Link: https://www.tecchannel.de/a/sichere-infrastruktur-fuer-e-mail-systeme,1779571

E-Mail-Security
Sichere Infrastruktur für E-Mail-Systeme

Datum: 21.01.2009
Autor(en): Johann Baumeister

Auf Grund seiner unternehmenskritischen Stellung muss das E-Mail-System gegen Ausfall abgesichert sein, Compliance-Regeln fordern den Schutz vor Datenverlust. Backup, CDP und Cluster sind Bausteine einer Sicherheitsstrategie.

Der Einsatz von elektronischen Nachrichten ist für Firmen längst zu einem unternehmenskritischen Faktor geworden. Ein Ausfall des E-Mail-Systems führt in den meisten Fällen zu gravierenden Leerzeiten und Verzögerungen bei den betrieblichen Abläufen. Daher wird eine permanente Verfügbarkeit des E-Mail-Systems erwartet – ja sogar gefordert. Dennoch lassen sich Hardware-Ausfälle oder Systemfehler nicht gänzlich ausschließen. Umso wichtiger ist es deshalb, im Fehlerfall die Betriebsbereitschaft mitsamt der schnellen Wiederherstellung der alten E-Mails sicherzustellen.

1. E-Mail-Inhalte umfassen mehr als nur Nachrichten

Für die Betriebssicherheit muss man zwischen dem Zugang zu den eigenen E-Mail-Daten und der Verfügbarkeit des E-Mail-Systems an sich unterscheiden. Ist der Zugang gestört, so sind natürlich auch alle Daten in diesem Moment nicht verfügbar.

Bei den E-Mail-Daten sind aber nicht nur die E-Mail-Nachrichten gemeint, sondern alle im E-Mail-System hinterlegten Inhalte. Oft arbeiten die E-Mail-Server gleichzeitig als Groupware-Server. Im Fall von Microsoft Exchange sind neben den eigentlichen E-Mails und deren Anhängen auch die Kontakte, die Aufgabenlisten und der Terminkalender bei einem Ausfall nicht mehr erreichbar.

Ist kein Zugang zum E-Mail-System mehr möglich, so führt das zu einer weitreichenden Einschränkung des Arbeitsumfelds. Ohne Kontaktdaten nützt dann häufig auch das Telefon nicht mehr viel. Werden gar Unified-Communication-Systeme eingesetzt, so versagt mit einem Ausfall der E-Mail-Server auch das Telefon.

Die Abhängigkeit vom E-Mail-System sollte insbesondere bei Disaster-Recovery-Szenarien beachtet werden. Es nützt wenig, wenn die wichtigen Telefonnummern und Anweisungen für den Fehlerfall just auf den Servern hinterlegt sind, die gerade ausgefallen sind.

In unserer Artikelserie zu Sicherheitsaspekten beim Einsatz von E-Mails widmete sich der erste Teil der **Absicherung des Posteingangs**[1], der zweite des **Postausgangs**[2]. In diesem abschließenden dritten Teil betrachten wird den Schutz des E-Mail-Systems gegen Ausfälle jeglicher Art.

Artikelserie

Teil 1: **Regeln für das sichere Erstellen von E-Mails**[16]

Teil 2: **Regeln und technische Schutzmaßnahmen beim E-Mail-Empfang**[17]

Teil 3: **Sichere Infrastruktur für E-Mail-Systeme**[18]

2. Absicherung der Daten und Programme

Die Absicherung des E-Mail-Systems muss sich auf alle notwendigen Daten und auch Prozesse beziehen. Aus Sicht der betroffenen Benutzer macht es keinen Unterschied, ob fehlende Daten, ein überlastetes Netzwerk oder ein ausgefallener Server-Dienst die Ursache für die Störung sind. Daher verschmelzen alle beteiligten Bausteine bei den Schutzkonzepten zu einer Einheit. Die traditionellen Backup-Verfahren sind inzwischen von komplexeren IT-Absicherungen abgelöst.

3. Vom RAID zum Geocluster

Beim Schutz der E-Mail-Daten gilt es auch das geografische Ausmaß des Datenschutzes zu betrachten. Die Spiegelung der Mail-Speicher, beispielsweise durch den Einsatz eines RAID-Verbunds, sichert die Daten vor dem Ausfall der Festplatte. Für den Ausfall des kompletten Rechners jedoch bieten RAID-Arrays keinen Schutz. Hiergegen hilft die Spiegelung auf ein separates Festplattensystem. Befindet sich dieser Plattenspiegel jedoch im gleichen Raum, so sind die Daten zwar vor dem Ausfall des Rechners, aber nicht vor dem Ausfall der Stromversorgung für diesen Raum abgesichert. Dies gilt auch bei sonstigen „lokalen Katastrophen“ wie etwa Feuer oder Hochwasser.

