Exchange 2016 – Dienste wiederherstellen

alias „Restore-Exchange-Services-After-Failed-Update-Skript“

Bei einer Installation von Exchange Updates deaktiviert das Setup als erstes die relevanten Dienste und stoppt diese um das System zu schützen. Bei einem Fehlschlag der Installation kann dies jedoch dazu führen, dass danach alle Dienste deaktiviert bleiben. Passiert schon nicht? Leider habe ich dies schon auf einem Kunden- sowie auf meinem Testsystem gesehen.

Microsoft bietet einen entsprechenden KB-Artikel, in welchem alle Dienste inkl. dem Standard-Startmodus aufgeführt sind. Man kann nun die Liste akribisch durchgehen und anschliessend die Dienste starten, oder aber man nutzt ein Skript.

Ich habe mit meinen bisher noch kleinen PowerShell Kenntnissen ein kleines Skript zusammengestellt, welches folgendes durchführt:

- benötigte Windows Dienste auf „Automatisch“ stellen und gleich starten
- vorausgesetzte Exchange Dienste auf „Automatisch“ stellen und gleich starten
- restliche Exchange Dienste gem. Microsoft Standard konfigurieren
- Alle Dienste, welche auf „Automatisch“ stehen kontrollieren und starten, falls diese gestoppt sind

(Ausnahme: Software Protection)

ExchangeServicesDefaultStartup.ps1Herunterladen

SMTP Relay mit Exchange 2016 und NetScaler einrichten

Ich bin mich wieder frisch am Einarbeiten in das Thema Exchange.

Das Grundsetup mit Exchange 2016 habe ich recht schnell hingekriegt und auch den externen Zugang via NetScaler war dank eines Skriptes von meinem Kollegen einfach hergestellt. Nun wollte ich jedoch noch für div. Dienste einen einfachen internen SMTP Relay Server erstellen.

Eine erste Anleitung dazu fand ich dann relativ schnell bei Paul Cunningham (Link).

Leider funktionierte dies nicht ganz so im Web GUI. Der Grund lag einfach gesagt an einem Bug von Microsoft und die Lösung war Powershell. Die Anleitung dazu fand ich dann bei Jeff Guillet (Link).

Nun funktionierte mein SMTP Relay zwar wenn ich den Exchange Server direkt ansteuerte, jedoch nicht via NetScaler. Und dies wollte ich dann auch noch lösen:

Die Ursache warum ich via die bereits eingerichtete NetScaler Konfiguration den SMTP Relay nicht ansteuern konnte war mir recht schnell klar. Der Exchange Server unterscheidet die Empfangskonnektoren jeweils anhand der Quell-IP und via

NetScaler ist dies immer die SNIP.

Was musste nun getan werden?

Dem Exchange Server müssen verschiedene Quellen vorgegaukelt werden. Im NetScaler kann dies mittels einer weiteren SNIP eingerichtet werden. Wichtig hierbei ist jedoch, dass die jeweiligen SNIP Adressen den richtigen vServern mittels Net Profiles zugewiesen werden, da ansonsten die Appliance mittels Round Robin die SNIP wechselt.

Schritt 1 – Erstellen einer weiteren SNIP und Konfiguration der Net Profiles:

```
add ns ip 192.168.100.12 255.255.255.0 -vServer DISABLED -gui DISABLED
add netProfile NP-192.168.100.11 -srcIP 192.168.100.11
add netProfile NP-192.168.100.12 -srcIP 192.168.100.12
```

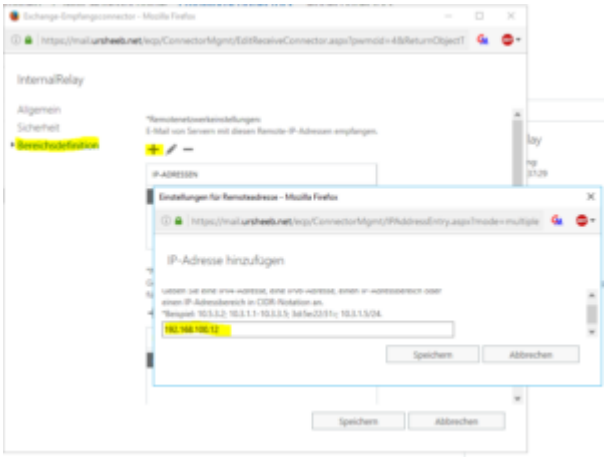
Schritt 2 – Erstellen eines weiteren LB vServers für den SMTP Relay:

```
add lb vserver lb-vsrv-mailrelay.domain.pit-SMTP TCP 192.168.100.90 25 -persistenceType NONE
bind lb vserver lb-vsrv-mailrelay.domain.pit-SMTP svc-smtp-pitex01
```

