



Virtual Center Site Recovery Manager

Wien, 17.03.2010



Ing. Alexander Kuchelbacher

Artaker Computersysteme GmbH
IT-Infrastructure & Virtualization

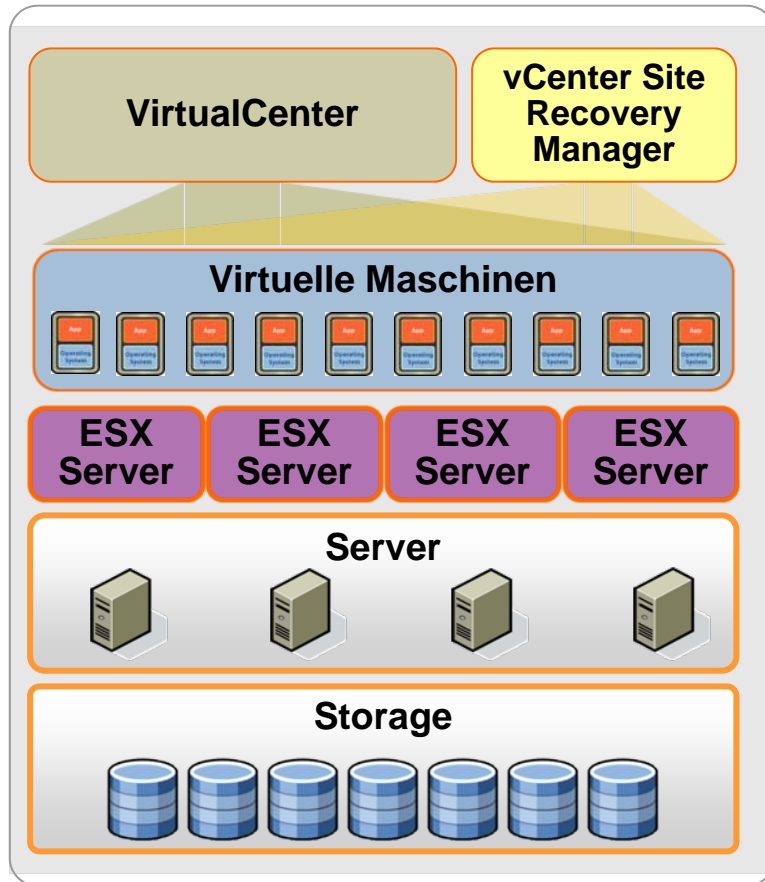


Kurzübersicht

- ▶ **Die VMware-Infrastruktur ist die Basis um Ihr Rechenzentrum einfach und günstig zu schützen**
- ▶ **Mit vCenter Site Recovery Manager können Sie folgende Aufgaben erfüllen:**
 - Vereinfacht und automatisiert die Hauptabläufe des Disaster Recovery: Setup, Testen, Failover
 - Vereinfacht und zentralisiert die Verwaltung von Recovery-Plänen
 - Erhöht den Nutzen in die Investitionen in Storage-Replikationstechnologien
- ▶ **Die kombinierte Automatisierungslösung zum Disaster Recovery eingebettet in VMware Infrastructure**
 - verringert die Wiederherstellungszeit, das Risiko, die Komplexität und die Kosten



Hauptfunktionen von vCenter Site Recovery Manager



Zentralisiertes Disaster Recovery-Management

- Erstellen, Testen, Aktualisieren und Ausführen von Recovery-Plänen von einer einzigen Verwaltungsstelle aus
- Enge Integration in VirtualCenter

Disaster Recovery-Automatisierung

- Erstellen des Wiederherstellungsvorgangs im Voraus
- Automatisiertes Testen der Recovery-Pläne
- Automatisiertes Ausführen des Wiederherstellungsvorgangs

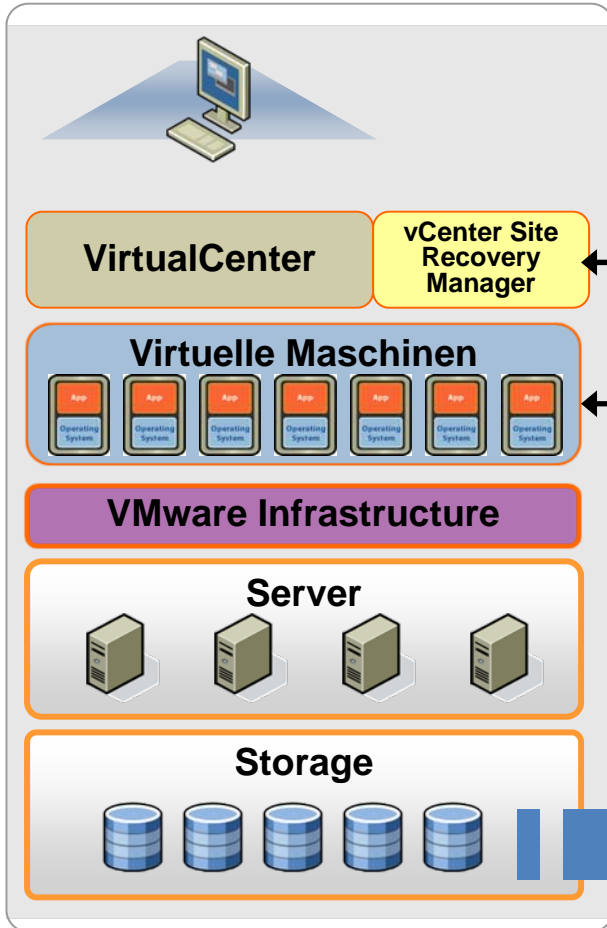
Vereinfachte Einrichtung und Integration

