーションサービスでコピーされます。

## AD への ISE の結合

Active DirectoryとISEの統合の前提条件

1. ISEでスーパー管理者またはシステム管理者の権限があることを確認します。
2. Network Time Protocol(NTP)サーバ設定を使用して、CiscoサーバとActive Directory間の時刻を同期します。ISEとADの最大許容時間差は5分です
3. ISE上で設定されたDNSは、追加のサイト情報の有無にかかわらず、DC、GC、およびKDCのSRVクエリに応答できる必要があります。
4. すべてのDNSサーバが、可能なActive Directory DNSドメインに対する順方向および逆方向DNSクエリに応答できることを確認します。
5. ADには、シスコが動作し、シスコがアクセス可能なグローバルカタログサーバが、シスコに参加するドメインに少なくとも1つ必要です。

## ADドメインへの参加

ISEはドメイン検出を適用して、参加ドメインに関する情報を3段階で取得します。

1. 参加したドメインのクエリ：フォレストからドメインを検出し、参加したドメインに対して外部から信頼されているドメインを検出します。
2. フォレスト内のルートドメインを照会する：フォレストとの信頼を確立します。
3. 信頼されたフォレストのルートドメインを照会する – 信頼されたフォレストからドメインを検出します。

さらに、Cisco ISEはDNSドメイン名 (UPNサフィックス)、代替UPNサフィックス、およびNTLMドメイン名を検出します。

ISEはDCディスカバリを適用して、使用可能なDCおよびGCに関するすべての情報を取得します。

1. 参加プロセスは、ドメイン自体に存在するADのスーパー管理者の入力クレデンシャルから開始されます。別のドメインまたはサブドメインに存在する場合、ユーザ名はUPN表記 (username@domain) で表記する必要があります。
2. ISEは、すべてのDC、GC、およびKDCレコードに対してDNSクエリを送信します。DNS応答にDNS応答が含まれていない場合、統合は失敗し、DNS関連のエラーが表示されます。
3. ISEはCLDAP pingを使用して、SRVレコード内の優先順位に対応するDCに送信されたCLDAP要求を介してすべてのDCとGCを検出します。最初のDC応答が使用され、ISEはそのDCに接続されます。

DCプライオリティの計算に使用される要因の1つは、CLDAP pingへの応答にDCが要する時間です。応答が速いほど、優先度が高くなります。

注：CLDAPは、ISEがDCとの接続を確立および維持するために使用するメカニズムです。最初のDC応答までの応答時間を測定します。DCからの応答がない場合は失敗します。応答時間が2.5秒より長い場合に警告します。CLDAPがサイト内のすべてのDCに対してpingを実行します ( サイトがない場合は、ドメイン内のすべてのDCにpingを実行します )。CLDAP応答には、DCサイトとクライアントサイト ( ISEマシンが割り当てられているサイト ) が含まれます。

4. ISEは、「ユーザの参加」クレデンシャルを含むTGTを受信します。
5. MSRPCを使用してISEマシンアカウント名を生成します ( SAMおよびSPN )。
6. ISEマシンアカウントがすでに存在する場合は、SPNでADを検索します。ISEマシンが存在しない場合、ISEは新しいマシンを作成します。
7. マシンアカウントを開き、ISEマシンアカウントパスワードを設定し、ISEマシンアカウントがアクセス可能であることを確認します。
8. ISEマシンアカウント属性 ( SPN、dnsHostnameなど ) を設定します。
9. KRB5でISEマシンのクレデンシャルを使用してTGTを取得し、すべての信頼されたドメインを検出します。
10. 参加が完了すると、ISEノードはADグループと関連付けられたSIDを更新し、SID更新プロセスを自動的に開始します。このプロセスがAD側で完了できることを確認します。

