



VENE Snap Automation Tool – ActiveCluster 3rd Site Replication

Benutzerhandbuch

Inhalt

1.	Vorwort	3
2.	System Anforderungen.....	3
3.	Script-Verzeichnis	4
3.1.	config.xml	4
3.2.	encryptAES.ps1.....	5
3.2.1.	Parameter	5
3.3.	functions.psm1	5
3.4.	podbackup.ps1	5
3.4.1.	Parameter	5
4.	Installation	6
5.	Betrieb	8
6.	Logik.....	9
6.1.	Haupt Prozess	9
6.2.	FlashArray prechecking	10
6.3.	Cloning the volumes and prepare to transfer	11
6.4.	Cleaning up	12
6.5.	Target FlashArray - Volume create and apply retention	12
7.	Beispiele	13
7.1.	encryptAES.ps1	13
7.2.	podbackup.ps1	15

1. Vorwort

Das Skript wurde für die Automatisierung des VM-Backups entwickelt, um die Datastores auf ein Pure Storage ActiveCluster System abzuliegen.

Während des Skript-Laufs werden VM-Snapshots erstellt. Nach der erfolgreichen VM-Snapshot-Erstellung wird ein POD-Kopie gemacht. Die Volumes der POD-Kopie werden in einer asynchron Protection Group hinzugefügt, und die Protection Group wird auf die Backup-Seite repliziert.

2. System Anforderungen

- Windows 8 Pro, Enterprise 64 bit
 - Windows 8.1 Pro, Enterprise 64 bit
 - Windows 10 Pro, Enterprise 64 bit
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016
-
- Windows Management Framework 3.0
 - Windows Management Framework 4.0
 - Windows Management Framework 5.0
 - Windows Management Framework 5.1
-
- .NET Framework 4.5
 - .NET Framework 4.6
 - .NET Framework 4.7
-
- VMware vSphere PowerCLI 6.0
 - VMware vSphere PowerCLI 6.3
 - VMware PowerCLI 6.5
-
- PureStoragePowerShellSDK 1.7.4.0

3. Script-Verzeichnis

Length Name

```
648 config.xml
1066 encryptAES.ps1
3972 functions.psm1
19481 podbackup.ps1
```

3.1. config.xml

Die Konfigurationsdatei ist eine XML-Datei. Alle Felder müssen ausgefüllt werden!

Es gibt 3 Sektionen:

<general>

<KeyFile>AES.key</KeyFile> - Mit der Datei wird das Passwort ver- und entschlüsselt. Die Datei existiert vor der ersten Benutzung nicht. Der encryptAES.ps1 generiert auch die Schlüsseldatei.

<FlashArray>

<SourceArray></SourceArray> - Ein Mitglied von ActiveCluster. Domainname oder IP-Adresse

<TargetArray></TargetArray> - Der Ziel-Array. Domainname oder IP-Adresse

<User>pureuser</User> - Benutzername. In dieser Sektion sind FlashArray und VMware auch verfügbar.

<SecureFile>SecFileFA.txt</SecureFile> - Diese Datei enthält das verschlüsselte Passwort für den Benutzernamen. In der Sektion FlashArray und VMware ist dies auch verfügbar.

<POD></POD> - Name des PODs, der auf das Backup-System (2nd Array) repliziert wird.

<WaitTransferSeconds>60</WaitTransferSeconds> - Während der Replikation muss so viele Sekunde gewartet werden bis zur nächste Abfrage.

<TargetPrefix>COPY</TargetPrefix> - Die Volumenamen werden bei der Backup-Seite mit folgendem Präfix beginnen. **Achtung!** Das Präfix ist nötig, um die Vorhaltezeit der Volumes zu verwalten!

<TargetRetention>28</TargetRetention> - Anzahl der zurückgehaltenen Volume-Kopien bei der Backup-Seite.

<vmware>

<vCenter></vCenter> - Die vCenter Domainname oder IP-Adresse

<User></User> - Benutzername. Dies ist auch In der Sektion FlashArray und VMware verfügbar.

<SecureFile>SecFileVC.txt</SecureFile> - Diese Datei enthält das verschlüsselte Passwort für den Benutzernamen. Auch dies ist in der Sektion FlashArray und VMware verfügbar.

<Datastores> - Unter dem Tag ist es möglich die Datastores zu definieren. Mehrere Datastores sind auch möglich.

<DatastoreName></DatastoreName> - Name des Datastores.

<WaitTaskSeconds>10</WaitTaskSeconds> - So viele Sekunde wird gewartet vor der Überprüfung der VM-Snapshot-Erstellung.

