Samba/LDAPによるWindowsドメイン 管理権限の分離と委譲

OSSTech

オープンソース・ソリューション・テクノロジ株式会社
2006/10/19
技術部 エキスパート 佐藤 文優

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

目次

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

管理権限の分離・委譲とは?

- システムの管理対象を適切な粒度で分離し、
- それぞれに管理者を立て管理権限を委譲し、
- 各々で自律して維持・管理させる。

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

なぜ管理権限を分離・委譲するのか?

- 管理作業の負荷分散
- 管理作業の迅速化
  - 中央管理者に頼らず管理できる
  - 例: パスワードのリセットくらい現場内で解決してほしい
- 管理・運営上の方針の分離
  - セキュリティポリシーの違い
  - そのほか様々な部門特有の事情に対応

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

本セミナーの対象

- Samba + LDAP による Windows (NT) ドメインの
- アカウントと共有を部門ごとに分け、
- 部門管理者に管理権限を委譲する方法。

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

管理対象: アカウントと共有

- アカウント
  - ユーザー
  - グループ
  - コンピューター
- 共有
  - 共有場所
  - アクセス権
  - 監査
  - クォータ

本セミナーではプリンタ共有、監査、クォータは対象外

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

部門管理者の権限

- 部門内のユーザーとグループ、
  部門用の共有フォルダを管理可能
- ほかの部門の管理はできない
- ただし子部門の管理権限を持つ

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

実現方法 (1)
NT ドメインの場合

- どうやって?
  - 部門ごとにドメインを立てる
  - ドメインごとに信頼関係を結ぶ
  - 管理者のユーザーアカウントにドメイン管理権限を付与
- 利点・欠点
  - 実績が多い
  - ドメインごとに DC となるサーバーが必要
  - Windows NT はサポート終了
  - そのほかに CAL (Client Access License) が必要など、Windows ならではの利点・欠点がある

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

実現方法 (2)
Active Directory の場合

- どうやって?
  - 部門ごとに AD ツリーを OU で分ける
  - ドメイン、ツリー、フォレスト (サイトでも?) で分けることも可能
  - 管理者のユーザーアカウントにサブツリー管理権限を付与

→ *LDAP 的な解*

- 利点・欠点
  - MS 純正なので安心(?)
  - AD ならではの機能も使える
    - 推移する信頼関係 (削除できないらしいので、場合によっては欠点?)
    - グループポリシー
    - サイト
  - そのほかに CAL (Client Access License) が必要など、Windows ならではの利点・欠点がある

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

実現方法 (3)
Samba 3 (NT) ドメインの場合

- どうやって?
  - ふつうに考えたら Windows NT と同じ、つまり複数ドメインと信頼関係
- 利点・欠点
  - 実績が多い
  - ドメインごとに DC となるサーバーが必要
  - そのほかに CAL (Client Access License) が不要など、Samba ならではの利点・欠点がある

LDAP を利用すれば…?

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

実現方法 (4)
Samba 3/LDAP (NT) ドメインの場合 [1/2]

- どうやって?
  - LDAP 必須 (passdb backend = ldapsam:...)
  - 単一ドメイン
  - 部門ごとに LDAP ツリーを OU で分ける
  - Samba の設定ファイルとスクリプトで細工
    - ふつうにアクセスすると全ツリーのアカウント情報が見える
    - 部門管理者のユーザーアカウントでアクセスすると特定 OU 以下のみ

→ *LDAP 的な解 + OSS ならではの工夫の余地を利用*

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

実現方法 (4)
Samba 3/LDAP (NT) ドメインの場合 [2/2]

- **利点・欠点**
  - AD **不要** (Windows Server 200X, Samba 4 **いらず**)
  - **環境構築の手間がかかる**
    → *弊社サービスをご利用ください!*
  - **懸案・制限事項あり (詳細は後述)**
    - **許容できるかどうかは要件次第**
    - **解決できるよう鋭意作業中…**
  - **そのほかに** CAL (Client Access License) **が不要など、** Samba **ならではの利点・欠点がある**

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

LDAP DIT の分離例 [1/3]
OU

- dc=example,dc=jp
  - ou=Tech (**技術部**)
    - ou=Users
    - ou=Groups
    - ou=Computers
    - ou=1st (**第1技術部**)
      - **同上**
    - ou=2nd (**第2技術部**)
      - **同上**
  - ou=Sales (**営業部**)
    - **同上**
  - ou=Marketing (**マーケティング部**)
    - **同上**

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

LDAP DIT の分離例 [2/3]
smb.conf

```
[global]
passdb backend = ldapsam:"ldap://localhost ldaps://ldap2"
ldap suffix = dc=example,dc=jp
ldap user suffix =
...
include = /etc/samba/smb.%U.conf
```

