Appleテクニカルホワイトペーパー

OS XとActive Directoryとの統合に関するベストプラクティス

OS X Mountain Lion v10.8

目次

概要.....3

OS XとActive Directoryの統合方法.....4

エンタープライズにおける統合に関する課題.....7

導入戦略.....9

ホームディレクトリ.....10

結論.....11

付録A： 関連情報.....12

付録B： サードパーティ製アドオンソリューション.....13

概要

OS XではActive Directoryがサポートされているので、MacクライアントとMacサーバを既存のActive Directoryにスムーズに統合できます。また単一のディレクトリサービスインフラストラクチャでMacとWindowsの両方のクライアントをサポートする選択肢もあります。

Appleの内蔵ソリューション

大規模組織では、ユーザーの識別情報と、組織内の環境でのさまざまなサービスへのアクセスを管理できる必要があります。ユーザー、グループ、コンピューティングリソースを集中管理型ディレクトリサービスインフラストラクチャに統合することが一般的です。OS Xは、箱から出してすぐに、Active Directoryを含むさまざまなディレクトリサービステクノロジーとシームレスに統合できます。

集中管理型ディレクトリサービスのAppleによる実装はOpen Directoryと呼ばれます。Open DirectoryはOS Xの基盤に組み込まれ、OS XクライアントとOS X Serverの両方に対して、ディレクトリサービスとネットワーク認証サービスを提供します。Open Directoryは、LDAPやKerberos、SASLなどのオープン標準のプロトコルを使用します。

AppleはOpen Directoryによって独自のネイティブなディレクトリサービスを提供していますが、OS XはActive Directoryを含むさまざまなほかのプラットフォームへのアクセスもサポートしています。Active Directoryのインストール環境は組織によってすべて異なりますが、OS Xは最小限の作業でほとんどのプラットフォームと統合できます。

OS Xは、ディレクトリサービスを通じてActive Directoryを統合します。このサポートにより、ユーザーは別個のディレクトリやユーザーレコードを管理することなく、OS Xシステムを利用できます。異なるコンピュータ間でユーザーを移動した場合も、強力な認証やネットワークリソースへのパスワード保護されたアクセスのためのエンタープライズポリシーが維持されます。

Active Directoryと完全に統合されたOS Xは、次のような完成された管理環境を提供します。

- ユーザーは、Windowsパソコンへのアクセスに使用するのと同じ認証情報を使用して統合環境内の任意のMacにアクセスできます。
- ユーザーにActive Directoryのパスワードポリシーの遵守を義務付けできます。
- ユーザーは、Kerberosを介してActive Directoryにシングルサインオンでアクセスできます。

ユーザーは、Active Directoryで指定されたネットワークベースのホームフォルダへのアクセスを維持しながら、ローカルのホームディレクトリを使用できます。

さらにOS X ServerでもActive Directoryをサポートしています。OS X Serverも、クライアントシステムと同様に簡単に統合できます。実際、作業のプロセスは基本的に同じです。OS X Serverを統合することで、Windowsベースのシステムを使用しているユーザーは、それまでどおりActive Directoryで本人確認や認証を行いながら、ファイル共有や、wiki、ブログ、プロファイルマネージャなどのウェブサービスをはじめとするOS X Serverのサービスを利用できるようになります。OS X Serverでホ

ストされる安全なネットワークサービスも、OS X ServerとWindowsクライアントの両方のシングルサインオンをサポートします。

アドレスブックとメール

OS Xに含まれているアドレスブックは、連絡先情報を柔軟かつ便利に保存するアプリケーションです。アドレスブックは、LDAPなどの一般的なネットワークテクノロジーを使用して、サーバに連絡先情報を問い合わせます。これにより、MacはActive Directory内で共有されている連絡先情報を検索できます。ユーザーは、使用するMacがActive Directoryドメインに統合されていなくても、LDAPサーバ（Active Directoryドメインコントローラなど）を使用するように構成できます。