3.2. encryptAES.ps1

Diese Datei wird für die Erstellung der verschlüsselten Passwort-Datei und Schlüssel-Datei benutzt. Nur bei Installation ist dies nötig, oder bei Änderung des Passworts.

3.2.1. Parameter

- KeyFile <File name> → Optional, wenn der Default-Wert passend ist. Default-Wert: AES.key
- NewKeyRequired → Optional. Switch Parameter. Wenn angegeben ist, dann wird die Schlüsseldatei neu generiert. **Achtung! Bei neu Erstellung der Schlüsseldatei müssen alle Passwort-Dateien neu generiert werden!**
- NewSecurePasswordFile <File name> → Optional, wenn der Default-Wert passend ist. Default-Wert: SecFileFA.txt
- Password <Password> → Obligatorisch

3.3. functions.psm1

Das enthält die Funktionen. Die Datei muss im Skript-Verzeichnis existieren!

3.4. podbackup.ps1

Haupt-Skript. Mit Aufruf wird der komplette Backup-Prozess durchgeführt.

3.4.1. Parameter

- Config <File name> → Optional, wenn der Default-Wert passend ist. Default-Wert: config.xml
- ApplyRetention → Optional. Switch Parameter. Wenn dieser angegeben ist, dann werden die Kopien vorgehalten und aktiviert.
- OverwriteStandaloneTarget → Optional. Switch Parameter. Wenn dieser angegeben ist, dann wird das eigenständige Volume von Volume-Kopien überschrieben.

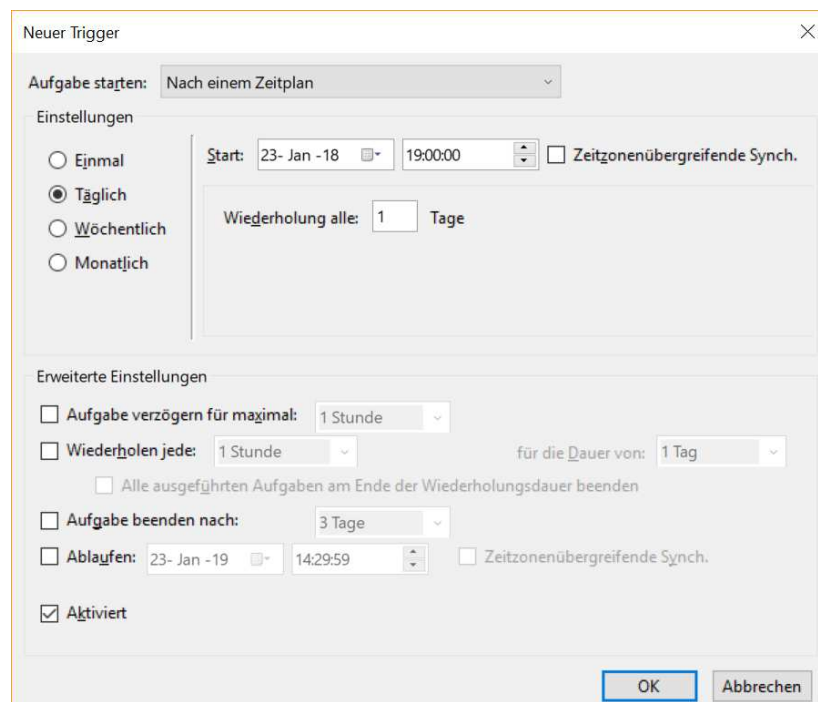
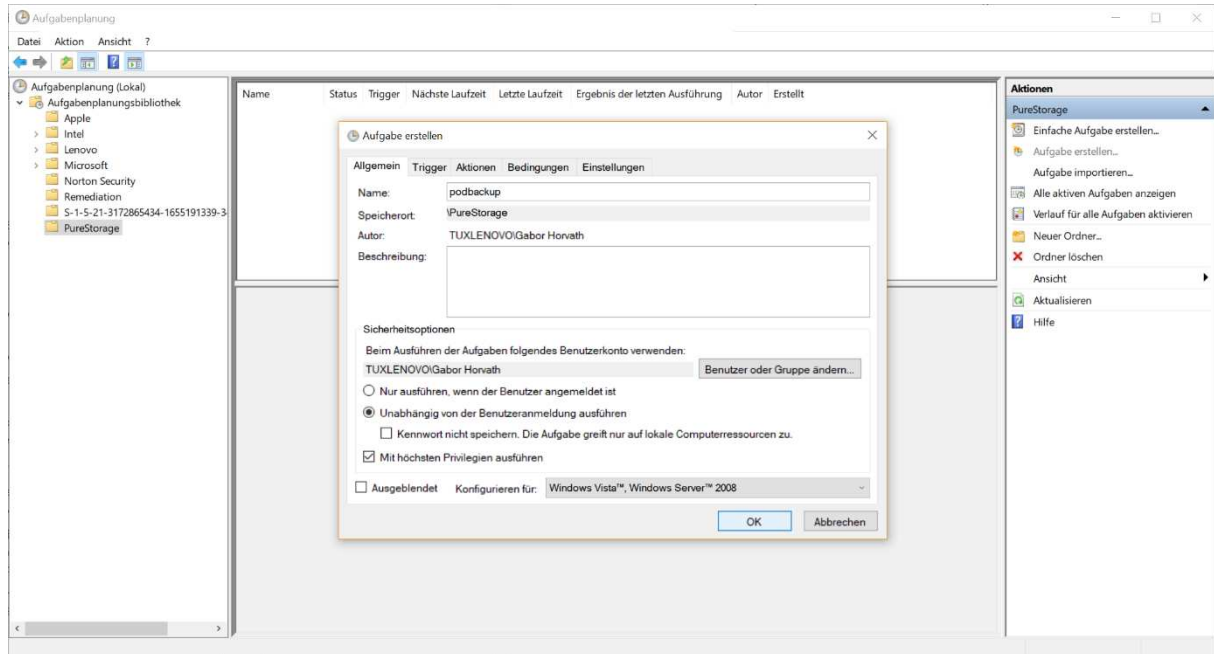
4. Installation

