

Varnost na enem mestu

Uporabniki računalnikov danes večinoma razumejo, da je treba imeti varnostno kopijo, vsega. A vse prepogoste so nejasnosti o pravih strategijah za izdelavo teh kopij in njihovo upravljanje.

Jure Forstnerič

Pogosto se tudi pozabi na nadgradnjo in prilagajanje strategij na nove izzive. Vprašanje je, ali proces, ki smo ga vzpostavili pred desetimi leti, še dohaja nove zahteve, nove naprave, operacijske sisteme, programe in podatke. Marljiva izdelava varnostne kopije nekega omrežnega diska nam nič ne pomaga, če smo vmes že večkrat zamenjali delovni proces.

Programov in rešitev za izdelavo varnostnih kopij je res ogromno. Najosnovnejši so programi, ki v nekem rednem intervalu prekopirajo vse podatke na zunanji medij – denimo mrežni pogon ali USB ali v katero izmed bolj popularnih oblčnih hramb.

Novejši operacijski sistemi, denimo Windows 10, imajo take možnosti vgrajene že v sam sistem. Tam se, poleg samih datotek, lahko naredi tudi varnostna kopija celotnega sistema, vključno s programi.

A taka strategija bo za zahtevne uporabnike, ki morajo skrbeti za več računalnikov, po možnosti pa še za strežnik ali dva, preveč časovno potratna. Ti potrebujejo celovito rešitev, ki na enem mestu ponudi različne možnosti varovanja. Tudi teh rešitev je veliko. Ena izmed elegantnejših je pred časom predstavljen Synology Active Backup.

Synology je sicer znan proizvajalec datotečnih omrežnih strežnikov NAS (*Network Attached Storage*). Tudi na naših preizkusih smo jih že večkrat pohvalili. Gre sicer za enega dražjih proizvajalcev teh naprav, a ponujajo enega najbolj preglednih in zmogljivih operacijskih sistemov, za katerega je na voljo veliko dodatnih aplikacij. Active

Backup so prvič predstavili že leta 2018, a takrat še v ne povsem dokončani obliki.

Preizkusili smo njihov paket Active Backup for Business – ta je na voljo prek njihove tržnice z aplikacijami za operacijski sistem DSM. Ob njem ponujajo sicer tudi Active Backup for G Suite (ta je namenjen izdelavi varnostnih kopij Googlevih spletnih storitev) ter Active Backup for Office 365 (torej za Microsoftove spletne storitve Office 365).

Z Active Backup for Business po njihovih besedah merijo na manjša in srednja podjetja. Torej podjetja, ki imajo omejitve pri finančnih in človeških virih ter iščejo dovolj enostavno in cenovno ugodno rešitev.

Po našem mnenju je ena izmed ključnih prednosti dejstvo, da za ta paket ne plačujemo mesečnih ali letnih licenc – strošek je le

nakup samega omrežnega strežnika (no, in seveda pogonov v njem). S tem bo tudi marsikateri računalničar lažje nagovoril nadrejene k nakupu take naprave.

Active Backup deluje na večini novejših Synologyjevih naprav višjega razreda (v imenu so označene z znakom +) – popoln seznam je sicer objavljen na njihovi spletni strani. Ena izmed zahtev pa je podpora za datotečni sistem BTRFS. Sami smo paket preizkusili na napravi DS-918+, ki sprejme štiri diskovne pogone.

Program ima štiri sklope za izdelavo varnostnih kopij. Vsi omogočajo določitev naprednih urnikov, povsod lahko nastavimo število in (ali) starost hranjenih kopij. Splošna omejitev za vzporedno izdelavo varnostnih kopij je deset naprav, ne glede na to, za kateri konkretni sklop gre. To je po našem mnenju

SYNOLOGY Active Backup for Business

Rešitev za celovito izdelavo in vodenje varnostnih kopij.

