

Arcserve Replication and High Availability PowerShell スクリプト実行ガイド

Rev2.0

目次

Arcserve Replication and High Availability PowerShell スクリプト実行ガイド

はじめに.....	4
1. RHA PowerShell について.....	5
1.1. RHA PowerShell とは.....	5
1.2. 事前準備.....	5
1.3. 構成イメージ	6
2. RHA PowerShell のインストール.....	7
3. RHA PowerShell スクリプト実行手順	12
3.1. パスワードファイルの作成	13
3.2. RHA PowerShell スクリプトファイルの作成	15
3.3. RHA PowerShell スクリプトを呼び出すためのバッチスクリプトの作成	17
付録 : RHA PowerShell サンプルスクリプト	18
指定したシナリオを開始する	18
指定したシナリオを一時停止する	19
一時停止されたシナリオを再開する.....	19
指定したシナリオの同期処理を実行する	20
指定したシナリオを停止する	20
ホストメンテナンスを利用して、マスタサーバの再起動準備をする	21
その他参考情報	22

改訂履歴

2014/09 r16.5 版 初版リリース

2014/10 製品名変更に伴う修正

2015/10 サンプルスクリプトに RHA コントロールサービスからの切断コマンドを追加

2022/01 18.0 ベースに改訂 (Rev2.0)

すべての製品名、サービス名、会社名およびロゴは、各社の商標、または登録商標です。

本ガイドは情報提供のみを目的としています。Arcserve は本情報の正確性または完全性に対して一切の責任を負いません。Arcserve は、該当する法律が許す範囲で、いかなる種類の保証（商品性、特定の目的に対する適合性または非侵害に関する黙示の保証を含みます（ただし、これに限定されません））も伴わずに、このドキュメントを「現状有姿で」提供します。Arcserve は、利益損失、投資損失、事業中断、営業権の喪失、またはデータの喪失など（ただし、これに限定されません）、このドキュメントに関連する直接損害または間接損害については、Arcserve がその損害の可能性の通知を明示的に受けていた場合であっても一切の責任を負いません。

© 2022 Arcserve (USA), LLC. All rights reserved.

はじめに

このドキュメントは Arcserve Replication and High Availability 18.0（以降 Arcserve RHA と表記）の Arcserve RHA PowerShell（以降 RHA PowerShell と表記）について、そのインストール方法やスクリプトの実行方法を解説します。

◆ドキュメントおよびサンプルスクリプト利用規定

このドキュメントに記載される内容やスクリプト利用にあたっての規定事項です。スクリプト利用の前に必ず一度お読みください。なお、この利用規定は巻末に記載している「付録：RHA PowerShell サンプルスクリプト」についても同様です。

1. このドキュメントは Microsoft Windows PowerShell（以降、Windows PowerShell と表記）について知識をお持ちの方を読者と想定しています。Windows PowerShell の詳細についてはマイクロソフト社の Web サイトなどで事前にご確認ください。
2. このドキュメントで紹介するスクリプトは全てサンプルです。利用の際には必ず事前検証を行い、希望する動作が正常に行われる事をご確認の上でご利用ください。
3. このドキュメントに記載されるスクリプトが、全ての環境で動作することは保障していません。
4. 改変・編集等は自由ですが、自己責任の上で実施してください。
5. このドキュメントに記載されるスクリプトを利用した事による直接あるいは間接的な損害も、著作者および Arcserve 社では一切の責任を負わないものとします。
6. このドキュメントは、Arcserve Replication and High Availability 18.0 SP3 をベースに作成しています。RHA PowerShell の一部のコマンドは Arcserve RHA の利用バージョンによっては利用できないことがあります。
7. この利用規定は予告なく改編・加筆を行うことがあります。

1. RHA PowerShell について

1.1. RHA PowerShell とは

RHA PowerShell は Windows PowerShell でスナップインとして動作する、Arcserve RHA の管理用コマンドラインインターフェースです。

