

# ドメコン間のレプリケーション

2022/07/19に公開



Active Directory



Tech

## はじめに

Active Directory Domain Serviceのサーバ（ドメインコントローラー）のレプリケーション周りについて整理。  
なお前提としてシングルフォレスト、シングルドメイン、マルチサイト構成を想定しています。

## レプリケーションの種類

ユーザアカウントやコンピュータアカウント、AD統合ゾーン等の情報（NTDS）のレプリ



fumfum

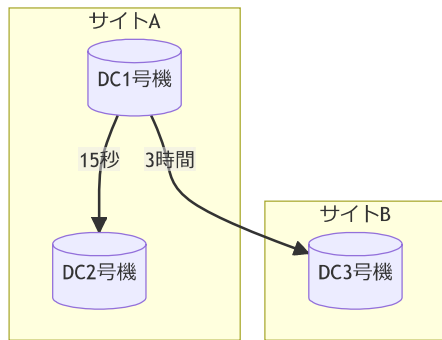
フォロー

一応インフラやってます

ケーションとグループポリシー等の情報（SYSVOL）のレプリケーションの大きく2種類にわかれている。

## レプリケーションの間隔

サイト内のドメコン間のレプリケーション間隔は15秒、サイトを越えたドメコン間のレプリケーション間隔は3時間（設定変更することで15分まで縮めることは可能）が基本。ただし、アカウントのパスワード変更のようなものはPDCに対してNetlogonサービスから変更通知を即時で実施する。その後PDCがあるサイト内のドメコン間は15秒間隔でレプリケーションが行われ、サイトを越えるドメコン間は3時間間隔でレプリケーションが行われる。パスワードの認証要求は最終的にはPDCに対して実施するので、レプリケーションがまだ行われていないサイトでも認証は可能らしい。（やったことないのでいつか試してみたい。）



## レプリケーション を即時実行したい ときにやること

レプリケーションをすぐに実施したいときは以下のコマンドを実行する。サイトが一つしかなかったりするとあまり活躍しないが、複数サイトで構成されている環境では本当にお世話になったコマンド。

```
repadmin /syncall /AeP
```

オプションのざっくりした意味は以下の通り

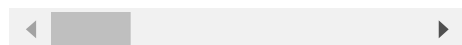
/A :すべての名前付けコンテキストをレプリケーション対象にする

/e :他サイトにあるドメコンをレプリケーション対象にする

/P :コマンドを実行するドメコンからプッシュでレプリケーションする（本オプションを消すとプルになる）

ただし、上記のコマンドではSYSVOLの内容はレプリケーションされないので要注意。SYSVOLの内容もすぐにレプリケーションしたい場合は以下コマンドを実行。

```
dfsrdiag SyncNow /RGName:"[
```



コマンド実行すると一時的に上記のtimeで指定したレプリケーション間隔になるが、すぐにレプリケーションしたいときでも、何となくサイト間レプリケーション間隔の最小値である15分を指定して使っていた。

[\[1\]](#)

なお、ドメコンの切り替えでユーザアカウントやコンピュータアカウントはレプリケーションされているのに、AD統合ゾーンの情報だけ何故かレプリケーションに時間がかかるという事象に何度か遭遇した。上記のrepdamin叩いてもダメ。もしかしたら/Aeでプルすればよかったのかもしれないが、だい

## 目次

はじめに

レプリケーションの種類

レプリケーションの間隔

レプリケーションを即時実行したいときにやること

○ レプリケーションがうまくいっていないときにやること

ドメコン切り替えのときによくやったこと

まとめ

たい翌日には何事もなかったようにレプリケーションが完了していたので、深追いはしていない。。

## レプリケーションがうまくいっていないときにやること

イベントログで2213が出てたらダーティシャットダウンとかしちゃった影響でSYSVOLのレプリケーションが止まっている可能性がある。Windows2012以降であれば自動回復が有効になっているので自動的に復旧してくれそうだが、Windows2008R2は無効になっている場合があるので、注意が必要。（ってWindows2008はもうさすがにないか。。）以下サイトがとても参考になる。