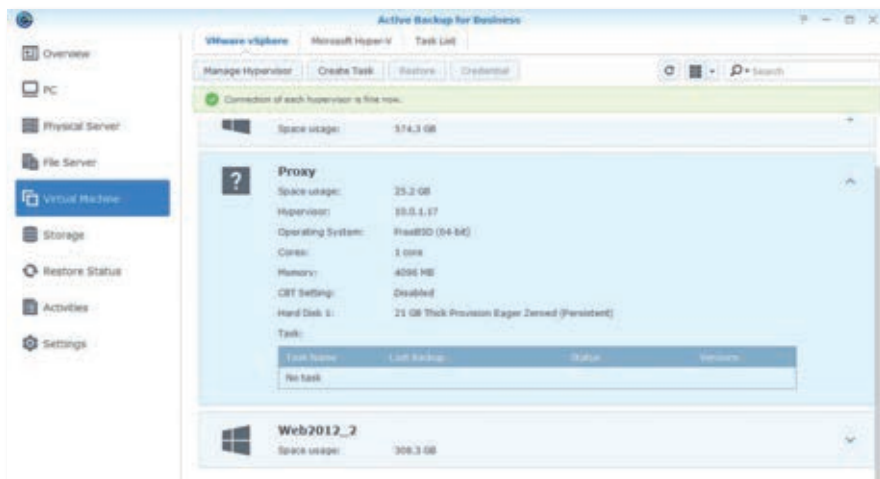
Prodaja: www.xenon-forte.si

- + Preprosta uporaba, veliko funkcij, možnost pogona virtualnih naprav neposredno na strežniku NAS.
- Cena samega strežnika, vezanost na enega ponudnika opreme.



Marljiva izdelava varnostne kopije nekega mrežnega diska nič ne pomaga, če smo vmes že večkrat zamenjali delovni proces.





△ Vmesnik za pregled nad napravami, za katere izdelujemo varnostne kopije, je pregleden in enostaven.

dovolj, saj hitro pridemo tudi do omejitvev pri hitrostih omrežja, za vsako opravilo pa lahko nastavimo ločen urnik. Uporabnikom lahko dodelimo posamezne pravice, denimo, da sami dostopajo do datotek z določene lokacije – recimo lastnega računalnika.

Najenostavnejši je sklop za izdelavo varnostnih kopij datotek, shranjenih na mrežnih pogonih. Tu lahko tudi izključimo določene mape ali datoteke, denimo po tipu datotek. Podprta sta SMB in Rsync, pri zadnjem prek gesla ali ključa SSH. Nastavimo lahko hrambo več različic datotek, zrcaljenje (torej prepis starih različic z novimi, brisanje neobstoječih datotek) ali inkrementalno hrambo (kjer se dodajajo vse nove datoteke, prepisujejo stare različice, a ne zbrisajo obstoječe, tudi če se izbršejo iz primarnega vira).

Naslednja dva sklopa sta namenjena izdelavi varnostnih kopij celotnih sistemov, tako osebnih računalnikov kot fizičnih strežnikov. Pri obeh (v uporabniškem vmesniku sta označena kot »PC« in »Physical Server«) moramo namestiti Synologyjev odjemalec, ki skrbi za komunikacijo s strežnikom in tudi pokaže status varnostne kopije. Tako lahko na računalniku vidimo, kdaj je bila narejena zadnja kopija sistema in kakšen je urnik, med izdelavo pa tudi to, koliko časa bo še trajalo in kakšna je hitrost kopiranja.

Pri obeh lahko s Synologyjevih programom izdelamo zagonski medij za restavriranje iz narejene varnostne kopije. Torej če računalnik (strežnik) fizično odpove, vzamemo drugega, na njem zaženemo omenjen zagonski medij, ki ponudi okolje, v katerem se le povežemo z mrežnim strežnikom, na katerem imamo shranjeno varnostno kopijo. Od tam nato namesti vse, kar je bilo shranjeno, vključno z operacijskim sistemom in vsemi nameščenimi programi ter s podatki. Lahko se odločimo tudi le za varovanje sistema ali določenega pogona (tudi zunanega pogona).

Tudi Vmware!