RHA PowerShell はシナリオをコントロールするためのコマンドを提供します。例えばシナリオの開始や停止、一時停止/再開、スイッチオーバーの実行、同期の実行などを行う際に利用します。ただし、必ずしも Arcserve RHA マネージャと同様の機能を提供するものではありませんのでご注意ください。RHA PowerShell で利用できる機能の詳細については製品マニュアル「Arcserve Replication and High Availability PowerShell コマンド操作ガイド」をご参照ください。

1.2. 事前準備

Arcserve RHA PowerShell を利用するには、以下の事前準備が必要です。

(1) Arcserve RHA のインストール

Arcserve RHA PowerShell を利用して Arcserve RHA の管理をするには、事前に Arcserve RHA コントロールサービス(以降、コントロールサービスと表記) および Arcserve RHA エンジン (以降、エンジンと表記) のインストールを済ませておく必要があります。コントロールサービスおよびエンジンのインストールについては製品マニュアル「Arcserve Replication and High Availability インストール ガイド」をご参照ください。

(2) シナリオの作成

PowerShell で操作するためのシナリオを RHA マネージャで事前に作成し、シナリオ名を控えておきます。

シナリオは、GUI 上で事前に実行し、問題なく動作することを確認してください。

(3) スクリプト実行権限の設定（任意）

スクリプトを自動実行させるには権限の設定が必要な場合があります。以下の方法により環境で設定されている実行権限を確認し、必要に応じて変更してください。スクリプトを独自で開発して実行する場合には RemoteSigned がお勧めです。権限についての詳しい説明はマイクロソフト社の Web サイトなどを確認してください。

実行権限の確認方法

```
PS > Get-ExecutionPolicy
```

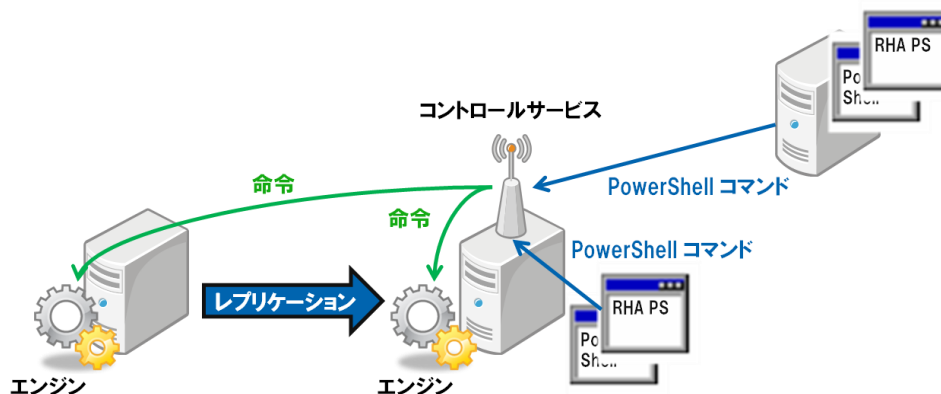
実行権限の設定方法（例）

```
PS > Set-ExecutionPolicy RemoteSigned
```

なお、このドキュメントでは上記の権限設定を行わない場合でも実行できる方法を記載します。

1.3. 構成イメージ

RHA PowerShell はコントロールサービスに接続して命令を実行します。そのため、RHA PowerShell はコントロールサービスと通信できるコンピュータにインストールしてご利用ください。以下は RHA PowerShell のコマンドがエンジンに渡り実行されるまでのイメージです。



このドキュメントではコントロールサービスがレプリカサーバに導入されている場合を想定して記載しますが、コントロールサービスがエンジンとは別のサーバに導入されている場合も RHA PowerShell コマンドの実行方法は同じです。