なお、レプリケーションが止まっている期間が長かったりす

ると、上記対処をしてもイベントログに4012がでて復旧できないことがある。（60日以上レプリケーションが止まっていると該当しちゃうかも。）その場合はレプリケーション元と先でMaxOfflineTimeInDaysを一時的に長い期間にしてDFSRサービスを再起動し、DFSRDIAG POLLAD<sup>[2]</sup>を実行して、レプリケーションされることを確認できたら、MaxOfflineTimeInDaysを元に戻してあげる。

ちなみに、SYSVOLがレプリケーションされているかを確認する手取り早い方法はSYSVOL配下に任意のファイルを置いて、レプリケーションされるかを確認する。（DFSRのレポートを確認していても異常を検知できなかったことがあった。。）

その他以下サイトも参考になる。



# ドメコン切り替えのときによくやったこと

特定サイトのドメコンをローリングアップデートとかするとサイトリンク周りでハマることがよくあった。時間が解決することもあるのだが、限られた時間内で切り替え作業をしなければならないときは、手動でパスを再生成するというのをよくやっていた。

具体的には、Active Directory サイトとサービスからサイト名  
→Servers→ADサーバ名  
→NTDS Settingsを選択し、右ペインに表示される自動生成されている接続オブジェクトを削除して、repadmin /kccとrepadmin /syncall /AePをレプリケーション元とレプリケーション先で実行するような感じ。

## まとめ

レプリケーションが止まっているというのは割と遭遇してきたので、定期的な稼働チェック  
(dcdiagを実行して確認、イベントログの確認、SYSVOLのレ

プリケーション状況の確認等)をして、早めに異常に気づけるようにしたいものです。

脚注

- 1. DFSR (not FRS) の場合、レプリケーションが最適化されており、SYSVOLの内容に変更があったら、即時レプリケーションされるみたいな記事もあるが、私が触った環境ではそのような動作にはなっていなかった。どちらかというとサイトリンクで定義した時間 (デフォルト3時間) に近い時間でレプリケーションがされているような印象。↩
- 2. 「DFS の管理」ツールを事前に導入しておく必要あり ↩



fumfum

一応インフラやっています

フォロー

Discussion





ログインするとコメントできます

Login

## Read next

**【Azure】 Azure上で  
ADDS構築〜ドメイン参  
加迄実施してみました！**



Massu 2021/04/27 ♡ 8

**Raspberry Pi 4、  
Ubuntu 22.04 LTS、  
Samba 4を使って…**



Yuya K... 2022/06/17 ♡ 6

**【AzureAD】「Azure  
AD Connect」とは？？**



Massu 2021/04/12 ♡ 5

**【AzureAD】 csvを利用  
したユーザー追加スクリ  
プト**



Massu 2021/04/06 ♡ 3

**Active Directory:ユー  
ザーの所属グループを  
CSV出力**

**Active Directory 設計  
時にスルーされがちだと  
思うポイント**



sou (0... 2021/01/12 ♡ 6

**【AzureAD】 AzureAD  
のデバイス管理の種類**



Massu 2021/04/24 ♡ 5

**【AzureAD】 ドメイン  
連携方法**



Massu 2021/04/10 ♡ 5

**Active Directory:CSV  
読み込んでユーザーの  
OU、所属グループを…**



はちくわ 2021/03/15 ♡ 3

**AzureFileSyncを試して  
みる その1**



fumfum 2022/09/20 ♡ 2



はちくわ 2021/03/14 4



エンジニアのための  
情報共有コミュニティ

About

Zennについて  
運営会社  
お知らせ・  
リリース

Guides

使い方  
Publication  
よくある質  
問

Links

Twitter  
GitHub  
メディア  
キット

Legal

利用規約  
プライバシー  
ポリシー  
特商法表記