## ADドメインを離れる

ISEが離れるときは、ADは次のことを考慮する必要があります。

1. 完全なAD管理者ユーザを使用して、脱退プロセスを実行します。これにより、ISEマシンアカウントがActive Directoryデータベースから削除されたことを確認できます。
2. ADにクレデンシャルが残されていない場合、ISEアカウントはADから削除されないため、手動で削除する必要があります。
3. バックアップまたはアップグレード後にCLIからISE設定をリセットするか、設定を復元すると、脱退操作が実行され、Active DirectoryドメインからISEノードが切断されます。( 結合されている場合 )。ただし、ISEノードアカウントはActive Directoryドメインから削除されません。
4. Active Directoryのクレデンシャルを使用して管理ポータルから脱退操作を実行することをお勧めします。これは、Active Directoryドメインからノードアカウントも削除されるためです。また、ISEホスト名を変更する場合にも推奨されます。

## DCフェールオーバー

何らかの理由でISEに接続されたDCがオフラインまたは到達不能になると、DCフェールオーバーがISEで自動的にトリガーされます。DCフェールオーバーは、次の条件によってトリガーされます。

1. ADコネクタは、CLDAP、LDAP、RPC、またはKerberos通信の試行中に、現在選択されているDCが使用できなくなったことを検出します。このような場合、ADコネクタはDC選択を開始し、新しく選択したDCにフェールオーバーします。
2. DCは起動し、CLDAP pingに応答しますが、ADコネクタは何らかの理由でDCと通信できません(例：RPCポートがブロックされ、DCが「中断レプリケーション」状態にあり、DCが適切に使用停止されていない)。

このような場合、ADコネクタはブロックされたリストを使用してDC選択を開始し ( ブロックされたリストに「不良」DCが配置されている )、選択されたDCとの通信を試みます。ブロックされたリストで選択されたDCはキャッシュされません。

ADコネクタは、妥当な時間内にフェールオーバーを完了する必要があります ( 失敗した場合は失敗します )。このため、ADコネクタはフェールオーバー中に限られた数のDCを試行します。

ISEは、回復不能なネットワークまたはサーバエラーが発生した場合にADドメインコントローラをブロックし、ISEが不正なDCを使用することを防止します。CLDAP pingに応答しない場合、

DCはblockedリストに追加されません。ISEは、応答しないDCの優先順位を下げるだけです。

## LDAPによるISE-AD通信

ISEは、次のいずれかの検索形式でAD内のマシンまたはユーザを検索します。マシンを検索した場合、ISEはマシン名の最後に「\$」を追加します。ADでユーザを識別するために使用されるIDタイプのリストを次に示します。

- SAM名：ドメインマークアップのないユーザ名またはマシン名。これはADのユーザログオン名です。例：sajedaまたはsajeda\$
- CN:はAD上のユーザ表示名であり、SAMと同じであってはなりません。例：sajeda Ahmed.
- ユーザープリンシパル名(UPN):は、SAM名とドメイン名(SAM\_NAME@domain)の組み合わせです。例：[sajeda@cisco.com](#)またはsajeda\$@cisco.com
- 代替UPN:は、ドメイン名以外のADで設定される追加または代替のUPNサフィックスです。この設定はADにグローバルに追加され(ユーザごとに設定されません)、実際のドメイン名のサフィックスである必要はありません。

各ADには、複数のUPNサフィックス(@alt1.com、@alt2.com、...など)を設定できます。例：メインUPN([sajeda@cisco.com](#))、代替UPN:sajeda@domain1、sajeda@domain2

- NetBIOSプレフィックス名：は、マシン名のドメイン名\ユーザ名です。例：CISCO\sajedaまたはCISCO\machine\$
- 修飾されていないマシンを持つホスト/プレフィックス：これは、マシン名のみを使用する場合にマシン認証に使用され、ホスト/マシン名のみを使用します。例：ホスト/マシン
- 完全修飾マシンを含むホスト/プレフィックス：これは、マシンFQDNが使用される場合にマシン認証に使用されます。通常、証明書認証の場合は、マシンのホスト/FQDNです。例：  
: host/machine.cisco.com
- SPN名：クライアントがサービスのインスタンスを一意に識別するために使用する名前(例：HTTP、LDAP、SSH)で、マシンのみで使用されます。