ユーザーは、アドレスブックでディレクトリサービスグループを選択し、連絡先を名前またはEメールアドレスで検索できます。連絡先が見つかったら、それらを自分のローカルアドレスブックにドラッグできます。この機能は、Active Directoryのレコードを変更する権限がないユーザーが、連絡先情報の追加や変更を行う場合に便利です。

アドレスブックは、メール、iChatなどのOS Xのアプリケーションと連係しています。そのため、これらのほかのアプリケーションでは、アドレスブックにあるすべての連絡先情報にアクセスできます。たとえばメールでは、ユーザーが連絡先の名前を入力すると、即座にActive Directoryにある連絡先情報が検索され、（Active DirectoryのユーザーアカウントにEメールアドレスが含まれている場合は）一致する連絡先をEメールアドレスのオートコンプリート機能で使用できます。

さらにMicrosoftの管理ツールを使用して、Active Directory内のユーザーアカウントに、インスタントメッセージングのユーザー名やブログアドレスなどの追加情報を登録することができます。この情報は、ほかの連絡先情報とともにアドレスブックに表示されます。

OS XとActive Directoryの統合方法

コンピュータアカウント
各Macシステムには、Active Directoryで固有のコンピュータアカウントが割り当てられています。システムのクローンを作成するか、NetBootをActive Directoryと統合すると、クローンとして作成したシステムに、同じコンピュータアカウントが割り当てられます。コンピュータアカウントを変更すると、そのアカウントを使用するすべてのシステムが認証できなくなるので、変更には十分に注意してください。ベストプラクティスは、イメージ処理後の手順でMacシステムをActive Directoryに接続することです。

はじめに

以下の簡単な手順によって、MacクライアントがDNSおよびActive Directoryを使用してActive Directoryドメインのジオメトリを判断し、最寄りのドメインコントローラを検出し、ドメイン内にコンピュータアカウントがまだ作成されていない場合は、選択されたコンピュータIDを使用して作成するように構成することができます。

Macクライアントで、アップルメニューからシステム環境設定の「ユーザとグループ」ペインを開きます。「ログインオプション」を選択し、「ネットワークアカウントサーバ」の下の「接続」（Macが別のディレクトリサービスにバインドされている場合は「編集」）をクリックします。展開されたシートで「ディレクトリユーティリティを開く」をクリックします。ディレクトリユーティリティアプリケーションが起動します。「サービス」が選択されていることを確認し、「Active Directory」をダブルクリックします。Active Directoryドメイン名を入力します。クライアントの「コンピュータ ID」はActive Directoryのコンピュータオブジェクト名で、デフォルトでMacのLocalHostNameが入力されます。これは、各組織のニーズに合わせて変更できます。

「詳細オプションを表示」の詳細表示三角形をクリックすることもできます。

- **ユーザ環境**
  - ログイン時にモバイルアカウントを作成
    ネットワーク非接続時にアクセスできるローカルアカウントを作成します。アカウントで最初にMacにログインした時に、確認ダイアログを表示するよう設定できます。
  - ローカル・ホームディレクトリを起動ディスクに設定
    ピュアネットワークのホームディレクトリを使用する場合は、このオプションを無効にします。このオプションはモバイルアカウントで必要です。
  - Active DirectoryからのUNCパスを使用してネットワークホームを設定
    このオプションを有効にすると、ユーザーアカウントのレコードでホームフォルダが指定されている場合は、MacがDockにその場所をマウントし、リンクを作成します。デフォルトのプロトコルはsmbですが、afpに設定することもできます。
  - デフォルトのユーザシェル
    UNIXシステムでコマンドラインシェルを必要とします。OS Xのデフォルトは「/usr/bin/bash」です。
- **マッピング**
  OS Xはデフォルトで、システム上のActive Directoryアカウントに固有のUIDとGIDを動的に生成します。通常はこれで十分ですが、UIDとGIDを管理する必要がある場合は、その値を含むActive Directoryにあるユーザーレコードの適切なフィールドにマッピングすることができます。
- **管理**
  - このドメインサーバを優先
    OS Xはデフォルトで、サイト情報とドメインコントローラの応答性を基に、使用に適切なドメインコントローラを判断します。このオプションは、この動作を変更します。
  - 管理を許可するユーザ
    このオプションを有効にすると、リスト表示されているActive Directoryグループのメンバーに、ローカルMacに対する管理権限が許可されます。デフォルトでは、ドメインの管理者とエンタープライズの管理者が表示されています。必要に応じてこれを変更できます。
  - フォレスト内の任意のドメインから認証
    OS Xはデフォルトで、すべてのドメインで認証を自動的に検索します。認証先のドメインとして特定のドメインを選択する場合は、この動作を無効にします。