- Zuteilen und Verwalten von Recovery-Ressourcen
- Einfache Integration in Speicherreplikationssysteme führender Hersteller

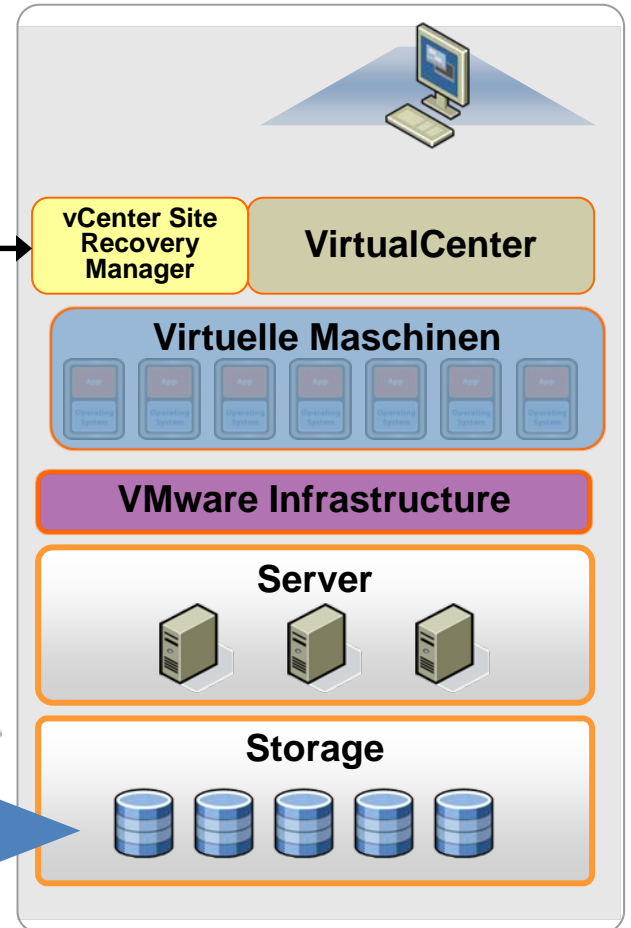


Hauptkomponenten

Produktion



Disaster Recovery



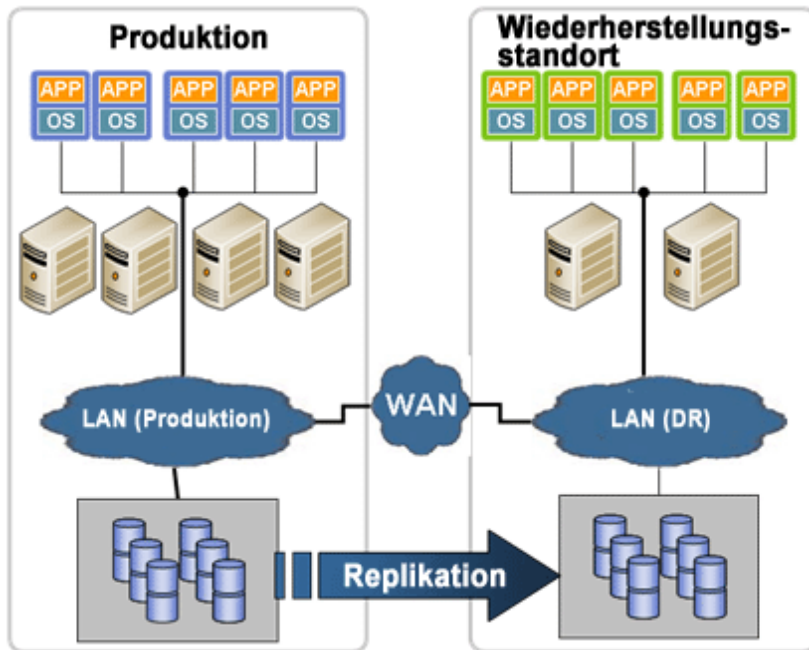
vCenter Site Recovery Manager

Geschützte virtuelle Maschinen



Partnerreplikation

Disaster Recovery - Einrichtung



Erstellen von Recovery-Plänen

- Für virtuelle Maschinen, Anwendungen, Geschäftsbereiche

Integrieren in Replikation

- Ermitteln der durch die Replikationskonfiguration geschützten virtuellen Maschinen

