TrueNas

Noah Gertsch

Bi21a M143

Inhaltsverzeichnis

Einleitung

Ich erhielt von dem Architekturbüro Eberhart AG den Auftrag ihr Backup System zu überarbeiten. Der Chef der Firma konsultierte mich, um ihn im Bereich Datensicherung zu beraten. In einem Gespräch erzählte mir der Geschäftsführer, dass in der momentanen Situation alle der 10 Mitarbeitenden ihre Dateien Lokal speichern. Da das momentane Konzept der Firma weder die 3-2-1 Regel berücksichtig noch gegen Ransomware oder ähnliches geschützt ist. Da dieser Zustand untragbar und es früher oder später zu Daten verlässt führt, muss sich etwas ändern.

Architekturbüro Eberhart AG

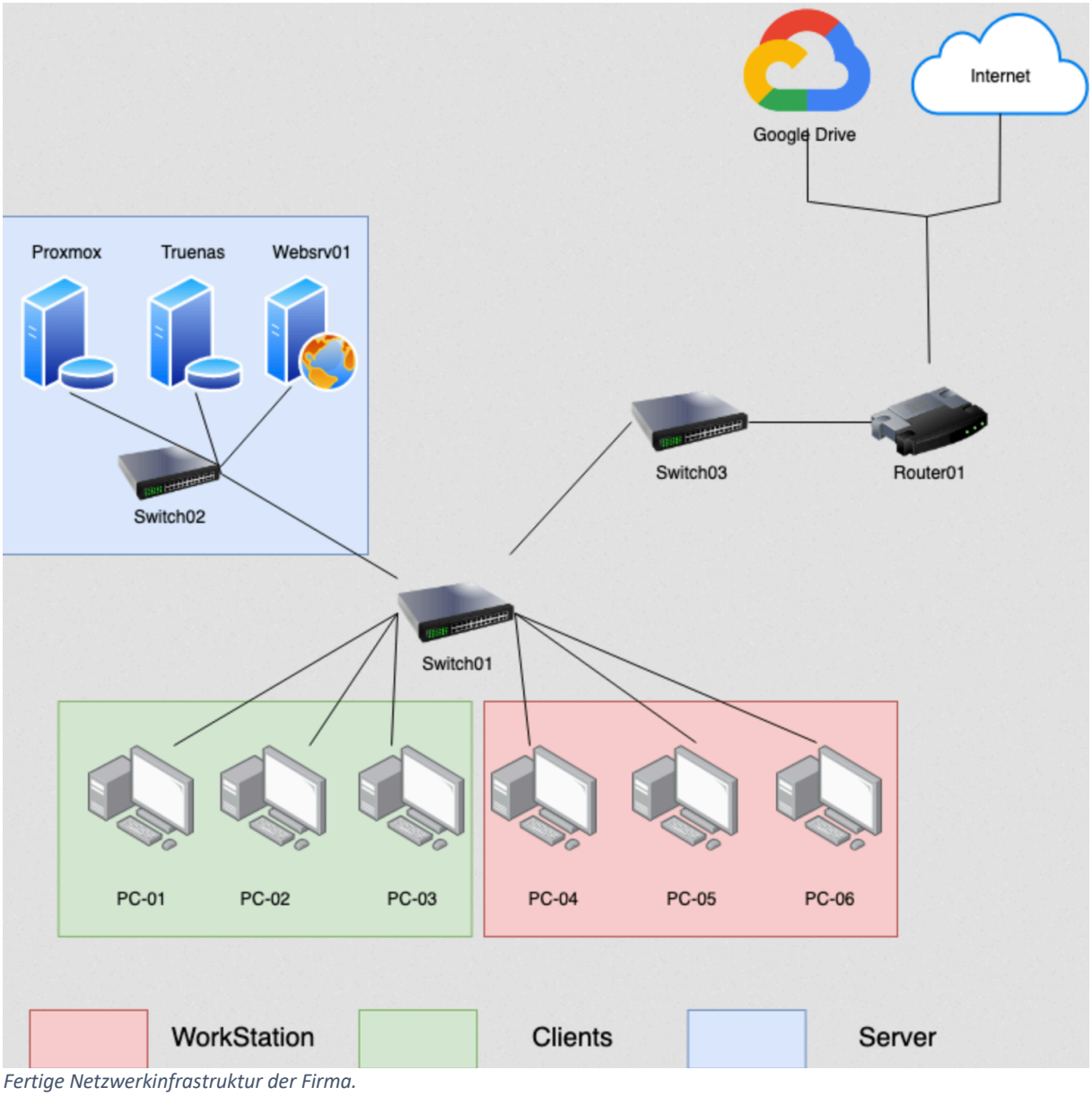
Datensicherheitskonzept

Damit in Zukunft die daten der Firma Architekturbüro Eberhart AG bestens gegen Hacker angriffen versehentliches löschen und Umwelt Katastrophen Geschütz sind. Werde ich hier ein Datensicherheitskonzept erstellen. Da die Auftraggeber Firma nur 10 Mitarbeiter hat, muss die Backup Infrastruktur nicht sehr Leistung stark sein. Dennoch sollte die Sicherheit der Daten nicht vernachlässigt werden, da alle Pläne, Kundendaten und Rechnungen für die Existenz der Firma unanbringlich sind.

Um die Datensicherheit zu gewährleisten ist sicherzustellen das die 3-2-1 Regel beachtet wird.
Die drei zwei eine Regel ist für Backups essenziell. Drei bedeutet dabei drei verschiedene Datenkopien (1 primär 2 Kopien), dass es zwei Speicherarten gibt (z.B HDD und Tape Drive) und das eins, das es extern gespeichert wird zum Beispiel in der Cloud oder auf einem externen Rechenzentrum.

