

Windows/Linux混合ネットワーク でディレクトリ サービス、認証、 セキュリティを管理する方法

Likewise Software
2006年6月

Manny Vellon 著
Vice President of Product Development
Likewise Software

ディレクトリ サービスは、コンピュータ ネットワークの適切な保護と効率的な管理を保証する上で重要な役割を果たします。Microsoft Windows ネットワーク内で実行している Linux マシンと Active Directory は相互運用できますが、構成は、特に Linux の専門知識がない管理者にとっては、複雑です。この白書では、ディレクトリ サービスを使用する場合の基本を説明し、Windows システムと Linux システム間の認証管理に使用するツールやプロトコルを解説し、これらのすべてを容易にしてくれる新しいソフトウェア ソリューションの概要を紹介します。

目次

はじめに.....	3
定義されているディレクトリ サービス.....	3
認証プロトコル.....	3
シングル サインオンの利点	4
シングル サインオンと Active Directory	5
セキュアな認証.....	5
セキュリティ プロトコル交渉.....	6
Samba が Windows/Linux の相互運用性を改善	9
混合ネットワークでの構成を容易にする新しいツール	9
Windows/Linux 統合ツールの利点.....	10
例：シングル サインオンを実行するように Apache Web サーバーを構成する	11
結論.....	11

→ はじめに

ディレクトリ サービスは、コンピュータ ネットワークの適切な保護と効率的な管理を保証する上で重要な役割を果たすことができます。あなたがMicrosoft® Windows®システムの管理者であるなら、Microsoft Active Directory®のサービス、そしてActive Directoryを使用することの利点と課題についてはよくおわかりでしょう。Microsoftシステム以外のシステムをどのようにディレクトリ サービスという絵にはめ込むかを考慮しないと、Active Directoryを適切に構成する作業が非常に難しくなる場合があります。Linux®マシンとActive Directoryは相互運用できますが、構成は、特にLinuxの専門知識がない管理者にとっては、複雑です。それでも、LinuxサーバーをActive Directoryに参加させることには、次のような重要な利点があります。

- Linuxサーバーとワークステーションの集中管理
- ファイル、印刷、Webを含む一般的なLinuxサービスの認証
- Linuxサーバーとワークステーションの拡大制御

この白書では、ディレクトリ サービスを使用する場合の基本から、WindowsシステムとLinuxシステム間の認証管理に使用するツール/プロトコル、Linuxマシンでシングル サインオンを活用できるようにするツール、そして最後にこれらのすべてを容易にしてくれる新しいソフトウェア ソリューションまでを解説しています。

→ 定義されているディレクトリ サービス

Microsoft Active Directoryやその他のディレクトリ サービス (Red Hat® Netscape® Directory Services、Novell® eDirectory™、OpenLDAPなど) は、単純な情報のディレクトリです。このため、どのようなものに関する情報も格納することができます。ただし、通常はユーザー、コンピュータ、その他のネットワーク リソースに関する情報を格納します。ディレクトリ サービスは、主に「認証」と「認可」に使用されます。

「認証」は、「プリンシパル」を識別するプロセスです。通常、プリンシパルは、ユーザーまたはコンピュータのことです。「認可」は、プリンシパルが「リソース」へのアクセス権を持っているかどうかを検証します。「リソース」は、ファイル、プリンタ、マシンなど、アクセス制限の概念をサポートするすべてのものです。たとえばスプレッドシートを、「会計部門」のみがアクセスできるものとして識別されるようにすることができます。この例では、ユーザーにこのファイルへのアクセス認可が出される前に、ディレクトリ サービスが使用されて、「資格情報」(名前とパスワード)が適切であるかどうかのチェックとユーザーが会計部門のメンバであるかどうかの検査が行われます。

認証プロトコル

現代のディレクトリ サービスの実装は、通常、情報の格納方法と検索方法を定義する軽量ディレクトリ アクセス プロトコル(LDAP)です。ディレクトリ サービスに認証と認可の情報を含めることはできますが、LDAP自体はセキュアな認証と認可を提供するには不十分です。Active Directoryなどのディレクトリ サービスは、たとえばKerberos™のような追加の通信プロトコルを実装することで、セキュアさを提供しています。

LDAPと認証プロトコルとを結合することで、Active Directoryや類似サービスは、ユーザーがリソースへの適切なアクセス認可を持っていることを保証して、ユーザーをセキュアに認証します。