「バインド」をクリックして、クライアントの接続を許可されているユーザーのユーザー名とパスワードを入力します。これは管理者ユーザーである必要はなく、任意のユーザーに権限を付与することができます。MacがActive Directoryにオブジェクトを作成する場合、ユーザーには、指定コンテナのすべての子オブジェクトの読み取りおよび作成権限が必要です。オブジェクトが事前に作成されている場合、ユーザーはActive Directoryユーザーとコンピュータで指定されたアカウントに接続可能なグループのメンバーである必要があります。

Windows Serverのバージョン
MacシステムのActive Directoryへの接続は、Windows Server 2000、2003、2003 R2、2008、2008 R2で検証済みです。ドメインはOS Xクライアントの機能を変更することなく、ネイティブモードまたは混合モードで使用できます。

コマンドラインによる構成

ディレクトリユーティリティの機能には、コマンドラインインターフェイスから`dsconfigad`コマンドを使用してもアクセスできます。たとえば、次のコマンドを実行すると、システムがActive Directoryに接続されます。

```
dsconfigad -preferred ads01.example.com -a COMPUTERNAME
–domain example.com -u administrator -p "password"
```

システムをドメインにバインドした後は、次のように`dsconfigad`を使用して、Directory Accessの管理オプションを設定できます。

```
dsconfigad -alldomains enable -groups domain
admins@example.com, enterprise admins@example.com
```

スクリプトで`dsconfigad`を使用する際は、ドメインへの接続用パスワードをクリアテキストで指定する必要があります。通常、ほかの権利権限を持たないActive Directoryユーザに、クライアントをドメインに接続する権限を委任します。このユーザー名とパスワードの組み合わせは、スクリプト内に保存されます。この情報がディスクに常駐しないよう、バインドの完了後にスクリプトを自動的に確実に削除することが一般的です。

構成プロファイルのバインド

構成プロファイルのディレクトリペイロードには、MacがActive Directoryに接続するよう設定できる機能があります。このオプションでも、すべてのMacコンピュータのActive Directoryへの接続を自動化できます。

詳細なディレクトリサービス情報

まずディレクトリサービスのデバッグログを有効にします。

```
odutil set log debug
```

これで、Active Directoryへの接続を試みる際に、「/var/log/opendirectoryd.log」でログを参照して処理状況を確認できます。

ログイン後に同じコマンドを使用すると、デバッグログが無効になります。

```
odutil set log default
```

また、ドメインへの接続を試みるクライアントのパケットトレースを調査すると役に立つことがあります。トラフィックは、デフォルトで暗号化されています。暗号化を無効にするには、次のコマンドを実行します。

```
/usr/sbin/dsconfigad -packetencrypt disable
```

暗号化を再度有効にするには、次のコマンドを実行します。

```
/usr/sbin/dsconfigad -packetencrypt allow
```

次の各ポートでは、異なる種類のデータのトラフィックをキャプチャすることができます。

UDP 53　　- DNS

TCP 88　　- Kerberos

TCP 389　　- LDAP

TCP/UDP 464　- Kerberosのパスワード変更（KPasswd）

TCP 3268　　- グローバルカタログ（LDAP）

たとえば、内蔵のEthernet接続を経由するトラフィックを「capture.out」というファイルにキャプチャするには、次の`tcpdump`構文を使用します。

```
tcpdump –K –i en0 –s 0 –w capture.out port 88 or port 464
or port 53 or port 389 or port 3268
```