Schritt 3 – Net Profiles den LB vServern korrekt zuweisen:

```
set lb vserver lb-vsrv-mail.domain.pit-SMTP -netprofile NP-192.168.100.11
set lb vserver lb-vsrv-mailrelay.domain.pit-SMTP -netprofile NP-192.168.100.12
```

Schritt 4 – Empfangskonnektor für SMTP mit neuer SNIP konfigurieren:



Und nun viel Spass beim Nachbauen :-)

Quellen: The EXPTA {blog} & exchangeserverpro.com

Skript: NS-ExSMTPRelay

WSUS Fehler nach Installation KB3159706

Hallo zusammen

Microsoft schafft es doch immer wieder zu beweisen, dass deren QS die Aufgabe nicht erfüllt.
Nachdem ich die letzten Windows Updates auf dem WSUS Server installiert hatte, kam ich nicht mehr auf den Server.

Was nun?

Nach einigen Recherchen fand ich dann endlich den notwendigen Input im Microsoft Forum, welcher in meinem Fall genützt hat:

- CMD als Administrator starten
- Unter `%ProgramFiles%\Update Services\Tools` den Befehl

wsusutil.exe postinstall /servicing ausführen
- Im Server Manager das Feature HTTP Activation unter .NET Framework 4.5 Feature installieren
- WSUS Dienst neu starten

Danach funktionierte bei mir auch der WSUS wieder.

Viel Erfolg!

Gruppenfilter für GPOs nach MS16-072

Hallo zusammen

Letztens wollte ich eine GPO nur für eine Gruppe freigeben.
So wie ich es früher immer anstellte, entfernte ich die „Authenticated Users“ und fügte meine Gruppe hinzu.
Das Resultat danach war ernüchternd. Die GPO wurde nicht angewandt mit dem Grund ‚unbekannt‘ (wie immer sehr hilfreich).

Nach ein wenig Suchen fand ich in einer Microsoft Diskussion einen Hinweis auf das Security Update MS16-072 welches genau diesen Fehler verursacht.
Die „Lösung“ aus dem Artikel ist so einfach wie wirkungsvoll.
Die zuvor entfernte Gruppe „Authenticated Users“ muss man wieder hinzufügen, jedoch nur mit Leserecht und nicht das Recht die GPO anzuwenden.

Danach läuft alles wieder wie man es gewohnt ist.

WSUS – Cleanup automatisieren

Hallo zusammen und ein frohes neues Jahr :-)

Mir ist es schon letztes Jahr oft aufgefallen, dass beim Ausführen vom Server Cleanup Wizard innerhalb des Windows Server Update Service (WSUS) die Konsole in ein Timeout läuft. Ich hatte dies immer wieder auf die doch schon in die Jahre gekommene MMC Konsole geschoben. Dieses Jahr wollte ich endlich einmal die Serverbereinigung mittels Skript automatisieren und hatte da auch die Hoffnung, dass die Problematik nur ein GUI Problem sei, welches man über Skripting umgehen könnte. Leider war dies nicht der Fall und die Lösung kommt weiter unten…

Ich will es nicht verheimlichen, dass ich eigentlich alles zusammen kopiert habe. Jedoch will ich mit diesem Blog mehrere Beiträge zusammenfassen um den kompletten Weg einer automatisierten WSUS Bereinigung aufzuzeigen. Natürlich sind am Schluss alle Quellen genannt ;-)

Skript

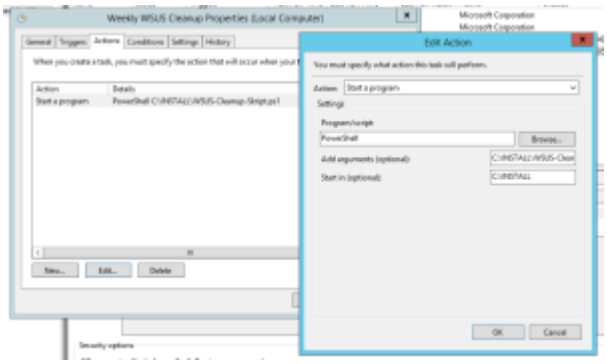
Als erstes habe ich eigentlich nur nach den notwendigen PowerShell Befehlen gesucht und ich wurde dann auf wsus.de mit einem kompletten Skript fündig.
WSUS-Cleanup-Skript (Skript als Textdatei) / Link zur Quelle: http://www.wsus.de/serverbereinigung2

Das Skript müsst ihr nur noch mit euern Parametern (Servername, Maileinstellungen, Bereinigungsparametern, etc.) anpassen und schon könnt ihr es als Administrator ausführen (UAC lässt grüssen).