Ich empfehle der Firma Einen Proxmox Backup Server, um ihre daten zu sichern. Um zusätzliche Sicherheit zu gewähren, werden die Daten in die Cloud (Google Drive) gesichert. Für alle 6 Mitarbeiter werden Home Ordner erstellt, auf die nur sie Berechtigung haben. Dann gibt es ein Ordner für Austausch, Projekte, Buchhaltung, GL und Administration. Alle diese Ordner werden auf dem Truenas Speicher der 5TB gross ist gespeichert. Um Daten Verlust durch korrupte Platten vorzubeugen, werden zwei 5TB Platten im Raid 1 gespiegelt. Die Firma hat zusätzlich einen Webserver, auf dem ihre Webseite läuft. Dieser wird mittels Windows Server Backup per SMB auch auf das Truenas gesichert. Da auf 3 Workstations eine CAD-Software installiert ist werden diese 3 Clients inklusive C Drive auf Truenas gesichert, da die manuelle Installation der Software sehr lange geht. Geplant ist, dass die Workstations Jeden Tag um 12:00 Uhr eine Inkrementelle Sicherung auf das Truenas zu machen, bis es nach 1 Woche wieder überschrieben wird. Um 23:59 soll das Truenas auf den Proxmox Backup Server gesichert werden, und nach 2 Monaten die älteste Sicherung überschrieben werden. Um den Cloud Speicher nicht zu verschwenden, werden nur die wichtigsten Daten wie User Data und Die Zeichnungen und Projekte werden täglich um 23:59 auf Google Drive gesichert.

Beim Truenas wird das Filesystem ZFS verwendet und beim Proxmox Backup wird ext4 verwendet, da es universell anwendbar ist. Der Proxmox Backup Server hat 10 TB in einem Raid 1, damit man das Doppelte der maximalen daten von Truenas speichern könnte. Auf eine Tapelibrary wird aus kosten gründen verzichtet, da es für so eine kleine Firma nicht betriebs relevant ist. Der Webserver sichert die Webseiten Daten auf einen SMB-Share auf dem Truenas



Fertige Netzwerkinfrastruktur der Firma.

Dieses Diagramm zeigt die gewünschte fertige Infrastruktur der Eberhart AG. Auf dem Plan ist ersichtlich, wie das Netzwerk aufgebaut ist. Ausserdem ist aufgezeigt welche Geräte im Netzwerk vorhanden sind.

Machbarkeit

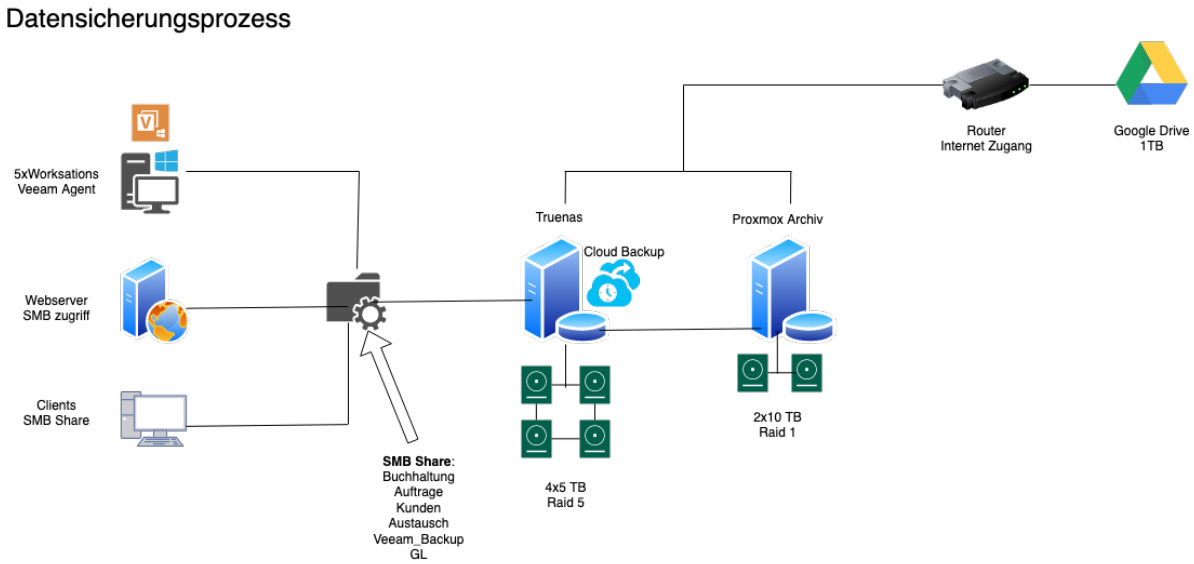
Da das Architekturbüro Eberhart eine sehr kleine Firma ist, ist es essenziell, dass die Machbarkeit geplant wird. Da die Firma bis jetzt noch keine Server Infrastruktur hat, muss alles neu angeschafft werden. Da das Truenas ein Betriebssystem ist, das nicht allzu viel Ressourcen braucht, fällt die Wahl auf einen kleinen Server. Auf dem Server läuft das Truenas mit einem Raid 5 an Festplatten, die zur Speicherung der Daten benutzt werden. Bei der Wahl der Festplatten setzten wir auf 4x5 TB HDD Platten. Diese sollten auf den Dauerbetrieb ausgelegt sein, da sonst das Risiko eines Platten Ausfalls steigt. Damit die Daten Intern nicht nur auf einem Server gespeichert sind werden sie zusätzlich auf einen 2 Server als «Archiv» gesichert. Auf dem 2 Server wird jede Woche eine komplette Kopie aller Daten, die auf dem Hauptserver sind, gespeichert. Diese monatliche Kopie wird so lange behalten biss auf dem sekundären Server kein platzt mehr ist. Damit die essenzielle Firmendaten doppelt gesichert sind werden die Rechnung, Kundenkartei, usw. immer um 12 Uhr abends in die Google Drive Cloud gesichert. Dadurch wird die Sicherung durch z.B Ransomware gewährleistet. Der CEO der Firma kann auf die Cloud zugreifen, um allfellig gelöschte daten von dort aus wieder herzustellen. Auf den Haupt Datei Server haben alle Mitarbeiter Zugriff jedoch nur lese und schreib rechte auf ihre persönlichen Ordner. Und eventuell auf gewisse Team Ordner. Auf den «Archiv» Server hat auch nur der CEO-Zugriff. Damit die Backups sauber durchlaufen wir bei Fehlern ein E-Mail an den Chef gesendet in der die Fehler beschrieben sind. Damit alle Daten vor unbefugten Zugriff geschützt sind wird im Turenas die Speicherpools verschlüsselt.