## ADフローに対するユーザ認証：

1. IDを解決し、IDの種類(SAM、UPN、SPN)を決定します。ISEがIDをユーザ名としてのみ受け取った場合、ADで関連付けられたSAMアカウントを検索します。ISEがusername@domainとしてIDを受信すると、一致したUPNまたはメールをAD内で検索します。どちらのシナリオでも、ISEはマシンまたはユーザ名に追加のフィルタを使用します。
2. ドメインまたはフォレストの検索(IDの種類によって異なります)
3. 関連付けられたすべてのアカウント(JP、DN、UPN、ドメイン)に関する情報を保持する
4. 関連付けられたアカウントが見つからない場合、ADはユーザに対する応答を認識しません。
5. 関連付けられたアカウントごとにMS-RPC(またはKerberos)認証を実行する
6. 入力IDとパスワードに一致するアカウントが1つだけの場合、認証は成功します
7. 複数のアカウントが着信IDと一致する場合、ISEはパスワードを使用してあいまいさを解決し、パスワードが関連付けられたアカウントが認証され、他のアカウントは不正なパスワード

ドカウンタを1増やします。

8. 着信IDとパスワードに一致するアカウントがない場合、ADは誤ったパスワードで応答します。

## ISE 検索フィルタ

フィルタは、ADと通信するエンティティを識別するために使用されます。 ISEは常にusersグループとmachinesグループでそのエンティティを検索します。

検索フィルタの例：

1. **SAM検索**：ISEがドメインマークアップのないユーザ名としてのみIDを受信した場合、ISEはこのユーザ名をSAMとして扱い、そのIDをSAM名として持つすべてのマシンユーザまたはマシンをADで検索します。

SAM名が一意でない場合、ISEはパスワードを使用してユーザを区別し、ISEはEAP-TLSなどのパスワードレスプロトコルを使用するように設定されます。

適切なユーザを見つけるための他の基準がないため、ISEは「あいまいなID」エラーで認証に失敗します。

ただし、ユーザ証明書がActive Directoryにある場合、Cisco ISEはバイナリ比較を使用してIDを解決します。

```
219 2020-01-20 16:33:48.251918 10.48.60.206 10.48.60.101 LDAP 295 SASL GSS-API Integrity: searchRequest(2) "dc=aaaalab,dc=com" wholeSubtree ✓
220 2020-01-20 16:33:48.253244 10.48.60.101 10.48.60.206 LDAP 384 SASL GSS-API Integrity: searchResEntry(2) "CN=anas Jehad,CN=Users,DC=aaaalab,... ✓
258 2020-01-20 16:33:48.306966 10.48.60.206 10.48.60.101 LDAP 105 ✓

<
> Frame 219: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits)
> Ethernet II, Src: Vmware_b6:ed:17 (00:50:56:b6:ed:17), Dst: Vmware_d5:6a:7d (00:0c:29:d5:6a:7d)
> Internet Protocol Version 4, Src: 10.48.60.206, Dst: 10.48.60.101
> Transmission Control Protocol, Src Port: 19997, Dst Port: 3268, Seq: 1430, Ack: 213, Len: 229
> Lightweight Directory Access Protocol
  SASL Buffer Length: 225
  > SASL Buffer
    > GSS-API Generic Security Service Application Program Interface
      > GSS-API payload (197 bytes)
        > LDAPMessage searchRequest(2) "dc=aaaalab,dc=com" wholeSubtree
          messageID: 2
          > protocolOp: searchRequest (3)
            > searchRequest
              baseObject: dc=aaaalab,dc=com
              scope: wholeSubtree (2)
              derefAliases: neverDerefAliases (0)
              sizeLimit: 0
              timeLimit: 0
              typesOnly: False
              > filter: (&(!((objectCategory=person)(objectCategory=computer)))(sAMAccountName=anos))
                > filter: and (0)
                  > and: (&(!((objectCategory=person)(objectCategory=computer)))(sAMAccountName=anos))
                    > and: 2 items
                      > Filter: ((!(objectCategory=person)(objectCategory=computer))
                        > and item: or (1)
                          > or: ((!(objectCategory=person)(objectCategory=computer))
                            > Filter: (sAMAccountName=anos)
                              > and item: equalityMatch (3)
                                > equalityMatch
                                  attributeDesc: sAMAccountName
                                  assertionValue: anos
                              > attributes: 4 items
                                AttributeDescription: sAMAccountName
                                AttributeDescription: userPrincipalName
                                AttributeDescription: objectCategory
                                AttributeDescription: userAccountControl
```