Das komplette Skript wird in einer ZIP-Datei bereitgestellt. In ersten Schritt bitte die ZIP-Datei überprüfen mit Hilfe von Validierungsdatei sha1. Die komprimierte Datei im Zielordner extrahieren.

Die Konfigurationsdatei muss sorgfältig ausgefüllt werden! (config.xml)

Mit Hilfe von Skript encryptAES.ps1 können Sie die Schlüssel- und die Passwortdateien erstellen.

Sie können jetzt das Skript mit den bestimmten Parametern zum Windows Task Scheduler hinzufügen.



```
powershell.exe  
-Command ". '.\podbackup.ps1' -ApplyRetention; exit $LASTEXITCODE"
```

Neue Aktion

Geben Sie die Aktion an, die von der Aufgabe ausgeführt werden soll.

Aktion: Programm starten

Einstellungen

Programm/Skript:
powershell.exe Durchsuchen...

Argumente hinzufügen (optional):
-Command ". '.\podbacku

Starten in (optional):
C:\VENE

OK Abbrechen

5. Betrieb

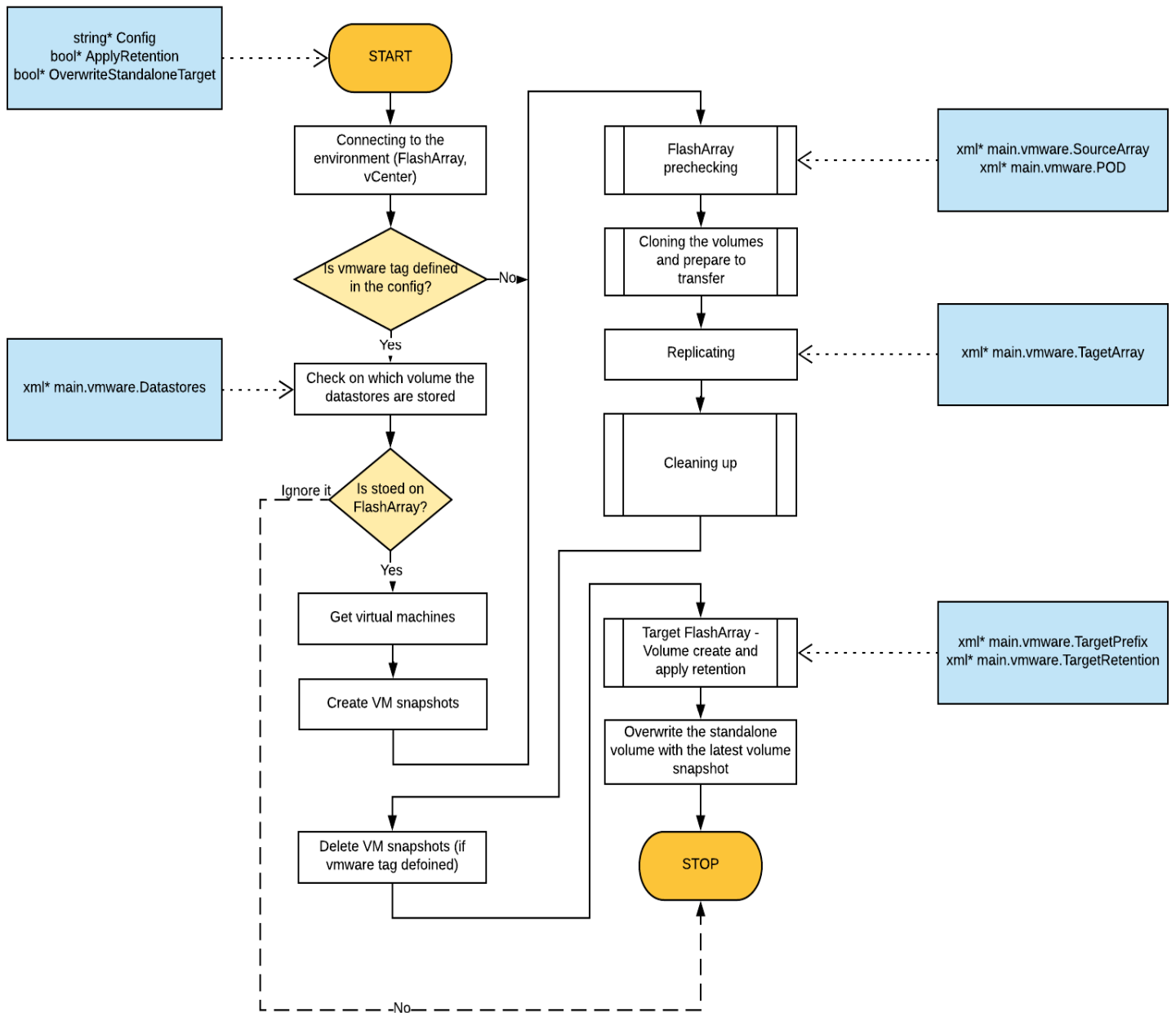
Der Task Scheduler ruft das Skript auf. Das Skript generiert eine LOG-Datei bei jedem Lauf (runlog_yyyyMMdd_HHmss.log). Die LOG-Datei enthält eine sehr detaillierte Information (DEBUG).