Wiresharkはグラフィカルなネットワークプロトコルアナライザで、OS Xバージョンも使用できます。

エンタープライズにおける統合に関する課題

サイトの認識

Open Directoryは、Active Directory内に保存されたDNSサービスレコードとサイト情報を使用して、最適なドメインコントローラ（通常、マルチサイトネットワーク内の近接するドメインコントローラ）を探して通信を行うことができます。Active Directoryに統合されたMacは、Active Directoryに対するサイト情報の問い合わせや、サイトのドメインコントローラへのポーリングによって、最寄りのドメインコントローラだけでなく、最も速く応答するドメインコントローラを見つけることができます。Open Directoryは、この情報を使用してドメインコントローラとグローバルカタログを選択し、ネットワークが変更されるか、ドメインコントローラが応答しなくなるまで、それらと通信を行います。

DNSサービス

Active DirectoryがDNSサービスのレコード（SRV）に依存しているため、Macクライアントはネットワーク上のすべてのWindowsクライアントと同じDNSサーバを使用する必要があります。Macが適切なDNSレコードを読み取れるかは、`dig`コマンドを使用してテストします。次の例の`example.com`を対象のActive DirectoryドメインのDNSと置き換えてください。

```
dig -t SRV _ldap._tcp.example.com
```

これにより、ドメインコントローラのIPアドレスが返されます。そうでない場合、Macシステムが使用するDNSサーバがActive Directoryクライアントと同じでないか、DNSサーバの設定が誤っています。

OS Xクライアントは、Active Directoryによってホストされるフォワード (A) レコードとリバース (PTR) レコードの両方のDNSレコードの動的なアップデートを試みます。

パスワード

OS X はKerberosを使用するので、本来的にActive Directoryパスワードポリシーをサポートし、クライアントシステムのパスワードの長さと複雑さを制限します。Macユーザーは、OS Xの「ユーザとグループ」環境設定ペインを使用してパスワードを変更することもできます。

パスワードの有効期限切までの数日間には、パスワードの有効期限がまもなく切れることを示す通知が表示されます。これによりユーザーは、Macクライアントの「ユーザとグループ」環境設定ペインを使用してActive Directoryのパスワードを変更することができ、それによって有効期限タイマーがリセットされます。パスワードの有効期限切れまで24時間を切った場合、ユーザーはパスワードを変更するまでログインを完了できません。

MacシステムをActive Directoryにバインドすると、コンピュータアカウントのパスワードが設定されてシステムキーチェーンに保存されます。このコンピュータアカウントのパスワードは、クライアントによって自動的に変更されます。デフォルトは14日ごとですが、`dsconfigad`コマンドラインツールを使用して、個別のポリシーが要求する日数に設定することができます。

シングルサインオン

AppleとMicrosoftはいずれもKerberosをサポートして、安全なシングルサインオン環境を提供します。Active Directory環境に統合されたOS Xは、すべての認証にKerberosのみを使用します。NTLMv1とNTLMv2の両方を含む、MicrosoftのNT LAN Manager（NTLM）スイートのプロトコルを必要に応じてネットワークで使用できないようにすることができます。この場合も、MacコンピュータやActive Directory環境でOS X Serverによって提供されるサービスに影響はありません。

ユーザーがActive Directoryアカウントを使用してMacにログインすると、Active Directoryドメインコントローラが自動的にKerberos Ticket Granting Ticket（TGT）を発行します。その後、ユーザーがKerberos認証をサポートするサービスをドメイン上で使用しようとすると、TGTによってサービス用のチケットが生成されるので、ユーザーは再度認証を行う必要がありません。