2. **UPNまたはメール検索**：ISEがusername@domainとしてIDを受信すると、ISEは各フォレストグローバルカタログを検索して、そのUPN IDまたはメールID「identity=matched UPN or email」に一致するものを探します。

一意の一致がある場合、Cisco ISEはAAAフローを続行します。

同じUPNとパスワード、または同じUPNとメールを持つ複数の参加ポイントがある場合、Cisco ISEは「あいまいなID」エラーで認証に失敗します。

461	2020-01-20 16:33:58.134338	10.48.60.206	10.48.60.101	LDAP	336 SASL GSS-API Integrity: searchRequest(3) "dc=aaalab,dc=com" wholeSubtree ✓
464	2020-01-20 16:33:58.137942	10.48.60.101	10.48.60.206	LDAP	384 SASL GSS-API Integrity: searchResEntry(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
471	2020-01-20 16:33:58.170678	10.48.60.206	10.48.60.101	LDAP	179 SASL GSS-API Integrity: searchRequest(6) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
472	2020-01-20 16:33:58.172663	10.48.60.101	10.48.60.206	LDAP	1413 SASL GSS-API Integrity: searchResEntry(6) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
476	2020-01-20 16:33:58.174754	10.48.60.206	10.48.60.101	LDAP	189 SASL GSS-API Integrity: searchRequest(7) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
479	2020-01-20 16:33:58.175528	10.48.60.101	10.48.60.206	LDAP	255 SASL GSS-API Integrity: searchResEntry(7) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
480	2020-01-20 16:33:58.176236	10.48.60.206	10.48.60.101	LDAP	241 SASL GSS-API Integrity: searchRequest(8) "dc=aaalab,dc=com" wholeSubtree ✓
481	2020-01-20 16:33:58.177307	10.48.60.101	10.48.60.206	LDAP	635 SASL GSS-API Integrity: searchResEntry(8) "CN=Users,CN=Builtin,DC=aaalab,DC=..." ✓
484	2020-01-20 16:33:58.178414	10.48.60.206	10.48.60.101	LDAP	271 SASL GSS-API Integrity: searchRequest(9) "dc=aaalab,dc=com" wholeSubtree ✓

```
> Frame 461: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits)
> Ethernet II, Src: Vmware_b6:ed:17 (00:50:56:b6:ed:17), Dst: Vmware_d5:6a:7d (00:0c:29:d5:6a:7d)
> Internet Protocol Version 4, Src: 10.48.60.206, Dst: 10.48.60.101
> Transmission Control Protocol, Src Port: 19997, Dst Port: 3268, Seq: 1659, Ack: 531, Len: 270
```

```
Lightweight Directory Access Protocol
  SASL Buffer Length: 266
  SASL Buffer
    > GSS-API Generic Security Service Application Program Interface
    > GSS-API payload (238 bytes)
    > LDAPMessage searchRequest(3) "dc=aaalab,dc=com" wholeSubtree
      messageID: 3
      protocolOp: searchRequest (3)
        searchRequest
          baseObject: dc=aaalab,dc=com
          scope: wholeSubtree (2)
          derefAliases: neverDerefAliases (0)
          sizeLimit: 0
          timeLimit: 0
          typesOnly: False
          Filter: (&((objectCategory=person)(objectCategory=computer))((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com)))
            filter: and (0)
              and: (&((objectCategory=person)(objectCategory=computer))((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com)))
                and: 2 items
                  Filter: ((objectCategory=person)(objectCategory=computer))
                    and item: or (1)
                      or: ((objectCategory=person)(objectCategory=computer))
                  Filter: ((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com))
                    and item: or (1)
                      or: ((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com))
```

