Virtual Hosts Disaster Recovery Plan

Τμήμα Πληροφορικής, Πανεπιστήμιο Κύπρου

Andry Michaelidou Papa

4 April 2016

Έκδοση 2η

Περιεχόμενα

Virtual Hosts Disaster Recovery Plan

Εισαγωγή

Το πλάνο αυτό μελετά την περίπτωση βλάβης που επηρεάζει τους Virtual Hosts και τον τρόπο επαναφοράς των εικονικών μηχανών και υπηρεσιών που υποστηρίζουν.

Ακολουθούν γενικές πληροφορίες, διαδικασίες και μέθοδοι λήψης αντιγράφων ασφαλείας καθώς επίσης και καθορισμός του χρόνου ανάκαμψης αλλά και προτεραιότητας ανάκαμψης αναλόγως με τις κρίσιμες λειτουργίες που εκτελεί κάθε εικονική μηχανή.

Στη συνέχεια ακολουθούν τα σενάρια που μελετά αυτό το Disaster Recovery Plan (DRP) καθώς και τα προτεινόμενα βήματα για ανάκαμψη των συστημάτων.

Συντομογραφίες

Ακρωνύμιο	
DRP	*Disaster Recovery Plan*
VM(s)	*Virtual Machine(s)*
VH(s)	*Virtual Host(s)*
LVM	*Logical Volume Manager*
VG	*Volume Group*
ISCSI	*Internet Small Computer System Interface*
TSM	*Tivoli Storage manager*
OTY	*Ομάδα Τεχνικής Υποστήριξης*

Γενικά

A. Καθορισμός Ρόλων-Αρμοδιοτήτων

Για την αποτελεσματικότερη εφαρμογή του Disaster Recovery Plan (DRP), θεωρείται ότι η ανάθεση των ρόλων και αρμοδιοτήτων σε περίπτωση εφαρμογής του πλάνου αυτού βασίζεται στον πίνακα ευθυνών ΟΤΥ καθώς και στην πάγια πρακτική μας για αντικατάσταση. Η εφαρμογή του DRP καθώς και οι σημαντικές αποφάσεις που θα ληφθούν για την ανάκαμψη των υπηρεσιών θα πρέπει να είναι προσυμφωνημένες με τον συντονιστή της ΟΤΥ, ή και το προεδρείο αν κριθεί απαραίτητο από τον συντονιστή της ΟΤΥ.

B. Καθορισμός χρόνου ανάκαμψης και αντιστοίχιση λειτουργιών για προτεραιοποίηση ανάκαμψης

Για την αποτελεσματική εφαρμογή του πλάνου αυτού, θα πρέπει αρχικά να αποφασιστεί ο επιδιωκόμενος χρόνος ανάκαμψης. Λόγω της ιδιαίτερης φύσης των υπηρεσιών αλλά και της ιδιαιτερότητας της κάθε υπηρεσίας ο χρόνος ανάκαμψης διαφέρει και βασίζεται στην διαβάθμιση κρισιμότητας συστημάτων (Πίνακας Κρισίμων Συστημάτων) που προκύπτει από τον πίνακα ευθυνών ΟΤΥ.

Σύμφωνα με τη διαβάθμιση αυτή τα συστήματα και **υπηρεσίες με βαθμό > 5 θα πρέπει να έχουν ανακάμψει εντός 1 ημέρας (24 ώρες)**, ενώ τα υπόλοιπα συστήματα μικρότερης κρισιμότητας εντός 3 ημερών ή 1ας εβδομάδας. Ο χρόνος αυτός θα κρίνεται αναλόγως σε κάθε περίπτωση από τον **υπεύθυνο εφαρμογής του DRP**, σύμφωνα με τους πόρους που θα έχει στη διάθεση του για την ανάκαμψη των συστημάτων.

Συνεπώς κατά το σχεδιασμό του DRP θα μπορούσε να επιλεχθεί με ασφάλεια ως επιδιωκόμενος χρόνος ανάκαμψης ο ελάχιστος απαιτούμενος, δηλαδή **1 ημέρα**, ενώ παράλληλα μπορούμε να ορίσουμε ως μέγιστο ανεκτό χρόνο ανάκαμψης για το σύνολο των συστημάτων και υπηρεσιών την **1 εβδομάδα** (5 εργάσιμες).

