OSSTech Samba AD DC アップグレード手順

OSSTech(株)

更新日 2022 年 6 月 10 日

目次

1 Samba AD DC のアップグレード手順

下記の要領で Samba AD DC 環境のアップグレードを実施してください。

1. Samba AD の動作状態の確認
   - Windows クライアントからのドメインログオンが問題なく動作すること。
   - ドメインユーザーによる SYSVOL 共有フォルダ (\\<**ドメイン名**>\SYSVOL, \\<DC **ホスト名**>\SYSVOL) への アクセスが問題ないこと。
   - Samba AD のデータベースに問題がないこと。
   - Samba AD のレプリケーションの動作に問題がないこと。 (複数 DC 構成の場合)
2. Samba の設定とデータベースのバックアップ
3. Samba パッケージのアップグレード
   - 複数の DC ホストが存在する場合、安全のため FSMO ロールを持たない DC ホストから アップグレードしてください。
   - 1 台の DC ホストの Samba パッケージをアップグレードする度に 手順 1 と同じ動作状態の確認を実施してください。
   - 可能であれば、アップグレード後に AD ユーザー / AD グループの追加・変更・削除とレプリケーションの動作確認も実施してください。

いずれかの手順で問題が生じた場合はアップグレード計画を中止し、 OSSTech サポートにお問合せください。

2 各手順の詳細

下記に記載するコマンドラインやコマンド出力の内容は以下の構成を前提としています。実際の環境に合わせて適宜読み代えて実行してください。

- Samba バージョン: OSSTech Samba 4.X
- AD ドメイン名: example.internal (NT ドメイン名: EXAMPLE)
- DC ホスト名:
  - dc1 (dc1.example.internal)
  - dc2 (dc2.example.internal)

2.1 FSMO ロールを持つ DC ホストの確認

Samba AD DC ホストのいずれかで下記のコマンドラインを実行し、 どの DC ホストが FSMO ロールを保持しているかを確認します。

```
# /opt/osstech/bin/samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=dc1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=example,DC=internal
InfrastructureMasterRole owner: CN=NTDS Settings,CN=dc1,CN=Servers,CN=Default-Fir
st-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=internal
RidAllocationMasterRole owner: CN=NTDS Settings,CN=dc1,CN=Servers,CN=Default-Firs
t-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=internal
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=dc1,CN=Servers,CN=Default-First
-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=internal
DomainNamingMasterRole owner: CN=NTDS Settings,CN=dc1,CN=Servers,CN=Default-First
-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=internal
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=dc1,CN=Servers,CN=Default-Fir
st-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=internal
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=dc1,CN=Servers,CN=Default-Fir
st-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=internal
```

例えば上記のようにコマンド出力のすべての行が**<ロール名>** `owner: CN=NTDS Settings,CN=dc1,...` にようになっていれば、DC ホスト dc1 がすべての FSMO ロールを保持している状態です。

2.2 FSMO ロールの転送

FSMO ロールを取得させたい Samba AD DC ホストで下記のコマンドラインを実行します。 いくつかの FSMO ロールの転送には Administrator 権限が必要となり、転送処理が実行される場合はパスワードの入力を求められます。

```
# /opt/osstech/bin/samba-tool fsmo transfer --role=all --username=Administrator
...省略...
Password for [EXAMPLE\Administrator]:<AD の Administrator のパスワードを入力>
...省略...
```

コマンドの出力 (パスワード入力プロンプトを除く) がすべて下記のいずれかになれば完了です。

- FSMO transfer of '<**ロール名**>' role successful
  - 該当 FSMO ロールを他 DC ホストから転送成功したとき。
- This DC already has the '<**ロール名**>' FSMO role
  - すでに該当 FSMO ロールを保持していたとき。

Samba 4.8 では FSMO 転送処理にいくつかのバグがあります。下記のようの対処してください。

- 複数の FSMO ロールの転送が必要な場合、2 つ目以降の転送処理中にコマンドが停止してしまう。
  - コマンド出力が数十秒以上停止した場合、キーボード割り込み (通常は Ctrl+C 押下) してコマンドを強制停止してください。
  - 問題が発生しなくなるまでコマンドラインを再実行してください。
- DNS 関連の FSMO ロールを転送するとコマンドが異常終了してしまう。(エラーメッセージ: ERROR(<type 'exceptions.AttributeError'>): uncaught exception - 'module' object has no attribute 'drs_utils' ... **省略**...)
  - FSMO ロールの転送処理は開始しているため、エラーは無視してください。
  - 問題が発生しなくなるまでコマンドラインを再実行してください。

2.3 AD データベースの検査

Samba AD DC ホストで下記のコマンドラインを実行し、 コマンド出力が Checked <AD **総オブジェクト数**> objects (0 errors) 表示となることを確認します。

```
# /opt/osstech/bin/samba-tool dbcheck --cross-ncs
Checking <AD 総オブジェクト数> objects
Checked <AD 総オブジェクト数> objects (0 errors)
```