2. RHA PowerShell のインストール

以下の手順に従い RHA PowerShell をインストールします。

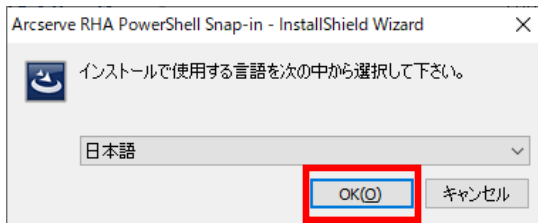
1. RHA PowerShell をインストールするコンピュータに、Administrator または Administrators グループのユーザでログオンし、「Arcserve Replication and High Availability メディア」をドライブにセットすると、インストーラ画面が自動的に起動します。起動しない場合は、エクスプローラより、メディアドライブのルート ディレクトリにある [setup.exe] を実行してください。[コンポーネントのインストール]をクリックします。



2. [PowerShell Snap-in のインストール] をクリックします。



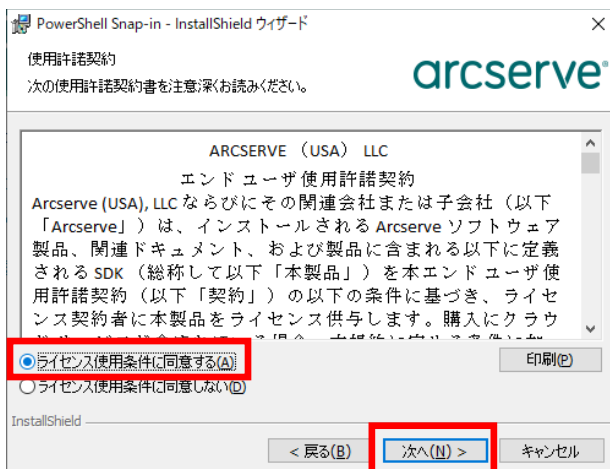
3. [日本語]が選択されていることを確認し、[OK]をクリックします。



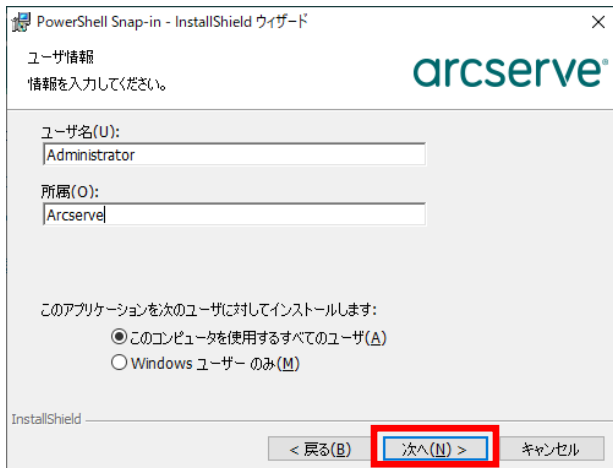
4. [次へ] をクリックします。



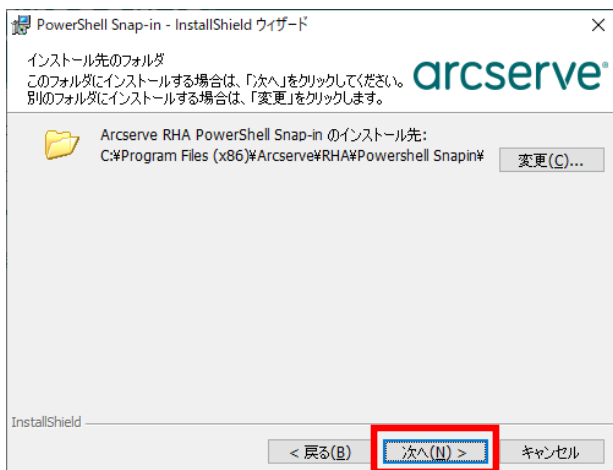
5. 使用許諾契約を最後まで確認し、同意する場合は[ライセンス使用条件に同意する]を選択し、[次へ]をクリックします。



