Keytabファイルを使用した統合Windows認証環境の構築手順

IceWall技術レポート

1. はじめに

統合Windows認証を行うことで、ユーザーがブラウザーにユーザーID、およびパスワードを入力せずにログインが可能です。

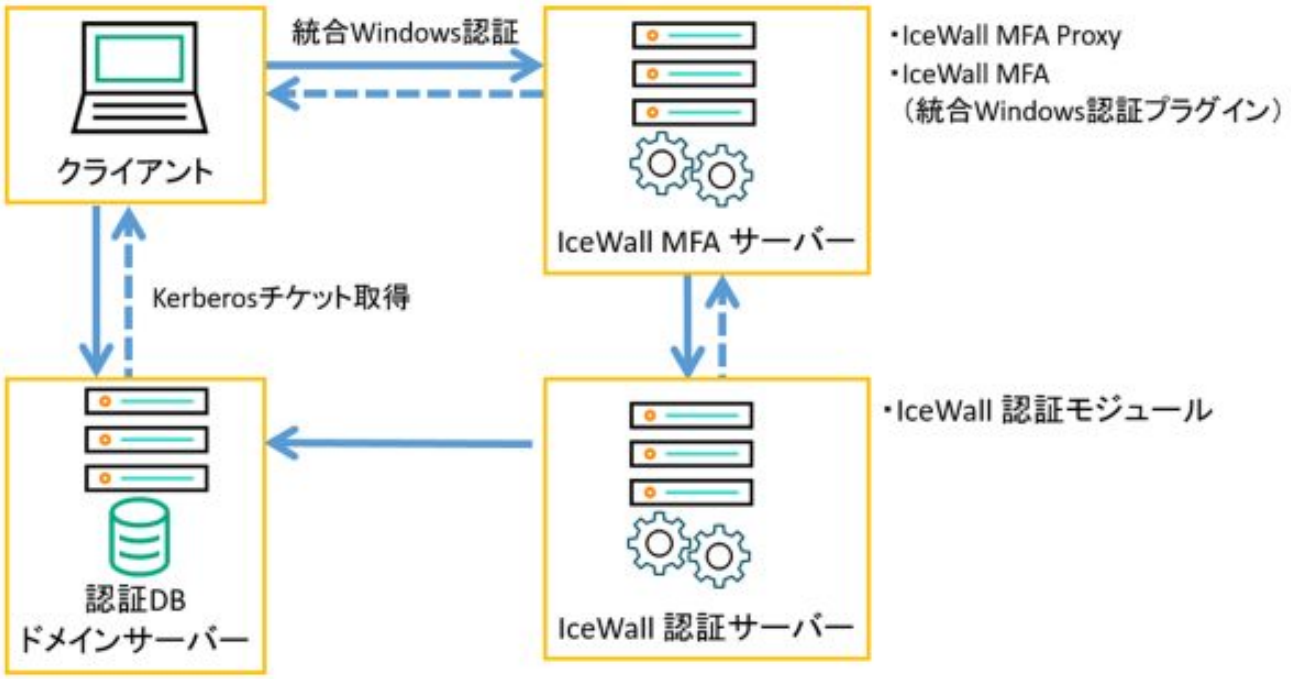
本技術レポートでは、Keytabファイルを使用した統合Windows認証の環境構築の手順を説明します。説明の対象となるIceWall製品は以下の2種類です。

- HPE IceWall MFA ー 統合Windows認証プラグイン
- HPE IceWall SSO ー Domain Gatewayオプション（Linux版）

以降の説明は、HPE IceWall MFAの内容で記載していますが、HPE IceWall SSOと差分がある箇所のみ併記しています。

2. システム構成例

例として記載するシステム構成は次の図のとおりです。



- HPE IceWall MFA サーバー（統合Windows認証プラグイン）
  HPE IceWall MFA バージョン : 4.0
  OS : Red Hat Enterprise Linux 9.1
- HPE IceWall 認証サーバー
  HPE IceWall 認証モジュール バージョン : 11.0
  OS : Red Hat Enterprise Linux 9.1
- 認証DB / ドメインサーバー
  DB種別 : Active Directory Domain Services
  （認証DB、およびドメインサーバーとして使用）
  OS : Microsoft Windows Server 2022
  Keytabファイル生成時に指定する暗号化方式 : AES256-SHA1
  ※認証DBは、Active Directory以外の種別のDBを参照することも可能です
- クライアント
  OS : Windows 11

