

M143 Arbeit DHLLC

Rayan Lee Bopp

Contents

Datensicherungskonzept.....	2
Datensicherungskonzept Idee	2
Datensicherungskonzept grafik.....	2
Datensicherheitsrichtlinien/Gesetzgebung	3
Datensicherheitsrichtlinien innerhalb der Doupont Holdings LLC	4
Datensicherungsverfahren	4
Beispiele Persönliche Daten:.....	4
Beispiele Betriebliche Daten:	4
Backups Richtlinien	5
Warum dieses Datensicherungsverfahren	5
Machbarkeit	6
Zu sichernde Daten	6
Optimale Speicherort.....	6
Bedarfsermittlung	7
Ressourcen des Hosts.....	7
Ressourcen des Windows Servers.....	7
Zu sichernde Datenmenge	8
Ablage Ort	9
Backup Interval	9
Lokal oder Cloud	9
Umsetzung	10
Vorgehen	10
Script Backup.....	10
Script erklärung.....	11
Script für Wiederherstellung:.....	12
Erklärung des Widerherstellungs scripts.....	13
Testen des Scripts.....	15
Reflexion.....	15
Schlusswort	16
Quellen.....	16

Datensicherungskonzept

Datensicherungskonzept Idee

Das Datensicherungs Konzept von DHLLC, ist nicht wirklich automatisch. Hiermit meine ich das die Mitarbeiter von dieser DHLLC-Filiale mit einem Netzwerk-Storage Driver arbeiten.

Dass heisst jeder mitarbeiter hat einen eigenen Speicher nämlich die **C://** Drive und die Company Drive **D://**.

Auf der **C://** Drive sind alle Persönlichen Daten abgespeichert wie: Lohnauszüge oder ID's und Private-Keys.

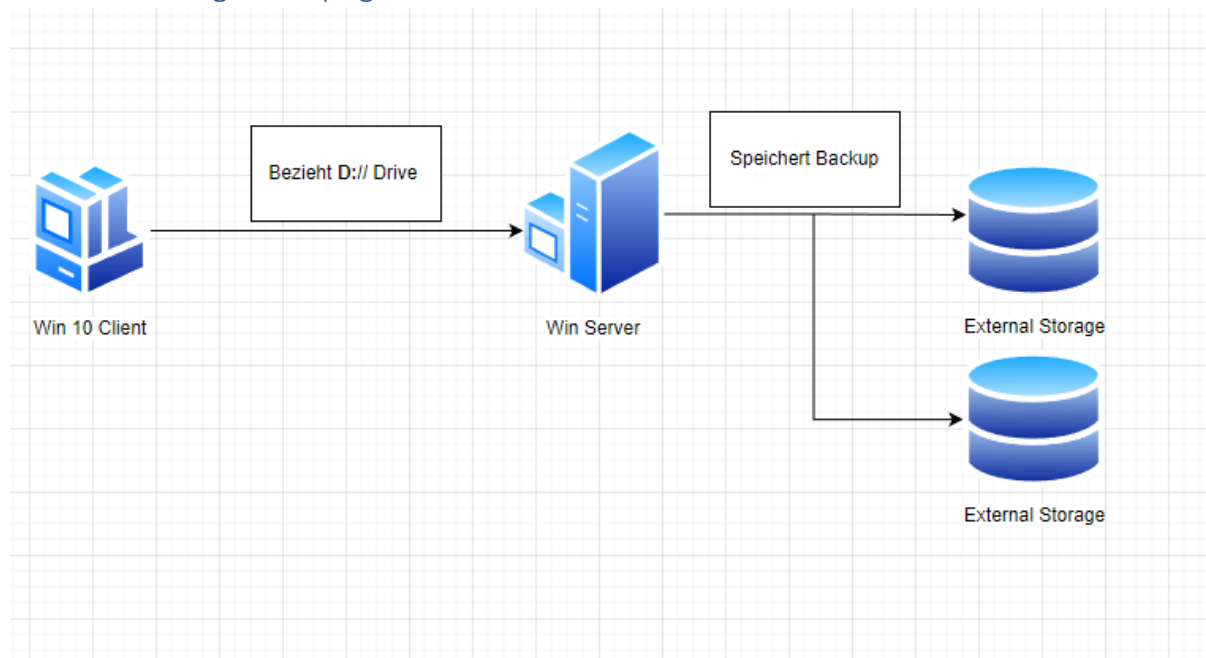
Auf der **D://** Drive sind alle Daten abgespeichert die geschäfts relevant sind. Die **D://** Drive ist auch die einzige Drive die gebacked up wird.