Return-Code Tabelle:

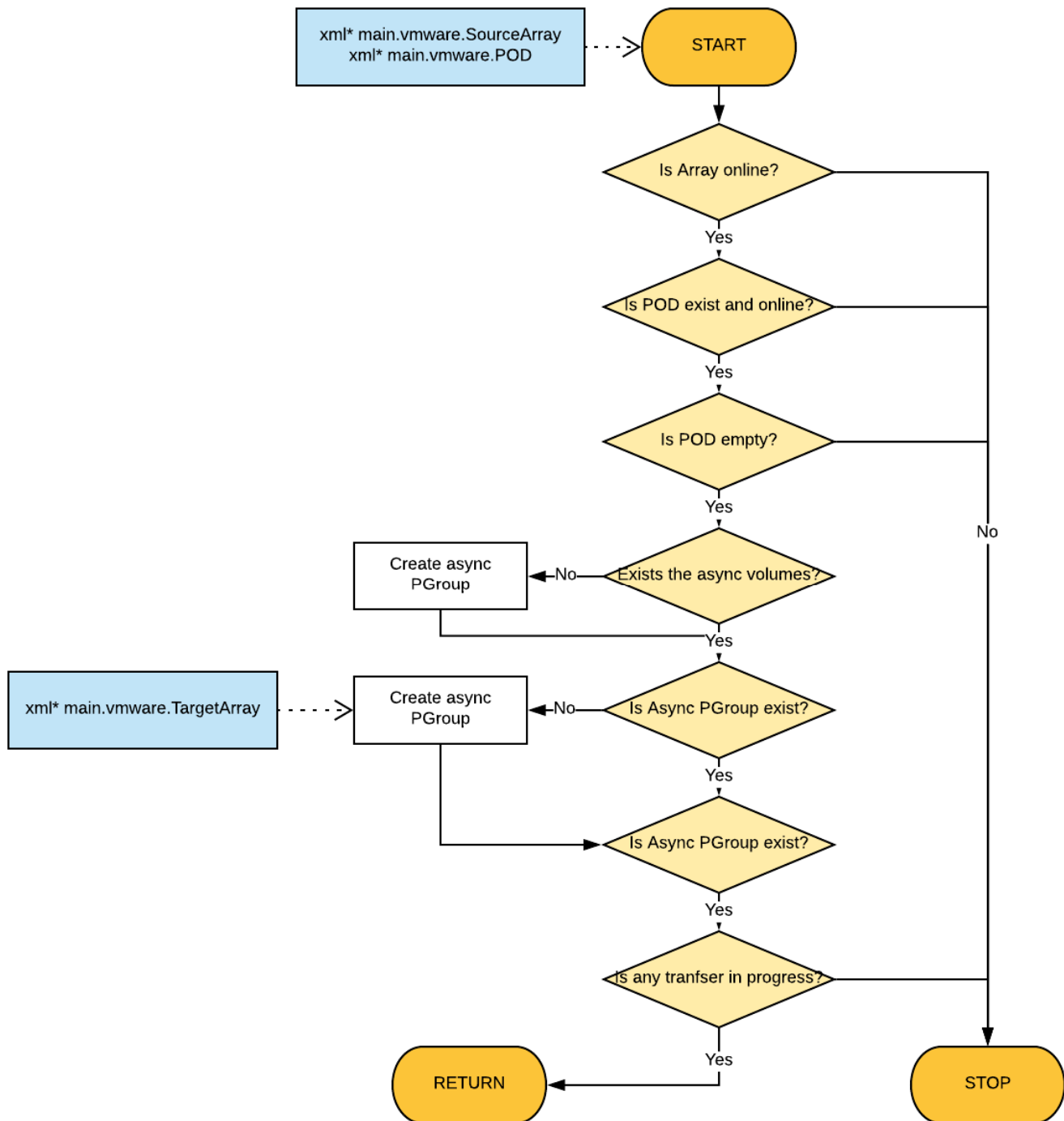
Return Code	Nachricht	Bemerkung
0	-	Keine Fehlermeldung. Das Skript ist in Ordnung gelaufen.
26	The POD '<POD>' is not healthy! Please repair it!	
27	The POD is empty or doesn't exists! POD: <POD>	
28	The clone POD doesn't exist or no volumes copied! POD: <POD>-podbackup	
33	Transfer is processing! Try again later!	
51	The source array isn't online!	
120		Allgemeine Fehlermeldung. Es kommt von FlashArray
125	All datastores has issues! Please check the logfile '<LOGFILE>'	
197	The Host or HostGroup isn't defined in the config file!	
266		Nicht erfolgreiche Replikation. Die Fehlermeldung von FlashArray
322	There is no target snapshot of ProtectionGroup '<SOURCE>:<POD>-async'!	