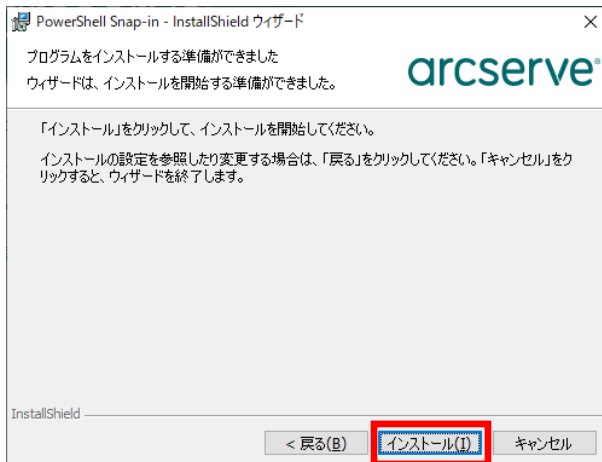
6. ユーザ名と所属を入力し、[次へ]をクリックします。



7. インストール先のフォルダを確認し、問題がなければ[次へ]をクリックします。



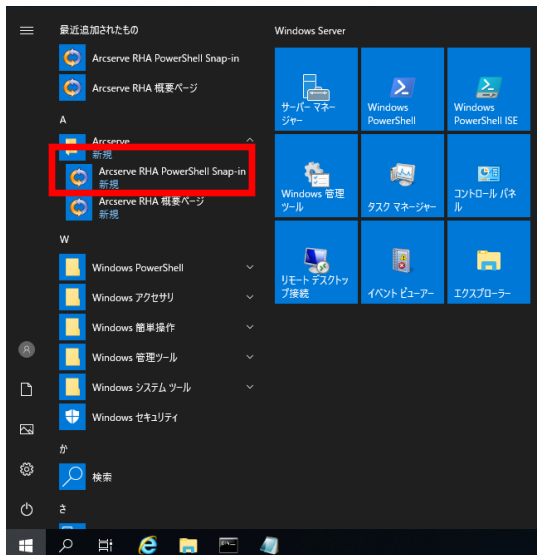
8. [インストール] をクリックします。



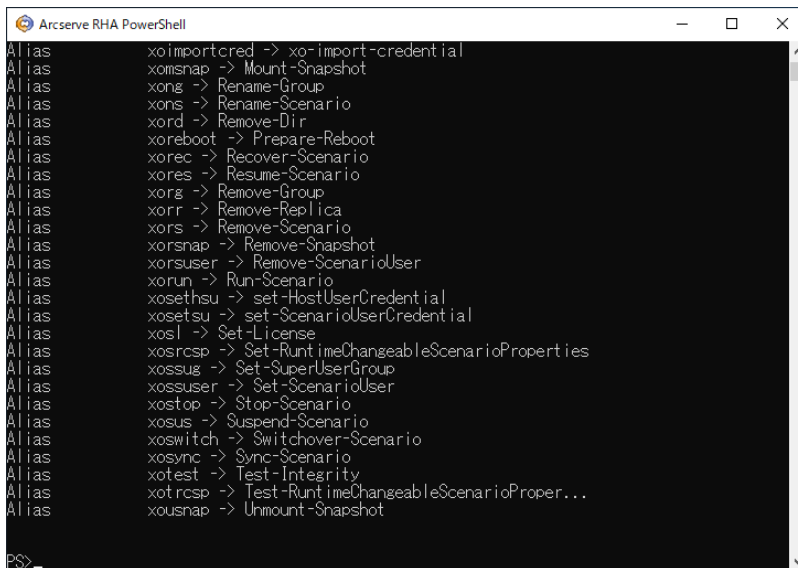
9. [完了] をクリックし、InstallShield Wizard 画面を閉じます。



10. Windows スタートメニューの、[Arcserve] - [Arcserve RHA PowerShell Snap-in]をクリックします。



11. RHA PowerShell のコンソール画面が表示され、エラーなく「PS>」と表示されることを確認します。



以上で RHA PowerShell のインストールは完了です。

3. RHA PowerShell スクリプト実行手順

RHA PowerShell スクリプトを実行してシナリオを操作・制御するために、以下の3つの手順を実行します。

1. [パスワードファイルの作成](#)