3. ドメインサーバーでの手順

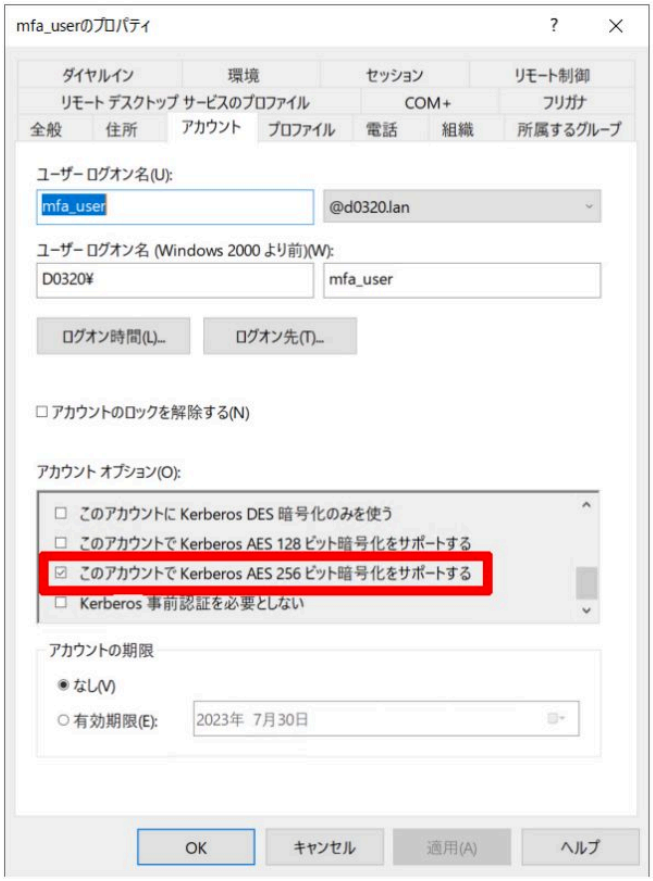
1. 「DNSサーバー」の役割をインストールします。
2. 「ActiveDirectoryドメインサービス」の役割をインストールします。

3. 「証明機関」の役割をインストールします。

4. 各役割の設定を行い、OSを再起動します。

5. Kerberosチケットの解析で使用するユーザー「mfa_user」を作成します。

6. 作成したユーザーのプロパティを開き、「アカウント」タブの「このアカウントでKerberos AES 256 ビット暗号化をサポートする」にチェックを入れます。



7. コマントプロンプトを立ち上げktpassコマンドを実行します。

ktpass -crypto [Kerberosチケットの暗号化方式] -princ [プリンシパル名(HTTP/FQDN@REALM)] -mapuser [Kerberosチケットの解析で使用するユーザー名] -pass [パスワード] -ptype [プリンシパルの種類] -out [Keytabファイル出力先]

※FQDNはホスト名が大文字の場合でも、小文字で指定する必要があります。
※REALMSは大文字で記述する必要があります。

コマンド実行例：

ktpass -crypto AES256-SHA1 -princ HTTP/mfa.d0320.lan@D0320.LAN -mapuser mfa_user -pass password -ptype KRB5_NT_PRINCIPAL -out C:\iw.keytab

Targeting domain controller: ad0323.d0320.lan
Successfully mapped HTTP/mfa.d0320.lan to mfa_user.
Password successfully set!
Key created.
Output keytab to C:\iw.keytab:
Keytab version: 0x502

```
keysize 79 HTTP/mfa.d0320.lan@D0320.LAN ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype
0x12 (AES256-SHA1) keylength 32
(0x68754e2c6e438a03982961b00a0ff7b655cd9095f4950f3493abc1c774c7ec59)
```

8. ユーザーアカウントに関連付けされているSPNを確認する為にsetspnコマンドを実行します。

```
setspn -L [ユーザー名]
```

コマンド実行例：

```
setspn -L mfa_user
次の項目に登録されている CN=mfa_user,OU=icewall02,DC=d0320,DC=lan:
HTTP/mfa.d0320.lan
```

9. ktpassコマンドで作成したKeytabファイル(C:\iw.keytab)をIceWallサーバーに転送します。

4. HPE IceWall MFA / HPE IceWall SSOサーバーでの手順

1. DNSクライアントの設定を行います。

コマンド例：

```
# vi /etc/resolv.conf
nameserver 172.16.x.x
```

※「172.16.x.x」には、ドメインサーバー等のDNSサーバーのIPアドレスを設定します
※「/etc/hosts」ファイルで複数の名前解決をする場合は、FQDNを先頭に記述する必要があります。
（例：172.16.x.x mfa.d0320.lan mfa）