### 3. NetBIOS検索 : ISEがNetBIOSドメインプレフィクス (例 : CISCO\sajedah) を持つIDを受信すると、ISEはフォレストでNetBIOSドメインを検索します。見つかったら、指定されたSAM名 (この例ではsajeda) を検索します

654	2020-01-20 17:06:29.243747	10.48.60.206	10.48.60.101	LDAP	295 SASL GSS-API Integrity: searchRequest(2) "dc=aaalab,dc=com" wholeSubtree ✓
655	2020-01-20 17:06:29.245154	10.48.60.101	10.48.60.206	LDAP	682 SASL GSS-API Integrity: searchResEntry(2) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
684	2020-01-20 17:06:29.290383	10.48.60.206	10.48.60.101	LDAP	179 SASL GSS-API Integrity: searchRequest(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
685	2020-01-20 17:06:29.292939	10.48.60.101	10.48.60.206	LDAP	1413 SASL GSS-API Integrity: searchResEntry(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
687	2020-01-20 17:06:29.294515	10.48.60.206	10.48.60.101	LDAP	189 SASL GSS-API Integrity: searchRequest(4) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
688	2020-01-20 17:06:29.295469	10.48.60.101	10.48.60.206	LDAP	255 SASL GSS-API Integrity: searchResEntry(4) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
689	2020-01-20 17:06:29.296186	10.48.60.206	10.48.60.101	LDAP	241 SASL GSS-API Integrity: searchRequest(5) "dc=aaalab,dc=com" wholeSubtree ✓
692	2020-01-20 17:06:29.297557	10.48.60.101	10.48.60.206	LDAP	635 SASL GSS-API Integrity: searchResEntry(5) "CN=Users,CN=Builtin,DC=aaalab,DC=..." ✓
693	2020-01-20 17:06:29.298761	10.48.60.206	10.48.60.101	LDAP	271 SASL GSS-API Integrity: searchRequest(6) "dc=aaalab,dc=com" wholeSubtree ✓
694	2020-01-20 17:06:29.299690	10.48.60.101	10.48.60.206	LDAP	650 SASL GSS-API Integrity: searchResEntry(6) "CN=Domain Users,CN=Users,DC=aaala..." ✓

```
SASL Buffer
  > GSS-API Generic Security Service Application Program Interface
  > GSS-API payload (197 bytes)
  > LDAPMessage searchRequest(2) "dc=aaalab,dc=com" wholeSubtree
    messageID: 2
    protocolOp: searchRequest (3)
      searchRequest
        baseObject: dc=aaalab,dc=com
        scope: wholeSubtree (2)
        derefAliases: neverDerefAliases (0)
        sizeLimit: 0
        timeLimit: 0
        typesOnly: False
        Filter: (&((objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
          filter: and (0)
            and: (&((objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
              and: 2 items
                Filter: ((objectCategory=person)(objectCategory=computer))
                  and item: or (1)
                    or: ((objectCategory=person)(objectCategory=computer))
                Filter: (sAMAccountName=anos)
                  and item: equalityMatch (3)
                    equalityMatch
```

### 4. マシンベース検索 : ISEがホスト/プレフィクスIDを持つマシン認証を受信すると、一致する servicePrincipalName属性をフォレストで検索します。

完全修飾ドメインサフィックス(host/machine.domain.comなど)がIDに指定されている場合、Cisco ISEはそのドメインが存在するフォレストを検索します。

IDがホスト/マシンの形式である場合、Cisco ISEはすべてのフォレストでサービスプリンシパル名を検索します。

一致が複数ある場合、Cisco ISEは「あいまいなID」エラーで認証に失敗します。



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。