Zuordnen von Recovery-Ressourcen

- Serverressourcen, Netzwerkressourcen, Management-Objekte

Festlegen des Recovery-Vorgangs

- Konvertieren des manuellen Run-Books in vorprogrammierte Abläufe
- Anpassbar durch Skripts und Callouts



vCenter Site Recovery Manager – Voraussetzungen

- ESX Server 3.0.2, ESX Server 3.5 oder ESX Server 3i, ESX4 oder ESX 4i
- VirtualCenter (VC) Server, Version 2.5 od.4, installiert am **geschützten Standort** und am **Recovery-Standort**
- SRM Server installiert am **geschützten** und am **Recovery-Standort**
- SRM-Plug-In installiert auf den VI-Clients, die auf den geschützten und den Recovery-Standort zugreifen
- Netzwerkkonfiguration, die TCP-Verbindungen zwischen VC-Servern und SRM-Servern ermöglicht
- Eine Oracle-oder SQL Server-Datenbank, die ODBC für Verbindungen am **geschützten Standort** und am **Recovery-Standort** verwendet
- Eine auf dem VC-Lizenzserver installierte SRM-Lizenz am **geschützten Standort** und am **Recovery-Standort**
- **Vorkonfigurierte Array-basierte Replikation zwischen dem geschützten Standort und dem Recovery-Standort**



Installationsablauf

Am geschützten Standort werden folgende Schritte ausgeführt:

- Installation des SRM-Servers
- Installation des SRM-Plug-Ins im VI-Client
- Installation des Storage Replication Adapters (SRA)

Am Recovery-Standort werden folgende Schritte ausgeführt:

- Installation des SRM-Servers
- Installation des SRM-Plugins im VI-Client *
- Installation des Storage Replication Adapters (SRA)

Die vCenter Site Recovery Manager-Abläufe müssen unbedingt in der in dieser Präsentation aufgeführten Reihenfolge ausgeführt werden.

* Hinweis: Optionaler Schritt, nur erforderlich, wenn eine andere Instanz des VI-Clients für den Zugriff auf Recovery-Standort verwendet wird

Sicherheitstipp: DNS-Validierung – die Viererregel

Prüfen der ordnungsgemäßen DNS-Funktion durch Durchführen der folgender DNS-Lookups für VC-, SRM- und ESX-Server

- Kurzname
- Langer Name
- Rückwärts
- Vorwärts

```
C:\>nslookup dr-vc-vim22
Server: vmc-ns1.eng.vmware.com
Address: 10.17.193.1

C:\>nslookup dr-vc-vim22.eng.vmware.com
Server: vmc-ns1.eng.vmware.com
Address: 10.17.193.1

C:\>nslookup 10.17.195.184
Server: vmc-ns1.eng.vmware.com
Address: 10.17.193.1

C:\>nslookup dr-vc-vim22.eng.vmware.com
Server: vmc-ns1.eng.vmware.com
Address: 10.17.195.184

C:\>nslookup 10.17.195.234
Server: vmc-ns1.eng.vmware.com
Address: 10.17.193.1

C:\>nslookup dr-vim22.eng.vmware.com
Server: vmc-ns1.eng.vmware.com
Address: 10.17.195.234

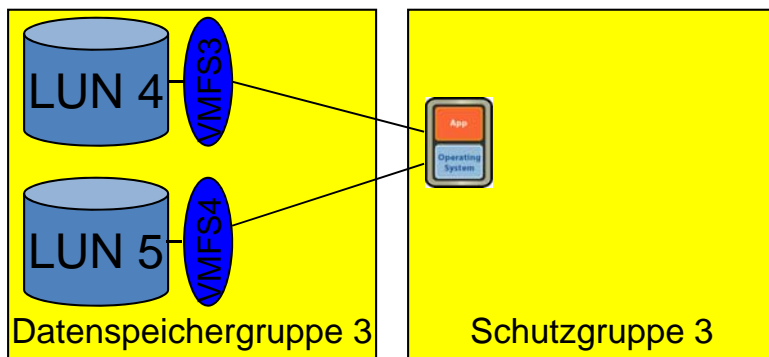
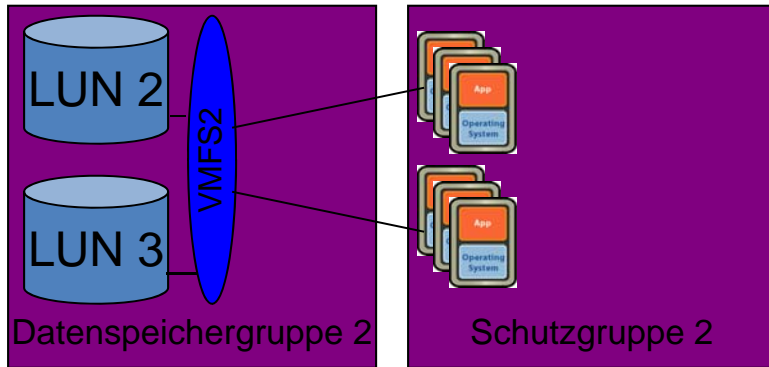
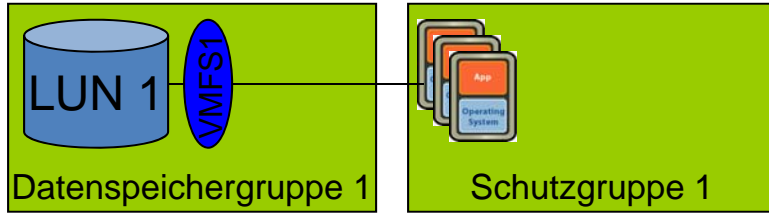
C:\>nslookup 10.17.195.106
Server: vmc-ns1.eng.vmware.com
Address: 10.17.193.1

C:\>nslookup eng.vmware.com
Server: vmc-ns1.eng.vmware.com
Address: 10.17.193.1

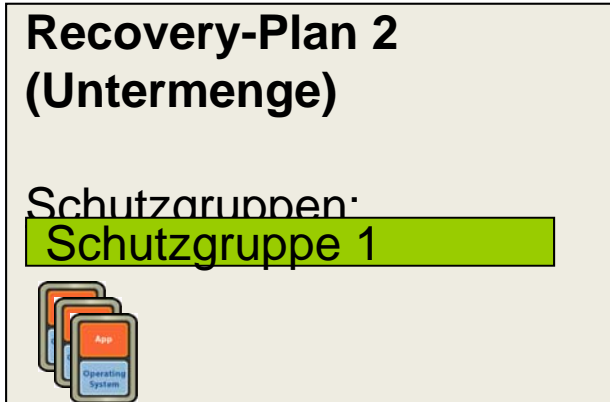
C:\>nslookup vim22.eng.vmware.com
Server: vmc-ns1.eng.vmware.com
Address: 10.17.195.106

C:\>nslookup eng.vmware.com
Server: vmc-ns1.eng.vmware.com
Address: 10.17.0.20
```