Die **D://** Drive wird von dem Windows Server, zur verfügung gestellt, dies hat seine Gründe, da man zum Beispiel bei einer Daten-Analyse nicht durch alle Clients durch gehen muss sondern nur auf dem File-Server

Diese **D://** Drive wird an einem Externen Ort gebacked up.

Ich habe diese Datensicherheitskonzeptidee gewählt, da ich nicht so gut in der Backup Welt versiert bin. Deswegen nehme ich eine Simple Methode. Ausserdem ist diese Datensicherheitskonzeptidee nicht nur sehr simple sondern auch kosteneffizient. Somit muss Doupont Holdings LLC nicht noch extra Dienste und Lizenzen kaufen und kann einen Grossteil ihrer On-Prem Infrastruktur bei sich behalten.

Datensicherungskonzept grafik



Datensicherheitsrichtlinien/Gesetzgebung

Die Datenschutzgesetzgebung in der Schweiz legt klare Vorgaben für die Speicherung und Verarbeitung personenbezogener Daten fest. Hier sind weitere wichtige Punkte, die in Bezug auf die Speicherung von Daten relevant sind:

1. Zweckbindung: Unternehmen sind gesetzlich verpflichtet, personenbezogene Daten nur für die Zwecke zu verwenden, für die sie ursprünglich erhoben wurden. Jede Änderung des Verwendungszwecks erfordert die Einwilligung der betroffenen Personen.

2. Datensicherheit: Unternehmen müssen angemessene technische und organisatorische Maßnahmen treffen, um die Sicherheit und Vertraulichkeit der gespeicherten Daten zu gewährleisten. Dies schließt den Schutz vor unbefugtem Zugriff, Datenverlust und Datenbeschädigung ein.

3. Informationspflicht: Unternehmen müssen betroffene Personen darüber informieren, wie ihre Daten verarbeitet werden, welche Rechte sie haben und wie sie diese ausüben können. Dies geschieht in der Regel durch Datenschutzrichtlinien und Einwilligungserklärungen.

4. Aufbewahrungsfristen: Unternehmen sollten die gesetzlichen Aufbewahrungsfristen beachten, die je nach Art der Daten variieren können. Im Allgemeinen erlaubt das DSG die Aufbewahrung von Daten, die aus rechtlichen Gründen archiviert werden müssen, für bis zu 10 Jahre, bevor sie gelöscht werden.

5. Recht auf Löschung: Gemäß dem DSG haben betroffene Personen das Recht, die Löschung ihrer Daten zu verlangen, sofern keine gesetzlichen Gründe für die Aufbewahrung vorliegen.

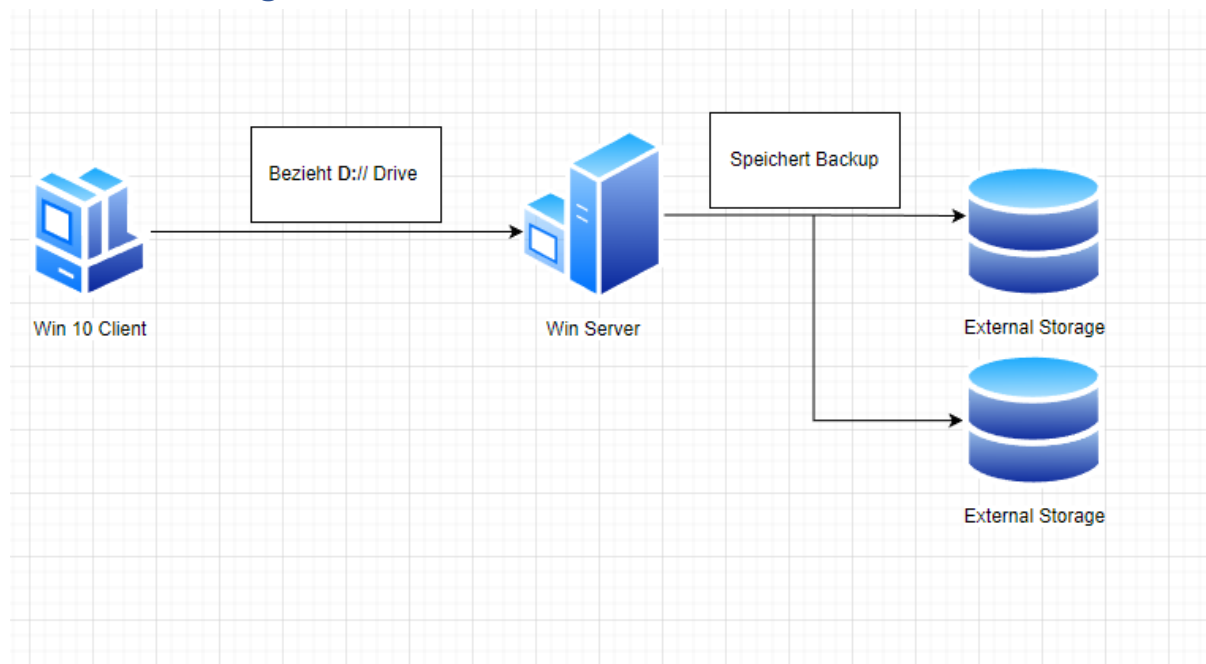
Durch die Einhaltung dieser gesetzlichen Bestimmungen können wir Doupont Holdings LLC sicherstellen, dass wir den Datenschutzvorschriften in der Schweiz gerecht werden und die Rechte der betroffenen Personen respektieren.