Bedarfsermittlung

In der Firma gibt es 3 Typen von Backups der PCs, Wichtige Geschäftsdaten und Daten Share. Die 3 Workstations machen jeweils täglich ein inkrementelles Backus des C-Drives auf das Truenas. Momentan sind die 3 Backus zusammen 1.5 TB gross. Jeden Samstag wird wieder ein Fullbackup gemacht und jeweils die anderen der letzten 7 Tage (nach und nach) gelöscht. Somit ist immer 1 Woche an Daten der Workstation Disk Abruf bereit. Der Zweite Punkt sind die Wichtigen Geschäfts daten. Diese nehmen etwa 100 GB in Anspruch und werden auf einem Datei Share auf dem Truenas gehalten. Da diese Daten für das Bestehen der Firma essenziell sind müssen diese besonders gesichert werden. Darum werden sie Täglich in die Google Cloud gesichert. Damit es in der Cloud genügend Speicherplatz hat wurde ein 1 TB GDrive Abo gelöst. Auf dem Data Share werden Team Ordner sowie auch die Persönliche Ordner gesichert. Der Data Share hat momentan eine Grösse von etwa 500 GB. Damit man in den nächsten paar Jahren noch ausreichen speicherplatzt hat wurden auf dem Truenas Server 4x5 TB eingebaut, das ergibt eine rohe Speichermenge von 30 TB. Da diese Platten in einem Raid 5 sind werden es nachher nur noch 18 TB, die zur Verfügung stehen. Momentan werden also um die 2.1 TB belegt. Somit ist die Firma gut für die Zukunft gerüstet. Auf dem Archiv Server werden die gesamten Daten also etwa 2.1 TB jede Woche gesichert. Damit der Server genügen Speicher hat. Sind in ihm 2x10 TB Platten im Raid 1 verbaut. Da auf dem Archiv Server nicht aktiv gearbeitete wird muss er nicht hoch redundant sein. Wenn der Archiv Server vollläuft, werden die jeweils ältesten Backus gelöscht. Die Wahl des Cloud Anbieters fiel auf Google Drive, da es ein gute Preis Leistung Verhältnis hat und ein übersichtliches UI.

SICHERUNGSPROZEDUREN

Um die Windows Workstations zu sicheren verwende ich den Veeam Agent for Windows. Diesen konfiguriere ich so, dass er die Backups in eine Separaten Ordner auf dem Truenas sichert. Damit es für die User möglichst einfach gestaltet ist, werde ich den Veeam Agent so Konfigurieren, dass er ein Automatisches Backup macht. Diese wird jeden Tag um 00:00 gemacht. Der Agent ist so konfiguriert, dass er den PC nach Abschluss des Backups automatisch herunterfährt. Damit die Sicherung der Workstations nicht allzu viel Platz in Anspruch nimmt habe ich eingestellt das die Backups nach 3 tagen überschrieb werden. Die Normal PCs müssen nicht komplett gesichert werden. Die Benutzer speichern ihre Office daten auf den Networkshare. Der Share wird sowohl in die Cloud als auch auf den Proxmox Archiv Server gesichert. Damit sichergestellt ist, dass das Backup um die richtige Zeit ausgeführt wird, ist im Veeam Agent ersichtlich wann das letzte Backus gemacht wurde und ob es Fehler gegeben hat. Beim Backup in die Cloud kann man die Log Files einsehen. Bei einem Fehlgeschlagenem Backup wird der Chef per Email benachrichtigt.



Visualisierung des Daten Sicherung Prozesses.

Damit die Daten der Benutzer nicht verloren gehen, müssen sie zwingen auf dem Fileshare gespeichert werden. Wenn Benutzer die Daten privat z.B auf OneDrive Speicher kann die Firma keinerlei Sicherung und Wiederherstellung der daten gewährleisten. Um diesem Problem entgegenzuwirken hat jeder Benutzer seinen eigen nur für ihn sichtbaren Ordner, in dem er seine Dinge speichern kann. Ausserdem gibt es den ordern Austausch, auf dem sich dich Mitarbeiter untereinander austauschen können. Zusätzlich gibt es noch die Ordner Buchhaltung, Aufträge, Kunden und GL. Der Ordner Veeam_Backup wird verwendet, um die Backups des Veeam Agent von den 5 Workstations zu speichern. Bei einem Fehler im Truenas Scale selbst kommt eine E-Mail an den Chef, der weiter Schritte einleiten kann (Problem Selber beheben, Support anfordern).

System- und Betriebsdokumentation

In dieser Berechtigung-Matrix wird festgelegt, welche benutzergruppen auf welche Ordner des Fileshare welche Berechtigungen haben.