Hauptkonzepte und ihre Beziehungen



Geschützter Standort



Recovery-Standort



Managementoberfläche von vCenter Site Recovery Manager

VMware Infrastructure Client

ration **Plugins** Help

Events Administration Maps Consolidation **Site Recovery**

dr-vim22

Summary Alarms Permissions

Local Site	Paired Site
VC Server:	VC Server:
DR Server:	DR Server:
Site Name:	Site Name:

Setup

This server has not completed set up for disaster recovery. To complete configuration, follow the steps below.

Connection:	Not Configured	Configure Break
Array Managers:	Not Configured	Configure
Inventory Preferences:	Not Configured	Configure
Protection Groups:	0 Group(s) Created	Create
Recovery Plans:	0 Plan(s) Created	Create

Einrichtung – Schutzstandort

Am Schutzstandort werden folgende Schritte zur Einrichtung ausgeführt:

- Der Standort wird am F...
- Sich...
- Serv...

Standort und
den VC-

Connect to Remote Site

Remote Site Information
Connect to a remote site.

Remote Site Information
Authentication
Complete Connections

VMware Site Recovery Manager

Certificate Type Selection

Choose a certificate method for authentication.

Certificate Source

Select a certificate source.

- Use a PKCS#12 certificate file.
You will be prompted to select a PKCS#12 certificate and optional password.
- Automatically generate a certificate.
Select this option if you wish to use an automatically generated certificate.

InstallShield

< Back Next > Cancel

Nicht ordnungsgemäß
führen zu gelben
Der Austausch
damit Sie mit der
fortfahren können.

✓ Reciprocity is established.



Einrichtung – Schutzstandort

Add Array Manager

Array Manager Information

Display Name:

Manager Type:

SP-A IP:

SP-B IP:

Username:

Password:

Array ID	Model
Wählen Sie im Dropdown-Feld „Manager Type“ den richtigen Manager Type für das SAN in Ihrer Umgebung	

Konfiguration von Array-Managern

- Wählen Sie den richtigen **Manager Type** im entsprechenden Dropdown-Feld aus

Einrichtung – Schutzstandort

- SRM identifiziert verfügbare Arrays und replizierte Datenspeicher und legt die Datenspeichergruppen fest.

Configure Array Managers

Protection Side Array Managers
Enter the location and credentials for array managers on the protection side.

Protection Side Array Manager:
[Recovery Side Array Managers](#)
[Review Mirrored LUNs](#)

Display Name	Manager Type	Address
vim22dc SAN	Symmetrix Native	vim22

Array ID	Model	Peer Array	LUN Count
000190102189	DMX3-24	000187461516	38

Configure Array Managers

Recovery Side Array Managers
Enter the location and credentials for array managers on the recovery side.