2. IceWallモジュールをインストールします。

■ HPE IceWall MFAの場合

2-1. 作成したKeytabファイルを「/tmp」等に配置します。

2-2. HPE IceWall MFAの「導入ガイドfor統合Windows認証オプション」を参照の上、インストールおよび設定を行います。

JAASログイン構成ファイル（jaas.conf）の設定例は、以下のとおりです。

```
principal="HTTP/mfa.d0320.lan@D0320.LAN"
keyTab="/opt/icewall-mfa/mfa/config/plugin/iwa/krb5.keytab"
```

2-3. KeytabファイルをJAASログイン構成ファイルで設定したパスに移動します。

コマンド例：

```
# mv /tmp/iw.keytab /opt/icewall-mfa/mfa/config/plugin/iwa/krb5.keytab
```

2-4. Keytabファイルの権限を設定します。

コマンド例：

```
# chown tomcat:tomcat /opt/icewall-mfa/mfa/config/plugin/iwa/krb5.keytab
```

■ HPE IceWall SSOの場合

2-1. 作成したKeytabファイルを「/tmp」等に配置します。

2-2. HPE IceWall SSOの「導入ガイドDomain Gateway Option for UNIX」を参照の上、インストールおよび設定を行います。

Domain Gateway Option 設定ファイル（dgfw.conf）の設定例は、以下のとおりです。

```
SERVICE_NAME=HTTP@dgo.d0320.lan
```