Kerberosは、MITが作成した認証プロトコルで、プリンシパルが適切な資格情報（通常、名前とパスワード）を持っていることを、コンピュータがセキュアに検証できるようにします。「セキュアに」とは、認証情報が盗めない、または傍受された場合でも侵害できないことを意味します。

他にも認証プロトコルはありますが（たとえば、昔のMicrosoftオペレーティング システムで使用されていたNTLM）、現代のほとんどのオペレーティング システムではKerberosが使用されています。ディレクトリ/認可/認証サーバーが、複数のオペレーティング システムとその複数のバージョンをサポートするために複数のプロトコルを実装している場合もあります。Active Directoryは、KerberosとNTLMの両方をサポートします。LDAPと認証プロトコルとを結合することで、Active Directoryや類似サービスは、ユーザーがリソースへの適切なアクセス認可を持っていることを保証して、ユーザーをセキュアに認証します。

図1では、ユーザーが共有フォルダにアクセスしようとしたときに、ファイル サーバーが、ユーザーが適切な資格情報とセキュリティ特権を持っているかどうかをディレクトリサーバーで調べています。

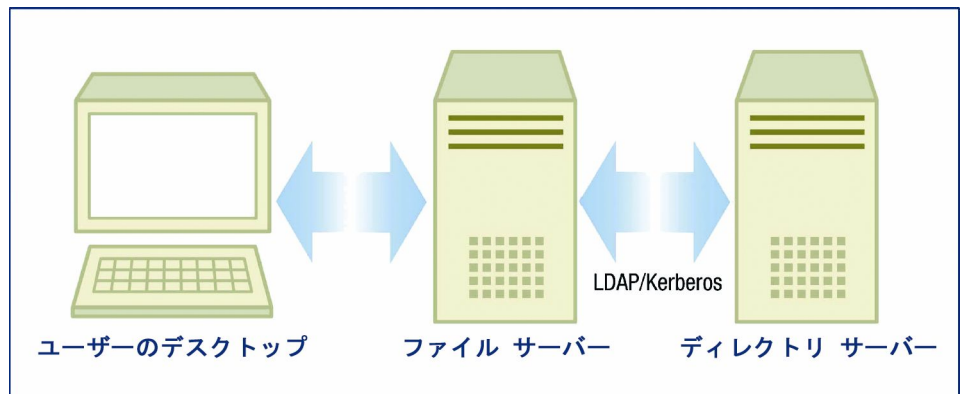


図1 - 認証と認可にディレクトリ サービスを使用する

⇒ シングル サインオンの利点

ディレクトリ サービスは、基本的なセキュリティを提供することにとどまらず、シングル サインオンという概念により、ユーザーやネットワーク管理者にとって認証と認可が煩わしくなくなるようにする手助けもします。ディレクトリ サービスが幅広く利用できるようになる以前、ユーザーは、さまざまなリソースにアクセスするときには、さまざまなユーザー名とパスワードを指定する（そして覚える！）必要がありました。ユーザー情報の管理（パスワードの変更やユーザーの削除）は、独自の認証データベースを保守しているリソース上（ファイル サーバー、プリント サーバーなど）でそれぞれ行う必要がありました。ディレクトリ サービスとシングル サインオンを使用すれば、ディレクトリ サービスと対話するすべてのネットワーク リソース全体でユーザー認証が実施されるようにすることができます。

シングル サインオンには、「単一のユーザー名/パスワード」以上の意味があります。シングル サインオンでは、ユーザーがユーザー名とパスワードを1回提示するだけで、認証を必要とするその他のリソースは再度資格情報を要求せずに、提示された資格情報を再利用することができます。

Linuxベースのシステムは、Kerberosをサポートします。多少手を加えることで、シングル サインオンもサポートするようにできます。

シングル サインオンとActive Directory

Active Directoryを使用する場合、シングル サインオンはマシンを特定の認証「ドメイン」に参加させることで実現できます（ドメインはKerberosの「レルム」に相当）。ドメインメンバシップは、ドメイン認証サーバーとメンバ サーバーとの間に信頼関係を確立するので、認証を容易にします。