[Protection Side Array Managers](#)
Recovery Side Array Managers
[Review Mirrored LUNs](#)

Display Name	Manager Type	Address
vim23dc SAN	Symmetrix Native	vim23

Array ID	Model	Peer Array	LUN Count
000190102189	DMX3-24	000187461516	0

Review Mirrored LUNs
Review the list of mirrored datastores and RDMs.

[Protection Side Array Managers](#)
[Recovery Side Array Managers](#)
Review Mirrored LUNs

- SAN Array 000190102189
 - LUN Group: [shared-san-1]
 - LUN Group: [shared-san-2]



Einrichtung – Schutzstandort

- Mithilfe des Inventory Preferences Mapper ordnet der Benutzer Ressourcen am geschützten Standort ihren Gegenstücken am Recovery-Standort zu.

Protection Groups

Summary | Protection Groups | **Inventory Preferences** | Permissions

This diagram indicates mappings between resources on the primary site and its secondary site. Resources used by a protected virtual machine on the primary site will be replaced by the mapped resources in the shadow virtual machines on the secondary site.

[Refresh](#) [Edit...](#) [Remove](#)

Primary Site Resources	Secondary Site Resources	Secondary Site Path
Networks		
vim22dc	---	
VM Network	VM Network	/Networks/vim23dc/
Compute Resources		
vim22dc	---	
vim22.eng.vmware.com	None Selected	
shared	None Selected	
local services	None Selected	
protected services	recovery	/Hosts & Clusters/vim23dc/vim23.eng.vmware.com/shared/
Virtual Machine Folders		
vim22dc	None Selected	
shared	recovery	/Hosts & Clusters/vim23dc/shared/



Einrichtung – Schutzgruppe

Eine Schutzgruppe ist eine Gruppe von VMs, für die ein Failover am Recovery-Standort durchgeführt wird

- Während Sie den Assistenten für Schutzgruppen durchlaufen, müssen Sie einen Speicherort für temporäre VirtualCenter Bestandslistendateien für die geschützten VMs am Recovery-Standort auswählen.

Create Protection Group

Datastore
Select a datastore in which to store the files for the virtual machines in this protection group

Name
Virtual Machines
Datastore
Configure VMs

Datacenters

- vim23dc
 - vim23-storage1

SRM erfordert einen Speicherort für die temporären VirtualCenter-Bestandslistendateien für die geschützten virtuellen Maschinen für die erstellte Schutzgruppe. Diese temporären Dateien sollten vorzugsweise in einem nicht replizierten Datenspeicher am Wiederherstellungsstandort abgelegt werden.

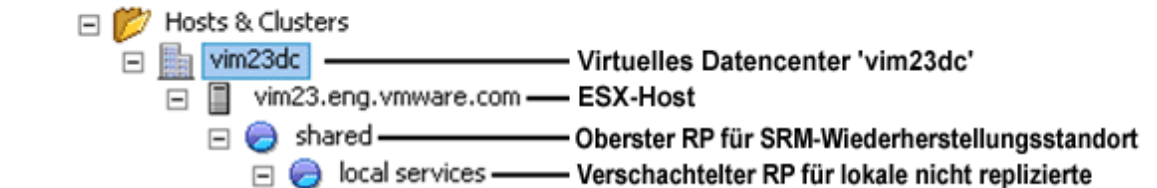
Im Datacenter vim 23dc, der den bezeichneten Wiederherstellungsstandort darstellt, sollten die temporären Dateien idealerweise im Datenspeicher vim23-storage1 abgelegt werden.



Einrichtung – Schutzgruppe

- Im Assistenten für Schutzgruppen wählt ein Benutzer aus, welche VMs geschützt werden müssen, und weist sie einer Schutzgruppe zu
- Die Erstellung einer Schutzgruppe führt zu Aktualisierungen der VC-Bestandsliste am Recovery-Standort

SRM-WIEDERHERSTELLUNGSSTANDORT NACH DER KONFIGURATION VON SRM-SCHUTZGRUPPEN



```

root@vim23:/vmfs/volumes/vim23-storage1/app_vm12
[root@vim23 vim23-storage1]# cd app_vm12
[root@vim23 app_vm12]# ls -al
total 1216
drwxr-xr-x  1 root  root    700 Feb  6 21:58 .
drwxrwxrwt  1 root  root   4760 Feb 11 16:03 ..
-rw-----  1 root  root      0 Feb  6 21:58 app_vm12.vmsd
-rw-r--r--  1 root  root    911 Feb  6 21:58 app_vm12.vmx
-rw-----  1 root  root   263 Feb  6 21:58 app_vm12.vmxfs
[root@vim23 app_vm12]#
    
```

- app_vm2
- app_vm3
- app_vm4
- app_vm5
- app_vm6
- app_vm7
- app_vm8
- app_vm9

wiedernerstellungs -RP registriert sind, der während der Konfiguration der SRM-Bestandslisteneinstellungen angegeben wurde.