	BUCHHALTUNG	GL	CHEF	ARCHITEKTEN	MITTARBEITER
BUCHHALTUNG	R,W	R,W	R,W	-----	-----
GL	------	R,W	R,W	-----	-----
KUNDEN_DATEN	R,W	R,W	R,W	R,W	R
VEEAM_BACKUP	------	-----	R,W	-----	-----
AUSTAUSCH	R,W	R,W	R,W	R,W	R,W
ORDER	R,W	R,W	R,W	R	R

Legende: **R**= Read **W**= Write **X=** Execute

In der unten ersichtlichen Tabelle ist festgehalten welche Benutzer in welchen Gruppen sind.

Benutzer und Gruppen:

Buchhaltung	GL	Chef	Architekten	Mitarbeiter
Annegret Müller, Fridolin Ferrari	Gordon Tromjelly, Mario Leclerc	Gordon Tromjelly	Mario Leclerc Lando Norris Franz Arzbacher Fernado Alonso	Alle + Valteri Russel Nicolas Latifi Toto Wolf

2FA:

Damit nur die befugten Personen auf die Weboberfläche des Truenas Zugriff hat, wurde ein 2FA Authentifizierung für den Web-dienst eingerichtet. Somit muss man, nachdem man sich mit Username und Passwort eingeloggt hat noch den 2FA key eingeben den man in der MFA-App findet.

Testprotokoll

Test	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
Restoren von der Cloud ins Truenas	Die Dateien, die in der Cloud gespeichert sind, sollten auf das Truenas gehen.	Der Restore aus der Cloud Funktionierte tadellos. Siehe Log: Logfile_Cloud_Restore.log	OK
Sicherung eines Windows Clients mit Veeam	Das Backup wird zur gewünschten zeit automatisch gemacht.	Hat funktioniert Siehe Bild: Veeam_Backup_Fertig.png	OK
Restore eines Windows Clients mit Veeam	Ordner oder Files können von beliebigen Backups Restored werden.	Ist Fertig Siehe Bild: Veeam_Restore_1-3.png	OK
Berechtigungen stimmen	Gruppen sind auf richtige Ordner berechtigt	Funktioniert. Bei nicht ausreichender Berechtigung gibt es ein Fehler.	OK
Funktioniert 2FA	Mit 2FA einloggen	Mit richtigem code kommt man rein	OK

Bilder:

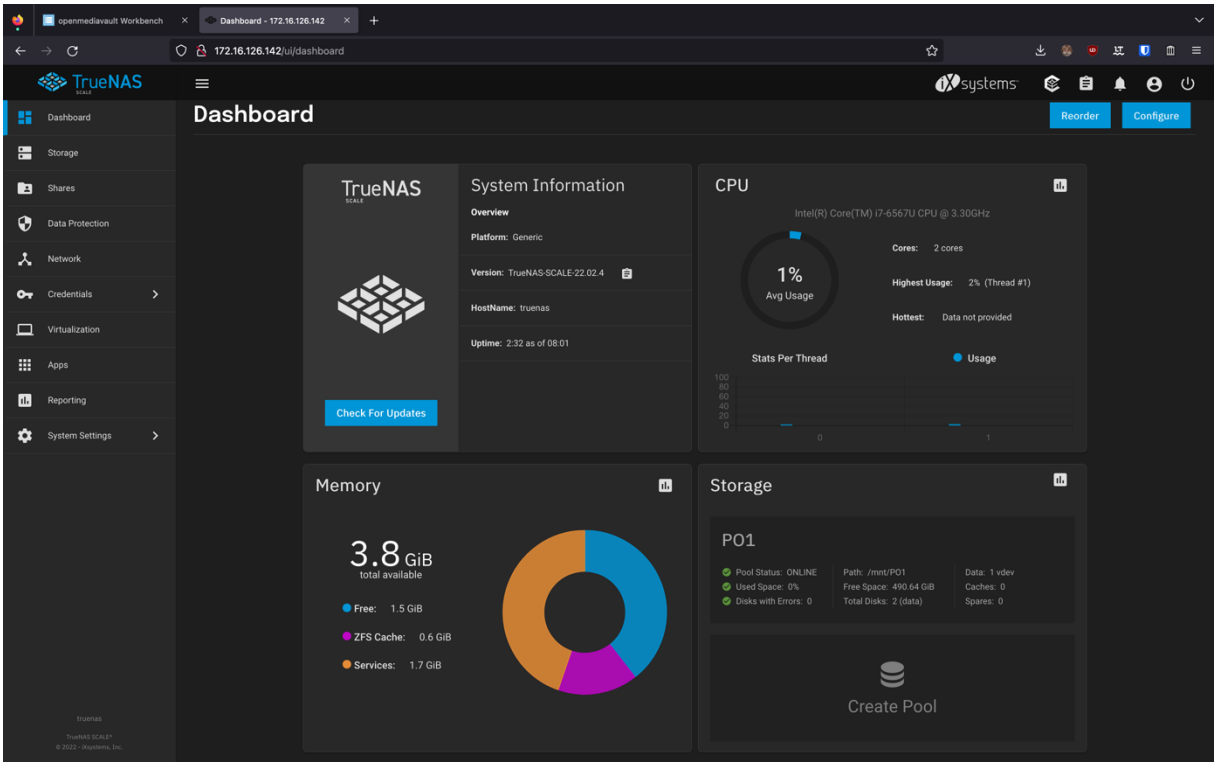


Bild01: TrueNas Dashboard

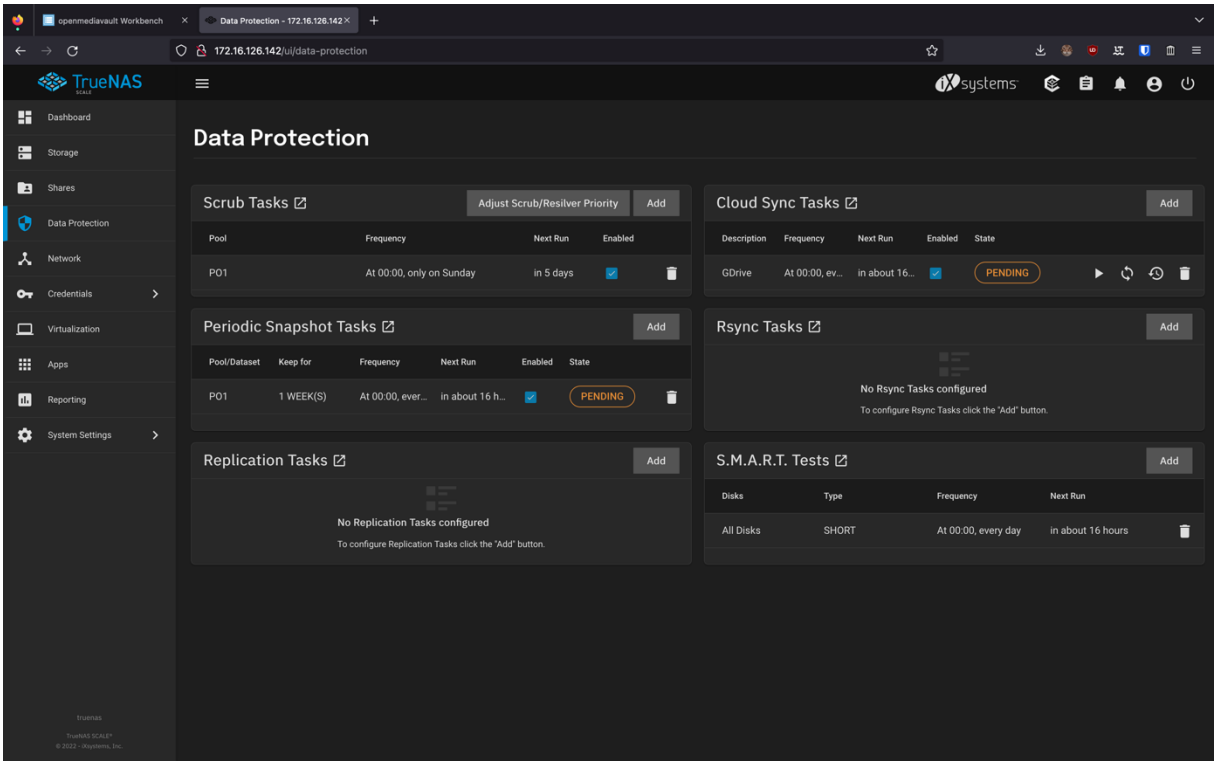


Bild02: Sicherungs Dashboard

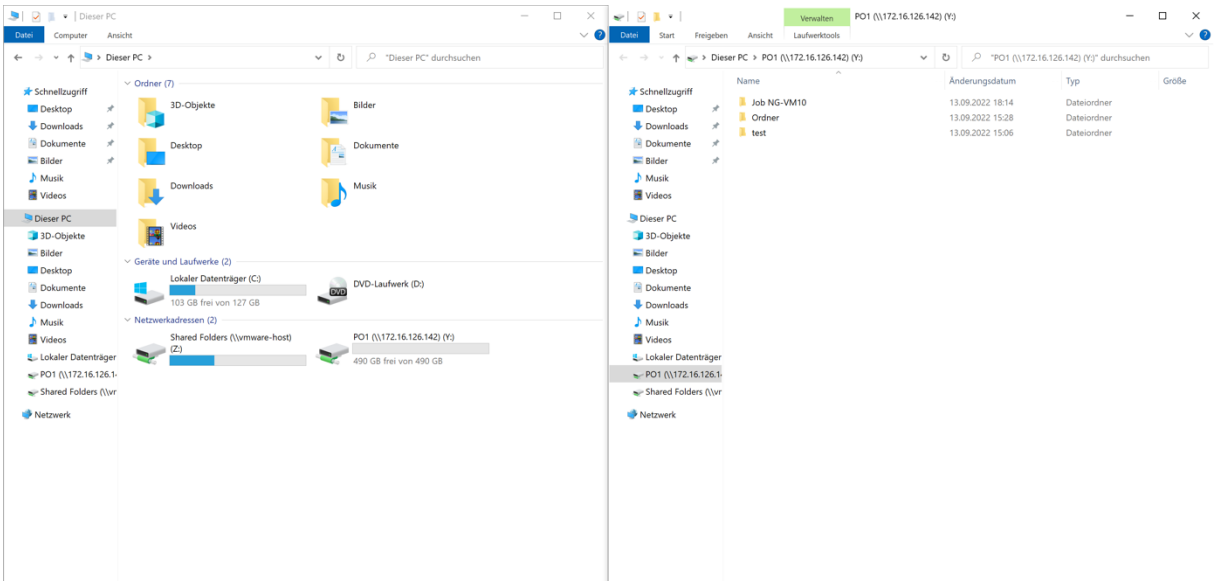


Bild03: Datashare im Windows Explorer (PO1)

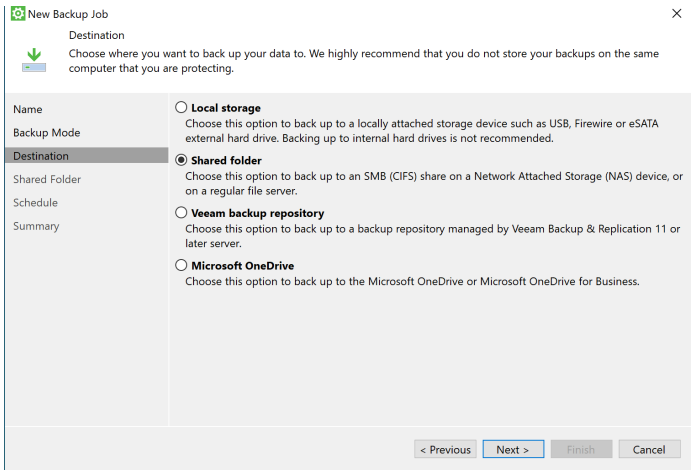


Bild04: Veeam Agent Konfiguration.