Um auch dagegen gewappnet zu sein, müssen die Sicherungssysteme weit genug von den primären Systemen, die es abzusichern gilt, entfernt sein. Dieser Gedanke lässt sich mehrfach fortführen und findet seine Ende in der Platzierung von Datenspiegeln oder Ausweichrechenzentren auf unterschiedlichen Kontinenten. Ob dabei nur die Daten gegen Verlust gesichert sind oder auch die E-Mail-Server selbst, ist im Prinzip beim Geoclustering unerheblich.

4. Datensicherung durch Backups

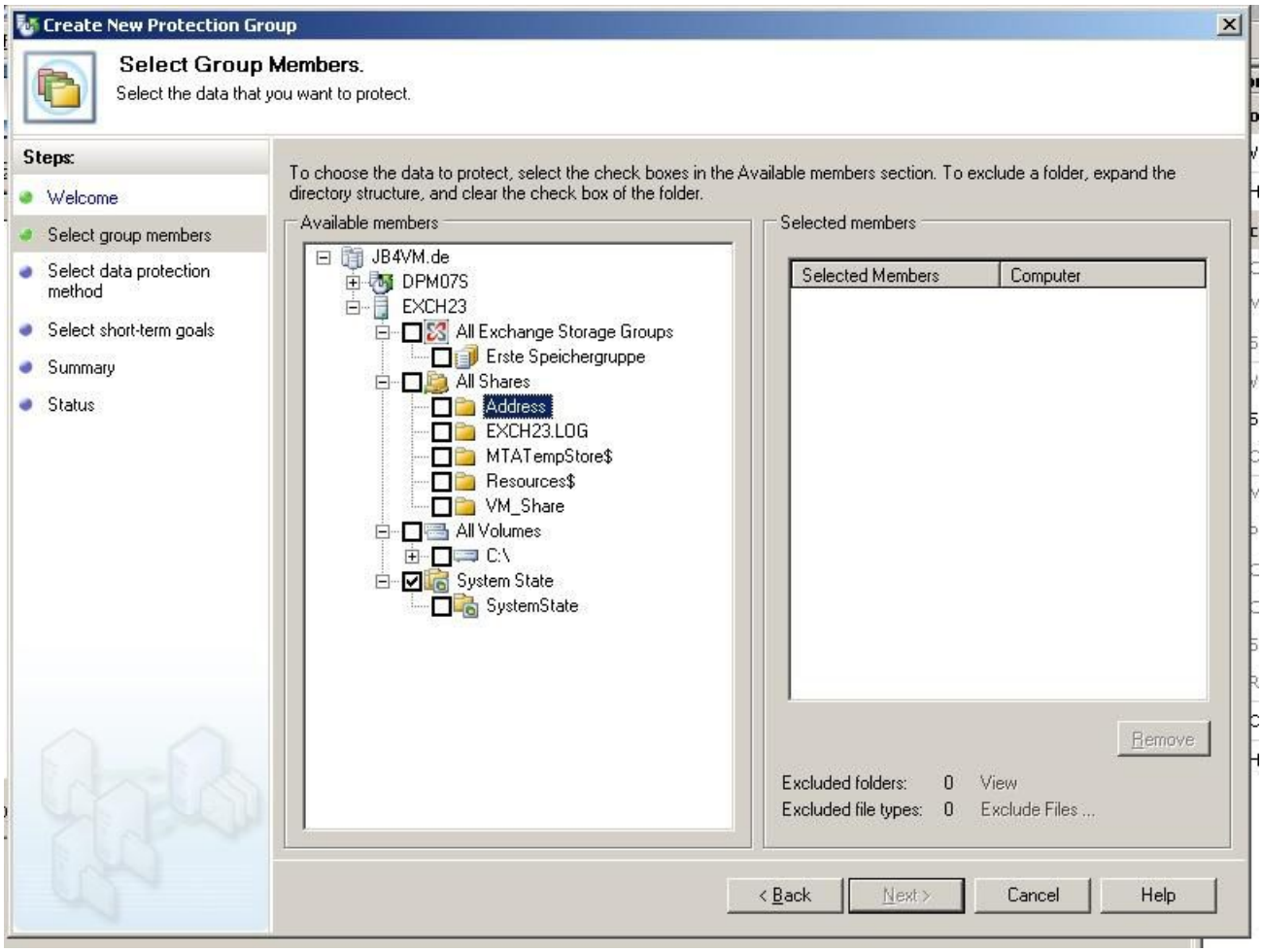
Der traditionelle Weg der Datensicherung erfolgt durch periodische Kopiervorgänge der Daten auf externe Bandmedien oder auch Bandbibliotheken. Die gängigsten Verfahren hierbei sind die Vollsicherung, die inkrementelle Sicherung oder differenzielle Sicherung. Die Sicherungen laufen meist in Zeiten mit wenig Last wie nachts oder am Wochenende.