Die VMs werden in der VC-Bestandsliste während der Konfiguration der SRM-Schutzgruppen registriert.

Einrichtung – Recovery-Standort

Am Recovery-Standort werden folgende Schritte zur Einrichtung ausgeführt:

- Der Benutzer erstellt einen Recovery-Plan, der mit einer einzelnen oder mehreren Schutzgruppen verknüpft ist

dr-vc-vim23.eng.vmware.com - VMware Infrastructure Client

File Edit View Inventory Administration Plugins Help

Inventory Scheduled Tasks Events Administration Maps Consolidation Site Recovery

Add Repair

Site Recovery

- Protection Groups
- Recovery Plans
 - Recovery Plan 1 - Protection Group 1
 - Recovery Plan 2 - Protection Group 2
 - Recovery Plan 3 - Complete Site Failover

Wiederherstellungspläne werden über den VI-Client hinzugefügt, der am Wiederherstellungsstandort mit dem VC-Server verbunden ist.

Klicken Sie in der obigen Symbolleiste auf die Schaltfläche „Add“, oder klicken Sie im Abschnitt „Commands“ auf „Add Recovery Plan“, um den Assistenten für Wiederherstellungspläne zu starten

Recovery Plans

Summary Recovery Plans Permissions

General

Recovery Plans: 3

Commands

- Add Recovery Plan
- Repair SAN Recovery Settings

vCenter Site Recovery Manager-Recovery-Plan

Geringe Priorität
VM-Wiederherstellung



Bereinigung
nach Test

Zurücksetzen
virtuelle
Festplatte



4. Recover VM "app_vm10"
5. Recover VM "app_vm11"
6. Recover Low Priority Virtual Machines
7. Recover No Power On Virtual Machines
8. Cleanup Virtual Machines Post Test
1. Remove Test VM "app_vm7"
2. Remove Test VM "app_vm8"
3. Remove Test VM "app_vm9"
4. Remove Test VM "app_vm10"
5. Remove Test VM "app_vm11"
6. Remove Test VM "app_vm12"
9. Cleanup DRS Clusters
10. Resume Non-critical Virtual Machines
11. Reset Virtual Disks Post Test
1. Reset Disks for Protection Group "Protection Group 2"

VMs, die am Wiederherstellungsstandort während eines 'Tests' des Wiederherstellungsplans eingeschaltet werden, werden am Wiederherstellungsstandort im Zuge der Prozeduren nach dem Test ausgeschaltet.

Der SRM-Wiederherstellungsstandort wird zurückgesetzt und verbleibt im Status „Bereit“ für das nächste SRM-Test- oder Failover-Ereignis aufgrund eines erklärten Notfalls.

vCenter Site Recovery Manager-Recovery-Pläne:

- Umwandeln manueller **BC/DR-Run-Books** in automatischen Prozess
- Festlegen der Schritte des Recovery-Vorgangs in VirtualCenter
- Bereitstellen einer Testmöglichkeit für BC/DR-Plan in einer isolierten Umgebung am Recovery-Standort ohne Beeinträchtigen der geschützten VMs am geschützten Standort



Testen eines Recovery-Plans

‘Testen’ Sie Recovery-Pläne durch Simulieren eines Failovers geschützter VMs ohne Ausfallzeit auf die geschützten VMs am geschützten Standort

dr-vc-vim23.eng.vmware.com - VMware Infrastructure Client

File Edit View Inventory Administration Plugins Help

Inventory Scheduled Tasks Events Administration Maps Consolidation Site Recovery

Test Pause Resume Stop Run

Site Recovery

- Protection Groups
- Recovery Plans
 - Recovery Plan 1 - Protection Group 1
 - Recovery Plan 2 - Protection Group 2
 - Recovery Plan 3 - Complete Site Failover

Recovery Plan 2 - Protection Group 2

Summary Virtual Machines Recovery Steps History Permissions

General

Name: Wiederherstellungsplan2 - Schutzg...
Description: Teil-Failover für app_vm7 auf ei...
Status:

Commands

- Edit Recovery Plan
- Test Recovery Plan
- Execute Recovery Plan
- Delete Recovery Plan

Tasks Alarms Administrator

Erweitern Sie auf dem VI-Client am Wiederherstellungsstandort im linken Teilfenster den Eintrag „Recovery Plans“, und wählen Sie den zu testenden Wiederherstellungsplan aus. Der simulierte Failover-Test kann gestartet werden, indem Sie entweder auf die oben hervorgehobene Schaltfläche 'Test' oder auf den Link 'Test Recovery Plan' im Abschnitt 'Commands' klicken