ネットワークにMicrosoft WindowsマシンとLinuxマシンの両方が含まれ、認証にActive Directoryを使用するようにセットアップされている場合、システム管理者は、LinuxマシンもActive Directoryに参加させることの利点を考慮すべきでしょう。Linuxベースのシステムは、Kerberosをサポートします。多少手を加えることで、シングル サインオンもサポートするようにできます。

マシンをActive Directoryドメインに参加させると、ユーザーがActive Directory資格情報を使用してログオンしたときに、この資格情報を他のネットワーク リソースに対するユーザー認証にも再利用することができます。ただし、Active Directory/Kerberosシングル サインオンは、単純にユーザー名とパスワードをキャッシュし、必要なときにこれを自動的に提供するだけでは実現されません。そこで、ユーザーが最初に認証されるときに、後で認証を必要とする他のサービスに提供できるセキュリティ「トークン」が作成されるのです。Kerberosと認証プロトコルの設計に関する詳細は、MIT Kerberos Webページ（<http://web.mit.edu/kerberos/www>）を参照してください。

セキュアな認証

マシンがドメインに参加すると、マシンと認証サーバーとの間で、以降のセキュアな認証関連通信に使用できる暗号鍵が交換されます。この暗号鍵を使用する点が、認証プロトコルとセキュリティ プロトコルとの密接な関係の特徴です（認証プロトコルは本質的にセキュアでなければ役に立ちません）。ネットワークのセキュリティを保証するためには、デスクトップ、サーバー、そしてディレクトリ サービスとの間の通信は十二分に注意して実行されなければなりません。たとえばパスワードが暗号化されていない形式（「クリア テキスト」）で通信されると、悪意のあるユーザーは、たとえばEtherealのようなネットワーク「スニファ」（盗聴）プログラムを使用して簡単にパスワードを盗むことができます。

セキュリティ プロトコルも、「なりすまし攻撃」、「中間者攻撃」、「再生攻撃」のようなさらに高度なセキュリティ攻撃を防ぐように設計されている必要があります。なりすまし攻撃は、偽のネットワーク リソースをセットアップし、ユーザーがこのリソースにアクセスするようにし向けてパスワードを盗みます。中間者攻撃は、ネットワークのノード間（たとえば、コンピュータAとBの間）に入り込み、両方のノードになりすまし（Aに対してはBになりすまし、Bに対してはAになりすまし）、ノード間のトラフィックを分析することでセキュリティ情報を盗みます。再生攻撃は、盗聴、なりすましなどの手段で盗んだ情報（たとえば仮パスワード）を使用し、古い資格情報を「リサイクル」する試みで、盗んだネットワーク トラフィックを再生します。Kerberosは、この種のセキュリティ攻撃を防ぐために、「両方」のプリンシパル（たとえば、ユーザーとユーザーがアクセスしようとしているリソース）を認証する「相互認証」を提供します。

このような攻撃の脅威を削減するために、さまざまなセキュアな通信プロトコルが設計されてきました。SSL（Secure Socket Layer）プロトコル（多くのセキュアなWebサイトで使用され、<https>を使用することで識別可能）は、セキュアな通信を提供するために暗号化と認証を使用します。NTLMとKerberosでは、認証情報を暗号化されていないチャンネル

を介して通信できますが、それでも従来のセキュリティの脅威に対する保護策は講じられています。

セキュリティ プロトコル交渉

現代のオペレーティング システムは複数のセキュリティ プロトコルをサポートしなければならないため、さまざまな外部サービスと通信することができます。しかしながら、複数のオペレーティング システムを採用するデータセンターの場合、適切に対話するためのプロトコルを取得し、整合性のあるセキュリティ インフラストラクチャを提供するのが難しいということが判明する場合があります。

異なるマシン上で実行している2つのソフトウェア コンポーネント間にセキュアで認証された通信チャネルを確立したいときに、まず初めにしなければならないのは、使用するプロトコルを決めることです。この問題の対処法はいくつかあります。問題の解決には、使用している最上位レベルのプロトコル（たとえば、*http*、*ftp*、または*ssh*）が関係します。図2は、ユーザーがhttpを使用するセキュアなWebサイトにアクセスしたときに起きることを図示しています。