2.4 AD レプリケーションの確認

2.4.1 AD レプリケーション状態の確認

確認対象の Samba AD DC ホストで下記のコマンドラインを実行し、 AD DIT (LDAP DIT) のすべてのサブツリーにおいて Last attempt @ <**曜日**> <**日時**> <**タイムゾーン**> was successful 表示となることを確認します。<**曜日**> <**日時**> <**タイムゾーン**> 部分は NTTIME(0) 表示になることもあります。

```
# /opt/osstech/bin/samba-tool drs showrepl
... 省略...

==== INBOUND NEIGHBORS ====

DC=example,DC=internal
        Default-First-Site-Name\<DC ホスト名> via RPC
                DSA object GUID: <GUID>
                Last attempt @ <曜日> <日時> <タイムゾーン> was successful
                <発生中のエラー継続数> consecutive failure(s).
                Last success @ <曜日> <日時> <タイムゾーン>

<サブツリー RDN>,DC=example,DC=internal
... 省略 (サブツリーごとに上記同様の出力が続く)...

==== INBOUND NEIGHBORS ====

... 省略 (同上)...
Warning: No NC replicated for Connection!
```

最後に Warning: No NC replicated for Connection! と表示されますが、 問題ありませんので無視してください。

2.4.2 AD DIT の比較

いずれかの Samba AD DC ホストで下記のコマンドラインを実行し、すべてのオブジェクトの比較結果が Result for [<オブジェクトの種類>]: SUCCESS 表示となることを確認します。

```
# /opt/osstech/bin/samba-tool ldapcmp \
  ldap://dc1.example.internal \
  ldap://dc2.example.internal \
  --username=Administrator \
  --filter=msDS-NcType,serverState,subrefs \
;
Password for [EXAMPLE\Administrator]:<AD の Administrator のパスワードを入力>

* Comparing [<オブジェクトの種類>] context...

* Objects to be compared: <オブジェクト総数>

* Result for [<オブジェクトの種類>]: SUCCESS

... 省略 (オブジェクトの種類ごとに上記同様の出力が続く)...
```

コマンドラインの 2 つの ldap://... には、 AD DIT (LDAP DIT) を比較したい DC ホストの LDAP URL を指定します。

2.4.3 AD レプリケーションのナレッジ整合性チェック (KCC)

いずれかの Samba AD DC ホストで下記のコマンドラインを実行し、 各の DC に対する実行結果が `Consistency check on <DC` **のホスト名**`> successful.` 表示となることを確認します。

```
# /opt/osstech/bin/samba-tool drs kcc dc1.example.internal
Consistency check on dc1.example.internal successful.
# /opt/osstech/bin/samba-tool drs kcc dc2.example.internal
Consistency check on dc2.example.internal successful.
```

2.5 Samba の設定とデータベースのバックアップ

バックアップ対象の Samba AD DC ホストで下記のコマンドラインを実行し、Samba の設定ファイルとデータベースのバックアップを取得します。バックアップファイルは `/opt/osstech/var/backup/samba` ディレクトリ下に作成されます。

```
# /opt/osstech/sbin/samba_backup
... 省略...
```

Samba 4.8 では一部の TDB ファイルのバックアップに失敗することがありますが、問題ありませんので無視してください。問題ないエラーメッセージの例:

```
# /opt/osstech/sbin/samba_backup
tdb_mutex_open_ok[./private/netlogon_creds_cli.tdb]:
  Can use mutexes only with MUTEX_LOCKING or NOLOCK
Failed to open ./private/netlogon_creds_cli.tdb
```

2.6 Samba パッケージのアップグレード

OSSTech サポートにサポート ID、動作環境 (OS 名とバージョン)、使用中の OSSTech Samba バージョン (`rpm -qa 'osstech*'` の実行結果)、Samba の設定情報 (`/opt/osstech/bin/testparm -s` の実行結果) を連絡して Samba パッケージアーカイブファイルを入手します。ファイル名は `osstech-samba-<Samba` **バージョン**`>-<` **リリース**`>.el<RHEL` **メジャーバージョン**`>.tar.gz` という形式です。

アップグレード対象の Samba AD DC ホストに Samba パッケージアーカイブファイルを転送したあと、下記のコマンドラインを実行してパッケージアーカイブファイルの展開とアップグレードを行ないます。

```
# tar xvfz osstech-samba-4.15.5-157.el7.tar.gz
# ./osstech-samba-4.15.5-157.el7/install.sh
... 省略...
================================================================================...
 Package                          Arch      Version           Repository      ...
```

```
================================================================================...
Installing:
... 省略（インストールされるパッケージ一覧）...
Updating:
... 省略（アップグレードされるパッケージ一覧）...
Installing for dependencies:
... 省略（依存関係によりインストールされるパッケージ一覧）...
Updating for dependencies:
... 省略（依存関係によりアップグレードされるパッケージ一覧）...
Transaction Summary
================================================================================...
... 省略...
Is this ok [y/d/N]: y
... 省略...
Complete!
```

アップグレードあるいは追加インストールされるパッケージ一覧が表示された後、確認のプロンプト `Is this ok [y/d/N]:` が表示されたらコマンド出力の内容を確認し、 `y` と Enter キーを入力するとパッケージアップグレードが実行されます。

パッケージのアップグレード処理の過程で Samba AD DC サービス (サービス名: `osstech-samba`) の再起動が自動的に実行されます。

コマンド出力の最後に `Complete!` (日本語の場合は**完了しました**!) が表示されてコマンドが終了すればパッケージアップグレードは完了です。

3 改版履歴

- 2022-06-03
  - 初版作成。