Συστήματα	Μέγιστος χρόνος ανάκαμψης
Συστήματα και υπηρεσίες με βαθμό κρισιμότητας > 5	1 ημέρα (24 ώρες)
Συστήματα και υπηρεσίες με βαθμό κρισιμότητας < 5	3 ημέρες (72 ώρες) - 1 εβδομάδα (5 εργάσιμες μέρες)

Ιδιαίτερη σημασία κατά τον καθορισμό του χρόνου ανάκαμψης πρέπει να δοθεί και στο χρόνο που μεσολαβεί από την εκδήλωση της καταστροφής μέχρι και την έναρξη της εφαρμογής του DRP. Στο ίδιο χρονικό διάστημα πρέπει να διερευνηθεί και να αποφασιστεί η αναγκαιότητα χρήσης

εναλλακτικών εγκαταστάσεων στα πλαίσια εφαρμογής του DRP. Για τη περίπτωση που μελετάμε επιλέγεται ως μέγιστος χρόνος για τη λήψη της παραπάνω απόφασης οι **4 ώρες**. Παράλληλα τίθεται ως χρονικό διάστημα-στόχος για τη δυνατότητα φιλοξενίας των συστημάτων σε εναλλακτικές εγκαταστάσεις οι **4 εβδομάδες**, στη διάρκεια του οποίου θα πρέπει να έχουν αποκατασταθεί πλήρως οι κυρίως εγκαταστάσεις και να είναι σε θέση να φιλοξενήσουν και πάλι τα συστήματα.

Γ. Κεντρική υποδομή storage

Στο πλάνο αυτό θεωρείται δεδομένο ότι τουλάχιστον μία από τις υποδομές για storage είναι σε λειτουργία και δεν μελετάται το ενδεχόμενο επαναφοράς των υπηρεσιών storage, καθότι αφορά άλλην υπηρεσία και η επαναφορά των υπηρεσιών πρέπει να αναφέρεται DRP της υπηρεσίας αυτής.

Μελετάται όμως ως σενάριο η πιθανότητα προβλήματος ή ολικής καταστροφής ενός εκ' των υποδομών storage και η επαναφορά των υπηρεσιών σε άλλη υποδομή storage.

Δ. Προστασία δεδομένων και μέθοδοι λήψης αντιγράφων ασφαλείας

Στο πλάνο αυτό θεωρείται δεδομένο ότι τα τρέχων αντίγραφα ασφαλείας των συστημάτων που επηρεάζονται και τα δεδομένα τους είναι άθικτα και διαθέσιμα.

Η λήψη των αντιγράφων βασίζεται στο TSM Backup policy, ενώ ο διαχειριστής της κάθε εικονικής μηχανής, αλλά και ο διαχειριστής της κάθε υπηρεσίας θα πρέπει να διασφαλίζει ότι τα αντίγραφα ασφαλείας λαμβάνονται σε τακτά χρονικά διαστήματα ώστε να εξασφαλίζεται η ύπαρξη αντιγράφου όλων των πρόσφατων αλλαγών.

Μέθοδοι λήψης αντιγράφων ασφαλείας

Πιο κάτω αναφέρονται οι μέθοδοι λήψης αντιγράφων ασφαλείας από τις VMs και τους VHs.

i. Εικονικές μηχανές και δεδομένα (Virtual Machines)

Όπως αναφέρθηκε και πιο πάνω ο διαχειριστής της κάθε εικονικής μηχανής, αλλά και ο διαχειριστής της κάθε υπηρεσίας θα πρέπει να διασφαλίζουν ότι τα αντίγραφα ασφαλείας λαμβάνονται σε τακτά χρονικά διαστήματα ώστε να εξασφαλίζεται η ύπαρξη αντιγράφου όλων των πρόσφατων αλλαγών. Σε κάθε εικονική μηχανή είναι καθήκον του διαχειριστή της μηχανής η εγκατάσταση και διαμόρφωση του TSM για την εξασφάλιση αντίγραφων ασφαλείας με τις πρόσφατες αλλαγές στα δεδομένα της μηχανής. Ο διαχειριστής της κάθε υπηρεσίας σε συνεργασία με τον διαχειριστής της μηχανής θα πρέπει να βεβαιωθεί ότι για τα δεδομένα των υπηρεσιών που χειρίζεται, λαμβάνονται τα απαραίτητα αντίγραφα ασφαλείας.

