RHEL7.0 および互換 OS への
SWANStor サーバインストール手順書

エリアビイジャパン株式会社
テクニカルサポート

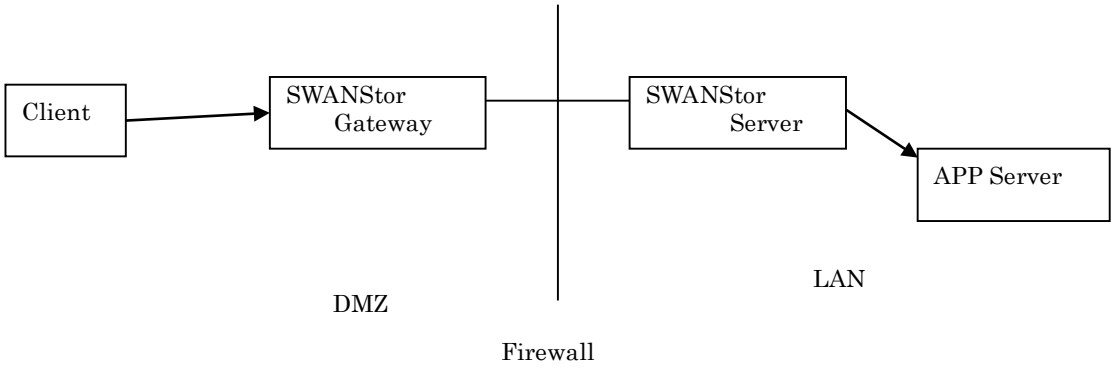
目次

1 システム構成

1.1 システム構成

SWANStor のシステム構成は、以下の通りです。

１）1 重化構成の場合



２）2 重化構成の場合

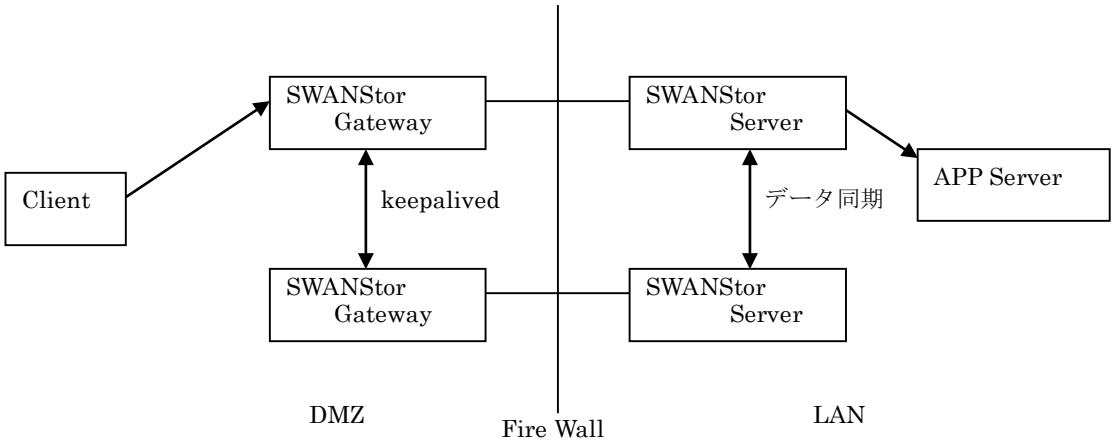


図１−１　システム構成

パッケージとして以下をインストールします。

表１　導入パッケージ

No	パッケージ
1	SWANStor Server パッケージ

また弊社では、Redhat Enterprise LINUX version 7.0 およびその互換 OS に SWANStor サーバをインストールする上での追加ファイルを以下のようにご提供させていただいております。こちらもご利用ください。追加ファイルは以下の URL でダウンロードできます。

https://ex.swanstor.com/download/pkgfile/rhel7-swanstorserver-additions.zip

追加ファイル	ディレクトリ	内容	参照先
public.xml	additions/firewalld	ファイアウォール設定	firewall 設定について

config	additions/selinux	selinux を無効化する設定	seLinux の扱いについて
sshd_config_add	addtions/sshd	SSH 鍵の強化（RHEL7.1 以降）	SSH 接続時の利用する暗号鍵の強化
compat-libstdc++-296-2.96-144.el6.i686.rpm	additions/swanstor	管理画面設定	SWANStor Server のインストール
swangui.conf	additions/swanstor	管理画面設定	swangui.conf ファイルの修正
swanstor.service	additions/swanstor	SWANStor 起動スクリプト	SWANStor Server 起動スクリプトのインストール
swanctl.conf	additions/sysctl	TCP パラメータ設定	TCP の Keepalived タイマーの設定