MacでKerberos管理ツールを使用すると、現在ユーザーに対して発行されているチケットを表示することができます。これには、コマンドラインからklistを実行して現在のチケットを表示するか、「/システム/ライブラリ/CoreServices/チケットビューア.app」にある、Kerberosチケットの表示や操作を行えるグラフィカルなチケットビューアユーティリティを使用します。

ネームスペースのサポート

OS Xでは、Active Directoryフォレスト内の異なるドメインに存在する複数のユーザーに同じショートネーム（またはロングネーム）を指定できるオプションが用意されています。`dsconfigad`コマンドラインツールを使用してネームスペースのサポートを有効にすると、1つのドメイン内のユーザーに対して、別のドメイン内のユーザーと同じショートネームを指定できます。これらのユーザーはいずれも、Windowsパソコンにログインする場合と同様に、ドメイン名の後にショートネームを使用して（ドメイン名\ショートネーム）指定します。

署名付き接続

Open Directoryは、Active Directoryとの通信に使用するLDAP接続に署名を付け、暗号化することができます。OS Xが署名付きServer Message Block（SMB）をサポートしているため、Macクライアントに対応するためにサイトのセキュリティポリシーを緩和する必要はありません。さらに署名付きおよび暗号化LDAP接続を使用すると、LDAP over SSL（Secure Sockets Layer）を使用する必要がなくなります。サイトでSSL接続が必要な場合は、次のコマンドによってOpen Directoryを設定してSSLを使用することができます。

```
/usr/sbin/dsconfigad -packetencrypt ssl
```

SSL暗号化が適切に機能するためには、ドメインコントローラで使用される証明書が信頼されている必要があります。ドメインコントローラの証明書が、一般に認知された証明書でないために、デフォルトでルートがインストールされない場合、システムキーチェーンにルート証明書をインストールして信頼する必要があります。ルート証明書を手動でインストールするには、構成プロファイルの証明書ペイロードを使って読み込むか、「/アプリケーション/ユーティリティ」にあるキーチェーンアクセスを使用するか、次の`security`コマンドを使用します。

```
/usr/bin/security add-trusted-cert -d -p basic -k /Library/
Keychains/System.keychain <証明書ファイルへのパス>
```

証明書の配備

802.1X、VPN、S/MIMEなど、セキュリティ保護されたテクノロジーで使用するクライアント側の証明書の配備がより一般的となっています。OS Xには、Microsoft認証局からクライアント証明書を取得する機能があります。OS X 10.8 Mountain LionではDCE/RPCプロトコルを使用して、ウェブ登録の必要性を回避しています。プロファイルマネージャのウェブUIは、構成プロファイルでの証明書要求ペイロードの定義を完全にサポートします。これを、同じ構成プロファイルでほかのペイロードと組み合わせて、証明書ベースのテクノロジー配備を簡素化することもできます。

たとえば、1つの構成プロファイルに、Active Directoryにバインドするディレクトリペイロード、Microsoft認証局のルート証明書を含む証明書ペイロード（必要な信頼確立のため）、クライアント証明書要求のためのAD証明書ペイロード、さらに802.1Xで認証されたネットワーク（EAP-TLSなど）のネットワークインターフェイスを構成するためのネットワークペイロードを含めることができます。この構成プロファイルの配備方法には、手動、スクリプトを使う、モバイルデバイス管理登録の一部として行う、またはクライアント管理ソリューションを使って行う方法があります。必要に応じて、その他のペイロードも構成できます。

導入戦略

ポリシー管理

OS Xは、Macユーザーエクスペリエンスのすべての側面について制限や制御ができる完全な管理対象クライアント環境を提供します。WindowsのグループポリシーがActive Directoryに実装されている方法とは技術的に異なりますが、非常に近い効果が得られます。完全に統合された場合、ユーザーによるあらゆるOS Xコンポーネントへのアクセスを制限できます。またユーザー環境（OS X機能やサードパーティ製のアプリケーションを含む）のプリセットや完全な制御ができるようになります。