Datensicherheitsrichtlinien innerhalb der Doupont Holdings LLC

Nur Qualifizierte Mitarbeiter der Doupont Holdings LLC dürfen auf Daten zugreifen.

Dass heisst Kundendaten sind nur für Kundensachbearbeiter zugänglich und zu Mitarbeitern anderer Abteilungen nicht ersichtlich. Doupont Holdings LLC verlässt sich darauf, dass die Mitarbeiter selber wissen in welcher Abteilung sie arbeiten.

Datensicherungsverfahren



Wie oben schon erwähnt sind die Mitarbeiter selber verantwortlich zu unterscheiden welche Daten persönlich sind und welche Daten für den Betrieb relevant sind. Doupont Holdings LLC vertraut in die zuverlässigkeit seiner Mitarbeiter und verlässt sich darauf, dass jeder Mitarbeiter sich bei Fragen ohne zu zögern bei seinem/seiner Vorgesetzten nach fragt.

Beispiele Persönliche Daten:

1. Lohnauszüge
2. Identifikation Ausweise
3. Staatliche Ausweise
4. Staatliche Dokumente
5. Bilder

Beispiele Betriebliche Daten:

1. Präsentationen
2. Kundenverträge
3. Kundendaten
4. Kundenausweise
5. Interne Dokumente

Doupont Holdings LLC erhofft sich von jedem/jeder Mitarbeiter:in, dass Er/Sie seine/ihre Aufgaben Pflichtenbewusst erfüllt.

Backups Richtlinien

Die Backups sollten folgender massen ausgeführt werden:

- Full Backup: 1x pro Woche, 2x pro Monat (compressed)
- Incremental backups: 6x pro Woche, 12x pro Monat (compressed)

Diese Backups werden immer nur von dem **D://** Drive gemacht, dass heisst es wird wirklich nur dieses gebacked up.

Hier gehe ich nicht von der realen Menge an Daten aus sondern von der Fiktiven der Doupont Holdings LLC Firma.

Ich würde mit der fiktiven Datenmenge im Monat 1300GB backupen. Ich habe dies mit [Wintelguy](#) berechnet

Warum dieses Datensicherungsverfahren

Warum ich dieses Datensicherungsverfahren ausgewählt habe ist sehr einfach. Dieses Datensicherungsverfahren erlaubt es den Mitarbeitenden und auch den Administratoren zu wählen welche Daten sie Backupen möchten und welche sie nicht zwingen backupen müssen. Sie ist ausserdem sehr praktisch für Doupont Holdings LLC, da sie Low-Maintenance ist.

Machbarkeit

Zu sichernde Daten

Die Daten die gesichert werden müssen befinden sich alle auf dem **D://** Drive. Hier werden alle Daten gesichert.

Hierbei gibt es verschiedene Ordner:

1. Kundensachbearbeiter
2. ProjektManagement
3. IT-Department
4. Exekutive

Diese Vier verschiedenen Ordner haben sind vier verschiedenen Gruppen zugeteilt:

1. Kundensachbearbeiter → Kundensachbearbeiter (SF)
2. ProjektManagement → ProjektManagement(PMgmt)
3. IT-Department → IT-Department(IT)
4. Exekutive → Exekutive(Exec)

Diese Vier gruppen haben unterschiedliche Rechte. Die rechte werden folgend kategorisiert:

1. **Low – DHLLC1:** In dieser Gruppe sind alle Kundensachbearbeiter, die keine extravaganten rechtebrauchen. Diese müssen nur auf den Kundensachbearbeiter Ordner zugreifen können und dort Änderungen vornehmen.
2. **Medium – DHLLC2:** In dieser Gruppe sind alle Mitarbeiter aus dem IT-Department und aus dem ProjektManagement. Diese verfügen über die Rechte der Prio-Guppe **Low – DHLLC1**. Aber können diesen Folder nur ansehen aber nicht drin verändern.
3. **High – DHLLC3:** In dieser Gruppe sind nur die Mitarbeiter von Doupont Holdings die in eine Exekutive Funktion besitzen. Dass heisst CEO, CFO, CTO, COO etc. Diese haben zugriff auf diesen Ordner und wiederum auf alle anderen Ordner aber sie haben keine Schreibrechte.