Bei täglichen Backups kann der Datenverlust im Störungsfall einen ganzen Arbeitstag betragen. Auch der Wiederherstellvorgang selbst kann mehrere Stunden bis Tage dauern. Das Angebot an Sicherungstools in diesem Segment ist recht umfangreich. Dazu gehören beispielsweise die Werkzeuge von CA (**ARCserve**[3]), EMC (**Legato Networker**[4]), HP (**Data Protector**[5]), IBM (**Tivoli Storage Manager**[6]) und Symantec (**Backup Exec**[7]). Daneben stehen aber auch noch viele kleinere Anbieter, die ähnliche Produkte offerieren.

5. Kontinuierliche Sicherung der Daten

Die traditionelle Sicherung hat den Nachteil eines relativ großen Datenverlusts und einer langen Wiederherstellungszeit. Durch die kontinuierliche Datensicherung (Continuous Data Protection / CDP) werden beide Werte reduziert. Die CDP-Sicherungsverfahren arbeiten meist mit sehr kleinen Sicherungsintervallen bis hinab zu wenigen Minuten. Gesichert wird meist auf Plattensysteme. Diese können im gleichen Raum oder weit entfernt stehen. Entfernte Sicherungssysteme werden über IP-Strecken angebunden und erfüllen implizit die Forderung nach einer Standortsicherung.

CDP-Verfahren bringen aber auch Änderungen hinsichtlich der Wiederherstellung der Mail-Daten. Die Rücksicherung kann meist durch die Benutzer selbst vorgenommen werden. Zur Umsetzung von CDP existieren sowohl eigene Server-Lösungen als auch eine Kombination mit globalen Speichersystemen und eigenen Routinen zur Datenspiegelung.



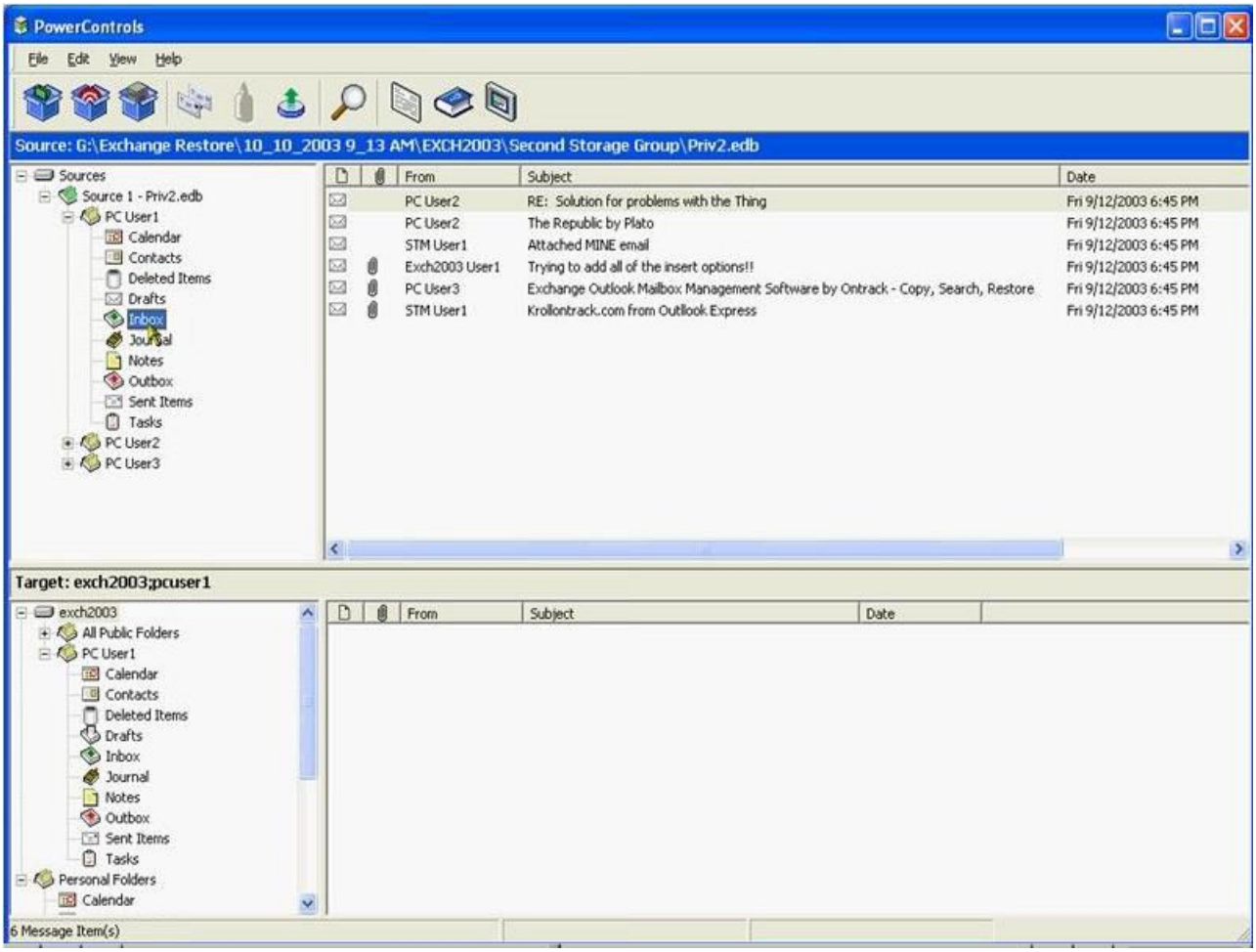
DPM: Der Data Protection Manager von Microsoft sichert nach dem CDP-Verfahren. In der Protection Group werden die zu sichernden Daten beschrieben.