組織が要求する管理レベルや、使用する統合レベルに応じて、Macコンピュータのクライアント管理は、次のような複数の実装方法から選択できます。

構成プロファイル
WindowsとOS Xでは環境設定の処理方法が異なるため、MacはActive Directoryでグループポリシーオブジェクト（GPO）を使用することができません。代わりに、構成プロファイルを使用して、Appleデバイスにポリシーデータを配布できます。

クライアントとアカウントの設定、ポリシーデータと証明書の配備はすべて構成プロファイルを使って行えます。これらのプロファイルは、配備用イメージの一部として手動で配布できます。または、デバイスをモバイルデバイス管理ソリューションに登録して管理することもできます。

クライアントでは引き続きActive Directoryでユーザー認証を行い、Open Directoryは管理された環境設定のみを提供します。

何もしない

Open Directoryによって、すべてのパスワードポリシーを含め、Active Directoryへの認証が自動的に有効になります。また、Active Directory内に含まれたMacユーザー用のネットワークホームディレクトリも設定できます。クライアント管理はできませんが、Macクライアント上で標準ユーザーを非管理者ユーザーとして設定できる完全な機能環境が提供されます。これにより、非管理者ユーザーによるシステム設定の変更を防止できます。

プロファイルマネージャを使用する

プロファイルマネージャを使用すると、管理者はディレクトリサービスの外側でポリシーを設定することができます。この方法では、ユーザーがサービス設定を許可するか、クライアントをウェブインターフェイス経由でプロファイルマネージャサーバに

接続します。その後、Active Directoryに対して認証を行い、ポリシーと設定はあらかじめMacクライアント上にローカルに配置します。Macがプロファイルサーバにバインドされている場合、ポリシーを変更するとプッシュ型の通知が実行されます。これにより、Macがプロファイルマネージャサービスにコンタクトして、ポリシーと設定が更新されます。

サードパーティ製の管理ソリューションを使用する

Absolute、AirWatch、JAMF Software、MobileIronなどのモバイルデバイス管理およびクライアント管理ベンダーを使用すると、プロファイルマネージャと同じように構成プロファイルを使ってOS Xポリシーデータを管理できます。これらのソリューションでは、クライアントがディレクトリサービスにアクセスすることなく、クライアントポリシーをアップデートできます。

サードパーティ製のActive Directoryソリューションを使用する

Beyond Trust、Centrify、Thursby、Questが提供する製品を使用すると、IT部門はスキーマを拡張せずにポリシーデータをActive Directoryドメインに保存できます。これらのソリューションでは一般的に、Windowsクライアントと同じように、Active Directoryでグループポリシーオブジェクトとしてポリシーを設定できます。各ソリューションは、OS Xのネイティブ Active Directory機能を、各サードパーティ製のクライアント側ディレクトリサービスプラグインに置き換えます。

ホームディレクトリ

ポリシー管理にどの方法を採用するかとは関係なく、Active Directoryのユーザーレコードで指定されたネットワークホームディレクトリへのアクセスに加え、ユーザーにローカルホームを設定できます。OS Xは、ログイン時にその共有を自動的にマウントするよう設定できます。

分散ファイルシステム（DFS）
OS Xはまた、ホームディレクトリおよびDFSによるファイル共有のマウントもサポートします。汎用名前付け規則（UNC）パスはSMBパスと同じですが、名前がDFSネームスペースでホストされている場合、共有が正しくマウントされます。

AFPネットワークホーム
ホームディレクトリに、afp:// URLを使用することもできます。Active Directoryでは、URLは標準UNCのままですが、Macでは、クライアントによるSMBパスからAFPパスへの変換を有効にすることができます。

ローカル

Directory ServicesでのAppleによるActive Directoryのデフォルト設定では、Active Directoryのユーザーレコードは変更されず、ユーザーのホームがローカルシステムにとどまります。ユーザーレコードでネットワークホームが定義されている場合、ユーザーのログイン時にその共有がデスクトップ上にマウントされます。