6. Logik

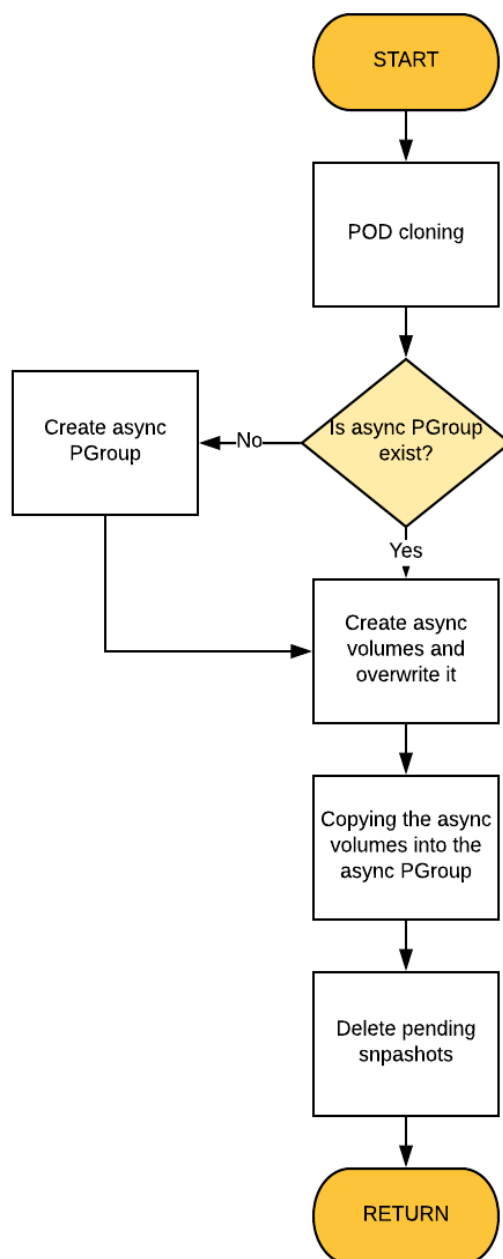
6.1. Haupt Prozess



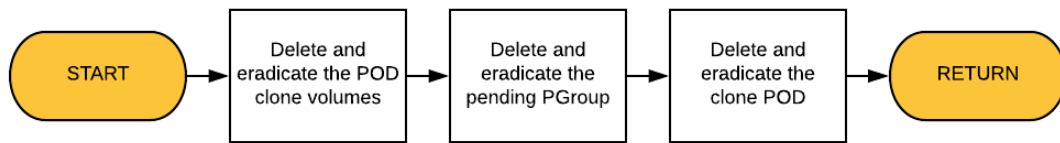
6.2. FlashArray prechecking



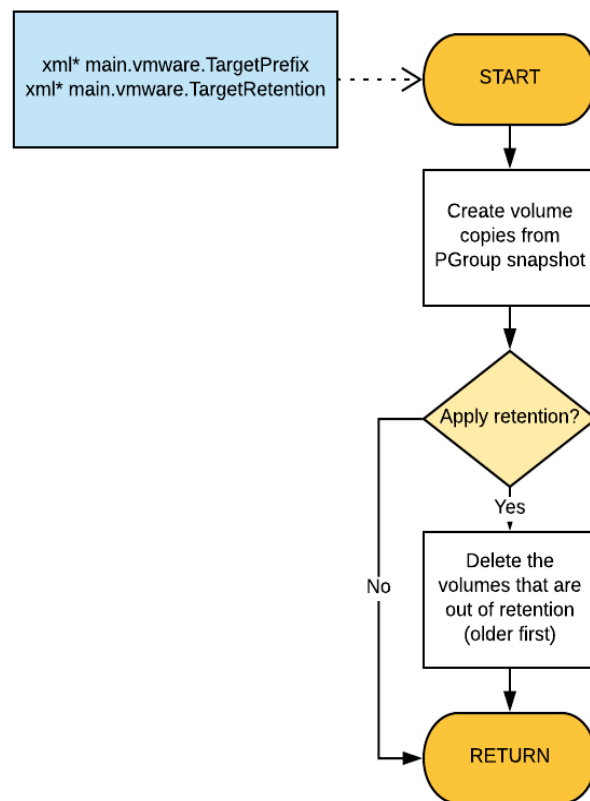
6.3. Cloning the volumes and prepare to transfer



6.4. Cleaning up



6.5. Target FlashArray - Volume create and apply retention



7. Beispiele

7.1. encryptAES.ps1

Erster Aufruf:

```
Windows PowerShell
PS C:\VENE> Get-ChildItem

Verzeichnis: C:\VENE

Mode                LastWriteTime         Length Name
----                -
-a----          21-Jan-18         16:53             648 config.xml
-a----          23-Jan-18         11:22            1015 encryptAES.ps1
-a----          22-Jan-18         10:25            3972 functions.psm1
-a----          22-Jan-18         12:15           19481 podbackup.ps1

PS C:\VENE> .\encryptAES.ps1 -NewKeyRequired -Password 'P4$$w0rd'
76492d1116743f0423413b16050a5345MgB8ADEARQB4AG8AMgBTAFAAUwB3ADMAWgBNAFAAbQBjAGMAYgBIAGSAAQBOAHCAPQA9AHwAYwBjADEAOABhAGUA