Die Anbieter der traditionellen Sicherungswerkzeuge bieten meist auch Varianten ihrer Tools mit der Möglichkeit zur kontinuierlichen Datensicherung an. Hinzu kommen aber auch spezialisierte Anbieter. Microsoft hat mit dem **Data Protection Manager**[8] (DPM) eines dieser Werkzeuge im Angebot. Der Data Protection Manager weist auch die notwendigen Interfaces zur Sicherung der Exchange-Inhalte auf. Zur Sicherung der Daten auf das Zweitsystem greift Microsoft auf einen im Betriebssystem verankerten Dienst, den Volume Shadow Service, zurück. Der potenzielle Datenverlust im Fehlerfall sinkt auf den Zeitpunkt seit der letzten Sicherung der Daten, dies sind im Minimum 15 Minuten. Die von den überwachten Exchange-Servern eingesammelten Daten speichert der DPM in einem Datenpool. Bei größeren Umgebungen legt man diesen auf ein separates Speichersystem.

Partielle Rücksicherung von E-Mail-Inhalten

Bei der traditionellen Bandsicherung sind immer vollständige Datenbestände als Einheit zurückzusichern. CDP ermöglicht hingegen eine feinere Abstufung der Rücksicherung sowie auch eine Wiederherstellung der Inhalte direkt durch die Benutzer.

Doch in der Praxis werden oftmals nur einzelne E-Mails oder Ordner gelöscht. Ein vollständiger Restore des gesamten Servers mit allen Daten wäre in diesem Fall kaum angemessen. Außerdem müssten dann auch alle Änderungen, die seit dem letzten Sicherungslauf von Nutzern vorgenommen wurden, aufwendig und manuell mit dem wiederhergestellten E-Mail-Bestand zusammengefügt werden.



Kroll Ontrack: Die PowerControlls erlauben das Management von Postfächern und einzelnen E-Mails.

Zur selektiven Wiederherstellung von einzelnen E-Mails, Postfächern oder sonstigen Inhalten dienen daher Erweiterungen zur Exchange-Datensicherung. Dazu zählen unter anderem die **PowerControls**[9] von Kroll Ontrack oder der **Recovery Manager**[10] für Exchange von Quest. Diese Tools erlauben eine sehr feingranulare Wiederherstellung von Informationen.