RHA PowerShell からコントロールサービスに接続する際に、ユーザ認証の操作やパスワードを入力せずに実行するため、接続に利用するユーザアカウント用に暗号化されたパスワードファイルを作成します。

2. [RHA PowerShell スクリプトファイルの作成](#)

RHA PowerShell のコマンドを利用したスクリプトファイルを作成します。RHA PowerShell コマンドの詳しい使用方法については、「Arcserve Replication and High Availability PowerShell コマンド 操作ガイド」をご覧ください。

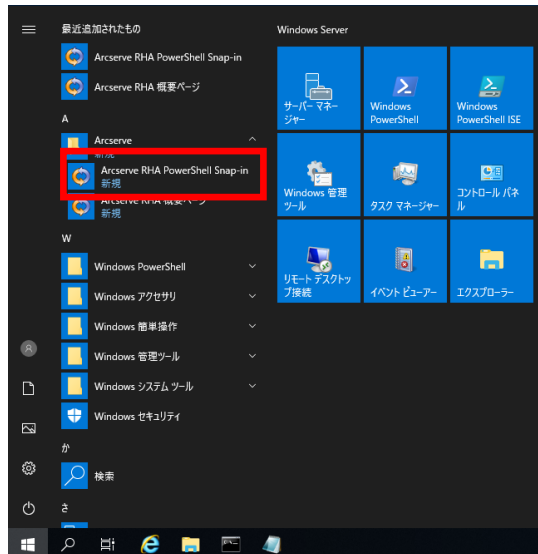
3. [RHA PowerShell スクリプトを呼び出すためのバッチスクリプトの作成](#)

PowerShell スクリプトはダブルクリックするだけでは実行できないため、作成した RHA PowerShell スクリプトを Windows 環境で呼び出すためのバッチスクリプトを作成します。Windows タスクスケジューラや他製品などから実行する場合などはこのバッチスクリプトを指定します。

3.1. パスワードファイルの作成

RHA PowerShell をインストールした環境で、以下の手順を実行します。

スタートメニューより、[Arcserve] - [Arcserve RHA PowerShell Snap-in]をクリックします。



以下のコマンドを実行します。

※ここではCドライブ直下にパスワードファイルを作成しています。任意の場所に作成してください。

```
PS> read-host -assecurestring | convertfrom-securestring | out-file C:¥securestring.txt
```

このコマンドを実行後、Enter キーを押下すると、文字の入力待ち状態となり、カーソルが一行下に移動します。

```
Alias          xosync -> Sync-Scenario
Alias          xotest -> Test-Integrity
Alias          xotrcsp -> Test-RuntimeChangeableScenarioProper...
Alias          xousnap -> Unmount-Snapshot

PS> read-host -assecurestring | convertfrom-securestring | out-file C:¥securestring.txt
```

コントロールサービスに接続するユーザアカウントのパスワードを入力します。パスワードはすべてアスタリスク（*）で表示されます。入力後、Enter キーを押下します。

```
Alias      xosync -> Sync-Scenario
Alias      xotest -> Test-Integrity
Alias      xotrcsp -> Test-RuntimeChangeableScenarioProper...
Alias      xousnap -> Unmount-Snapshot

PS>read-host -assecurestring | convertfrom-securestring | out-file C:\%securestring.txt
*****
```

C ドライブ直下に securestring.txt というファイルが作成されていることを確認してください。

※このファイルは、移動してもファイル名を変更しても構いませんが、中身は編集しないでください。



【重要】 パスワードファイルはスクリプト実行に必要なファイルです。RHA PowerShell スクリプトを実行するマシンを移動する場合には、パスワードファイルを移動した先のサーバにて再作成してください。

