FAST LTA

Achtergrondartikel

Wat maakt back-ups zo complex?

Back-ups hebben ten doel om bescherming te bieden tegen gegevensverlies. Als bronbestanden verloren gaan, kunnen deze kopieën als vangnet dienen. Zo eenvoudig zou gegevensbescherming kunnen zijn in een wereld zonder RTO's, RPO's, ransomware en natuurrampen. Maar helaas moeten IT-beheerders tegenwoordig met aanzienlijk meer factoren rekening houden om tot een veilige, betrouwbare en betaalbare back-upstrategie te komen.

December 2021

Van back-ups naar een recovery-strategie

De toenemende complexiteit van back-upomgevingen is het gevolg van een ingrijpende paradigmaverschuiving. Geruime tijd was het voornaamste doel van back-ups om een laatste verdedigingslinie tegen gegevensverlies te bieden die hopelijk nooit gebruikt hoefde te worden. Tegenwoordig is het echter nodig om een allesomvattende strategie toe te passen die het mogelijk maakt om gegevens op elk gewenst moment snel, betrouwbaar en tot in kleinste detail te herstellen. De kans dat dit nodig zal zijn is met de komst van ransomware aanzienlijk toegenomen.

De grote boosdoener: ransomware

Ransomware heeft menselijke fouten (zoals onopzettelijke verwijdering of foutieve configuraties) van de troon gestoten als belangrijkste oorzaak van gegevensverlies. En gegevensverlies is op zijn beurt niet langer de belangrijkste reden achter de noodzaak van gegevensherstel. Ransomware versleutelt bedrijfsgegevens, zodat die niet langer bruikbaar zijn. Daarmee komen IT-processen tot stilstand. De resulterende downtime, herstelprocedures en/of betaling van losgeld gaan met hoge kosten gepaard. Naast het bieden van bescherming tegen ransomware-infecties is een gedegen back-upstrategie daarom de belangrijkste maatregel.

Tegenwoordig is het niet langer voldoende om gegevens te beschermen volgens het oude vertrouwde principe van B2D2T (Backup to Disk to Tape), waarbij afzonderlijke bestanden snel vanaf de schijf worden hersteld en volledige datasets vanaf tape. Bij gerichte ransomware-aanvallen proberen cybercriminelen tegenwoordig eerst de back-ups onklaar te maken alvorens over te gaan tot het versleutelen van bedrijfsgegevens. Tegen de tijd dat de IT-afdeling zich realiseert wat er is gebeurd zijn de back-ups vaak al onbruikbaar of gewist. Dit geldt ook voor tapegebaseerde back-ups die niet uit het systeem zijn verwijderd volgens het principe van air gapping (opslag op een veilige externe locatie).

De gevolgen voor back-ups

Het toenemende aantal ransomware-aanvallen heeft directe gevolgen voor de back-upstrategie. En daarmee neemt de complexiteit alleen maar toe.

1 – Een zo kort mogelijke RTO vraagt om flash-opslag

Het leeuwendeel van alle kosten die met een succesvolle ransomware-aanval gepaard gaan houdt verband met downtime van IT-systemen. Hoe sneller de voor de dagelijkse bedrijfsvoering benodigde gegevens hersteld kunnen worden, hoe beter de totale kosten in de hand kunnen worden gehouden. De recovery time objective (RTO) speelt daarbij een grote rol. Dit is de maximale tijd die het herstellen van gegevens in beslag mag nemen. Het minimaliseren van de RTO vraagt om snelle storage-systemen die in staat zijn om gegevens te herstellen uit diverse incrementele back-ups. Moderne back-upsoftware biedt de mogelijkheid om virtuele machines al tijdens de herstelprocedure direct vanuit de back-up te starten om de downtime verder terug te dringen. Veeam noemt dit InstantRecovery®. Op flash gebaseerde opslagvoorzieningen hebben daarmee een belangrijke positie voor zich verworven als primaire back-upbestemming. Maar omdat flash-opslag aanzienlijk duurder is dan schijfopslag worden gegevens normaliter slechts een paar dagen in het op flash gebaseerde opslagsysteem bewaard.