Η λήψη των αντιγράφων ασφαλείας για τα δεδομένα μέσα από τις εικονικές μηχανές βασίζεται στο TSM Backup policy.

ii. Virtual Host και δεδομένα

1. Αντίγραφα ασφαλείας δεδομένων εξυπηρετητή

Όσον αφορά τους VHs και τα δεδομένα τους, δεν έχει καταστεί προς το παρόν ανάγκη για εκτεταμένη ύπαρξη αντιγράφων ασφαλείας. Για σκοπούς όμως μεγαλύτερης ταχύτητας επαναφοράς των εικονικών μηχανών σε περίπτωση βλάβης, καθώς και για ελαχιστοποίηση του χρόνου ανάκαμψης λόγω λανθασμένης ή μη ενημερωμένης τεκμηρίωσης, αποφασίστηκε όπως για κάθε σύστημα δημιουργούνται αντίγραφα ασφαλείας για τους υποκαταλόγους **/etc/libvirt/** και **/etc/lvm** όπου υπάρχουν όλα τα configuration files που αφορούν τις εικονικές μηχανές , το storage και το LVM configuration.

Το αντίγραφο αυτό γίνεται σύμφωνα με το TSM Backup και το Schedule: CS_BACKUP_SERVERS_DAILY.

2. Αντίγραφα ασφαλείας των VMs images (raw space)

Σύμφωνα με την πολιτική δημιουργίας εικονικών μηχανών προτείνεται όπως χρησιμοποιείται LVM logical volume (raw space) για την εγκατάσταση. Ο χώρος αυτός πιθανό να βρίσκεται σε 2 τοποθεσίες στον VH:

/ dev/VMvgLocal/ (Local storage disk του VH)
/dev/ VMvgRemote/ (Remote storage disk, iscsi storage infrastructure**)**

Για κάθε μηχανή έχει γίνει πλάνο δημιουργίας αντίγραφων ασφαλείας (LVM snapshot) των images **αυτών ανά 2 εβδομάδες στους VH που εξυπηρετούν τις υπηρεσίες του τμήματος και ανά 4 εβδομάδες στους VH που εξυπηρετούν ερευνητικούς σκοπούς.**

Το αντίγραφο αυτό μπορεί να χρησιμοποιηθεί ανεξάρτητα σε οποιοδήποτε VH και με χρήση του τελευταίου αντίγραφου ασφαλείας των δεδομένων της εικονικής μηχανής μπορούμε να έχουμε ένα πλήρες και ενημερωμένο αντίγραφο της εικονικής μηχανής.

Η χρήση των images των μηχανών και η επαναφορά τους είναι κάτι εντελώς νέο που πρώτη φορά δοκιμάζεται στην υποδομή μας. Σε κάθε περίπτωση, εάν αποτύχει η επαναφορά του image, για την επαναφορά της VM θα ακολουθηθούν τα βήματα επαναφοράς όπως εάν ήταν physical μηχανή, δηλαδή με εγκατάσταση από την αρχή και επαναφορά των δεδομένων από το backup.

Σενάρια καταστροφής

Πιο κάτω μελετούνται κάποια σενάρια καταστροφής, όπου θέτουν μερικές ή όλες τις μηχανές κάποιου VH εκτός λειτουργίας. Στα σενάρια αυτά συγκεκριμενοποιούνται οι ζημιές και τα βήματα που θα πρέπει να ακολουθηθούν για ανάκαμψη των μηχανών.

Σενάριο 1: VHost Hardware Failure

Στο σενάριο αυτό μελετάται η βλάβη στο hardware ενός VH και τα βήματα που πρέπει να ακολουθηθούν σε κάθε περίπτωση ξεχωριστά για την ανάκαμψη της μηχανής ή την ανάκαμψη των εικονικών μηχανών που εξυπηρετούσε.

Σε κάθε μια από τις πιο κάτω περιπτώσεις πρέπει σύμφωνα με τον πίνακα συντήρησης υλικών, καθώς και την περίοδο εγγύησης των VH να γίνεται άμεση επικοινωνία με την εταιρεία που παρέχει συντήρηση στη μηχανή για άμεση αντικατάσταση του προβληματικού hardware.

Οι Virtual Hosts είναι εφοδιασμένοι με RAID controller και δύο δίσκους με configuration RAID 1. Σε περίπτωση βλάβης πρέπει ως πρώτο βήμα να γίνει έλεγχος εάν το πρόβλημα οφείλεται σε προβληματικό δίσκο. Εάν είναι μόνο ο ένας από τους 2 δίσκους χαλασμένος μπορεί να αφαιρεθεί από το array ούτως ώστε να γίνουν οι απαραίτητες ενέργειες για επανεκκίνηση της μηχανής. Εάν δεν είναι δυνατή η επανεκκίνηση του εξυπηρετητή, τότε ισχύουν τα πιο κάτω.