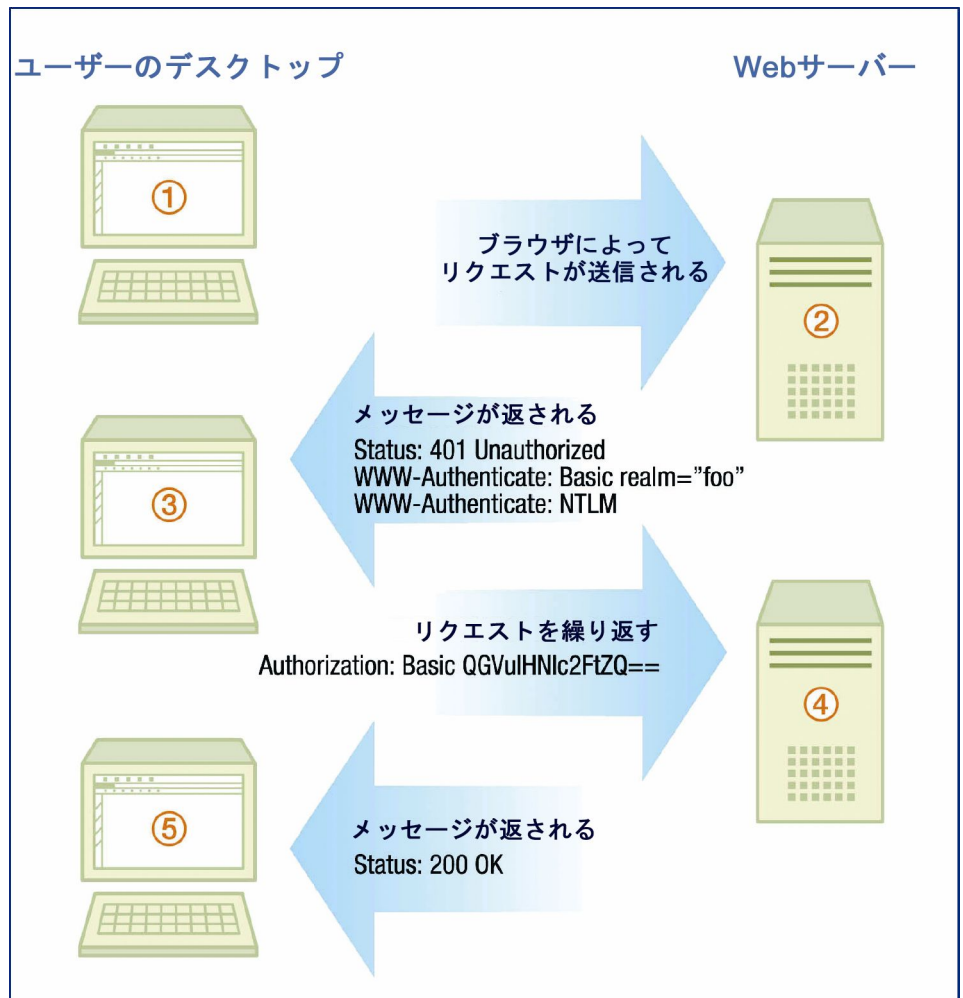


図2 - HTTP認証

図では、ブラウザとWebサーバーとの間で、次の対話が発生します。

- ブラウザがWebページ リクエストを開始します。これは、ユーザーがアクセスしたURLに関連付けられているWebサーバーに送信されるHTTP GETメッセージとなります。
- Webサーバーは、該当URLは認証されたユーザーのみが利用可能であると判断し、401ステータス コードで応答します。このコードは、ブラウザに、該当サイトは認証なしではアクセスできないことを伝えます。WWW-Authenticateヘッダは、ブラウザにWebサーバーが「Basic」とNTLMの両方の認証プロトコルをサポートすることを伝えます。
- ブラウザはHTTP GET操作を繰り返すことで応答しますが、Basic認証をサポートするヘッダ（「Authorization : Basic...」）を追加します。ブラウザは、ブラウザとWebサーバーの両方がサポートする認証体系の中で最もセキュアなものを選択します。この例では、BasicはNTLMよりもセキュアではありませんが、ブラウザがNTLMをサポートしないので、Basicを選択しています。