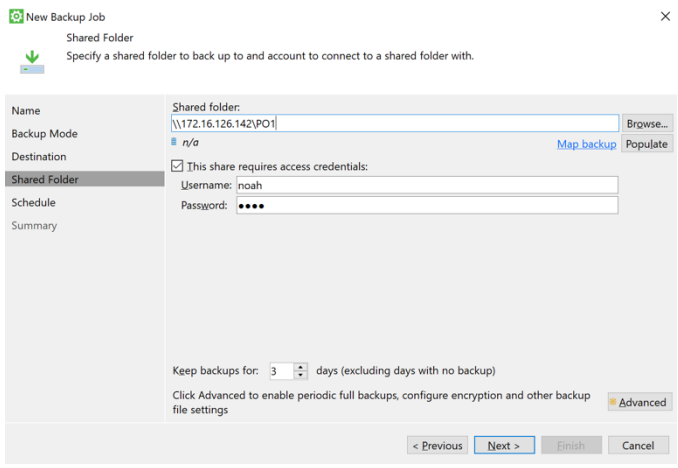


Bild05: Veeam Agent Konfiguration.

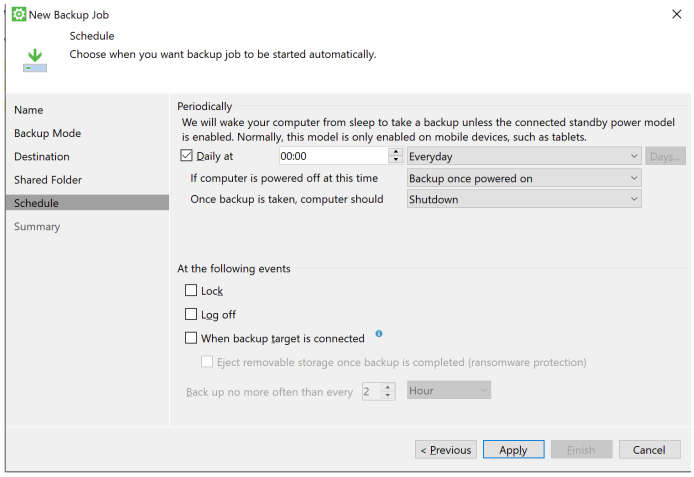


Bild06: Veeam Agent Konfiguration.

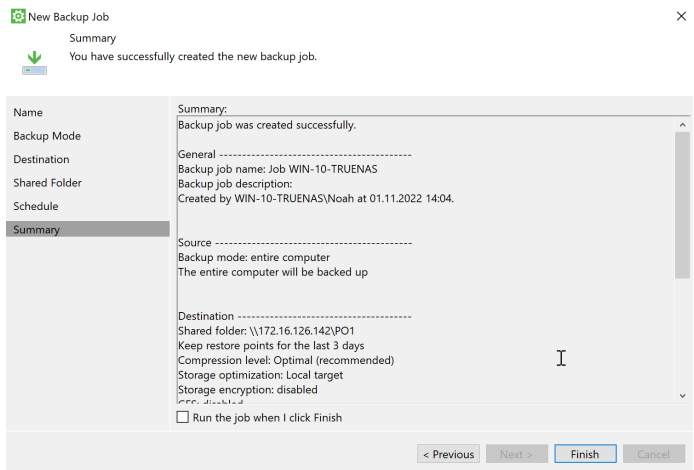


Bild07: Veeam Agent Konfiguration.

