

ReadOnly 設定について

版	日付	記述		
	発行	作成	確認	承認
版	日付	記述		
	発行	作成	確認	承認
版 1	日付	20171115	記述 新規発行	
	発行	プロフェッショナルサービス	作成 大島龍博	確認 承認
表題			No	版
ReadOnly 設定について			PSG-20171115	1
				ページ 1/5

READONLY にする方法は、以下の 3 ステップです。

1. /etc/fstab のオプション部分に “ro” を指定する

下記設定では、/home は、別のパーティションであるため、通常の Read/Write が行いますが、/(ルート)パーティションは、READONLY になります。

/boot パーティションも ReadOnly 設定にすることが望ましい場合には、同様に RO を追記してください。

```
#
# /etc/fstab
# Created by anaconda on Wed Sep 27 09:45:39 2017
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/centos-root    /          xfs     defaults,ro    0 0
UUID=UUID 番号           /boot      xfs     defaults        0 0
/dev/mapper/centos-home   /home      xfs     defaults        0 0
/dev/mapper/centos-swap   swap        swap    defaults        0 0
```

2. /etc/sysconfig/readonly-root を編集し、READONLY=yes,TEMPORARY_STATE=yes に設定する。

3. /etc/rwtab を編集し、ReadOnly 設定した中にある、書き込みを行う必要のある部分を追記する(例:/root 等ホームディレクトリを追記しないと、xlogin 出来ない)

備考

- サービスが起動しているか/var/log/boot.log ファイルを確認してください
[OK] Started Configure read-only root support.
- read-only で起動した後、何か書き込みたい時：
mount -o remount,rw /

表 題	ReadOnly 設定について	No PSG-20171115	版	1
			ページ	2/5

ReadOnly 設定の仕組み

RHEL/CentOS/RedHawk では、システム設定ファイルを変更することで、簡単に READONLY マウントを実現することが出来ます。

V6 系列では、`/etc/rc.d/rc.sysinit` から、V7 系列では、`/usr/lib/systemd/rhel-readonly` から、システムファイルのマウント動作が開始され、下記のファイルを READONLY 設定のために呼び出します。

V6 も V7 も、`grub` の起動時設定に `readonlyroot` を追記し、`/etc/sysconfig/readonly-root` を設定する事で READONLY になります。

● V6 系列: `/etc/rc.d/rc.sysinit`

```

readonly=
if [ -f /etc/sysconfig/readonly-root ]; then
    . /etc/sysconfig/readonly-root
fi
if strstr "$cmdline" readonlyroot ; then
    readonly=yes
    [ -z "$RW_MOUNT" ] && RW_MOUNT=/var/lib/stateless/writable
    [ -z "$STATE_MOUNT" ] && STATE_MOUNT=/var/lib/stateless/state
fi
if strstr "$cmdline" noreadonlyroot ; then
    readonly=no
fi

```

`/etc/sysconfig/readonly-root` の結果で yes になる

ReadOnly 設定に加えて一部を RW マウントにする

● V7 系列: `/usr/lib/systemd/rhel-readonly`

```

#!/bin/bash
#
# Set up readonly-root support.
#
:
:
# Only read this once.
[ -z "${cmdline}" ] && cmdline=$(cat /proc/cmdline)
readonly=
if [ -f /etc/sysconfig/readonly-root ]; then
    . /etc/sysconfig/readonly-root
fi
if strstr "$cmdline" readonlyroot ; then
    readonly=yes
    [ -z "$RW_MOUNT" ] && RW_MOUNT=/var/lib/stateless/writable
    [ -z "$STATE_MOUNT" ] && STATE_MOUNT=/var/lib/stateless/state
fi
if strstr "$cmdline" noreadonlyroot ; then
    readonly=no
fi
:

```

`/etc/sysconfig/readonly-root` の結果で yes になる

ReadOnly 設定に加えて一部を RW マウントにする

表題	ReadOnly 設定について	No PSG-20171115	版 1 ページ 3/5
----	-----------------	--------------------	----------------------