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

LDAP DIT の分離例 [3/3]
smb.部門管理用ユーザー名.conf

```
[global]
ldap user suffix = ou=Users,ou=部門名
...
add user script = アカウント管理コマンド "部門名" "%u"
...
[IPC$]
admin users = 部門管理用ユーザー名
[C$]
path = /部門用共有フォルダ
```

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

DIT 分離に対応したアカウント管理コマンド

- 独自に開発
- smbldap-tools のラッパースクリプト
  - sh スクリプト/Perl スクリプト群
  - smbldap-tools は実装が嫌いなので将来は捨てたい (個人的意見)
- 指定された部門の OU 以下のアカウント情報を操作
- CSV ファイルによるバッチ処理にも対応

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

管理方法 (1)
GUI

- アカウントは Windows NT Server の管理ツールで管理
  - サーバーマネージャ
  - ユーザーマネージャ
- 共有は MMC で管理

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

サーバーマネージャ/ユーザーマネージャの入手方法

- Windows NT Server 4.0 のインストール CD-ROM
  - \clients\srvtools 以下
- マイクロソフト サポート情報 JP173673
  - http://support.microsoft.com/kb/173673/
  - 英語版サーバー/ユーザーマネージャ
  - 日本語の表示・編集も可能
- Windows 2000 サービスパック 4 (SP4) 日本語版
  - http://www.microsoft.com/japan/windows2000/downloads/servicepacks/sp4/default.asp

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

ユーザーマネージャの問題点

- ユーザー/グループ名の最大長に 20 バイト (CP932 換算) 制限あり
- ユーザー/グループの一覧はフラットに表示される
  - 検索、絞り込みもできない
- メールアドレスなどの情報を管理できない
- ライセンスが不明確
- Windows Vista で動作しない

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

管理方法 (2)
CSV ファイルによりバッチ処理

- CVS ファイル投入用の共有を用意
  smb.部門管理用ユーザー名.conf
  [AccountCVS]
  path = /admin/accountcvs/部門名
- 部門管理用ユーザーで \\PDC名\AccountCSV にアクセス
- フォルダ構造
  - \queue
    - CSV ファイルを投入するフォルダ
  - \result
    - 処理結果と処理済み CSV ファイルが置かれるフォルダ
  - \current
    - 処理前後の部門のアカウント情報を CSV ファイルで出力するフォルダ

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

CSV ファイルの例

- **ユーザーの管理**: user.csv

```
操作,ユーザー名,主グループ,副グループ,パスワード,氏名,説明,email,会社番号,社員番号,雇用形態
A,satoh,tech,,my-secret...,佐藤太郎,技術部部長,satoh@example.jp,C1,E200601,T1
A,suzuki,sales,,foo!bar!,鈴木次郎,社員,suzuki@example.jp,C1,E200602,T1
A,tanaka,sales.2nd,,UryyyOraOra,田中三郎,社員,tanaka@example.jp,C1,E200603,T1
D,kondoh
```

- **グループの管理**: group.csv

```
操作,グループ名,説明
A,webmasterls,Web コンテンツ管理者
A,regulars,正社員
D,parttimer
```

- **グループのメンバー管理**: member.csv

```
操作,グループ名,ユーザー名,...
A,webmasterls,satoh,suzuki
A,regulars,tanaka
D,parttimer,kondoh
```

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

制限事項・問題点 (1)

- ユーザーマネージャの制限
- 部門ごとに管理専用アカウントが必要
  - ユーザーカウントに権限を付与できない
  - Windows NT 管理ツールを利用した場合の制限
    (サーバーマネージャ、ユーザーマネージャなど)
    別途 LDAP DIT 管理ツールを用いれば問題ない
- 他部門のユーザーにグループ権を付与できない
  - 他部門 (子部門を除く) のユーザー/グループは表示さえできない
  - 付与先のユーザーと付与するグループ、両方の管理権限が必要

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

制限事項・問題点 (2)

- アカウントポリシーの分離ができない
  - NT ドメインの仕様上、1ドメインに 1ポリシー
  - LDAP DIT で細工すれば可能かもしれないが?
- セキュリティは大丈夫?
  - ［IPC$］ admin users = 部門管理用ユーザー名 は権限が大きすぎ
  - SeAddUsersPrivilege, SeDiskOperatorPrivilege 権限だけで十分そう (要調査)

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.

今後の予定

- 環境構築の自動化
  - 手作業でやるには複雑すぎる
- アカウント管理コマンドのブラッシュアップ
- サーバー/ユーザーマネージャの代替品の検討あるいは開発
  - LAM (LDAP Account Manger) で対応可能?
  - 開発するなら Web, Java, Perl or Ruby で? C# (Mono?)?!
- 他部門のユーザーの表示とグループ権付与を可能にする
- Samba 4 対応
  - AD 互換とのことなので不要?
- 実績を増やす

Copyright © 2006 Open Source Solution Technology Corporation All Rights Reserved.