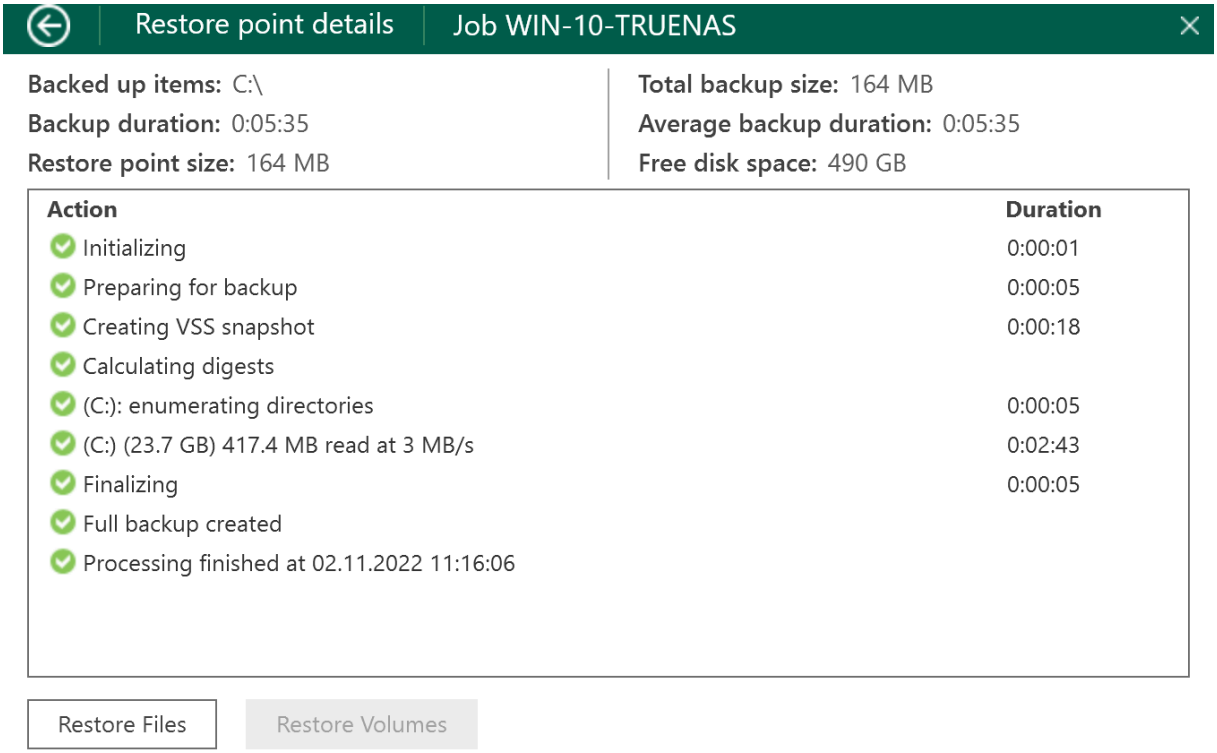


Bild09: Erfolgreiches Backup

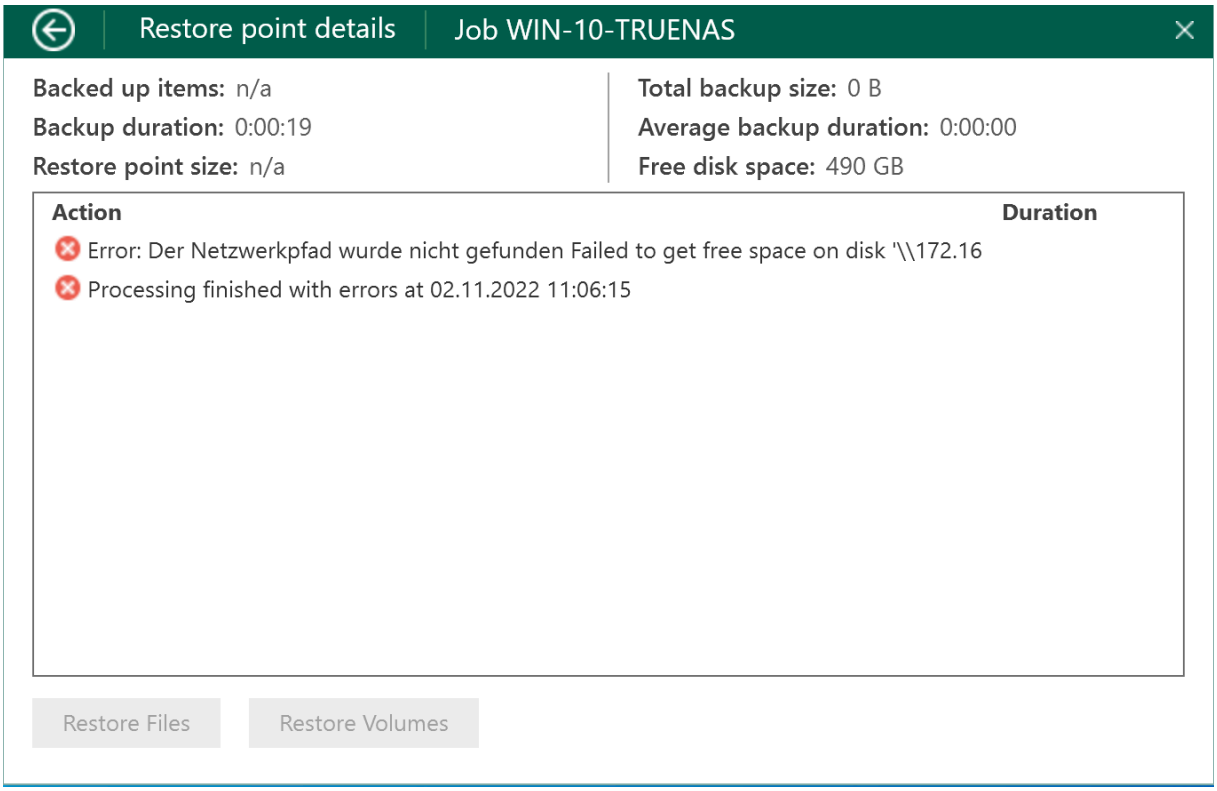


Bild10: Fehlerhaftes Backup (Als Beispiel)