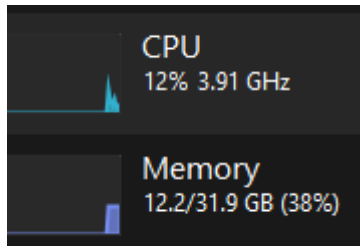
Daten die von der **High – DHLLC3** und **Medium – DHLLC2** Prio-Gruppe sind werden verschlüsselt und in einem hochgesicherten Raum aufbewahrt, in dem nur autorisierte Personen zugriff haben. Diese Storage medien die diese Daten enthalten müssen ebenso gesichert werden, dass heisst das Sie verschlüsselt werden. Die Physischen Geräte werden so konfiguriert, dass man keinen Stick oder anderwertiges in sie reinstecken kann und somit Daten abzapfen oder zerstören kann.

Optimale Speicherort

Wie ich es schon vorher erwähnt habe werden die Daten der verschiedenen Prioritäts Gruppen anders gespeichert. Die Prioritäts Gruppe **Low – DHLLC1** wird in einem Raum mit adequater sicherung aufbehalten bei Daten die von der **High – DHLLC3** und **Medium – DHLLC2** Prio-Gruppe sind sieht das anders aus. Gewisse Daten die von der **Medium – DHLLC2** Prioritäts Gruppe stammen haben sensible Daten drinnen und müssen deshalb in solch einem Hochsicherheitsraum aufbewahrt werden. (wie oben erwähnt). Jedoch gibt es auch daten der gruppe **Medium – DHLLC2** die nicht in einem solchen Sicherheits raum aufbewahrt werden müssen.

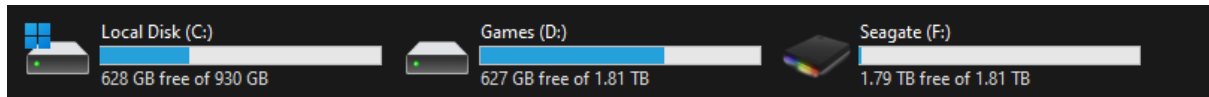
Bedarfsermittlung

Ressourcen des Hosts



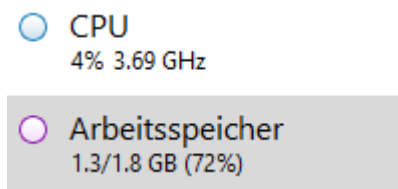
Meine Ressourcen auf meinem PC Zuhause sind nicht so begrenzt wie die auf meinem Laptop, deswegen kann ich mir Zuhause noch ein paar zusätzliche VMs leisten, jedoch bleibe ich bei den drei VMs, da mein PC sonst anfängt zu ruckeln und, dass möchte ich nicht.

Memory: 32GB



Auch der Speicherplatz wird kein Problem sein, da ich mehr als genug besitze. Ich werde als mein external Storage medium meine Seagate External Harddrive benutzen.

Ressourcen des Windows Servers



Ich möchte darauf Hinweisen, dass der Arbeitsspeicher sich Dynamisch anpassen kann. Hierbei kann er bis zu 16GB hoch sein. Das gleiche ist der Fall bei der CPU, Diese passt sich auch dynamisch an.