3.2. RHA PowerShell スクリプトファイルの作成

(1) RHA PowerShell スクリプトファイルを作成します。

テキストを任意の場所に作成し、以下のコマンドを記述します。

```
1: add-pssnapin XOPowerShell  
2: $pass = cat C:¥securestring.txt | convertto-securestring  
3: $mycred = new-object -typename System.Management.Automation.PSCredential  
   -Argumentlist "<ドメイン名>¥<ユーザ名>",$pass  
4: connect-xo -host <コントロールサービス導入サーバのホスト名または IP アドレス> $mycred  
   -protocol <HTTP もしくは HTTPS>
```

注1: 上記サンプルの左側の数字は段落番号です。スクリプトを記述する際は無視してください。

注2: Workgroup 環境で実行する場合にはドメイン名の代わりにコントロールサービス導入サーバのホスト名を入力します。

注3: 斜体文字は環境に合わせて適宜変更してください。

(2) 上記スクリプトに続けてシナリオ操作を行う RHA PowerShell コマンドを記述します。

例) 「FileServer」という名前のシナリオを実行する

Run-scenario -Name "FileServer" -Mode F -Ignore 1

(3) コントロールサービスから切断する Disconnect-XO コマンドを追加して内容を保存し、このファイルの拡張子を「.ps1」に変更します。

スクリプトファイルの例: run_scenario.ps1

```
1: add-pssnapin XOPowerShell  
2: $pass = cat C:¥securestring.txt | convertto-securestring
```

```
3: $mycred = new-object -typename System.Management.Automation.PSCredential  
   -Argumentlist "Administrator",$pass  
4: connect-xo -host Replica $mycred -protocol http  
5: Run-scenario -Name "FileServer" -Mode F -Ignore 1  
6: Disconnect-XO
```


3.3. RHA PowerShell スクリプトを呼び出すためのバッチスクリプトの作成

RHA PowerShell スクリプトファイルを呼び出すバッチスクリプトを作成します

- (1) 以下のコマンドをコマンド プロンプトで 1 度実行し、スクリプトが正常に実行できるかを確認してください。引数の最後に、作成した PowerShell スクリプトファイルを直接パスで指定します。

```
C:¥Windows¥SysWOW64¥WindowsPowerShell¥v1.0¥powershell.exe -Noninteractive -  
command set-executionpolicy RemoteSigned; <.ps1 ファイルへの直接パス>
```

例) run_scenario.ps1 ファイルを実行する場合

```
C:¥Windows¥SysWOW64¥WindowsPowerShell¥v1.0¥powershell.exe -Noninteractive -  
command set-executionpolicy RemoteSigned; C:¥script¥powershell¥run_scenario.ps1
```

- (2) 上記 (1) のコマンドをテキストファイルに保存します。その際、スクリプトのパス以外の引数はすべて削除します。（「- Noninteractive -command set-executionpolicy RemoteSigned;」を削除）

例)

```
C:¥Windows¥SysWOW64¥WindowsPowerShell¥v1.0¥powershell.exe <.ps1 ファイルへの直接パス>
```

- (3) ファイルの拡張子を.bat などに変更します。

以上で RHA PowerShell スクリプトを実行するために必要なファイルが作成できました。必要に応じて作成したバッチスクリプトを実行するアプリケーションや Windows タスク スケジューラに登録します。

付録：RHA PowerShell サンプルスクリプト

RHA PowerShell サンプルスクリプトです。ここでご紹介するサンプルは全て以下の設定を元に記載しています。環境に応じて適宜変更してください。

注：スクリプトの左側の番号は段落番号です。スクリプト利用時には必要ありませんので削除してください。

【想定環境】

- ① 環境：Workgroup
- ② マスタサーバ名：Master
- ③ レプリカサーバ名：Replica
- ④ コントロールサービス導入サーバ名：Replica
- ⑤ コントロールサービス接続プロトコル：http
- ⑥ コントロールサービス接続ユーザ：Administrator
- ⑦ パスワードファイルパス：C:¥securestring.txt
- ⑧ シナリオ名：FileServer