ネットワーク

MacユーザーのActive Directoryレコード内にネットワークホームディレクトリを定義するには、Windowsユーザーに対するのと同様、「\\server\share\user」の形式でURLを使用します。Mac上のActive Directory構成による解釈時に、サーバ名にActive Directoryのドメインが追加され、「smb://server.ad.domain/share/user」の形式のURLが作成されます。

注：ユーザーのドメインがユーザーのホームフォルダのドメイン名と異なる場合、URLでサーバの完全修飾名の使用が必要になることがあります。
この場合、「//server/share/user」の代わりに、「//server.userad.domain/share/home」を使用します。Macユーザーにとって

使いやすい名前付け規則を使用しても、ネットワーク上のWindowsシステムには影響はありません。

Macユーザーのネットワークホームは、AFPまたはSMBを使用してOS X Server上とWindowsサーバ上のいずれにもホストできます。さらに、OS X Server上でOS Xクライアントと Windowsクライアントの両方をホストし、AFP経由でMacサービスを、SMB経由でWindowsサービスを提供することもできます。

結論

OS XではActive Directoryがサポートされているので、MacクライアントとMacサーバを既存のActive Directoryにスムーズに統合できます。また単一のディレクトリサービスインフラストラクチャでMacとWindowsの両方のクライアントをサポートする選択肢もあります。

OS XとWindowsでは、環境設定の処理方法が異なります。OS Xは構成プロファイルを使って配布されたxmlデータを使用して構成、ポリシー、証明書をアップデートし、Active Directoryのグループポリシーオブジェクトと同じ役割を果たします。

本書で説明したベストプラクティスをはじめ、OS XシステムとActive Directoryとの統合に関する詳細については、Appleの営業担当者またはApple製品取扱店にお問い合わせください。

付録A：
関連情報

詳しくは、以下のAppleサポート記事を参照してください。

- **Mac OS X：Active Directory - バインド時の名前に関する考慮事項**
  http://support.apple.com/kb/ts1532?viewlocale=ja_JP
- **OS X Server：Active Directoryクライアントでの SSLを使ったパケット暗号化**
  http://support.apple.com/kb/HT4730?viewlocale=ja_JP
- **DCE／RPCおよびActive Directory証明書プロファイルのペイロードを使ってMicrosoft認証局からの証明書を要求する方法**
  http://support.apple.com/kb/HT5357?viewlocale=ja_JP
- **ADCertificatePayloadPluginを使ってMicrosoft認証局からの証明書を要求する方法**
  http://support.apple.com/kb/HT4784?viewlocale=ja_JP

付録B：
サードパーティ製アドオンソリューション

導入環境に分散ファイルシステム（DFS）共有またはグループポリシーオブジェクト（GPO）が必要な場合、Appleソリューションの機能を拡張する以下のようなサードパーティ製品を使用できます。

- **GroupLogic ExtremeZ-IP** www.grouplogic.com
  このWindows対応のAppleファイリングプロトコル（AFP）サーバを使用すると、Macクライアントがネイティブなファイル共有プロトコルであるAFPを使ってWindowsサーバ上のファイルにアクセスできます。
- **Centrify DirectControl** www.centrify.com
  このActive Directoryプラグインを使用すると、OS Xはスキーマ変更を適用せずにActive Directory GPOを使用することができます。
- **PowerBroker Identity Services Enterprise Edition**
  www.beyondtrust.com
  このActive Directoryプラグインを使用すると、OS Xはスキーマ変更を適用せずにActive Directory GPOを使用することができます。
- **Thursby ADmitMac** www.thursby.com
  ディレクトリサービスActive Directoryプラグインであり SMBクライアントとして、DFS共有をサポートします。
- **Objective Development Sharity** www.obdev.at/products/sharity
  このSMBクライアントはDFS共有をサポートします。
- **Quest Authentication Services** www.quest.com
  このActive Directoryプラグインを使用すると、OS Xはスキーマ変更を適用せずにActive Directory GPOを使用することができます。

2013年1月15日