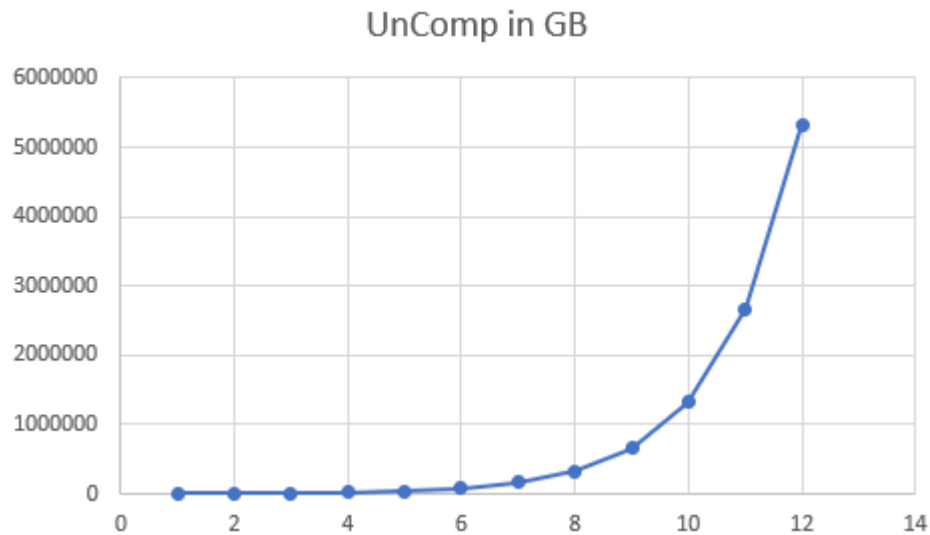


Hierbei ist der Speicherplatz nicht Dynamisch, dass wäre sonst eine Katastrophe für meinen PC. Deshalb habe ich sie als **fixed volume** konfiguriert, dass heisst dass die Drives nicht mehr als 60GB platz haben.

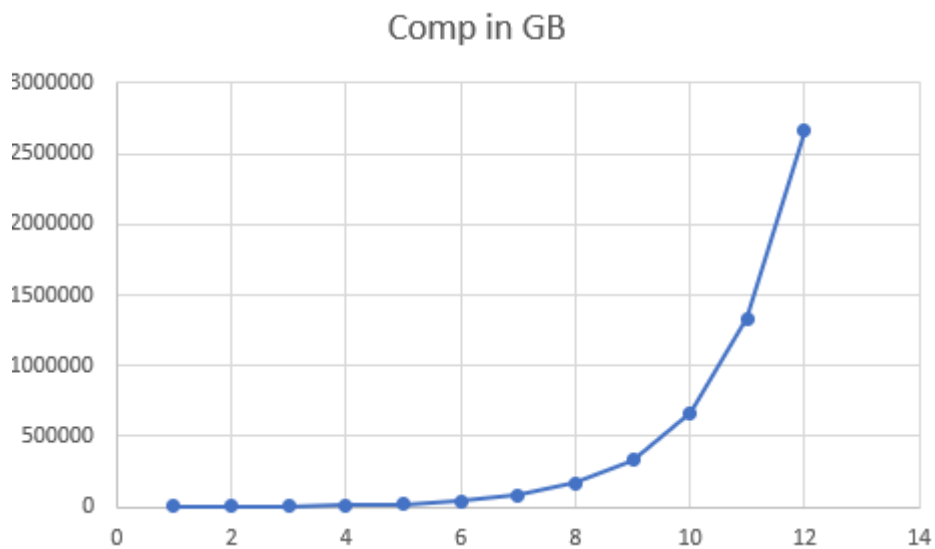
Zu sichernde Datenmenge

Der Datenzuwachs bei den Daten von Doupont Holdings LLC ist nicht so immens, natürlich haben diese einen Immensen Daten zufluss jedoch nicht all zu viel.

Hier ist ein Diagramm das den Datenzuwachs visualisiert falls er nicht komprimiert ist:



Und hier wäre der Datenzuwachs visualisiert falls er komprimiert ist:



Man kann laut WinterGuy davon ausgehen dass man bei einer Kompression von der Daten, die Datenmenge +/- bis zu 50% oder sogar weniger verringern kann.

Ablage Ort

Der Ablage Ort aller Daten wird wie schon gesagt die **D://** Drive sein. Hierbei werden auch die verschiedenen Ordner die ich vorher erwähnt habe gebackuped.

Hierbei gibt es verschiedene Ordner:

5. Kundensachbearbeiter
6. ProjektManagement
7. IT-Department
8. Exekutive

Diese Vier verschiedenen Ordner haben sind vier verschiedenen Gruppen zugeteilt:

5. Kundensachbearbeiter → Kundensachbearbeiter (SF)
6. ProjektManagement → ProjektManagement(PMgmt)
7. IT-Department → IT-Department(IT)
8. Exekutive → Exekutive(Exec)

Backup Interval

Das Backup Interval sollte Folgendermassen aussehen:

Woche

- **1x Full backup**
- **6x Incremental backup**

Monat

- **2x Full Backup**
- **12x Incremental backup**

Die backups werden immer zur der Zeit gemacht an der am wenigsten Aktivität ist. Dass heisst in unserem Falle wäre dies immer Abends um 22:00 Uhr.

Lokal oder Cloud

Das ist die Frage der Fragen sollte das Backup Lokal gemacht werden oder sollte es in der Cloud gemacht werden. Ich weiss die Antwort schon aus meiner Perspektive Lokal, da der Cloud Account müll ist aber für Doupont Holdings LLC wäre das vielleicht anders.