指定したシナリオを開始する

run_scenario.ps1

```
7: add-pssnapin XOPowerShell
8: $pass = cat C:¥securestring.txt | convertto-securestring
9: $mycred = new-object -typename System.Management.Automation.PSCredential
    -Argumentlist "Administrator",$pass
10: connect-xo -host Replica $mycred -protocol http
11: Run-scenario -Name "FileServer" -Mode F -Ignore 1
12: Disconnect-XO
```

指定したシナリオを一時停止する

suspend.ps1

```
1: add-pssnapin XOPowerShell
2: $pass = cat C:¥securestring.txt | convertto-securestring
3: $mycred = new-object -typename System.Management.Automation.PSCredential
   -Argumentlist "Administrator",$pass
4: connect-xo -host Replica $mycred -protocol http
5: Suspend-Scenario -Name "FileServer" -Host Replica
6: Disconnect-XO
```

一時停止されたシナリオを再開する

resume.ps1

```
1: add-pssnapin XOPowerShell
2: $pass = cat C:¥securestring.txt | convertto-securestring
3: $mycred = new-object -typename System.Management.Automation.PSCredential
   -Argumentlist "Administrator",$pass
4: connect-xo -host Replica $mycred -protocol http
5: resume-Scenario -Name "FileServer" -Host Replica
6: Disconnect-XO
```

指定したシナリオの同期処理を実行する

(ファイルレベル同期、同一サイズ/タイムスタンプのファイルを無視)

sync_scenario.ps1

```
1: add-pssnapin XOPowerShell  
2: $pass = cat C:¥securestring.txt | convertto-securestring  
3: $mycred = new-object -typename System.Management.Automation.PSCredential  
   -Argumentlist "Administrator",$pass  
4: connect-xo -host Replica $mycred -protocol http  
5: Sync-Scenario -Name "FileServer" -Mode F -Ignore 1  
6: Disconnect-XO
```

指定したシナリオを停止する

stop_senario.ps1

```
1: add-pssnapin XOPowerShell  
2: $pass = cat C:¥securestring.txt | convertto-securestring  
3: $mycred = new-object -typename System.Management.Automation.PSCredential  
   -Argumentlist "Administrator",$pass  
4: connect-xo -host Replica $mycred -protocol http  
5: Stop-Scenario -Name "FileServer"  
6: Disconnect-XO
```

ホストメンテナンスを利用して、マスタサーバの再起動準備をする

Reboot_master.ps1

```
1: add-pssnapin XOPowerShell
2: $pass = cat C:¥securestring.txt | convertto-securestring
3: $mycred = new-object -typename System.Management.Automation.PSCredential
   -Argumentlist "Administrator",$pass
4: connect-xo -host Replica $mycred -protocol http
5: Prepare-Reboot Master
6: $i = 0
7: Start-Sleep -s 60
8: Do {$i = $i + 1;if(get-events "FileServer" |Select -last $i |Select ID |Select-String
   "SR00393" -quiet){$i = 0;start-sleep -s 60} } Until (get-events "FileServer" |Select -
   last $i |Select ID |Select-String "IR00556" -quiet)
9: Write-Host “再起動の準備ができました”
10: Disconnect-XO
```

注：6～8 行目は、再起動の準備が整ったことを、イベントログから確認しています

その他参考情報

RHA PowerShell スクリプトで問題が発生する場合は、RHA PowerShell 画面で同じ内容のコマンドを実行しスクリプトの内容に問題ないことを確認してください。

また、以下の技術文書も参照してください。

◎UAC が有効な環境で Arcserve RHA PowerShell が正常起動しない

<https://support.arcserve.com/s/article/204814959?language=ja>

◎r16.5 SP7 以降の "Arcserve RHA PowerShell" が CLRVersion の相違により Windows 2008/R2 で動作しない

<https://support.arcserve.com/s/article/360000108543?language=ja>

◎Arcserve Replication/High Availability のアップグレードについて

<https://support.arcserve.com/s/article/2020100801?language=ja>