Geplanter Task

Als nächstes muss ein geplanter Task erstellt werden. Weil es mein erster mit PowerShell war, musste ich mich auch hier schlau machen.
Fündig wurde ich dann hier: http://www.metalogix.com/help/Content%20Matrix%20Console/SharePoint%20Edition/002_HowTo/004_SharePointActions/012_SchedulingPowerShell.htm

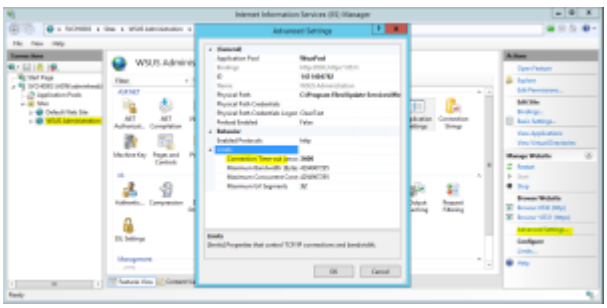
Zusammenfassend sind beim geplanten Task folgende Punkte zu beachten:
– ausführen ob Benutzer angemeldet ist oder nicht
– Benutzer des Tasks muss lokaler Administrator sein (Run as Admin)
– Ausgeführt wird PowerShell mit dem Skriptpfad als Argument



Timeout Problem

Bei einer grossen Menge an Updates wird der WSUS in ein Timeout laufen:

Um dem Abhilfe zu schaffen müsst ihr dieses Timeout im IIS anpassen:



IIS > Sites > WSUS Administration / Advanced Settings… / Limits > Connection Time-out (seconds)
Ich habe dieses bei meinem Server nun von 180 auf 3600 Sekunden erhöht und seither läuft die Bereinigung ohne Probleme.

Viel Erfolg beim Einrichten :-)

> *Quellen:*
> *http://www.wsus.de*
> *http://www.metalogix.com*
> *http://social.technet.microsoft.com*

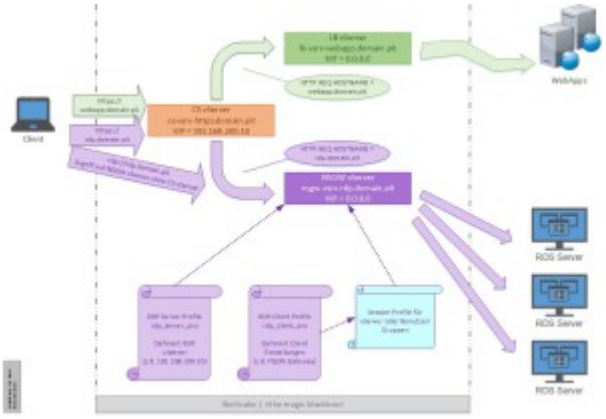
RDP Proxy mit NetScaler 11.x einrichten

Hallo zusammen

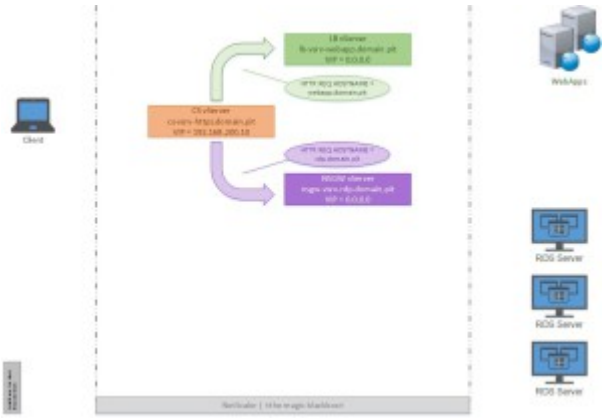
Eine der Neuerungen mit NetScaler 11 war die Einführung des RDP Proxy. Ich habe mich im Rahmen einer Kursvorbereitung ein wenig mit dem Feature auseinander setzen dürfen/müssen. Nunja was soll ich sagen… es ist eigentlich gar keine Hexerei.

Vorraussetzungen: NetScaler Enterprise (RDP Proxy ist Bestandteil vom Unified Gateway) sowie NetScaler Gateway Universal Licenses

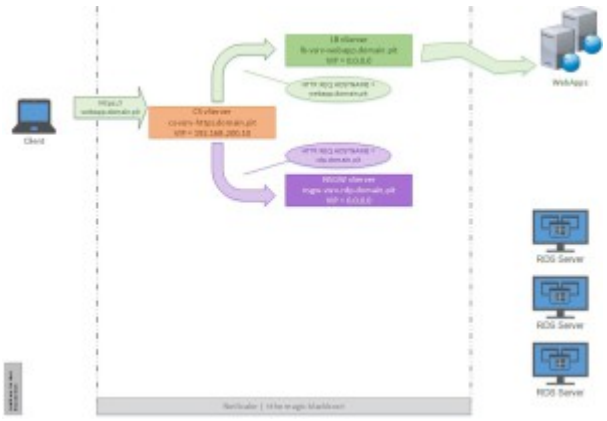
Wie ist funktioniert der RDP Proxy nun? Die komplette Grafik sieht nun so aus:



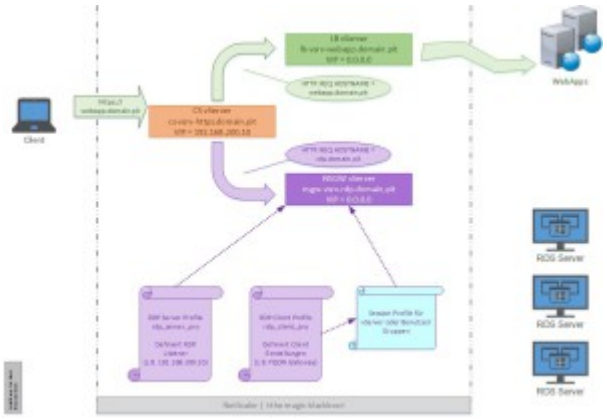
Die Skizze ist mit einer Unified Gateway Installation gezeichnet, wobei der NetScaler Gateway (NSGW) vServer ohne IP (0.0.0.0) hinter einem Content Switching (CS) vServer mit der entsprechenden VIP (z.B. 192.168.200.10) steht. In einer klassischen Konfiguration kann man den CS vServer weg denken und die VIP ist auf dem NSGW vServer konfiguriert.



Klassische CS Konfiguration:
– CS vServer hört auf die VIP
– Anfragen auf den Hostname webapps.domain.pit werden auf den Loadbalancing (LB) vServer der Webapplikationen geleitet
– Anfragen auf den Hostname rdp.domain.pit werden auf den NSGW vServer geleitet



Anfrage der Webapplikationen verlaufen ohne spezielle Konfigurationen direkt auf die Webserver der Applikationen.



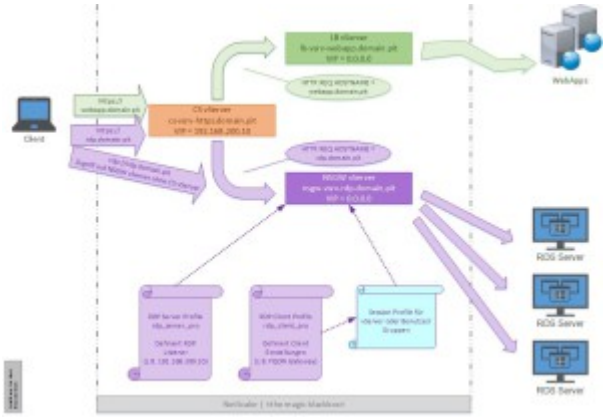
Mittels RDP Server Profilen (z.B. rdp_server_pro) werden die Listener-Einstellungen wie FQDN unseres Gateway, Port, etc. konfiguriert.
Dieses „RDP Server Profile“ muss an den NSGW vServer gebunden werden, damit dieser neu auch auf Anfragen auf den konfigurierten Port reagiert.
Der Zugriff von extern muss nun nebst dem bekannten 443 Port auch den Port für die RDP Verbindung (Standard: 3389) gewährleistet sein.
Zugriffe werden nun auf dem NSGW vServer mit der entsprechenden VIP terminiert.

Update 04.05.16: nach neusten Erkenntnissen kann auch der Port 443 für die RDP Verbindung genutzt werden. Dabei muss jedoch Stand heute eine weitere IP verwendet werden. Gemäss Aussage von Citrix soll „Port Sharing“ in einer der nächsten Versionen funktionieren.

Update 08.07.16: Mit der neuen Version 11.1 funktioniert nun

das „Port Sharing“ und man benötigt für einen RDP Proxy nur noch eine IP und kann alle Zugriffe via Port 443 konfigurieren (analog ICA Proxy).

Im „RDP Client Profile“ sind sämtliche für den Client relevanten Einstellungen hinterlegt wie z.B. die FQDN unseres Gateway, welche Mappings wir erlauben, etc.
Dieses Profile muss an eine Session Policy gebunden sein, welche wiederum entweder direkt dem NSGW vServer oder einer Gruppe/einem Benutzer zugeordnet ist.