Ζημιές:

/etc/libvirt : όλα τα configuration files που αφορούν τις εικονικές μηχανές και το storage
/etc/lvm: όλα τα configuration files που αφορούν το LVM configuration
/dev/VMvgLocal: Local storage disk του VH (περιλαμβανομένων όλων των εικονικών μηχανών που ήταν αποθηκευμένες στον χώρο αυτό)
/dev/ VMvgRemote: Remote storage disk, iscsi storage infrastructure (περιλαμβανομένων όλων των εικονικών μηχανών που ήταν αποθηκευμένες στον χώρο αυτό)

Βήματα επαναφοράς:

Βήμα 1°: Restore /etc/libvirt και **/etc/lvm**
Βήμα 2°: Σύμφωνα με το κεφάλαιο «Καθορισμός χρόνου ανάκαμψης και αντιστοίχιση λειτουργιών για προτεραιοποίηση ανάκαμψης» που αναφέρθηκε πιο πάνω εντοπίζονται οι μηχανές που πρέπει να επανεκκινήσουν εντός της ημέρας και προτεραιοποιούνται.
Βήμα 3°: Καθορισμός του χώρου για επαναφορά των μηχανών. Η επαναφορά μπορεί να αφορά είτε VMs που ήταν στον τοπικό δίσκο του VH (**/ dev/VMvgLocal**) είτε VMs που ήταν στον απομακρυσμένο δίσκο (iscsi) του VH (**/ dev/VMvgRemote**)

Περίπτωση 1: Επαναφορά από το /dev/VMvgLocal σε άλλο VH

Βήμα 1°: Δημιούργησε τα Logical Volumes για κάθε μηχανή στον νέο VH με:
lvcreate -L <size>GB -n <name> VMvg<>
Βήμα 2°: Κάνε restore το image της μηχανής με:
dd if=/vm-backup/<host>/vm_backup.gz | gzip -c -d | dd of=/dev/ VMvg<>/destination_lv
Βήμα 3°: Αντέγραψε το /etc/libvirt/qemu/{guestname}.xml από restore του παλιού VH στον νέο.
Βήμα 4°: Τρέξτε virsh create /etc/libvirt/qemu/{guestname}.xml
Βήμα 5: Εκκίνησε την μηχανή κανονικά και κάνε restore τα τελευταία δεδομένα εάν χρειάζεται (μέσα από την μηχανή).

Περίπτωση 2: Επαναφορά του /dev/VMvgRemote σε άλλο VH

(Πρέπει να γίνουν δοκιμές με το vgcfgrestore και το vgimport κατά πόσον οι εικονικές μηχανές που είναι στο iscsi storage μπορούν να επανέλθουν με την σύνδεση του storage με άλλο VHost. Αν ναι τότε θεωρητικά με πιο κάτω commands θα είναι διαθέσιμος ο χώρος σε άλλο VH.)

iscsiadm -m discovery -t sendtargets -p 10.16.254.x

iscsiadm -m node -T iqn.x -p 10.16.254.x --login

pvcreate –uuid <<UUID OF VMvgRemote**>> /dev/sdx1 ***<Where <x> is iscsi disk name appear in the fdisk -l>***

vgcreate VMvgRemoteNEW /dev/sdx1 *explain new name of Volume Group

vgcfgrestore -f /etc/lvm/backup/VMvgRemote VMvgRemoteNEW

For each guest:

copy /etc/libvirt/qemu/{guestname}.xml (from restore) to new VH

virsh create /etc/libvirt/qemu/{guestname}.xml

Start the guests as usual

** Can be found at /etc/lvm/backup/VMvgRemote of the backup files

Εάν δεν μπορεί να επιτευχθεί σύνδεση του storage με άλλον VH, τότε θα ακολουθηθούν τα ίδια βήματα όπως πιο πάνω στην **Περίπτωση 1: Επαναφορά από το /dev/VMvgLocal σε άλλο VH** με επαναφορά των images από το backup.

Σενάριο 2: ISCSI Storage Failure

Στο σενάριο αυτό μελετάται η βλάβη στην κεντρική υποδομή του iscsi storage και τα βήματα που πρέπει να ακολουθηθούν σε κάθε περίπτωση για την ανάκαμψη των εικονικών μηχανών που είχαν το storage στην κεντρική υποδομή που εμφάνισε το πρόβλημα.