/etc/sysconfig/readonly-root

● デフォルト設定

```
# cat /etc/sysconfig/readonly-root
# Set to 'yes' to mount the system filesystems read-only.
READONLY=no
# Set to 'yes' to mount various temporary state as either tmpfs
# or on the block device labelled RW_LABEL. Implied by READONLY
TEMPORARY_STATE=no
# Place to put a tmpfs for temporary scratch writable space
RW_MOUNT=/var/lib/stateless/writable
# Label on local filesystem which can be used for temporary scratch space
RW_LABEL=stateless-rw
# Options to use for temporary mount
RW_OPTIONS=
# Label for partition with persistent data
STATE_LABEL=stateless-state
# Where to mount to the persistent data
STATE_MOUNT=/var/lib/stateless/state
# Options to use for persistent mount
STATE_OPTIONS=
```

上記の設定の通り、READONLY=no 、TEMPORARY_STATE=no です。

ここで、TEMPORARY_STATE は、いわゆる TEMPFS（RAM ディスク）を ON/OFF させる仕組みです。

つまり、ディスク全体を READONLY に設定しておき、Read/Write を行う必要のある部分だけ、TEMPFS を使用し、その初期値（ファイルの内容）は、READONLY のディスクからコピーする仕組みです。

● READONLY 設定

READONLY 設定では、この2つの設定が共に yes になります。

```
# cat /etc/sysconfig/readonly-root
# Set to 'yes' to mount the system filesystems read-only.
READONLY=yes
# Set to 'yes' to mount various temporary state as either tmpfs
# or on the block device labelled RW_LABEL. Implied by READONLY
TEMPORARY_STATE=yes
# Place to put a tmpfs for temporary scratch writable space
RW_MOUNT=/var/lib/stateless/writable
# Label on local filesystem which can be used for temporary scratch space
RW_LABEL=stateless-rw
# Options to use for temporary mount
RW_OPTIONS=
# Label for partition with persistent data
STATE_LABEL=stateless-state
# Where to mount to the persistent data
STATE_MOUNT=/var/lib/stateless/state
# Options to use for persistent mount
STATE_OPTIONS=
```

表題	ReadOnly 設定について	No	PSG-20171115	版	1
				ページ	4/5

● TEMPFS 設定

次に TEMPFS の設定は、/etc/rwtab で行います。このファイルでは、作成するディレクトリ(dirs)、空のファイル(empty)、コピーするファイル(files)の定義を行います。

dirs	/var/cache/man
dirs	/var/gdm
dirs	/var/lib/xkb
dirs	/var/lock
dirs	/var/log
dirs	/var/run
dirs	/var/puppet
dirs	/var/lib/dbus
dirs	/var/lib/nfs
empty	/tmp
empty	/var/cache/foomatic
empty	/var/cache/hald
empty	/var/cache/logwatch
empty	/var/cache/mod_ssl
empty	/var/cache/mod_proxy
empty	/var/cache/php-pear
empty	/var/cache/systemtap
empty	/var/db/nsd
empty	/var/lib/dav
empty	/var/lib/dhcp
empty	/var/lib/dhclient
empty	/var/lib/php
/empty	/var/lib/pulse
empty	/var/lib/ups
empty	/var/tmp
empty	/var/tux
empty	/media
files	/etc/adjtime
files	/etc/ntp.conf
files	/etc/resolv.conf
files	/etc/lvm/.cache
files	/etc/lvm/archive
files	/etc/lvm/backup
files	/var/account
files	/var/arpwatch
files	/var/cache/alchemy
files	/var/lib/gdm
files	/var/lib/iscsi
files	/var/lib/logrotate.status
files	/var/lib/ntp
files	/var/lib/xen
files	/var/lib/xend
files	/var/empty/ssh/etc/localtime
files	/var/lib/random-seed
files	/var/spool
files	/root
files	/home

ログインディレクトリを追記しないと
X でログイン出来ない

注意

- この内容は、システムが停止した場合には、すべて失われることに注意してください。
- また、READONLY 設定にすると、その起動ディスクでは、以後変更することは出来ません。
- 起動時にディスクから TEMPFS にコピーするため、起動時間が増加します。

もし、ファイルシステムの一部を通常のディスクとしてマウントする場合には、/etc/fstab 中の記述を行ってください。

表題	ReadOnly 設定について	No	PSG-20171115	版	1
				ページ	5/5