Der RDP Client greift bei einem Aufruf der Verbindung direkt auf den NSGW vServer zu, dieser terminiert die Frontend RDP Verbindung und baut eine entsprechende RDP Verbindung zum gewünschten Backend Computer auf. Et voilà, so funktionierts… vereinfacht gesagt ;-)

Wie wird dies nun konfiguriert? Hier die Schritt-für-Schritt Anleitung in Form von CLI Kommandos (im GUI entsprechend abbilden):

Das RDP Proxy Feature muss separat aktiviert werden, falls nicht im Basis-Setup bereits geschehen:

enable feature RDPProxy

Nun müssen das RDP Client und Server Profile erstellt werden wobei der SharedKey bei beiden identisch sein müssen. Der Parameter -rdpFileName definiert nur, wie die Datei heisst, welche zum Client übermittelt werden soll:

```
add rdp clientprofile rdp_client_pro -rdpFileName pit.rdp -rdpHost rdp.domain.pit -psk Password1
add rdp serverprofile rdp_server_pro -rdpIP 192.168.200.10 -psk Password1
```

Nun muss das RDP Server Profile dem definierten NSGW vServer angebunden werden:

```
set vpn vserver nsgw-vsrv-rdp.domain.pit -rdpServerProfileName rdp_server_pro
```

Als nächstes benötigen wir entsprechende Session Policies in welchen wir den Zugriff erlauben, Clientless auf ALLOW setzen und das entsprechende RDP Client Profile zuweisen. Falls bereits Policies vorhanden sein sollten, können diese ggf. einfach angepasst werden:

```
add vpn sessionAction rdp_prof -defaultAuthorizationAction ALLOW -clientlessVpnMode ON -rdpClientProfileName rdp_client_pro
add vpn sessionPolicy rdp_pol ns_true rdp_prof
```

Diese Policies werden nun dem NSGW vServer angebunden:

```
bind vpn vserver nsgw-vsrv-rdp.domain.pit -policy rdp_pol -priority 100
```

Nach erfolgreicher Anmeldung wählt man den Clientless Access, sofern man nicht automatisch dahin geleitet wurde:

Mit der Eingabe *https://FQDN-des-Gateways/rdpproxy/Ziel* (z.B. https://rdp.domain.pit/rdpproxy/192.168.100.10) kann man sich nun eine RDP Verbindung via RDP Proxy aufbauen.
Bequemer für den Benutzer ist es, wenn man die Verbindungen als Bookmark erfasst und dem vServer bzw. den Gruppen zuweist:

```
add vpn url rdp_pitserver1 "PIT Server1"
```

```
"rdp://192.168.100.11" -clientlessAccess ON
add vpn url rdp_pitserver2 "PIT Server2"
"rdp://192.168.100.12" -clientlessAccess ON
add vpn url rdp_pitserver3 "PIT Server3"
"rdp://192.168.100.13" -clientlessAccess ON
bind vpn vserver nsgw-vsrv-rdp.domain.pit -urlName
rdp_pitserver1
bind vpn vserver nsgw-vsrv-rdp.domain.pit -urlName
rdp_pitserver2
bind vpn vserver nsgw-vsrv-rdp.domain.pit -urlName
rdp_pitserver3
```

So sieht ein Benutzer nach erfolgreicher Anmeldung direkt seine Server auf welche er sich mittels RDP verbinden kann:

Damit eine Verbindung erfolgreich aufgebaut werden kann, muss sich der angemeldete Benutzer überhaupt auch ohne Proxy via RDP anmelden können.
Der RDP Proxy macht ein Single-Sign-On und es erfolgt keine Benutzer/Passwort Abfrage mehr.

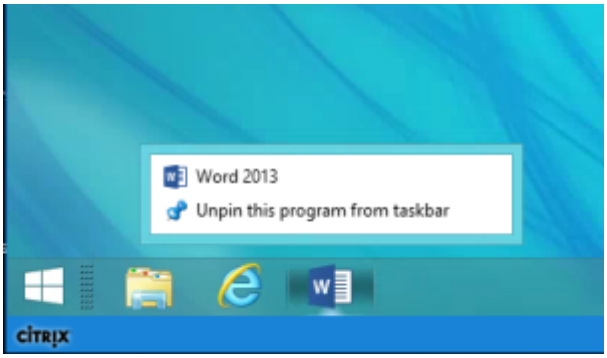
Nun wünsch ich euch viel Spass beim Nachbauen ;-)

Skript: NS-RDPProxy

Umgang mit gepinnten

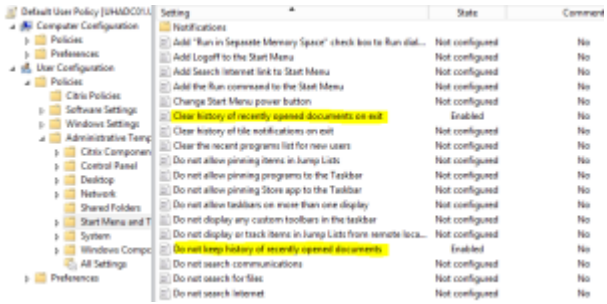
Dokumenten

In einem meiner letzten Citrix XenDesktop Kursen schilderte mir ein Teilnehmer die Problematik, dass bei Ihnen die gepinnten Dokumente (also Dokumente, welche z.B. bei Word in der Taskleiste fixiert wurden) nach einer Neuanmeldung eines Benutzers nicht mehr vorhanden waren:



Aus dieser Schilderung heraus haben wir ein wenig Brainstorming zu den möglichen Ursachen vorgenommen und hier ein wenig die Zusammenhänge:

Die eigentliche Ursache für das Verhalten ist weder bei den Roaming Profiles noch bei Citrix Profile Management zu suchen, sondern bei GPO Einstellungen welche gerne eingestellt werden:



Clear history of recently opened documents on exit

Diese Einstellung bewirkt, dass Dateien während einer Benutzersitzung in der Taskleiste erscheinen und auch angepinnt werden können.
Beim Abmelden werden diese jedoch gelöscht.
Dieses Verhalten kann falls gewünscht mittels Citrix Profile

Management angepasst werden.

Do not keep history of recently opened documents

Diese Einstellung bewirkt, dass Dateien selbst während einer Benutzersitzung in der Taskleiste gar nicht erst erscheinen und somit nicht angepinnt werden können.
Dieses Verhalten kann selbst mit Citrix Profile Management nicht angepasst werden.

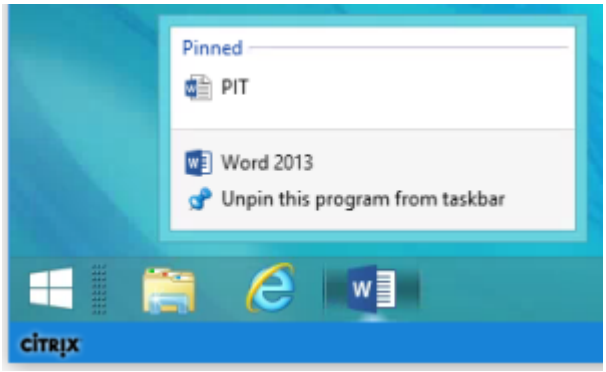
***

Lösungsansatz mittels Citrix Profile Management (CPM)

Mittels CPM können die einmal geöffneten Dateien in das Profil übernommen werden, so dass diese auch nach einer Neuanmeldung des Benutzers noch verfügbar sind.
Dazu wird folgender Pfad einmal ein den durch CPM verarbeiteten Ordner ausgeschlossen dafür mittels Ordner-Spiegelung während der Sitzung gleich in die Profilfreigabe geschrieben:

> *!ctx_roamingappdata!\Microsoft\Windows\Recent\AutomaticDestinations*

Danach sind die gepinnten Dokumente auch nach einer Neuanmeldung noch vorhanden:



Ich hoffe, ich konnte dem einen oder anderen ein wenig

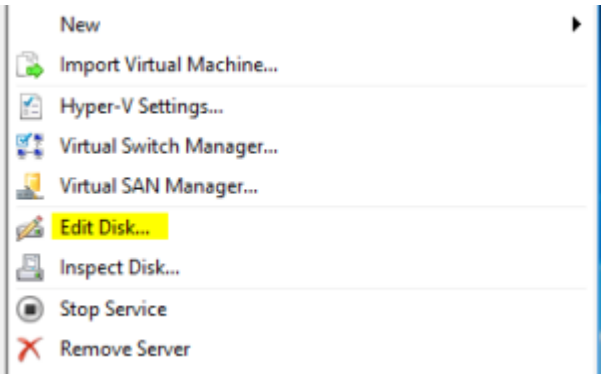
weiterhelfen :-)