2-3. Keytabファイルをデフォルトの読み込み先パスに移動します。

コマンド例：

```
# mv /tmp/iw.keytab /etc/krb5.keytab
```

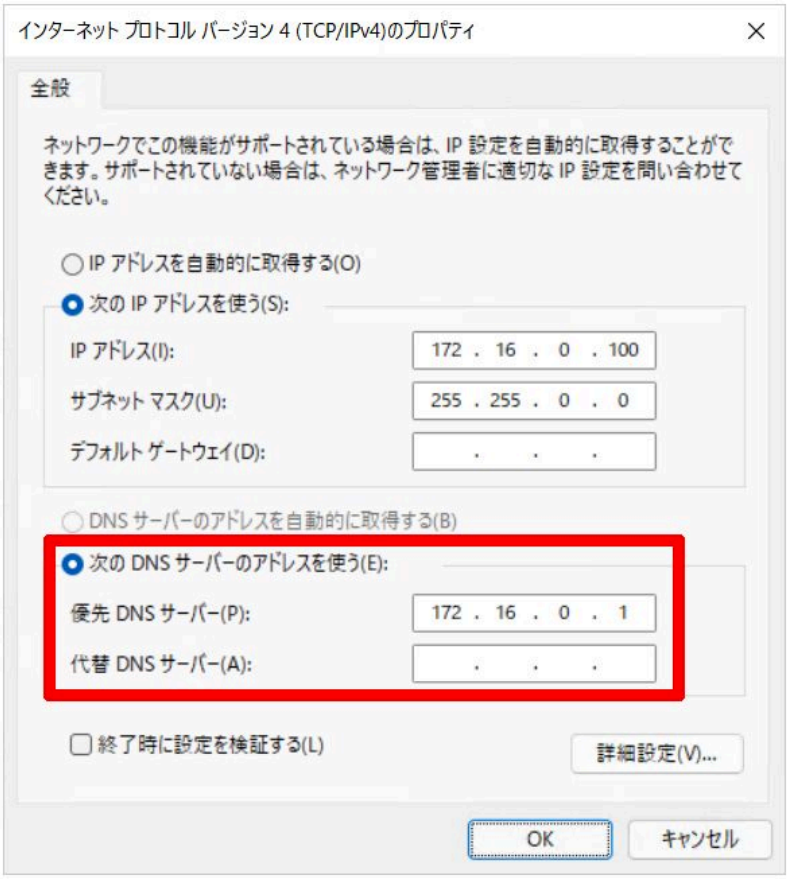
2-4. Keytabファイルの権限を設定します。

コマンド例：

```
# chown apache:apache /etc/krb5.keytab
```

5. クライアント端末での手順

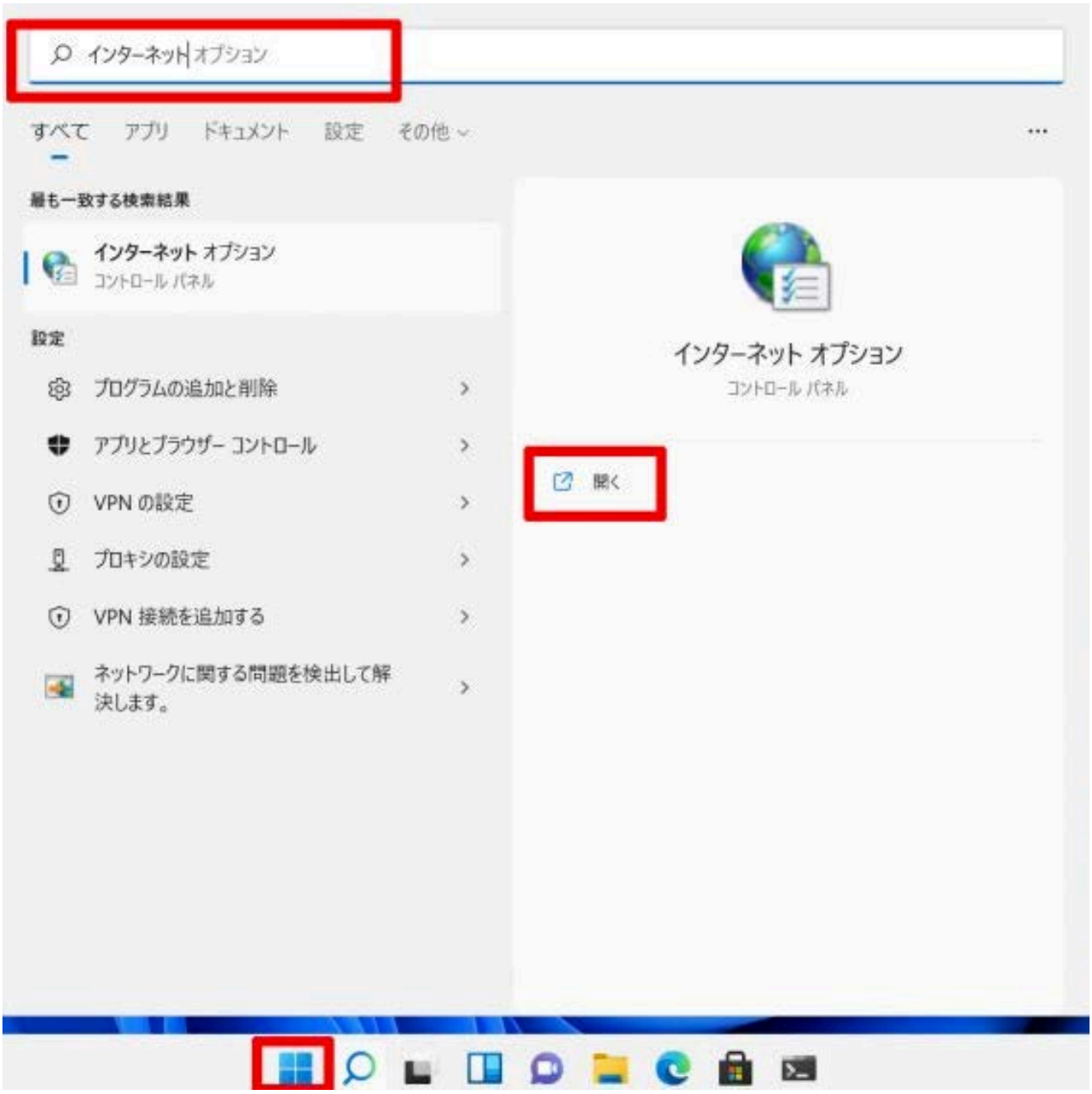
1. IceWallサーバー、およびMSADドメインサーバーの名前解決ができるようにDNSクライアント設定を行います。