Doupont Holdings LLC hatte bevor sie die meisten Applikationen in die Cloud verschoben hat eine sehr grosse On-Prem Infrastruktur. Diese müssten sie jetzt entweder wiederverwerten oder verkaufen, jedoch macht es für sie mehr Sinn laut „Eric Doulmont“ die On-Prem Infrastruktur als Backup-Lösung zu gebrauchen, da die Infrastruktur oder bessergesagt die Komponenten nicht mehr gut verkaufbar seien. Ein weiterer Grund war, dass sie Ihre Kundendaten bzw. Kundendokumente nicht in der Cloud haben wollen sondern dort, wo sie zu 96.9% sicher sind.

Umsetzung

Vorgehen

Ich habe mir zuerst gedanken gemacht wie ich dies am besten mache. Dann habe ich eine geniale Idee gehabt. Wieso sollte ich mir den Aufwand machen um das ganze Unterfangen mühsam zu Konfigurieren, wenn ich ein ganz einfaches Script verwenden kann. Ich habe danach ein einfaches Script erstellt.

Script Backup

```
# Definieren der Pfade für das Laufwerk, das Backup-Ziel und den Zeitstempel
$SourcePath = "D:\\"
$BackupDestinations = @("External-Drive", "DaS")
$TimeFormat = Get-Date -Format "yyyyMMdd_HH:mm:ss"

# Überprüfen, ob es sich um den ersten Backup-Durchlauf handelt
foreach ($Destination in $BackupDestinations) {
    $FullBackupPath = Join-Path $Destination "FullBackup_$TimeFormat"
    if (-Not (Test-Path $FullBackupPath)) {
        # Erster Backup-Durchlauf: Vollbackup erstellen
        robocopy $SourcePath $FullBackupPath /MIR
    } else {
        # Alle weiteren Backup-Durchläufe: Inkrementelles Backup erstellen
        $IncrementalBackupPath = Join-Path $Destination "IncrementalBackup_$TimeFormat"
        robocopy $SourcePath $IncrementalBackupPath /MIR
    }
}

# Prüfen, ob es sich um den ersten Backup-Durchlauf in der Woche oder im Monat handelt
$CurrentDayOfWeek = (Get-Date).DayOfWeek
$CurrentDayOfMonth = (Get-Date).Day

if ($CurrentDayOfWeek -eq "Sunday" -and $CurrentDayOfMonth -eq 1) {
    # Erster Backup-Durchlauf der Woche: Vollbackup erstellen
    foreach ($Destination in $BackupDestinations) {
        robocopy $SourcePath (Join-Path $Destination "FullBackup_$TimeFormat") /MIR
    }
}

if ($CurrentDayOfMonth -eq 1) {
    # Erster Backup-Durchlauf des Monats: Vollbackup erstellen
    foreach ($Destination in $BackupDestinations) {
        robocopy $SourcePath (Join-Path $Destination "FullBackup_$TimeFormat") /MIR
    }
}

# Optional: Alte Backups gemäß Ihrem Retentionsplan löschen
# Beispiel: Behalten Sie 6 Wochen vollständige Backups und 6 Monate inkrementelle Backups
$RetentionWeeks = 6
$RetentionMonths = 6

foreach ($Destination in $BackupDestinations) {
    Get-ChildItem $Destination | Where-Object {
        $_.CreationTime -lt (Get-Date).AddDays(-7 * $RetentionWeeks) -or
        ($_.CreationTime -lt (Get-Date).AddMonths(-$RetentionMonths) -and $_.Name -like
        "IncrementalBackup*")
    } | ForEach-Object {
        Remove-Item $_.FullName -Force -Recurse
    }
}
```

Script erklärung

1. Pfade und Variablen festlegen:

Zuerst definieren wir die Pfade für das Quellverzeichnis (hier "D:\") und die Backup-Zielorte (hier "External-Drive" und "DaS"). Außerdem legen wir ein Zeitstempel-Format fest.

```
1. $SourcePath = "D:\"
2. $BackupDestinations = @"\\External-Drive\backup", "\\DaS-Home\backup"
3. $TimeFormat = Get-Date -Format "yyyyMMdd_HH:mm:ss"
4.
```

2. Überprüfen, ob es sich um den ersten Backup-Durchlauf handelt:

Wir verwenden eine Schleife, um die Backup-Zielorte zu durchlaufen und zu überprüfen, ob bereits ein Vollbackup für jedes Zielverzeichnis vorhanden ist. Wenn nicht, wird ein neues Vollbackup erstellt.

```
1. foreach ($Destination in $BackupDestinations) {
2.     $FullBackupPath = Join-Path $Destination "FullBackup_$TimeFormat"
3.     if (-Not (Test-Path $FullBackupPath)) {
4.         # Erster Backup-Durchlauf: Vollbackup erstellen
5.         robocopy $SourcePath $FullBackupPath /MIR
6.     } else {
7.         # Alle weiteren Backup-Durchläufe: Inkrementelles Backup erstellen
8.         $IncrementalBackupPath = Join-Path $Destination "IncrementalBackup_$TimeFormat"
9.         robocopy $SourcePath $IncrementalBackupPath /MIR
10.    }
11. }
12.
```