この交渉はHTTPで明示的に処理できますが、使用できる一般体系(SPNEGO - Simple and Protected Negotiation) もあります。SPNEGOは、ソフトウェア コンポーネントが使用するセキュリティ プロトコルを交渉できるようにすることで、拡張性と柔軟性を提供します。図2では、Webサーバーはステータス コード401を返し、WWW-Authenticateヘッダのいずれかで「Negotiate」を指定できます。WebブラウザがSPNEGOを実装している場合、認証に実際に使用するべきセキュリティ プロトコルを判断するのにSPNEGOを使用することができます。SPNEGOは任意のセキュリティ プロトコル間で交渉できますが、多くは、Kerberosとこれより古いNTLM認証のいずれかを選択するのに使用されます。

各プログラムに利用可能なすべてのプロトコル以外にSPNEGOも実装しなければならないとしたら、アプリケーションにセキュリティ プロトコルを実装する作業は非常に厄介になります。しかし、幸いなことに、このような作業は必要ありません。なぜなら、この作業を単純化するために、Unix/LinuxとWindowsの両方で利用できるソフトウェア ライブラリがあるからです。Microsoft Windows Security Support Provider Interface(SSPI)は、認証をサポートする必要があるすべてのプログラムで使用できるAPIを提供します。UnixシステムやLinuxシステムでSSPIに相当するのが、Generic Security Service(GSS)です。GSSまたはSSPIを使用するアプリケーションは、さまざまな認証プロトコルを実装することなく、さらにこれらのプロトコルの詳細を知らなくても、これらのプロトコルを採用することができます。