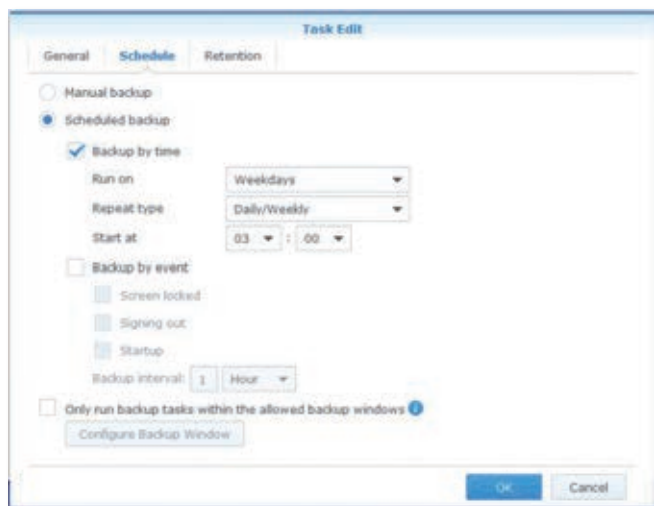
Najbolj nas je zanimalo delovanje zadnjega sklopa, imenovanega Virtual Machine. Gre za izdelavo varnostne kopije virtualnih sistemov, ki jih gostimo na strežnikih z Microsoftovim Hyper-V ali VMware vSphere. Pri tem je izredno uporabna prednost ta, da lahko naredimo kopijo med tem, ko sistem obratuje. To sicer zmorejo tudi nekateri drugi ponudniki, med bolj znanimi so izdelki podjetja Veeam, a ti ne delujejo v primeru uporabe brezplačnih različic VMware ESXi. Hkrati so te rešitve vezane na letne licence, kar zna biti za manjša podjetja kar huda ovira.

Sami smo preizkusili izdelavo varnostne kopije virtualnih naprav s sistemom Linux in Windows Server. V obeh primerih moramo imeti znotraj sistema nameščen paket VMware Tools, na samem strežniku mora biti omogočena povezava SSH, koristna pa je tudi tehnologija Changed Block Tracking. Ta omogoča, da kasneje prenesemo le bloke, ki so bili vmes spremenjeni. Na sistemih, kjer delujejo aplikacije z zbirkami podatkov, denimo Microsoftov strežnik za elektronsko pošto Exchange, moramo imeti vključeno tudi tehnologijo Volume Shadow Copy Service (VSS), s katero se zagotovi doslednost pri izdelavi varnostne kopije in morebitni obnovi podatkov.

Izdelava varnostnih kopij poteka hitro in brez opaznih upočasnitev sistema. Pri tem je bil najzahtevnejši primer strežnika, na katerem teče zgoraj omenjeni Exchange, a tudi tu ni bilo nobenih težav. Zanimivo, da lahko prek spletnega vmesnika pridemo tudi do posameznih datotek znotraj virtualnih sistemov. Tudi tu lahko posameznim uporabnikom dodelujemo napredne pravice.

Kako pa nazaj?

Seveda pa je izdelava varnostne kopije le polovica zgodbe – vedno moramo preizkusiti tudi restavriranje oziroma vzpostavitev sistema po morebitnem izpadu. Tu imamo