6. Sicherung des Exchange-Mail-Systems

Die bis dato betrachteten Varianten fokussierten sich auf die Sicherung der Daten. Um auch die Prozesse, also den Exchange-Server-Dienst, gegen den Ausfall abzusichern bieten sich unterschiedliche Verfahren an:

- Imaging und Snapshooting
- CDP mit Failover kombiniert

- Clustering der Exchange-Server
- Duplizierung aller Komponenten
- Virtualisierung

7. Imaging und Snapshooting

Beim Imaging oder Snapshooting werden Festplatten oder Partitionen eines Rechners als eine Einheit kopiert. Da hierbei direkt und unter Umgehung des Dateisystems auf die Festplatten zugegriffen wird, ist es konkurrenzlos schnell. Es eignet sich vor allem dann, wenn von einem Rechnersystem eine Kopie erzeugt werden soll beziehungsweise diese im Fehlerfall schnell wiederhergestellt werden muss.

Dieses Vorgehen wird als Bare-Metal-Restore bezeichnet. Der Nachteil ist, dass das gesicherte Image nur auf einer nahezu identischen Hardware lauffähig ist. Durch das Imaging lassen sich nur fertig konfigurierte Server mitsamt Betriebssystem und Applikationen sinnvoll absichern. Zur Sicherung von Daten ist das Verfahren nicht geeignet. Die Daten müssen getrennt gesichert und im Fehlerfall eingebunden werden.

8. CDP mit Failover kombiniert

Die Werkzeuge dieser Kategorie ermöglichen eine Absicherung von Server-Systemen über IP-Strecken hinweg. Über spezielle Integratoren erfolgt die Anbindung an die E-Mail-Systeme wie etwa Exchange. Gesichert werden sowohl die Daten als auch die Applikationsdienste und alle Konfigurationseinstellungen der Registry. Durch den Rückgriff auf eine IP-Verbindung ist der Einsatz auf keine Region begrenzt.

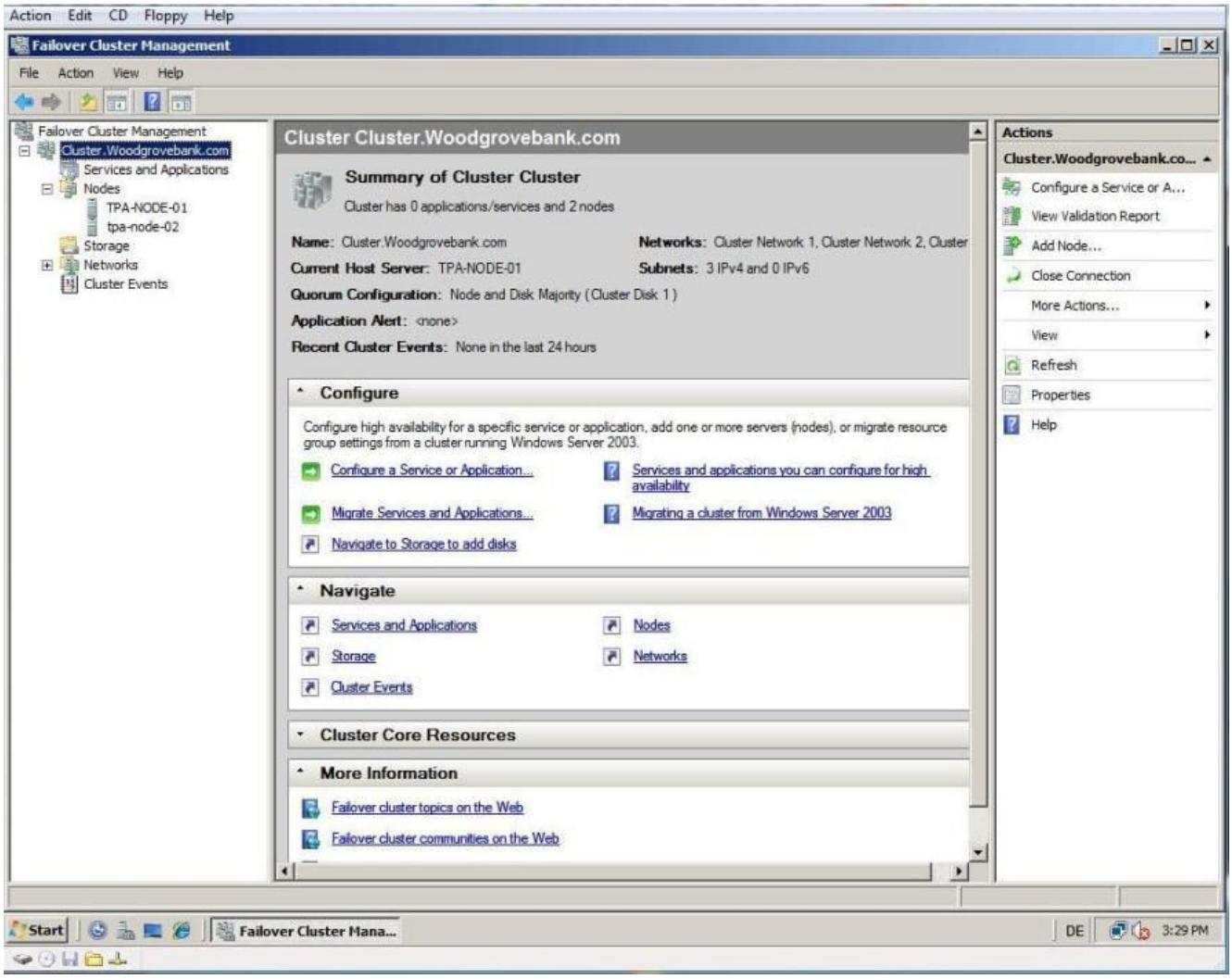
Das Prinzip dieser Verfahren basiert auf zwei identischen Rechnersystemen im Aktiv/Passiv-Betrieb. Der aktive Rechner spiegelt dabei seine Daten fortwährend an den passiven Partner. Dessen Rolle ist die Entgegennahme der Daten vom aktiven Partner und die Überwachung dessen auf Funktionsfähigkeit. Dies passiert durch einen Heartbeat, der zwischen den Geräten ausgetauscht wird.