3. Überprüfen, ob es sich um den ersten Backup-Durchlauf in der Woche oder im Monat handelt:

Wir verwenden den aktuellen Wochentag und den Tag des Monats, um zu überprüfen, ob es sich um den ersten Backup-Durchlauf der Woche oder des Monats handelt. In diesen Fällen wird erneut ein Vollbackup erstellt.

```
1. $CurrentDayOfWeek = (Get-Date).DayOfWeek
2. $CurrentDayOfMonth = (Get-Date).Day
3.
4. if ($CurrentDayOfWeek -eq "Sunday" -and $CurrentDayOfMonth -eq 1) {
5.     # Erster Backup-Durchlauf der Woche: Vollbackup erstellen
6.     foreach ($Destination in $BackupDestinations) {
7.         robocopy $SourcePath (Join-Path $Destination "FullBackup_$TimeFormat") /MIR
8.     }
9. }
10.
11. if ($CurrentDayOfMonth -eq 1) {
12.     # Erster Backup-Durchlauf des Monats: Vollbackup erstellen
13.     foreach ($Destination in $BackupDestinations) {
14.         robocopy $SourcePath (Join-Path $Destination "FullBackup_$TimeFormat") /MIR
15.     }
16. }
17.
```

4. Optional: Alte Backups löschen:

Schließlich löschen wir alte Backups gemäß Ihrem Retentionsplan. Hier werden 6 Wochen vollständige Backups und 6 Monate inkrementelle Backups beibehalten.

```
1. $RetentionWeeks = 6
2. $RetentionMonths = 6
3.
4. foreach ($Destination in $BackupDestinations) {
5.     Get-ChildItem $Destination | Where-Object {
6.         $_.CreationTime -lt (Get-Date).AddDays(-7 * $RetentionWeeks) -or
7.         ($_.CreationTime -lt (Get-Date).AddMonths(-$RetentionMonths) -and $_.Name -like
8.         "IncrementalBackup*")
9.     } | ForEach-Object {
10.        Remove-Item $_.FullName -Force -Recurse
11.    }
12. }
```

Script für Wiederherstellung:

```
1. # Definieren des Zielverzeichnis für die Wiederherstellung
2. $RestorePath = "D:\Restore"
3.
4. # Definieren des Pfads zum externen Speichermedium, auf dem die Backups gespeichert sind
5. $BackupSource = "External-Drive"
6.
7. # Suchen nach dem neuesten inkrementellen Backup im Backup-Quellverzeichnis
8. $LatestIncrementalBackup = Get-ChildItem (Join-Path $BackupSource "IncrementalBackup*") |
9. Sort-Object CreationTime | Select-Object -Last 1
10.
11. # Überprüfen, ob ein neuestes inkrementelles Backup gefunden wurde
12. if ($LatestIncrementalBackup -ne $null) {
13.     # Erstellen eines Zielverzeichnisses für die Wiederherstellung
14.     $RestoreDestination = Join-Path $RestorePath $LatestIncrementalBackup.Name
15.     New-Item -ItemType Directory -Path $RestoreDestination
16.     # Kopieren der Dateien aus dem neuesten inkrementellen Backup in das
17.     # Wiederherstellungsverzeichnis
18.     robocopy $LatestIncrementalBackup.FullName $RestoreDestination /MIR
19.     Write-Host "Die Wiederherstellung des neuesten inkrementellen Backups wurde
20.     abgeschlossen."
21. } else {
22.     Write-Host "Es wurde kein neuestes inkrementelles Backup gefunden."
```

Erklärung des Wiederherstellungs scripts

1. Zielverzeichnis für die Wiederherstellung definieren:

Hier legen wir den Pfad fest, in dem die wiederhergestellten Dateien gespeichert werden sollen.

```
1. $RestorePath = "D:\Restore"
```

2. Pfad zum externen Speichermedium und Suche nach dem neuesten inkrementellen Backup:

Wir geben den Pfad zum externen Speichermedium (BackupSource) an und suchen nach dem neuesten inkrementellen Backup.

```
1. $BackupSource = "External-Drive"  
2. $LatestIncrementalBackup = Get-ChildItem (Join-Path $BackupSource "IncrementalBackup*") |  
Sort-Object CreationTime | Select-Object -Last 1  
3.
```

Das Skript sucht nach Dateien im Verzeichnis "External-Drive" mit Namen, die "IncrementalBackup" enthalten, und wählt das zuletzt erstellte Backup aus.