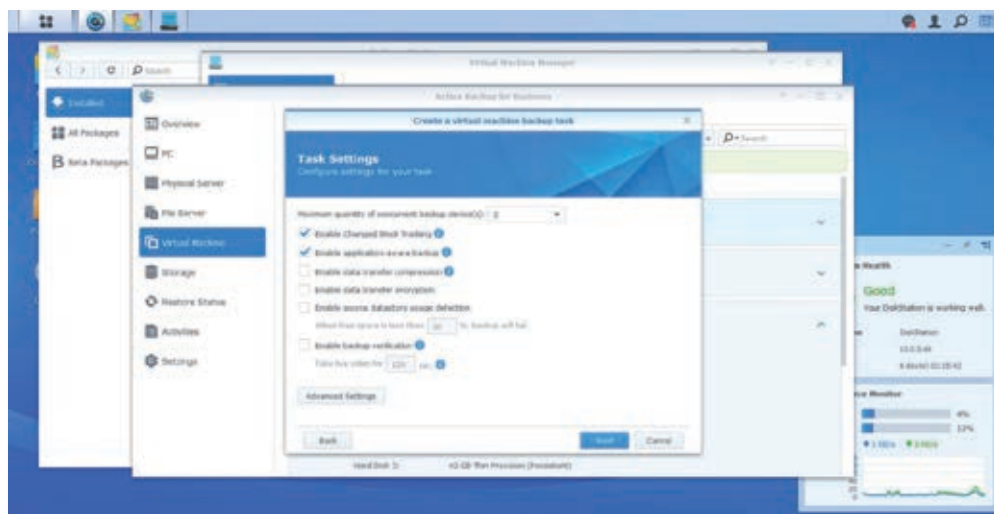


△ Napredne možnosti za urejanje časovnih okvirov, v katerih se izvede varnostno kopiranje, so standard za vse tovrstne programe.

nekaj različnih možnosti. Izredno zanimiv je zagon virtualne naprave neposredno na Synologyjevem strežniku NAS. Ti imajo že nekaj časa vgrajen tudi hipervizor za pogon virtualnih naprav.

V našem primeru je to delovalo tako pri Linuxu kot pri Windows Serverju. Pri prvem je bilo sicer treba vnesti nastavitve nove mrežne kartice, drugih težav pa nismo imeli. Velja sicer opozoriti, da moramo biti pozorni na

▽ Varnostno kopiranje obstoječih virtualnih naprav je izredno enostavno.



Vedno preizkusimo tudi vzpostavitev sistema po morebitnem izpadu!

strojne omejitve strežnika NAS. Če ima strežnik v svojem virtualnem okolju na voljo 32 GB pomnilnika, bo na NAS, v katerega je vgrajenih 8 GB, delovanje pač okrnjeno. A delovalo vendarle bo (vsaj v našem primeru je).

Druga možnost je zagon na nekem obstoječem strežniku s hipervizorjem (v našem primeru ESXi). Tu imamo spet dve možnosti. Če se nam izredno mudi, lahko na hipervizor prenesemo le zagonsko osnovo, vse ostalo, torej same virtualne pogone, pa pustimo na Synologyju. Tako se lahko virtualno napravo zažene v le nekaj minutah. Hitrost delovanja bo zaradi omrežne povezave med hipervizorjem in NAS nekoliko manjša, a vseeno omogoča,

da izredno hitro vzpostavimo delujoče stanje. Kasneje pa pač prenesemo še vse virtualne pogone – to je sicer tretja možnost, ki jo imamo pri vzpostavitvi sistema. Hitrost prenosa je pri tem seveda odvisna od hitrosti mreže.

Priznati moramo, da smo bili nad Synologyjevim paketom navdušeni. Zelo je enostaven za vzpostavitev različnih tipov varnostnih kopij, podpira pa tudi izvoz teh kopij naprej, denimo v oblak ali na tretji strežnik. Še najpomembnejša pa je podpora virtualnim napravam, kjer je res dobro izvedena vzpostavitev sistemov po izpadu. Za prvo silo bomo lahko kako virtualno napravo poganjali kar neposredno na samem NAS, dokler si pač ne priskrbimo kakšne druge rešitve. Tudi možnost reševanja posameznih datotek iz varnostnih kopij virtualnih naprav zna biti koristna.

Kot smo povedali v uvodu, je različnih strategij in tehnologij za izdelavo varnostnih kopij veliko. Synologyjeva rešitev je med njimi seveda vezana na njihove fizične naprave – strežnike NAS. A ti so, po našem mnenju, med najboljšimi, sama Active Backup for Business pa tudi ena izmed enostavnejših in bolj elegantnih rešitev za celovito varovanje različnih podatkov. Plus je tudi dejstvo, da za njeno uporabo ne potrebujemo trajnih licenc, kar vsaj do neke mere odtehta nakup same naprave. ◀