Durch den Einsatz von IP als Kommunikationsverbindung können diese Verfahren sowohl zur Absicherung von Server-Systemen in Rechenzentren als auch für das Desaster Recovery über Weitverkehrsnetzen (WAN) eingesetzt werden. Im Fehlerfall übernimmt der bis dato passive Rechner die Arbeit des ausgefallen aktiven Geräts.

Zu den Anbietern in diesem Segment zählen **Neverfail Heartbeat**[11] von Neverfail, **Doubletake**[12] oder etwa **WANsync von CA**[13]. Wenngleich die prinzipiellen Ausführungen der Tools vergleichbar sind, gibt es Unterschiede in der Implementierung. Diese liegen beispielsweise darin, ob die verwendeten Server-Systeme hinsichtlich der Hardware identisch sein müssen oder nicht. Neverfail beispielsweise verlangt keine gleiche Hardware. Die Rechner dürfen sich durchaus bezüglich der CPU, des BIOS, des Mainboards, des Speicherausbaus oder der Netzwerkanbindung unterscheiden. Damit erlaubt Neverfail auch den Einsatz eines älteren Rechners, der nicht die gleichen Leistungswerte aufweisen muss wie das primäre System.

9. Absicherung durch Clustering

Die geringste Ausfallzeit und damit die höchste Verfügbarkeit erreicht man mit einem Failover-Cluster. Hierbei handelt es sich um vollständig redundante Server-Systeme, die mit einem gemeinsamen Datenträger ausgestattet sind. Alle Knotenrechner zusammen bilden eine Ressourcengruppe. Diese tritt nach außen als ein geclusterter Dienst in Erscheinung. Folglich wird der gesamte Failover-Cluster als ein einzelner Exchange-Server im Netzwerk dargestellt. Dahinter verbergen sich aber mehrere Knoten des Clusters.



MS-FO-Cluster: Im Windows Server 2008 hat Microsoft die Verwaltung der Cluster vereinfacht und stellt dazu einen Cluster Manager bereit.

Im Fehlerfall, also bei Ausfall eines dieser Knoten, übernehmen die anderen den Dienst. Dies kann, sofern die Applikation mitspielt, völlig unbemerkt vom Benutzer erfolgen. Damit federn Failover-Cluster Ausfälle einer Server-Hardware, aber auch des Mail-Servers ab, denn der Benutzer wird bei korrekter Funktionsweise davon nichts bemerken. Im Windows Server 2008 hat Microsoft diese Cluster-Funktionen vereinfacht. Das Aufsetzen und Betreiben eines Clusters wird damit gegenüber der Vorgängerversion bedeutend einfacher. Neu ist auch die Unterstützung von geografisch verteilten Clustern.

10. Duplizierung aller Komponenten

Eine andere Variante des Ausfallschutzes verwendet eine Duplizierung aller Komponenten, von der Hardware über alle Software-Systeme hinweg. Als Anbieter in diesem Segment fungiert **Stratus**[14] mit seinem ftServer. Dabei handelt es sich genau genommen um zwei identische Server-Systeme im 19-Zoll-Formfaktor, die sich gegenseitig überwachen. Durch eine Verlängerung des Rechnerbusses über ein Zusatzmodul an der Rückseite des Geräts erfolgt die Durchschleusung der Signale an dem Partnerrechner.