2 SWANStor サーバインストールの準備

2.1 Red Hat Enterprise LINUX version 7.0 のインストール

本資料は RedHat Enterprise Linux version 7.0 をベースにしていますが、RedHat の 7.0 以上の OS および CentOS7 系の OS にも対応しています。
OS はまず最小構成でインストールします。
次に以下の必要なパッケージ群をインストールします。

パッケージ	必要性	理由
perl	必須	プロセスの起動スクリプトで使用しているため

2.2 seLinux の扱いについて

selinux については無効化（disabled または permissive）にしてください。selinux を有効化した場合、SWANStor ServerManager(cgi プログラム)が起動しなかったり、構成情報の反映が正しくできない場合があります。
getenforce コマンドで Permissive と表示されることを確認し、そうでない場合には次のコマンドで selinux を無効化してください。

```
#getenforce
Enforcing
# setenforce permissive
# getenforce
Permissive
```

また、この設定を再起動時も有効にするために、/etc/selinux/config の設定を書き換えるか追加ファイルの selinux/config で上書きして、
SELINUX=disabled
としてください。

2.3 firewall 設定について

SWANStor サーバは管理画面アクセスで TCP ポート 4443 を使用します。Linux のデフォルト状態ではこのポートへのアクセスはフィルタされているので、これを許可します。また、SWANStor サーバのクラスタ機能を利用したり、LANMANAGER でインストールされた SWANStor

サーバの状態を見る場合には、TCP:4444 と UDP:4444 のポートへのアクセスも許可する必要があります。
追加ファイルの firewalld/public.xml に上記を設定したものがあります。このファイルを /etc/firewalld/zone/public.xml に上書きし、以下のコマンド投入で設定が有効になります。

```
#firewall-cmd --reload
success
```

3 SWANStor Server の導入及び設定

詳細は、SWANStor Server PRO EX 2.0Jのマニュアルも合わせてご参照ください。

3.1 SWANStor Server のインストール

SWANStor Serverをインストールします。パッケージのバージョン番号は変更されることがあります。また、コマンドはrpmパッケージが保管されているディレクトリで実行する必要があります。

```
# yum install compat-libstdc++-296-2.96-144.el6.i686.rpm
# yum install swanstor2-7.05.0070-1_ex.i386.rpm
```

compat-libstdc++-296 のインストールには 32 ビット glibc パッケージのインストールが追加で必要な場合があります。更に、以下のパラメータが必要な場合があります。
--setopt=protected_multilib=false

また、yum で上記パッケージをインストールするためには以下のパラメータが必要な場合があります。
--nogpgcheck

インストール後、”/etc/httpd/conf.d”配下に「swangui.conf」、”/usr/local”配下に”swanstor”フォルダが作成されます。

3.2 SWANStor Server 起動スクリプトのインストール

追加ファイルの swanstor.service を/usr/lib/systemd/system にコピーして、次のコマンドで有効化します。

```
# systemctl enable swanstor
```

また、httpd もシステム再開時に自動起動するようにしておきます。

```
# systemctl enable httpd
```

3.3 swangui.conf ファイルの修正

RHEL7.0 にパッケージされている Apache サーバ（2.4.6）はディレクトリへのアクセス権限の指定方法が変更になっており、それにともなう swangui.conf ファイルへの追記が必要となります。

追加ファイルの swangui.conf をインストールされた/etc/httpd/conf.d/swangui.conf に上書きします。

追加ファイルの swangui.conf では、以下のように、”Require all granted"の一行が追加されています。

```
Listen 0.0.0.0:4443

#User espeak
#Group espeak
<VirtualHost *:4443>
       DocumentRoot /usr/local/swanstor/gui
       AddHandler cgi-script .cgi
       DirectoryIndex ezlogout.cgi
       AddType application/octet-stream .dat
</VirtualHost>

<Directory "/usr/local/swanstor/gui">
       AllowOverride Options
       Options +ExecCGI
       Order allow,deny
       Allow from all
       Require all granted
</Directory>

<Directory "/usr/local/swanstor/bin">
       AllowOverride None
       Options None
       Allow from all
</Directory>

<Directory "/usr/local/swanstor/server">
       AllowOverride None
       Options None
       Allow from all
</Directory>
```