3. Überprüfen, ob ein neuestes inkrementelles Backup gefunden wurde:

Wir überprüfen, ob ein neuestes inkrementelles Backup gefunden wurde.

```
1. if ($LatestIncrementalBackup -ne $null) {
```

4. Zielverzeichnis für die Wiederherstellung erstellen:

Wenn ein neuestes inkrementelles Backup gefunden wurde, erstellen wir ein Verzeichnis für die Wiederherstellung im angegebenen Pfad.

```
$RestoreDestination = Join-Path $RestorePath $LatestIncrementalBackup.Name  
New-Item -ItemType Directory -Path $RestoreDestination
```

5. Dateien aus dem neuesten inkrementellen Backup wiederherstellen:

Wir verwenden `robocopy`, um die Dateien aus dem neuesten inkrementellen Backup in das Wiederherstellungsverzeichnis zu kopieren.

```
robocopy $LatestIncrementalBackup.FullName $RestoreDestination /MIR
```

6. Meldung zur erfolgreichen Wiederherstellung ausgeben:

Am Ende des Skripts wird eine Meldung angezeigt, um den Abschluss der Wiederherstellung anzuzeigen.

```
1. Write-Host "Die Wiederherstellung des neuesten inkrementellen Backups wurde  
   abgeschlossen."
```

7. Meldung bei fehlendem neuesten inkrementellen Backup:

Wenn kein neuestes inkrementelles Backup gefunden wurde, gibt das Skript eine Meldung aus.

```
1.   } else {  
2.       Write-Host "Es wurde kein neuestes inkrementelles Backup gefunden."  
3.   }  
4.
```

Das Skript durchsucht das externe Speichermedium nach dem neuesten inkrementellen Backup und stellt es im angegebenen Zielverzeichnis wieder her. Bitte passen Sie die Pfade und Verzeichnisse an Ihre spezifischen Anforderungen an und führen Sie das Skript auf dem System aus, auf dem Sie die Wiederherstellung durchführen möchten.

Testen des Scripts

Testperson 1

Frage an Testperson 1: Wird bei dem zweiten Backup wirklich ein Inkrementeles Backup erstellt.

Aktion	Erwartet	Tatsächlich
Force execute first	Es wird full gebacked upt	Es wird full gebacked upt
Force execute second	Es wird Inkrementell gespeichert.	Es wird Inkrementell gespeichert.

Testperson 2

Frage an Testperson 2: Ist ein Restore möglich?

Aktion	Erwartet	Tatsächlich
Restore ausführen	Ist automatisch ohne user input	Ist okay
Robocopy restore funktioniert	Befehl funktioniert	Ist okay

Testperson 3

Frage an Testperson 3: Werden die Backups mit Timestamps versehen?

Aktion	Erwartet	Tatsächlich
Überprüfen der backups	Wurde mit timestamp versehen	Wurde mit Timestamp versehen yyyyMMdd_HH:mm:ss

Reflexion

18.10.2023

Ich habe heute versucht zu planen für das Backup von meiner Cloud Infrastruktur. Ich fing an mit dem Scripten auf meinem Laptop

20.10.2023

Ich realisierte, dass mir einige Permissions fehlen für die Backups. Ich dropte also diese Idee.

22.10.2023

Heute habe angefangen neu zu planen. Ich habe mich ausserdem intensiv mit Powershell scripting auseinander gesetzt. Ich habe dann gedacht ich werde es vielleicht in mein Backup-Projekt nehmen.

23.10.2023

Ich habe heute mit dem Programmieren des Script angefangen. Zudem habe ich mit meiner Doku angefangen.

05.11.2023

Ich habe heute mein Script meinen Kollegen vorgestellt und sie haben mir mein Testprotokoll ausgeführt.

07.11.2023

Heute habe ich meine Dokumentation vollendet und nochmals getestet es funktionierte bei mir ohne Probleme.

Schlusswort

Ich bin nicht so zufrieden mit meiner Arbeit, da ich dachte ich könnte es viel besser machen. Ich hätte mir mehr Zeit nehmen sollen anstatt soviel Zeit mit dem Cloud Modul zu verbringen. Der grösste Zeitraubfaktor waren wie ich schon gesagt habe, die Permissions des AWS Learner Labs. Ich konnte mich nebst aufregen auch noch freuen, da ich verschiedensten Leuten aus meiner Klasse helfen konnte Ihr Projekt gut durchzuführen jedenfalls hoffe ich das.

Quellen

Script example habe ich von einem Subreddit

Alexander Marcel Bühler ein Kolleg der sich damit auskennt.