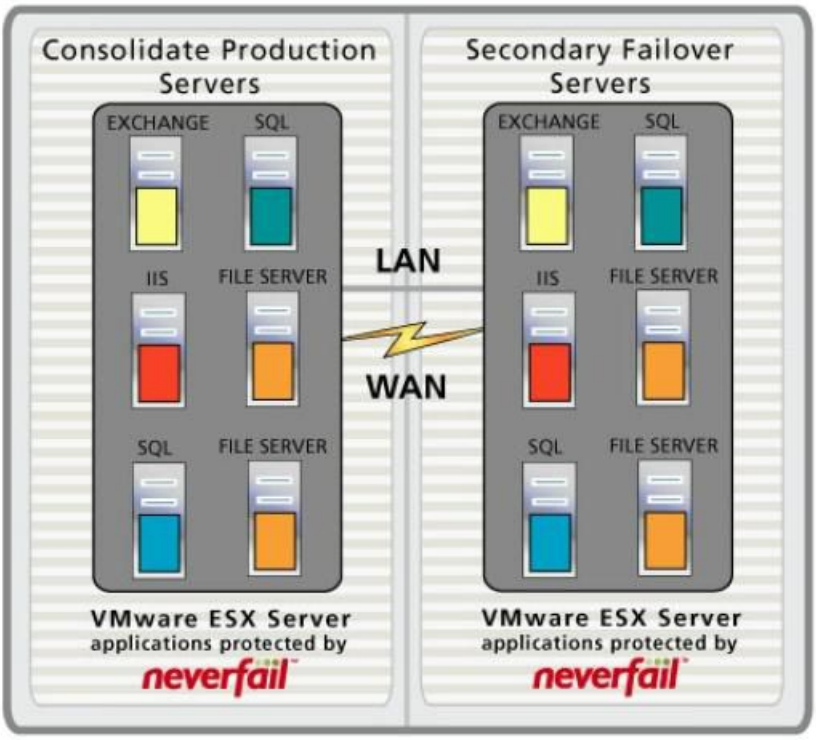
Server-Spiegelung: Stratus dupliziert in seiner ft-Server-Reihe alle Komponenten. Die beiden Server sichern sich und die Applikationen dabei gegenseitig ab.

Beim Ausfall einer Komponente übernimmt der noch fehlerfrei operierende Partner dessen Aufgaben. Das Verfahren arbeitet unabhängig von der Applikation und kann somit auch E-Mail-Server absichern. Der Vorteil dieses Verfahrens liegt in der Unabhängigkeit der Überwachung von jeglichen Software-Systemen. Auf dem Server-System dürfen sich daher auch weitere Dienste befinden, die parallel mit abgesichert werden.

Nachteilig erweist sich, dass die sich überwachenden Baugruppen aufgrund technischer Gegebenheiten, wie der Signallaufzeiten, in unmittelbarer Nachbarschaft stehen müssen. Eine Hochverfügbarkeit über Räume hinweg oder gar größere Distanzen ist damit nicht machbar.

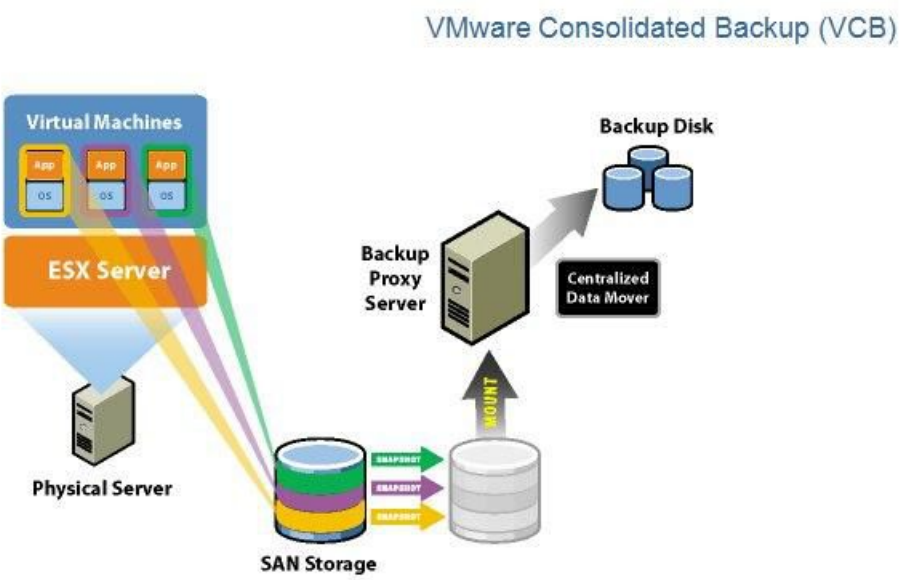
11. Neue Sicherungsverfahren durch Virtualisierung