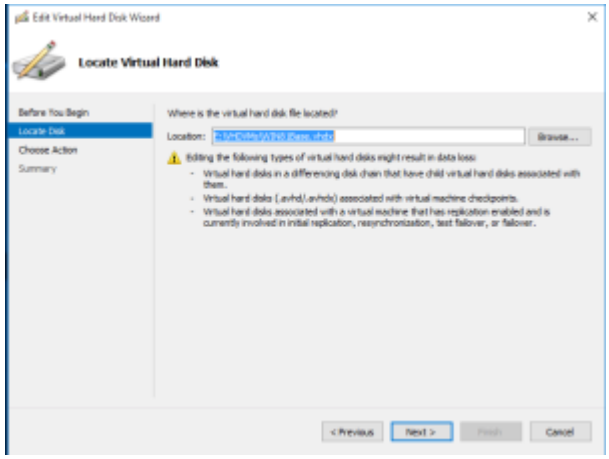
Viel Erfolg beim Nachbau…

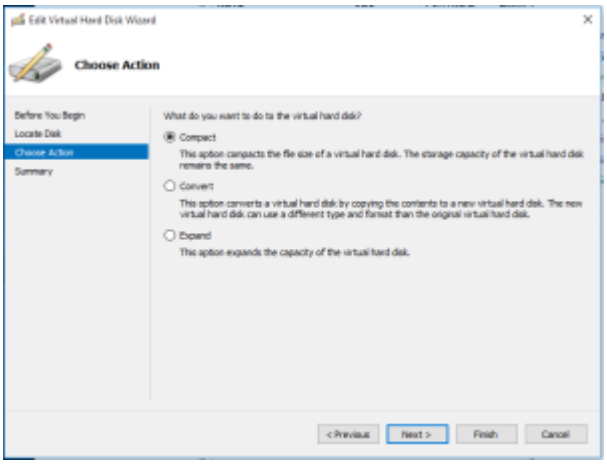
VHD verkleinern

Hallo zusammen

Wer schon einmal versucht hat eine VHD/VHDX im Hyper-V über den normalen Weg zu verkleinern, wird sicherlich schon hier gestrandet sein:



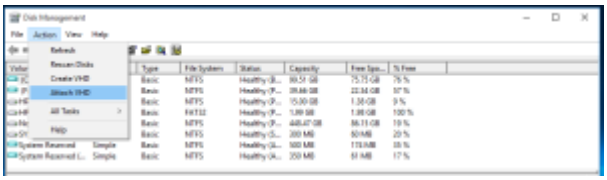


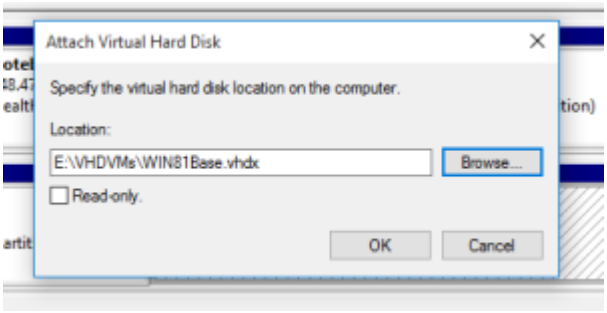


Standardmässig wird kein „verkleinern“ angeboten. Wenn man im weiten Internet sucht wird auch nur von vergrössern gesprochen, bzw. auf ein altes Tool verwiesen, welches nicht mehr verfügbar ist bzw. welches nur VHD aber keine VHDX

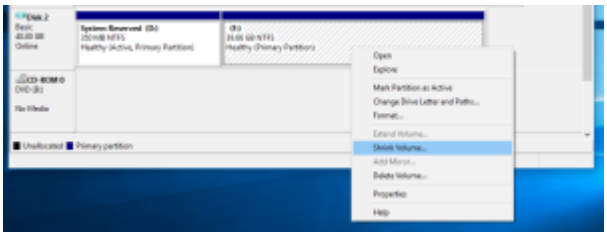
Dateien handhaben kann.

Der Trick ist dass man den Weg über das Datenträger-Management gehen muss.
Innerhalb der Datenträgerverwaltung fügt man die gewünschte virtuelle Disk hinzu. Erwähnenswert ist hier, dass die Disk natürlich nicht in Gebrauch sein darf!

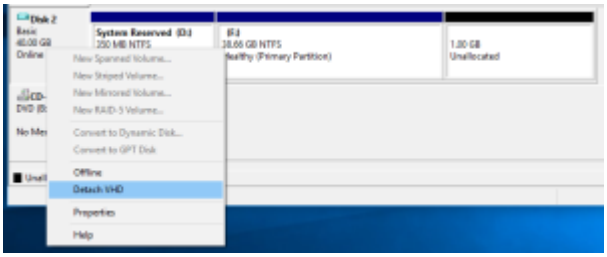




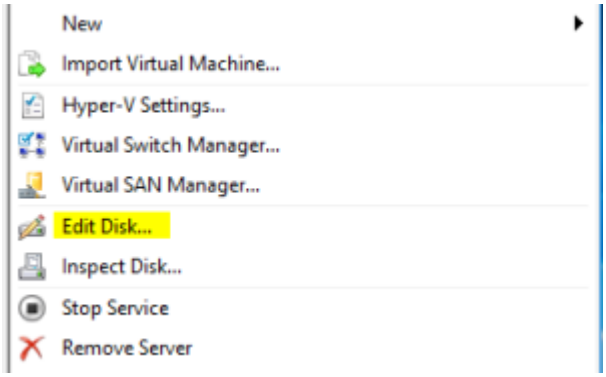
Anschliessend kann man wie bei einer normalen Festplatte die Partitionen vergrössern oder in unserem Fall verkleinern:

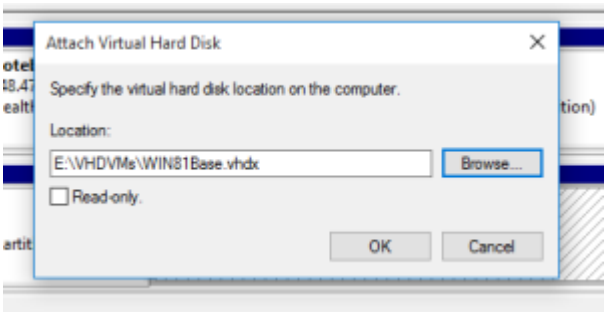


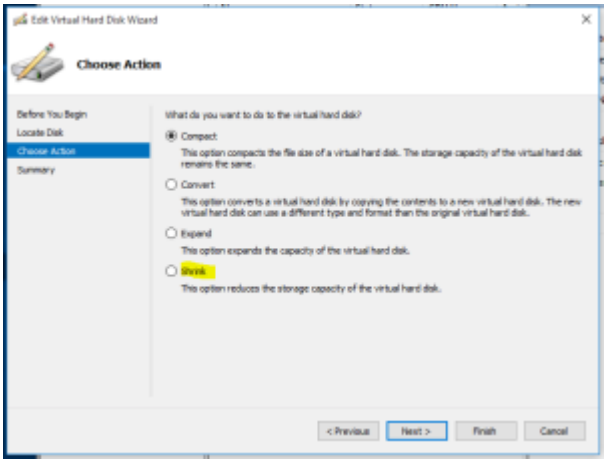
Jetzt wo wir wieder nicht zugewiesenen Speicherplatz haben, müssen wir uns wieder von der VHD trennen, damit wir im Hyper-V die virtuelle Disk verkleinern können:

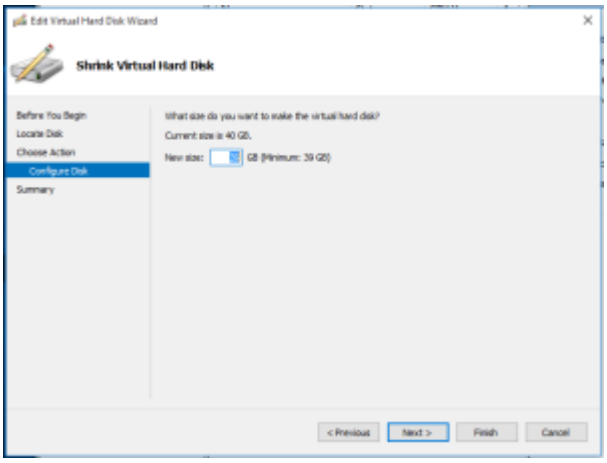


Im Hyper-V gehen wir wieder die Schritte wie am Anfang und werden feststellen, dass nun die Option zur Verkleinerung der Disk zur Verfügung steht:









Mir ist bewusst, dass dieser Task weniger in produktiven Umgebungen benötigt wird. Jeder der jedoch selbst eine kleine Test- bzw. Demo-Umgebung betreibt ist da sicherlich schon an die Grenzen der Speicherkapazitäten gestossen und wollte die ursprünglich grosszügig bemessenen Disks wieder verkleinern.

Viel Erfolg dabei :-)

Was wurde aus dem Microsoft Patchday?

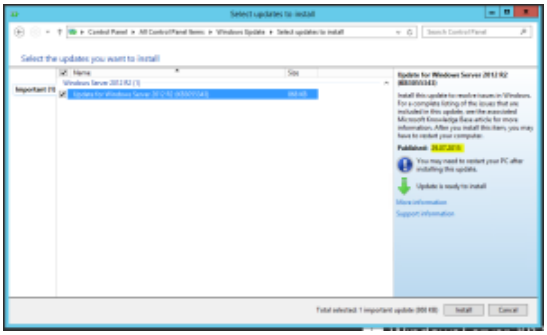
Hallo Microsoft

Gerade bin ich dabei die Demo Umgebung unserer Firma zu aktualisieren. Wie in den meisten Netzwerken betreiben wir

einen WSUS um die Windows Updates zentral zu verwalten.

Ich kann mich noch an Zeiten erinnern wo man noch genau wusste, am zweiten Dienstag im Monat ist Patchday bei Microsoft. Vorher und Nachher musste man sich um die „normalen“ Hotfixes nicht kümmern (Cummulative Updates, Definition Updates, etc. mal ausgenommen).

Seit längerem ist jedoch zu beobachten, dass auch ausserhalb dieser Tage Patches freigegeben werden:



(siehe Erscheinungsdatum)

Microsoft, ich frage euch: wie soll man da noch ein vernünftiges Wartungsfenster planen, wenn auf euch nicht mehr verlass ist?

Ich verstehe es, wenn ein Security Update für ein aktuelles Sicherheitsproblem zeitnah veröffentlicht wird, doch es sind eben nicht nur diese…