NABhAGIAYwBhADKANQA1AGYAQQAYADMANQA5AGUAMgA3AGIAYgA2AGEANwA1ADgAQQAADCAMQBjADIAZQBjAGUANABmADUAMwAYAGIAYwBmADUAAQA1ADgA
ZgA4ADEAZAA1AGIAOQA4ADQAMgBjAGEAYWA=
PS C:\VENE> Get-ChildItem

Verzeichnis: C:\VENE

Mode                LastWriteTime         Length Name
----                -
-a----          23-Jan-18         11:44             298 AES.key
-a----          21-Jan-18         16:53             648 config.xml
-a----          23-Jan-18         11:22            1015 encryptAES.ps1
-a----          22-Jan-18         10:25            3972 functions.psm1
-a----          22-Jan-18         12:15           19481 podbackup.ps1
-a----          23-Jan-18         11:44             558 SecFileFA.txt

PS C:\VENE> Get-Content .\SecFileFA.txt
76492d1116743f0423413b16050a5345MgB8AGYAKwBEAEANQB0AHQAQBIAEUAMAAVAEOANQA2AEwAZABVAEMAOQBQAEAPQA9AHwAZQBjAGYAMQBjAGMAMAA2AGMANQBjAGIAOQBjAD
MANABKAGEAZgAXADUANQAXADIAMAAZADgAMwBmAGUAZAAYADkAYwA3ADkAZQBjADEAOAAyADgAQQA2AGMANQA1ADMAOQBmADAAOQBmAGYANGBjADAAMAAGUAMQBjAGMANWA=
PS C:\VENE>
```