Ausführen des Failovers

The screenshot shows the VMware Infrastructure Client interface. The title bar reads "dr-vc-vim23.eng.vmware.com - VMware Infrastructure Client". The menu bar includes "File", "Edit", "View", "Inventory", "Administration", "Plugins", and "Help". The toolbar contains icons for "Inventory", "Scheduled Tasks", "Events", "Administration", "Maps", "Consolidation", and "Site Recovery". Below the toolbar, there are control buttons for "Test", "Pause", "Resume", "Stop", and "Run". The left pane shows a tree view under "Site Recovery" with "Protection Groups" and "Recovery Plans". "Recovery Plan 2 - Protection Group 2" is selected. The right pane shows the details for "Recovery Plan 2 - Protection Group 2", with tabs for "Summary", "Virtual Machines", "Recovery Steps", "History", and "Permissions". The "Recovery Steps" tab is active, showing a "General" section with fields for Name, Description, and Status, and a "Commands" section with buttons for "Edit Recovery Plan", "Test Recovery Plan", "Execute Recovery Plan", and "Delete Recovery Plan". A red box highlights the "Execute Recovery Plan" button. A text box at the bottom left contains instructions in German.

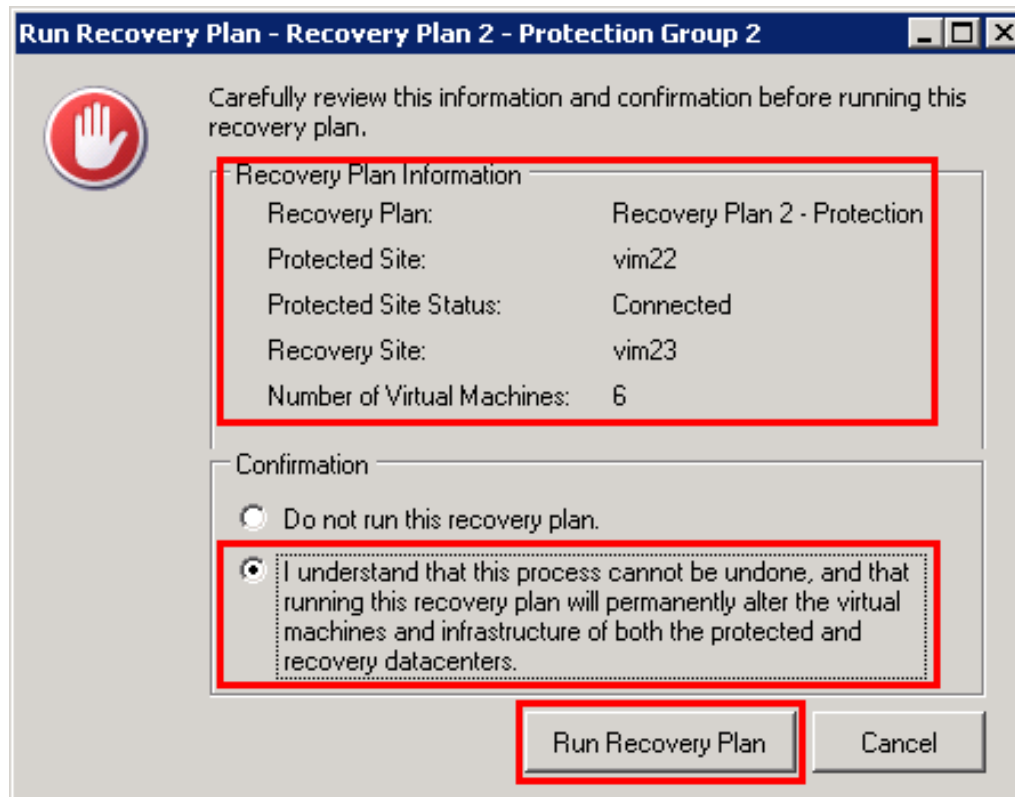
Erweitern Sie auf dem VI-Client am Wiederherstellungsstandort im linken Teilfenster den Eintrag „Recovery Plans“, und wählen Sie den bei Failover auszuführenden Wiederherstellungsplan aus. Der Failover kann gestartet werden, indem Sie entweder auf die oben hervorgehobene Schaltfläche 'Run' oder auf den Link 'Execute Recovery Plan' im Abschnitt 'Commands' klicken

WARNUNG - Die Ausführung eines echten Failovers verändert dauerhaft die virtuellen Maschinen und die Infrastruktur des geschützten und des Recovery Standorts



Ausführen des Failovers

WARNUNG - Die Ausführung eines echten Failovers verändert dauerhaft die virtuellen Maschinen und die Infrastruktur des geschützten und des Recovery Standorts





Alarmer und Statusüberwachung des Standorts

vCenter Site Recovery Manager unterstützt folgende Alarmaktionen:

- Senden einer E-Mail an festgelegte Adresse
- Senden einer SNMP-Trap an VC-Trap-Empfänger
- Ausführen eines festgelegten Befehls auf VC-Host

Wir empfehlen die Einrichtung von Alarmbenachrichtigungen in folgenden Fällen:

- Remote-Site nicht verfügbar
- Anpingen der Remote-Site fehlgeschlagen
- Replikationsgruppe entfernt
- Recovery-Plan zerstört
- Lizenzserver nicht erreichbar



vCenter Site Recovery Manager-Serverüberwachung

vCenter Site Recovery Manager löst VirtualCenter-Ereignisse für folgende Bedingungen aus:

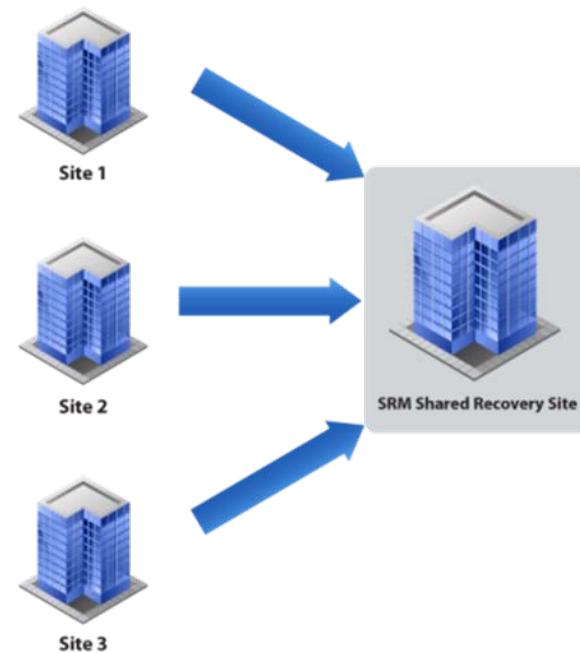
- Wenig Festplattenspeicher
- CPU-Nutzung übersteigt Grenzwert
- Wenig Arbeitsspeicher
- Remote-Site antwortet nicht
- Test des Recovery-Plans gestartet, beendet, erfolgreich, fehlgeschlagen oder abgebrochen
- Wiederherstellung der virtuellen Maschine gestartet, beendet, erfolgreich, fehlgeschlagen oder gibt eine Warnung zurück

vCenter Site Recovery Manager - Neuerungen

NFS SUPPORT

ESX 4 SUPPORT

MANY TO ONE FAILOVER





Was sollten Sie bei der Planung berücksichtigen!

Machen Sie sich über folgendes im Projekt Gedanken:

- Synchroner Spiegelung
- Asynchroner Spiegelung
- Block Level Konsistenz
- VMDK Konsistenz
- Filesystem Konsistenz
- Applikations Konsistenz



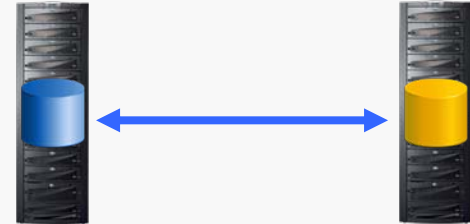
SRDF Family

The ultimate business continuity and disaster recovery solution for the broadest range of use cases



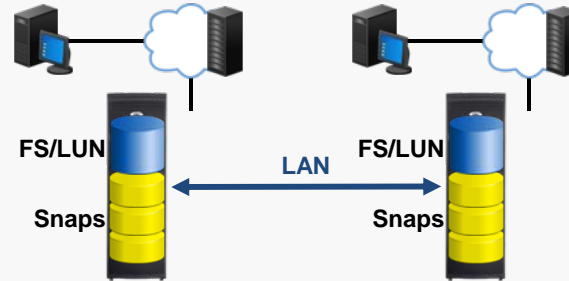
MirrorView

Synchronous replication for flexible recovery-point and recovery-time objective requirements



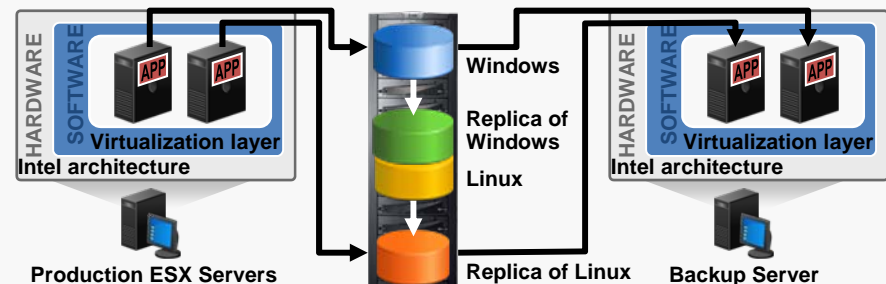
Celerra Replicator

IP replication with Quality of Service to optimize LAN/WAN bandwidth utilization



RecoverPoint

Host, array, fabric continuous data protection (CDP), continuous remote replication (CRR), concurrent local and remote (CLR) data protection; and compression





www.artaker.at

Ing. Alexander Kuchelbacher
Consulting IT-Infrastructure & Virtualization

a.kuchelbacher@artaker.at

*Artaker Computersysteme GmbH
Heumühlgasse 11
A-1040 Wien
Tel. 01 / 588 52 – 180
Fax. 01 / 588 52 - 52
E-Mail: office@artaker.at*