Σημειώνεται ότι στην περίπτωση αυτή δεν μελετάται το ενδεχόμενο επαναφοράς των υπηρεσιών storage, καθότι αφορά άλλην υπηρεσία και πρέπει να αναφέρεται στο DRP της υπηρεσίας αυτής. Μελετάται όμως ως σενάριο η πιθανότητα προβλήματος ή ολικής καταστροφής ενός εκ' των υποδομών storage και η επαναφορά των υπηρεσιών των VH σε άλλη υποδομή storage.

Ζημιές:
/dev/VMvgRemote/: Remote storage disk, iscsi storage infrastructure

Βήματα επαναφοράς:
Βήμα 1°: Σύμφωνα με το κεφάλαιο «Καθορισμός χρόνου ανάκαμψης και αντιστοίχιση λειτουργιών για προτεραιοποίηση ανάκαμψης» που αναφέρθηκε πιο πάνω εντοπίζονται οι μηχανές που πρέπει να επανεκκινήσουν εντός της ημέρας. Μαζεύονται οι ανάγκες για storage και προτεραιοποιούνται.
Βήμα 2°: Καθορισμός του χώρου για επαναφορά των μηχανών. Η επαναφορά μπορεί να γίνει είτε στον ίδιο VH αλλά σε άλλο device (από άλλο iscsi storage) είτε εάν δεν υπάρχει διαθέσιμο storage στο μέγεθος που χρειάζεται σε άλλους VHs.

Περίπτωση 1: Επαναφορά στον ίδιο VH

Βήμα 1°: vgrename VMvgRemote VMvgRemoteOLD
Βήμα 2°: Ακολούθησε τις οδηγίες για **"Connect to a storage"** από https://wiki.cs.ucy.ac.cy/index.php/OTY_Internal:Virtual_Host_Configuration#Connect_to_remote_iscsi_storage
Βήμα 3°: Δημιούργησε τα Logical Volumes για κάθε μηχανή με: **lvcreate -L <size>GB -n <name> VMvgRemote**
Βήμα 4°: Κάνε restore το image της μηχανής με:
dd if=/vm-backup/<host>/vm_backup.gz | gzip -c -d | dd of=/dev/ VMvg<>/destination_lv
Βήμα 5°: Εκκίνησε την μηχανή κανονικά και κάνε restore τα τελευταία data αν χρειάζεται (μέσα από την μηχανή)

Περίπτωση 2: Επαναφορά σε άλλον VH

Βήμα 1ο: Δημιούργησε τα Logical Volumes για κάθε μηχανής στον νέο VH με: **lvcreate -L <size>GB -n <name> VMvgRemote**
Βήμα 2ο: Κάνε restore το image της μηχανής με :
dd if=/vm-backup/<host>/vm_backup.gz | gzip -c -d | dd of=/dev/VMvg<>/destination_lv
Βήμα 3ο: Αντιγράψτε το /etc/libvirt/qemu/{guestname}.xml από τον παλιό VH στον νέο.
Βήμα 4ο: Τρέξτε virsh create /etc/libvirt/qemu/{guestname}.xml
Βήμα 5ο: Εκκίνησε την μηχανή κανονικά και κάνε restore τα τελευταία δεδομένα εάν χρειάζεται (μέσα από την μηχανή).

Σημειώνεται ότι σε περίπτωση που το ISCSI storage failure αναφέρετε σε βλάβη του συστήματος NetApp, τότε, δεδομένου ότι το /vm-backup που περιέχει τα τελευταία αντίγραφα των images των εικονικών μηχανών θα πρέπει να ανακτηθεί από το backup με επιπλέον χρόνο ανάκαμψης των εικονικών μηχανών.

Αναθεώρηση και συντήρηση του Disaster Recovery Plan

Προτείνεται η τακτική επικαιροποίηση του DRP σε ετήσια βάση, καθώς και εκτάκτως μετά από κάθε αλλαγή που μπορεί να επηρεάσει την αποτελεσματικότητά του. Εκτός της αναθεώρησης και συντήρησής του που κρίνονται επιβεβλημένες προτείνεται ανά τακτά χρονικά διαστήματα δειγματοληπτικός έλεγχος του DRP και επαναφορά μηχανών τυχαία για έλεγχο των σενάριων καταστροφής και την αποτελεσματικότητα του DRP για επαναφορά.

Ιστορικό αναθεωρήσεων

Έκδοση 1η	13 Νοεμβρίου 2013
Έκδοση 2η	04 Απριλίου 2016