Erster Aufruf ohne Parameter:

```
Windows PowerShell
PS C:\VENE> Get-ChildItem

Verzeichnis: c:\VENE

Mode                LastWriteTime         Length Name
----                -
-a----          21-Jan-18         16:53             648 config.xml
-a----          23-Jan-18         12:45            1021 encryptAES.ps1
-a----          22-Jan-18         10:25            3972 functions.psm1
-a----          22-Jan-18         12:15           19481 podbackup.ps1

PS C:\VENE> .\encryptAES.ps1 -NewKeyRequired

Cmdlet encryptAES.ps1 an der Befehlspipelineposition 1
Geben Sie Werte für die folgenden Parameter an:
Password: P4$$w0rd
76492d1116743f0423413b16050a5345MgB8AGYAKwBEAEANQB0AHQAQBIAEUAMAAVAEOANQA2AEwAZABVAEMAOQBQAEAPQA9AHwAZQBjAGYAMQBjAGMAMAA2AGMANQBjAGIAOQBjAD
MANABKAGEAZgAXADUANQAXADIAMAAZADgAMwBmAGUAZAAYADkAYwA3ADkAZQBjADEAOAAyADgAQQA2AGMANQA1ADMAOQBmADAAOQBmAGYANGBjADAAMAAGUAMQBjAGMANWA=
PS C:\VENE> Get-ChildItem

Verzeichnis: C:\VENE

Mode                LastWriteTime         Length Name
----                -
-a----          23-Jan-18         12:52             302 AES.key
-a----          21-Jan-18         16:53             648 config.xml
-a----          23-Jan-18         12:45            1021 encryptAES.ps1
-a----          22-Jan-18         10:25            3972 functions.psm1
-a----          22-Jan-18         12:15           19481 podbackup.ps1
-a----          23-Jan-18         12:52             558 SecFileFA.txt

PS C:\VENE>
```

Erster Aufruf mit einer anderen Schlüssel-Datei und einer anderen Passwort-Datei:

```
Windows PowerShell
PS C:\VENE> Get-ChildItem

Verzeichnis: C:\VENE

Mode                LastWriteTime         Length Name
----                -
-a----          21-Jan-18         16:53           648 config.xml
-a----          23-Jan-18         12:45          1021 encryptAES.ps1
-a----          22-Jan-18         10:25          3972 functions.psm1
-a----          22-Jan-18         12:15          19481 podbackup.ps1

PS C:\VENE> .\encryptAES.ps1 -keyFile AES_keyfile.txt -NewKeyRequired -NewSecurePasswordFile SecPass.txt -Password 'P4ssw0rd!'
76492d1116743f0423413b16050a5345MgB8AHQAVWbNAcsAcQBhAFYAUQBWAHAUQBRADUANABWAGYAdQBWAE0AVQBUAHcAPQA9AHWANGB1AGUAQOBmADgANABiADgAMwA5AGUAMwAWAG
EAYQAZADgAZABkADgAMABKADcAQQBmAGQAOABiADUAYGbJADEAYgAZADgAMgAXADKAOAB1ADKAMAA4AGUAYGbKAGUAMwA2ADcAZAAXADAAMAAYADIAYQAZAGEAOAAAXADUAYgA=
PS C:\VENE> Get-ChildItem

Verzeichnis: C:\VENE

Mode                LastWriteTime         Length Name
----                -
-a----          23-Jan-18         12:46           274 AES_keyfile.txt
-a----          21-Jan-18         16:53           648 config.xml
-a----          23-Jan-18         12:45          1021 encryptAES.ps1
-a----          22-Jan-18         10:25          3972 functions.psm1
-a----          22-Jan-18         12:15          19481 podbackup.ps1
-a----          23-Jan-18         12:46           558 SecPass.txt

PS C:\VENE> Get-Content \SecPass.txt
76492d1116743f0423413b16050a5345MgB8AHQAVWbNAcsAcQBhAFYAUQBWAHAUQBRADUANABWAGYAdQBWAE0AVQBUAHcAPQA9AHWANGB1AGUAQOBmADgANABiADgAMwA5AGUAMwAWAG
EAYQAZADgAZABkADgAMABKADcAQQBmAGQAOABiADUAYGbJADEAYgAZADgAMgAXADKAOAB1ADKAMAA4AGUAYGbKAGUAMwA2ADcAZAAXADAAMAAYADIAYQAZAGEAOAAAXADUAYgA=
PS C:\VENE>
```