Door het verkorten van de RTO zijn gegevens weer snel beschikbaar.

2 – Het opslagsysteem voor schijfgebaseerde back-ups moet schaalbaar en veilig zijn

Voor de tweede tier vertegenwoordigt de kostenefficiëntere opslag van back-ups op schijf de beste oplossing. Aangezien het soms weken kan duren voordat ransomware zich kenbaar maakt door het versleutelen van data moeten gegevens voor de lange termijn worden opgeslagen. Bovendien is er binnen alle sectoren sprake van een exponentiële groei van de datavolumes. Reguliere RAID-systemen zijn daarmee niet langer toereikend als network attached storage (NAS)-systeem. Ze zijn namelijk onvoldoende schaalbaar en niet ontwikkeld met het oog op lange-termijnopslag. In plaats daarvan zijn er schijfgebaseerde systemen nodig die speciaal zijn bedacht op jarenlange opslag en waarvan de capaciteit naar behoefte kan worden uitgebreid (scale-up).

Organisaties die zich willen wapenen tegen gerichte cyberaanvallen die back-ups versleutelen moeten speciale veiligheidsmaatregelen treffen voor de back-ups die ze voor de lange termijn op schijf opslaan. Daarover leest u meer in onze whitepaper “Back-ups tegen ransomware beschermen”. Deze whitepaper kunt u downloaden van https://fastlta.com/backups-schuetzen. Op deze website treft u ook een video aan.

Download at https://fastlta.com/dl-proctecting-backups

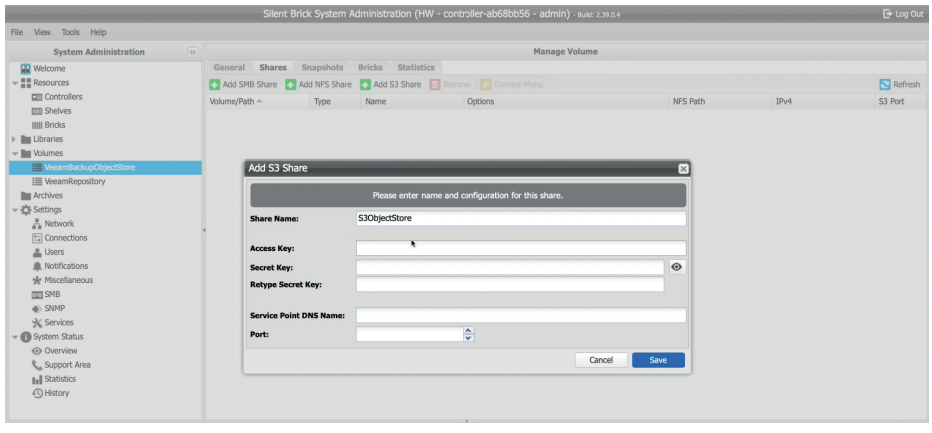
3 – Airgapping vraagt om offline back-upmedia

Organisaties moeten regelmatig complete datasets opslaan op back-upmedia die geschikt zijn voor offline gebruik en fysiek gescheiden van het opslagsysteem moeten worden bewaard (air gapping). Als gevolg hiervan beleeft tape sinds 2016, het jaar waarin de eerste serieuze ransomware-aanvallen zich voordeden, een comeback die tot op de dag van vandaag voortduurt. Al naar gelang de datavolumes en recovery point objective (RPO)-strategie (hoe ver moet ik teruggaan in mijn back-ups om gegevens volledig te herstellen) kan de tape-infrastructuur die louter voor dit doel wordt gebruikt op zichzelf al bijzonder complex en onderhoudsintensief zijn. Omdat offline opslagmedia alleen in het uiterste noodgeval voor gegevensherstel worden ingezet is het belangrijk dat ze zo goedkoop mogelijk zijn. En de enige oplossing die goedkoper is dan tape is geen tape. Dat houdt in dat men afziet van het gebruik van een complete aanvullende infrastructuur waarvoor een afzonderlijk onderhoudscontract geldt.

De Silent Brick is een voor airgapping geschikte opslagcontainer voor het Silent Brick System.