図3に、アプリケーションが通信の認証にどのようにGSSおよびSSPIを使用するかを示します。

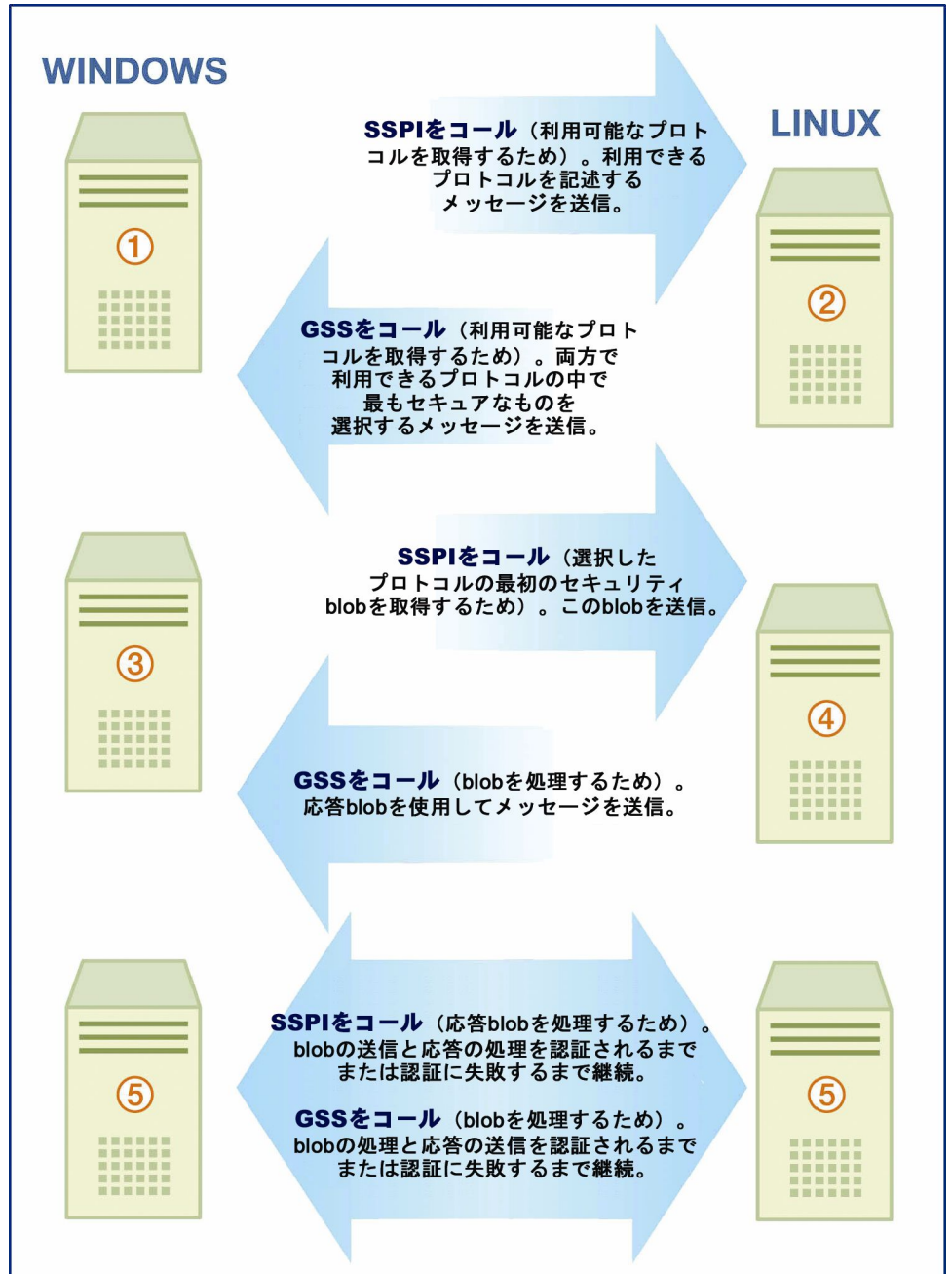


図3 - SSPI/GSS認証

どちらのアプリケーションも選択された特定のセキュリティ プロトコルに関する知識を必要としません。アプリケーションの観点からは、実行していることは、セキュリティ ライブラリが認証に成功または失敗したと知らせるまで不透明なblobを送受信し続けることだけです。

さまざまなコンポーネントを使用することで、WindowsマシンとLinuxベース マシンとの間の認証とシングル サインオンを実現できますが、これらのマシンを1つに張り合わせるための接着剤が足りません。たとえば、Windows上ではSSPIが利用でき、Linux上ではGSSが利用でき、これらのライブラリをオペレーティング システム間での認証に使用するこ

とはできますが、これらのライブラリを使用しないユーティリティもまだいくつかあります（たとえば、Linux *ftp*の標準バージョン）。Linux上でGSSは利用できますが、典型的なLinuxディストリビューションにはGSS SPNEGOの実装は含まれていません。

→ SambaがWindows/Linuxの相互運用性を改善

Linuxシステムは、出荷されたままの状態ではKerberos、LDAP、その他のセキュリティ/認証プロトコルはサポートしますが、ほとんどの場合Windowsを使用したシングル サインオンを実行できるようなっていません。システム管理者は、専用のプロプライエタリソフトウェアを購入すればLinux上にシングル サインオンを実装することができます。ただし、追加のソフトウェアをいっさい使用しなければ、LinuxシステムにActive Directoryベースのシングル サインオンを部分的に実装できるにすぎません。

Sambaは、LinuxとWindowsの相互運用を可能にするオープンソース パッケージです。Sambaを使用して、Active DirectoryにLinuxマシンを参加させ、Active Directoryドメインコントローラを使用する認証を実行できます。Sambaは、共有ファイル サービスも提供し、共有ファイルやプリンタへの受信接続がActive Directoryで認証されているかどうかを検証します。最後に、SambaはLinuxファイル システムと対話し、アクセス制御リスト（ACL）がActive Directoryユーザーに対して指定され、これが尊重されるようにすることができます。

ただし、これらの操作を実行するようにSambaを構成することは、些細なタスクとは言えません。Samba構成を指定するだけでなく、Linuxシステムのファイアウォール、Kerberos、PAM（プラグ可能認証モジュール）サブシステムも構成する必要があります。また、すべてが適切に機能するようにするためには、一部のパッケージの最新バージョンをダウンロードしてインストールしなければならない場合もあります。

→ 混合ネットワークでの構成を容易にする新しいツール

幸いにも、このプロセスを単純化し、構成タスクや管理タスクを自動化するために特別に設計された新世代のツールがあります。今年の初めにリリースされたCenteris® Likewise™を使用すれば、システム管理者は、Linuxベースのマシンにリモートから迅速にエージェント ソフトウェアをインストールして、Active Directoryベースのシングル サインオンを単純にすることができます。

Likewise Enterpriseは、リモートから標準的なWindowsコンソールを使用してLinuxマシン（および関連付けられているファイル、印刷、Webサービス）を管理するのに使用できます。共有ファイルや印刷リソースが作成されたときには、Likewiseがこの情報のActive Directoryへの公開をサポートします。