Spätere Passwort-Änderung:

```
Windows PowerShell
PS C:\VENE> Get-ChildItem

Verzeichnis: C:\VENE

Mode                LastWriteTime         Length Name
----                -
-a----          23-Jan-18         12:48           280 AES.key
-a----          21-Jan-18         16:53           648 config.xml
-a----          23-Jan-18         12:45          1021 encryptAES.ps1
-a----          22-Jan-18         10:25          3972 functions.psm1
-a----          22-Jan-18         12:15          19481 podbackup.ps1
-a----          23-Jan-18         12:48           558 SecFileFA.txt

PS C:\VENE> .\encryptAES.ps1 -keyFile .\AES.key -NewSecurePasswordFile .\SecFileFA.txt -Password 'Password'
76492d1116743f0423413b16050a5345MgB8AEKARGBZAEHAQGBCAHGARGB1AGKAdwB3AGYAEQBqAEQARwB1AEUAbABpAGCAPQA9AHWANWA5ADgAMgAXADYAMgA5ADcANAA4AGEAMwA0AG
MAZQA3AGIAMAA4AGMANGA2ADIAZgAXADKAYWB1ADIAMGA2ADAAYGB1AGQAMWA4AGYANQA0ADYANAA5ADKAZgAZAGUAOAB1AGMAZQB1ADAANGB1ADUAYgA4AGUAZQA4ADQANGA=
PS C:\VENE> Get-ChildItem

Verzeichnis: C:\VENE

Mode                LastWriteTime         Length Name
----                -
-a----          23-Jan-18         12:48           280 AES.key
-a----          21-Jan-18         16:53           648 config.xml
-a----          23-Jan-18         12:45          1021 encryptAES.ps1
-a----          22-Jan-18         10:25          3972 functions.psm1
-a----          22-Jan-18         12:15          19481 podbackup.ps1
-a----          23-Jan-18         12:49           558 SecFileFA.txt

PS C:\VENE>
```

7.2. podbackup.ps1

Aufruf ohne Parameter:

```
Windows PowerShell
PS C:\VENE> Get-ChildItem

Verzeichnis: c:\VENE

Mode                LastWriteTime         Length Name
----                -
-a-----         23-Jan-18      12:52           302 AES.key
-a-----         20-Jan-18      18:53           768 config.xml
-a-----         23-Jan-18      12:45          1021 encryptAES.ps1
-a-----         23-Jan-18      13:07          3972 functions.psm1
-a-----         23-Jan-18      13:07         19493 podbackup.ps1
-a-----         23-Jan-18      12:52           558 secFileFA.txt
-a-----         23-Jan-18      12:52           558 secFileVC.txt

PS C:\VENE> .\podbackup.ps1
PS C:\VENE> Get-ChildItem

Verzeichnis: c:\VENE

Mode                LastWriteTime         Length Name
----                -
-a-----         23-Jan-18      12:52           302 AES.key
-a-----         20-Jan-18      18:53           768 config.xml
-a-----         23-Jan-18      12:45          1021 encryptAES.ps1
-a-----         23-Jan-18      13:07          3972 functions.psm1
-a-----         23-Jan-18      13:07         19493 podbackup.ps1
-a-----         23-Jan-18      13:08          2992 runlog_20180123_130803.log
-a-----         23-Jan-18      12:52           558 secFileFA.txt
-a-----         23-Jan-18      12:52           558 secFileVC.txt

PS C:\VENE>
```

Andere Konfigurationsdatei und Zurückhaltungsaktivierung:

```
Windows PowerShell
PS C:\VENE> Get-ChildItem

Verzeichnis: c:\VENE

Mode                LastWriteTime         Length Name
----                -
-a-----         23-Jan-18      12:52           302 AES.key
-a-----         23-Jan-18      12:45          1021 encryptAES.ps1
-a-----         23-Jan-18      13:07          3972 functions.psm1
-a-----         23-Jan-18      13:07         19493 podbackup.ps1
-a-----         20-Jan-18      18:53           768 PROD-config.xml
-a-----         23-Jan-18      12:52           558 secFileFA.txt
-a-----         23-Jan-18      12:52           558 secFileVC.txt

PS C:\VENE> .\podbackup.ps1 -Config .\PROD-config.xml -ApplyRetention
PS C:\VENE> Get-ChildItem

Verzeichnis: c:\VENE

Mode                LastWriteTime         Length Name
----                -
-a-----         23-Jan-18      12:52           302 AES.key
-a-----         23-Jan-18      12:45          1021 encryptAES.ps1
-a-----         23-Jan-18      13:07          3972 functions.psm1
-a-----         23-Jan-18      13:07         19493 podbackup.ps1
-a-----         20-Jan-18      18:53           768 PROD-config.xml
-a-----         23-Jan-18      13:14          3006 runlog_20180123_131432.log
-a-----         23-Jan-18      12:52           558 secFileFA.txt
-a-----         23-Jan-18      12:52           558 secFileVC.txt

PS C:\VENE>
```