4 – Vanuit kosten- en onderhoudsperspectief zijn er object stores nodig

Voordat ransomware zijn entree maakte was er duidelijk sprake van een trend om volledig van tape af te stappen. De reden hiervoor was dat het gebruik van tape gepaard gaat met complexe beheerprocessen en een hoge onderhoudsoverhead. De komst van object storage lijkt deze trend nieuw leven in te blazen. Aanvankelijk was deze vorm van gegevensopslag alleen in de cloud beschikbaar. Maar omdat veel organisaties grip op hun data willen behouden (of daartoe door de wet- en regelgeving worden gedwongen), zijn er met S3 compatibele oplossingen voor object storage ontwikkeld die deze functionaliteit nu ook lokaal (on premise) beschikbaar stellen. Dankzij intelligente functionaliteit voor gegevensbeheer binnen de back-upsoftware is het mogelijk om het aantal volledige back-ups (die onder meer voor airgapping nodig zijn) en de benodigde opslagcapaciteit fors terug te dringen. Als datasets ook nog eens worden beschermd op basis van immutability (regelmatige snapshots die alleen via een speciale beheerdersaccount toegankelijk zijn), wordt het mogelijk om een fors aantal tape-systemen te vervangen. Het nadeel is alleen dat hiervoor meestal weer een extra storage-systeem is benodigd.



In het Silent Brick-systeem kan elk volume ook als een met S3 compatibele netwerkshare beschikbaar worden gesteld om het parallelle gebruik van on premise object storage mogelijk te maken.

Op ons YouTube-kanaal vindt u onder meer een video over met S3 compatibele object stores.

https://fastlta.com/youtube

De complexiteit terugdringen

Een typische omgeving voor de opslag van back-ups bestaat dus uit flash-arrays, verschillende disk systemen, tape voor air gapping en met S3 compatibele object storage. In veel gevallen moet de bestaande infrastructuur minimaal tot het einde van de afschrijvingsperiode of het verlopen van het onderhoudscontract in gebruik blijven. Dit resulteert in heterogene opslagstructuren met tot wel vier of meer systemen, user interfaces, onderhoudscontracten en contactpersonen. De complexiteit van een dergelijke omgeving boezemt veel IT-managers angst in en vraagt om intensief advies. Moderne systemen voor de opslag van back-ups beloven een reductie van de beheer- en onderhoudsoverhead en kostenbesparingen, maar bieden vaak geen ondersteuning voor alle aspecten van de back-upstrategie en/of vragen om een complete vervanging van de bestaande infrastructuur.

„Start Anywhere“ met het Silent Brick System

Met de Silent Bricks van FAST LTA kunt u beschikken over een storage-systeem dat integrale en individuele ondersteuning biedt voor alle hierboven beschreven aspecten. Silent Bricks zijn afzonderlijk configureerbare opslageenheden die als NAS (op basis van SMB/NFS), virtual tape library (VTL) of met S3 compatibele object storage kunnen worden ingezet. Hierbij kan worden gekozen tussen flash- of schijfconfiguraties en traditionele en mobiele opslagcontainers. Elk onderdeel kan op elk gewenst moment afzonderlijk worden opgeschaald. Als er voor de start van het traject de vervanging van een standaard RAID-systeem door schijfgebaseerde Silent Bricks staat gepland, kunnen de overige componenten, zoals flash-storage, air gapping en VTL of de met S3 compatibele object storage op elk gewenst moment worden toegevoegd. In de meeste gevallen volstaat dan een eenvoudige uitbreiding van de opslagcapaciteit. Dit zorgt voor een aanzienlijke reductie van de incrementele kosten.

De beloning aan het einde van de rit is een opslagsysteem dat tegemoetkomt aan alle eisen van moderne back-upstrategieën, de complexiteit ingrijpend terugdringt en op de lange termijn voor merkbare kostenbesparingen zorgt.

PROUDLY MADE IN EUROPE

COMEX

FAST LTA

COMEX | Vogt 21 | NL-6422 RK Heerlen | office@comex.eu | **www.comex.eu**

FAST LTA | Ruedesheimer Str. 11 | 80686 Munich, Germany | info@fast-lta.de | **www.fast-lta.com**