Zu den neuesten Verfahren der Server-Absicherungen zählen Virtualisierungslösungen. Hierbei läuft ein Server in einer virtuellen Umgebung auf einem physischen Host-Server. Fällt der Host-Server aus, so wird die virtuelle Instanz kurzerhand auf einem anderen Host neu gestartet. Die Logik zur Überwachung des Gesamtsystems mitsamt dem Transfer der virtuellen Maschinen hat beispielsweise VMware in **vMotion**[15] und den Distributed Resource Scheduling bereits integriert.



Virtuelle Sicherheit: VMware Neverfail ist in der Lage, virtuelle Server, die unter der Verwaltung des VMware ESX stehen, abzusichern.

Das Verfahren ähnelt dem, das unter „CDP mit Failover kombiniert“ erwähnt wurde. Die Absicherung der Daten ist aber ausgegliedert und erfolgt autark durch ein angeschlossenes Speichersubsystem. Nur die Server-Prozesse, also Betriebssystem mit Applikationen, laufen in virtuellen Maschinen.



VMware VCB: Durch Consolidated Backup sichert VMware die Inhalte der virtuellen Maschinen mitsamt ihren Applikationen.

12. Fazit

Zur Absicherung der E-Mail-Systeme gibt es mittlerweile eine Vielzahl an unterschiedlichsten Verfahren. Gegenüber den traditionellen Konzepten mit einem Restore der Daten im Fehlerfall hat sich inzwischen eine Reihe von weitaus effizienteren Techniken entwickelt, die bedeutend leistungsfähiger sind. Diese ermöglichen eine gleichzeitige Absicherung von Daten und Applikationen. Wenn notwendig, kann dies selbst über weite Entfernungen erfolgen. Somit bieten diese Lösungen auch eine standortübergreifende Sicherheit. (ala)

Artikelserie

Teil 1: **Regeln für das sichere Erstellen von E-Mails**[19]

Teil 2: **Regeln und technische Schutzmaßnahmen beim E-Mail-Empfang**[20]

Teil 3: **Sichere Infrastruktur für E-Mail-Systeme**[21]

Links im Artikel:

[1] **https://www.tecchannel.de/kommunikation/e-mail/1778559/sicherer_postausgang/**
[2] **https://www.tecchannel.de/kommunikation/e-mail/1779570/e_mail_sicherheit_spam_filter_mailbox_backup/index.html**
[3] **http://www.ca.com/de/products/product.aspx?ID=4536**
[4] **http://www.legato.com/**
[5] **http://h10010.www1.hp.com/wwpc/at/de/sm/WF05a/18964-18964-304618-305392-305392-1144272.html**
[6] **http://www.ibm.com/software/tivoli/products/storage-mgr/**
[7] **http://www.symantec.com/de/de/business/backup-exec-for-windows-servers**
[8] **http://www.microsoft.com/germany/systemcenter/dpm/default.mspx**
[9] **http://www.ontrack.de/powercontrols/**
[10] **http://www.quest.com/recovery-manager-for-exchange/**
[11] **http://www.neverfailgroup.com/products/heartbeat.aspx**
[12] **http://www.doubletake.com/**
[13] **http://www.ca.com/us/products/product.aspx?ID=5879**
[14] **http://www.stratus.de/**
[15] **http://www.vmware.com/de/products/vi/vc/vmotion.html**
[16] **https://www.tecchannel.de/kommunikation/e-mail/1778559/sicherer_postausgang/**
[17] **https://www.tecchannel.de/kommunikation/e-mail/1779570/e_mail_sicherheit_spam_filter_mailbox_backup/index.html**
[18] **https://www.tecchannel.de/link.cfm?pk=1779571**
[19] **https://www.tecchannel.de/kommunikation/e-mail/1778559/sicherer_postausgang/**
[20] **https://www.tecchannel.de/kommunikation/e-mail/1779570/e_mail_sicherheit_spam_filter_mailbox_backup/index.html**
[21] **https://www.tecchannel.de/link.cfm?pk=1779571**