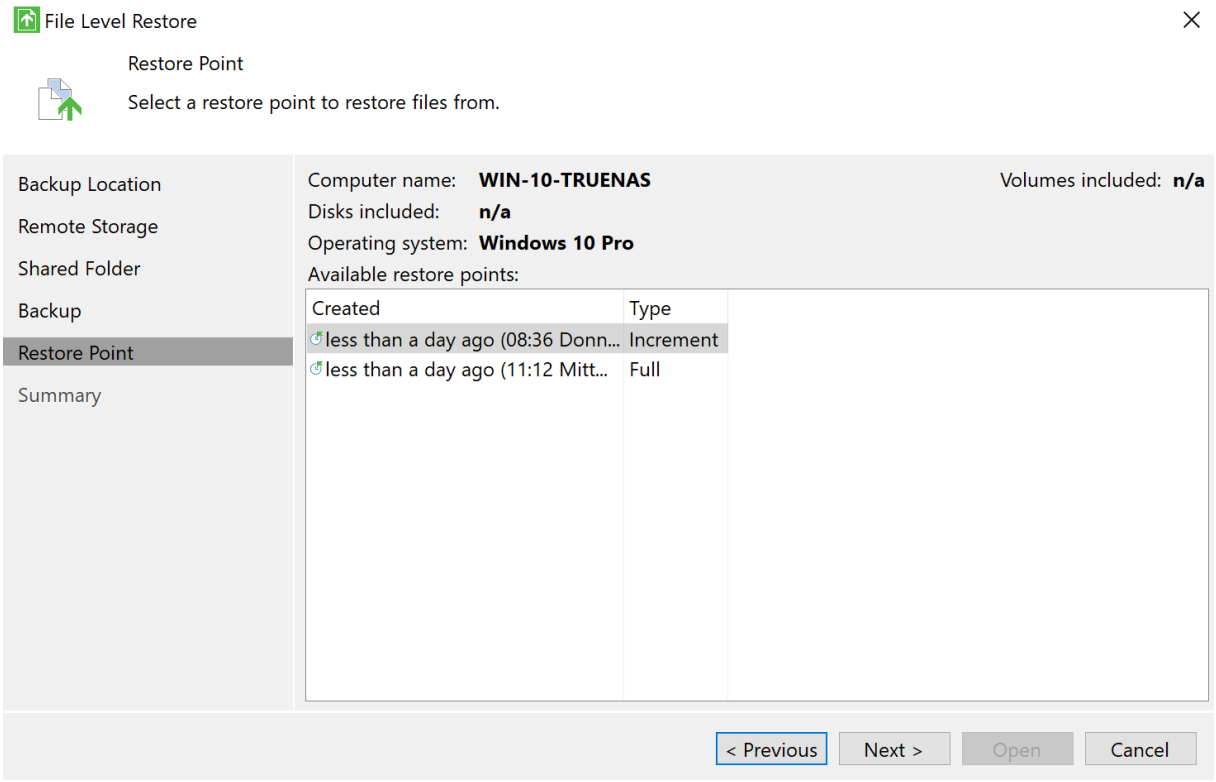


Bild11: Restore mit Veeam Backup

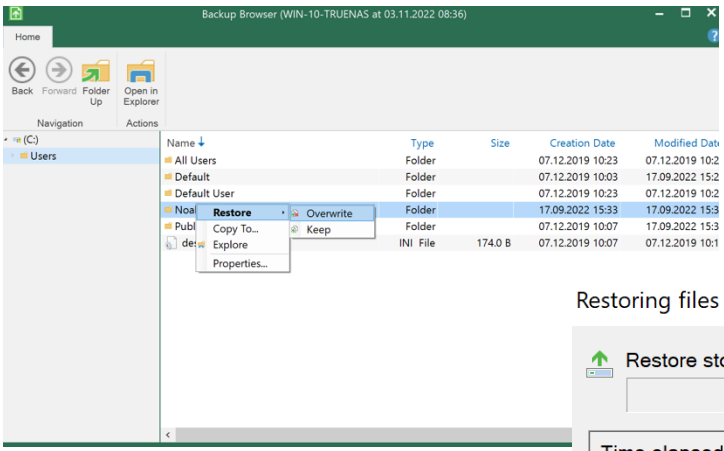


Bild12: Restore mit Veeam Backup

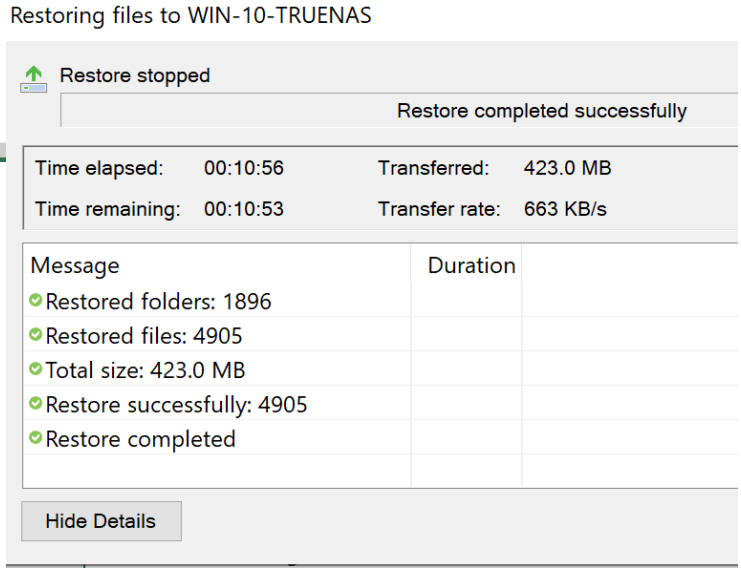


Bild13: Restore mit Veeam Backup

Rückblick und Fazit:

Rückblickend kann ich sagen das ich eine ganze Menge neu Dinge in diesem Modul gelernt habe. Einerseits aus technischer Sicht mit dem Truenas. Andererseits auch wie man ein Projekt plant und umsetzt. Ich habe gelernt, wie wichtig es ist sich die Zeit richtig einzuplanen und in der geplanten Zeit nur am Projekt zu arbeiten. In Zukunft kann ich nun auch die wichtigsten Backup Kriterien evaluieren und gegebenen falls umsetzten. Ich denke auch, dass ich mit diesem Projekt etwas zur IPA mitnehmen kann und so besser darauf vorbereitet bin.