Likewiseは、Active Directory認可情報に対してイントラネットWebブラウザ ユーザーを認証するようにLinux Apacheサーバーをセットアップするのにも使用できます。

残念ながら、これらの操作を実行するようにSambaを構成することは、些細なタスクとは言えません。Samba構成を指定するだけでなく、Linuxシステムのファイアウォール、Kerberos、PAM（プラグ可能認証モジュール）サブシステムも構成する必要があります。

→ Windows/Linux統合ツールの利点

相互運用性を改善するためにLinuxとMicrosoft Windowsを構成することには、次のような管理上およびセキュリティ上大いなる利点があります。

LinuxをActive Directoryに参加させることによってセキュリティを改善

- Linuxサーバーとワークステーションの集中管理にActive Directoryを活用できる
- ファイル、印刷、Webを含む一般的なLinuxサービスに対してActive Directoryでユーザーを認証できる
- Linuxサーバーとワークステーションをさらに制御できる

Linuxの管理に既存のスタッフを活用

- 日常管理関連の人的費用を削減できる
- 高額なトレーニングなしでWindows管理者に権限を与えられる
- 構成に使い慣れたWindowsウィザードやグラフィカル ツールを使用できる

→ 例: シングル サインオンを実行するようにApache Webサーバーを構成する

手動による構成

Likewiseのようなツールがなければ、システム管理者は、手動でApache WebサーバーをActive Directoryシングル サインオンを実行するように構成しなければなりません。Mod_auth_kerb、つまりKerberos Module for Apache

(<http://modauthkerb.sourceforge.net> で入手可能) が、必要な機能のすべてを提供します。ただし、このモジュールを機能させるためには、管理者は次の手順を実行しなければなりません。

1. システムがmod_auth_kerbを提供するLinux ディストリビューションでない限り、管理者はこのソフトウェアをダウンロードし、コンパイルしなければなりません。このプロセスは、ソフトウェア開発者ではない管理者にとっては困難な場合があります。
2. 管理者は、Linux Kerberos認証ソフトウェアが適切に構成されたことを検証しなければなりません。これには、krb5.confキーを編集し、kinitプログラムを使用しなければならない場合があります。
3. 管理者は、Apacheサーバーと関連付けられたKerberosサービス キーを格納するためのキータブ ファイルを生成しなければなりません。すでにSambaをインストールしている場合、必要なエントリをデフォルト キータブに追加する「net ads keytab add HTTP」コマンドを使用することでキータブを生成できます。Sambaをインストールしていない場合は、この手順が分かりにくい場合があります。

管理者は、Apache構成ファイルを修正して、認証を使用するディレクトリ セクションそれぞれにmod_auth_kerbディレクティブが含まれるようにしなければなりません。

Likewiseを使用した構成

Likewiseは、構成手続きを自動化することで、このタスクを単純にします。Likewiseを使用すれば、管理者は、Windows管理者コンソールを使用してLinuxマシンに必要なソフトウェアをリモートからインストールし、LinuxマシンがActive Directoryベースのシングルサインオンを実行するように構成できます。

いったん構成が済めば、Likewiseを使用してリモートから、Windowsコンソール経由でLinuxマシンを管理できます。

→ 結論

このドキュメントで説明したツールとプロトコルを使用すれば、混合ネットワークで認証、ディレクトリ サービス、セキュリティを管理することはできます。ただし、このようなタスクは、Linuxの専門知識がない管理者にとっては敷居が高く面倒な作業です(時間と費用がかかることは言うまでもありません)。Likewise Enterpriseのような新しいツールは、これらのタスクを非常に単純にしてくれるだけでなく、Linuxサーバーの日常管理を容易にし、LinuxがWindowsとうまく連携して機能するように構成する作業に必要なネットワーク管理者の時間も削減してくれます。

Information

- 株式会社 東陽テクニカ Centeris サイト
<http://www.toyo.co.jp/it/centeris>
- ホワイトペーパー ダウンロードサイト
http://www.toyo.co.jp/it/centeris/c_download.html
- 評価版申し込み
http://www.toyo.co.jp/it/centeris/c_hyoka.html
- 資料請求
http://www.toyo.co.jp/it/centeris/c_shiryu.html
- 新着情報
http://www.toyo.co.jp/it/centeris/c_news.html
- 連絡先
centeris@toyo.co.jp