3.4 SWANStor Server の起動

SWANStor　Server 管理用の Apache サーバと SWANStor Server のプロセスを起動します。

```
          # systemctl start httpd
          # systemctl start swanstor
```

なお、SWANStor サーバプロセスを停止する場合は以下のコマンドとなります。

```
          # systemctl stop swanstor
```

3.5 SWANStor Server の初期設定

以下、SWANStor　Server管理画面にアクセスして、PSEファイルのインストール、接続設定の確認、URLやグループの設定などと進めていきます。その詳細はSWANStor Server PRO EX

2.0Jのマニュアルをご参照ください。

SWANStor Server 管理画面へのアクセスは、マニュアルに記載のとおり、SWANStor Server がインストールされたセグメント及び接続が許可された PC よりインターネットブラウザにて以下の URL でアクセスします。
接続先 URL：http://swanstor-server-host:4443/

また管理画面へのログインする際のパスワードは初期状態では、以下の通りです。
管理者パスワード：admin

4 SWANStor サーバのパフォーマンスに関わる設定

4.1 TCP の Keepalived タイマーの設定

TCP はその通信が終了（TCP FIN を送った、または受け取った）場合でも設定された待ち時間だけそのリソースを保持し続けます。これはアプリケーションが TCP の受信バッファからデータを受け取り切るまでの調整時間なのですが、Linux をデフォルトでインストールした状態の設定値は必要以上に長く（CentOS7.0 では 7200 秒）、SWANStor サーバのように複数のセッションを処理するサーバシステムでは、TCP リソースが消費し続け不足する場合があります。
このための設定として swanstor.conf ファイルを用意しているので、/etc/sysctl.d ディレクトリにコピーし、次のように読み込ませます。

```
#sysctl -p swanstor.conf
net.ipv4.tcp_keepalive_time = 10
net.ipv4.tcp_keepalive_probes = 2
net.ipv4.tcp_keepalive_intvl = 3
# sysctl -a | egrep keepalive
net.ipv4.tcp_keepalive_intvl = 3
net.ipv4.tcp_keepalive_probes = 2
net.ipv4.tcp_keepalive_time = 10
```

4.2 TCP セグメンテーションオフロードの無効化

Linux を仮想マシン環境下で動作させる場合には、インタフェース自身が実ハードウエアではないため、TCP セグメンテーションオフロードが有効だと通信パフォーマンスに影響を及ぼす場合があります。TCP セグメンテーションオフロードとは、分轄されて送られていくる TCP パケットの組み立てや順序制御をハードウエアで実行する仕組みです。
以下のコマンドで TCP セグメンテーションオフロードを無効化するとともに、/etc/rc.d/rc.local にも追記して、システム再起動時自動的に反映されるようにします。

```
#/sbin/ethtool -K eth0 rx off tx off tso off
```

5 SWANStor サーバのセキュリティに関わる設定

5.1 不要なプロセスの無効化

不要なプロセスは無効化します。現在有効化されたサービスは以下のコマンドでチェックできます。

```
# systemctrl –type=service
```

例として、postifx.serviceの無効化の手順を示します。

```
#systemctl disable postfix
rm ’/etc/systemd/system/multi-user.target.wants/postfix.service’
# systemctl stop postfix
```

5.2 SSH 接続時の利用する暗号鍵の強化

以下の処理を行うことで、SSH 接続時に利用する暗号鍵を強度の高いものに制限します。

1. /etc/ssh/moduli から、ビット長が2000bit以下のものをコメントアウトする。またはビット長を2048bit以上にして、同ファイルを新規に生成する。
2. /etc/ssh/sshd_config で、「KexAlgorithms」ディテクティブで鍵交換の方式を制限する。

KexAlgorithms

diffie-hellman-group-exchange-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,curve25519-sha256@libssh.org

ただし、KexパラメターはRHEL7.0では動作しないので注意してください。

追加ファイルではKexAlgorithmsパラメータの指定部分のみ切り出したsshd_config_addを用意しています。/etc/ssh/sshd_configファイルの最後にこれを追記し、sshdを再起動すると設定が反映されます。