2. クライアント端末をActive Directory Domain Servicesにドメイン参加させます。

3. デスクトップ画面左下のWindowsマークを左クリックし、検索の入力枠のところに「インターネットオプション」と入力します。

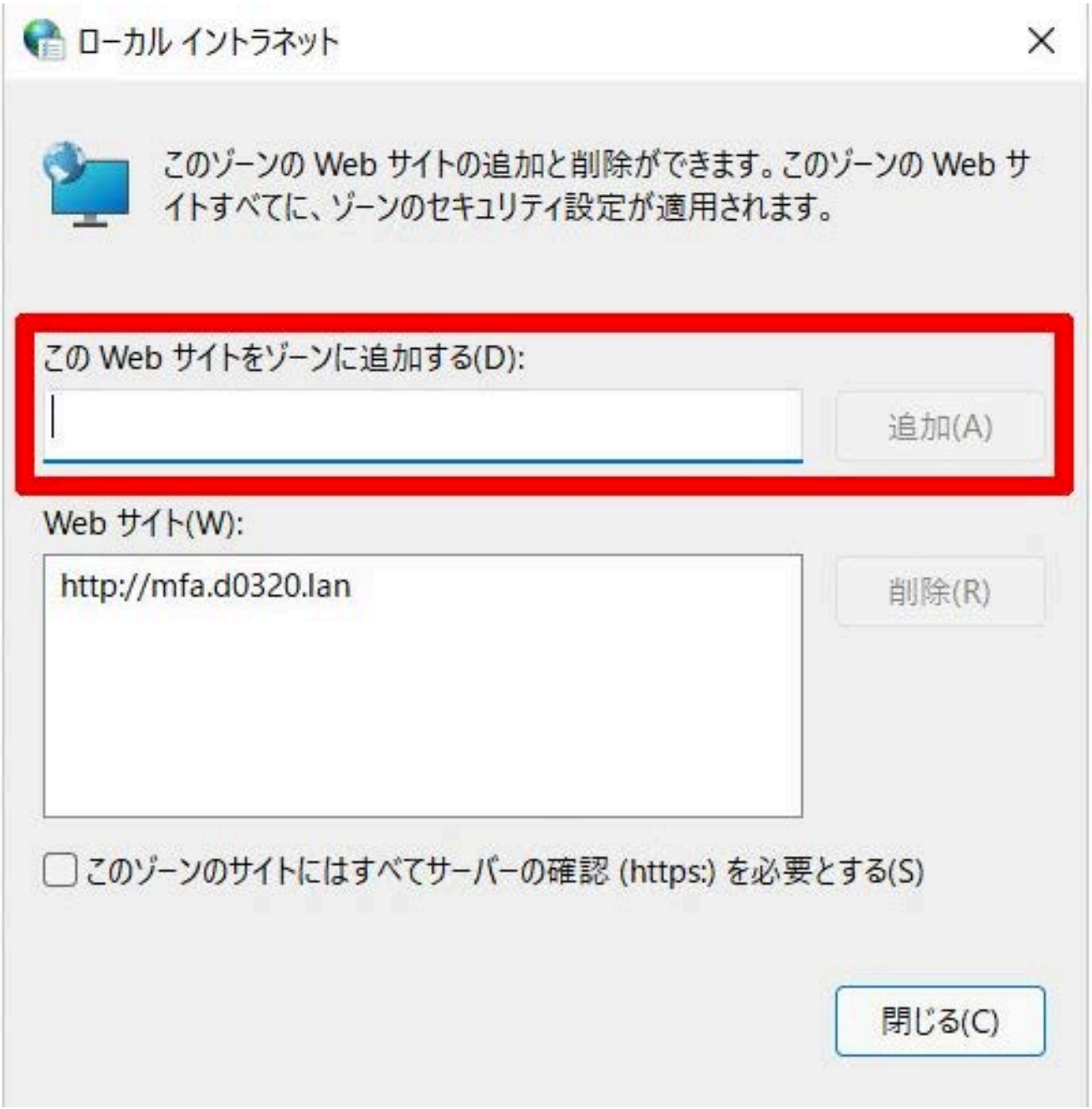
インターネット オプションの「開く」をクリックします。



4.「セキュリティ」タブから「ローカル イントラネット」を選択し、「サイト」をクリックします。

5. 「詳細設定」をクリックします。

6. 「このWebサイトをゾーンに追加する」に、IceWallサーバーのURLを入力し「追加」をクリックします。



7. ブラウザ設定をデフォルトから変更している場合は、以下の設定を変更します。

「セキュリティ」タブから「ローカル イントラネット」を選択し、「レベルのカスタマイズ」をクリックします。

「ユーザー認証」の「ログオン」から、「イントラネット ゾーンでのみ自動的にログオンする」を選択します。

8. ブラウザを起動し、IceWallにアクセスして統合Windows認証でログインを行います。

URL例:

■ HPE IceWall MFAの場合
http://mfa.d0320.lan/iwproxy/bk01/

■ HPE IceWall SSOの場合
http://dgo.d0320.lan/fw/dfw/bk01/

※ アクセス先URLは、IPアドレス形式での指定ではなく、FQDNで指定する必要があります。

6. 統合Windows認証が失敗する場合の確認点

■クライアント端末でのKerberosチケット取得の確認手順
クライアント端末でKerberosチケットが取得できているか確認する手順を説明します。

1. ブラウザを起動し、統合Windows認証を行います。

2. コマンドプロンプトを起動し「klist」コマンドを実行します。

klistコマンドで該当サーバーのKerberosチケットが表示されない場合は、Kerberosチケットの取得に失敗しています。

コマンド実行例：

```
klist
#2>クライアント: user01 @ D0320.LAN
サーバー: HTTP/mfa.d0320.lan @ D0320.LAN
Kerberos チケットの暗号化の種類: AES-256-CTS-HMAC-SHA1-96
チケットのフラグ 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
開始時刻: 6/30/2023 16:20:22 (ローカル)
終了時刻: 6/30/2023 18:18:03 (ローカル)
更新期限: 7/4/2023 12:03:03 (ローカル)
セッション キーの種類: AES-256-CTS-HMAC-SHA1-96
キャッシュ フラグ: 0
呼び出された Kdc: ad0323.d0320.lan
```

■Keytabファイルに含まれる鍵情報の確認手順
HPE IceWall MFA、HPE IceWall SSOサーバーに配置したKeytabファイルに含まれている鍵情報を確認する手順を説明します。

1.「ktutil」コマンドを使用するために「krb5-workstation」をインストールします。

コマンド実行例：

```
# yum install krb5-workstation
```

2. Keytabファイルを読み込み、鍵情報を表示します。

HPE IceWall MFAでのコマンド実行例：

```
# ktutil
ktutil:  read_kt /opt/icewall-mfa/mfa/config/plugin/iwa/krb5.keytab
ktutil:  list
slot KVNO Principal
```

```
---- ---- -------------------------------------------------------------------
   1    3           HTTP/mfa.d0320.lan@D0320.LAN
ktutil:  quit
```

HPE IceWall SSOでのコマンド実行例：

```
# ktutil
ktutil:  read_kt /etc/krb5.keytab
ktutil:  list
slot KVNO Principal
---- ---- -------------------------------------------------------------------
   1    3           HTTP/dgo.d0320.lan@D0320.LAN
ktutil:  quit
```

■その他の確認点

統合Windows認証でログインできない場合の他の問題として以下が考えられます。

- Red Hat Enterprise Linux 8以降でKerberos チケットの暗号化の種類を「RC4-HMAC」で設定している
- MSADドメインサーバー、IceWallサーバー、クライアントの時刻が大きくずれている
- REALMを大文字で統一していない
- DNSサーバーにCNAMEで登録している等の理由でFQDN形式になっていない
- KeytabファイルにWebサーバーのアクセス権がない

7. まとめ

事前にActive DirectoryでKeytabファイルを生成し、IceWallサーバーに設定することで統合Windows認証が可能となります。
クライアント端末がActive Directoryから取得するKerberosチケットは、IceWallサーバーのKeytabファイルから復号できることで、クライアント端末から正しいKerberosチケットを受け取ったことが確認できます。
Kerberosチケットを復号して取得したユーザーIDを利用して、IceWallは認証を行います。

また、IceWallサーバーに配置するKeytabファイルには、複数のKeytab情報が格納できます。
ドメイン信頼がない複数ADドメイン環境でも、適切に設定を行えば統合Windows認証が可能です。
設定方法については、以下の技術レポートをご参照下さい。

ご参考URL：
ドメイン信頼がない複数ADドメイン環境でのシングルサインオン

2023.9.8　新規掲載

執筆者　：日本ヒューレット・パッカード合同会社
HPE Services統括本部 IceWallビジネス推進部
神原 健太

技術レポート一覧へ →

お探しの情報は見つかりましたか？

検索のサポート

ご購入方法
製品サポート
営業へのお問い合わせ
お問い合わせ先一覧

ソフトウェア & ドライバー

標準保証確認

オペレーショナルサポート

教育とトレーニング

製品リサイクル

機器部品の妥当性確認

コミュニティ

HPE Japan ブログ

リソース

お客様事例

ご購入方法

オンラインストア

HPE Customer Center

Eメール登録

ドキュメントライブラリ

Resource Library

ビデオギャラリー

金融サービス

日本 (ja)