Služba zálohování

Version 7.9

UŽIVATELSKÁ PŘÍRUČKA

Revize: 25.4.2019

Obsah

1 O službě zálohování 7

2 Softwarové požadavky 7

2.1 Podporované prohlížeče 7

2.2 Podporované operační systémy a prostředí 7

2.3 Podporované verze serveru Microsoft SQL Server 9

2.4 Podporované verze Microsoft Exchange Server 9

2.5 Podporované verze služby Microsoft SharePoint 9

2.6 Podporované virtualizační platformy 10

2.7 Kompatibilita se šifrovacím softwarem 13

3 Podporované systémy souborů 14

4 Aktivace účtu 15

5 Přístup ke službě zálohování 15

6 Instalace softwaru 16

6.1 Příprava 16

6.2 Nastavení proxy serveru 19

6.3 Linuxové balíky 21

6.4 Instalace agentů 23

6.5 Nasazení Agenta pro VMware (Virtual Appliance) z šablony OVF 25

6.5.1 Než začnete 25

6.5.2 Nasazení šablony OVF 26

6.5.3 Konfigurace virtuálního zařízení 26

6.5.4 Použití místně připojeného úložiště 27

6.6 Instalace agentů pomocí zásad skupiny 28

6.7 Aktualizace agentů 30

6.8 Odinstalování agentů 31

7 Zobrazení konzoly pro zálohování 32

8 Zálohování 33

8.1 Shrnutí plánu zálohování 34

8.2 Výběr dat pro zálohování 36

8.2.1 Výběr disků nebo svazků 36

8.2.2 Výběr souborů a složek 38

8.2.3 Výběr stavu systému 40

8.2.4 Výběr konfigurace ESXi 40

8.3 Výběr cíle 41

8.3.1 O službě Secure Zone 41

8.4 Plán 43

8.4.1 Plánování podle událostí 45

8.4.2 Podmínky spuštění 46

8.5 Pravidla zachování 52

8.6 Replikace ... 52
8.7 Šifrování ... 53
8.8 Spouštění zálohy ručně ... 55
8.9 Možnosti zálohování ... 55
8.9.1 Výstrahy ... 58
8.9.2 Slučování záloh ... 58
8.9.3 Formát zálohy ... 59
8.9.4 Ověření zálohy ... 60
8.9.5 Podmínky spuštění zálohování ... 61
8.9.6 Sledování změněných bloků (CBT) ... 61
8.9.7 Úroveň komprese ... 61
8.9.8 Zpracování chyb ... 62
8.9.9 Rychlá přírůstková/rozdílová záloha ... 63
8.9.10 Filtry souborů ... 63
8.9.11 Snímky záloh na úrovni souborů ... 64
8.9.12 Zkrácení protokolu ... 65
8.9.13 Zachycování snímků LVM ... 65
8.9.14 Přípojné body ... 65
8.9.15 Snímek více svazků ... 66
8.9.16 Výkon ... 66
8.9.17 Odesílání fyzických dat ... 67
8.9.18 Příkazy před-po ... 68
8.9.19 Příkazy před/po získání dat ... 69
8.9.20 Plánování ... 71
8.9.21 Zálohování sektor po sektoru ... 72
8.9.22 Rozdělování ... 72
8.9.23 Zpracování selhání úlohy ... 72
8.9.24 Služba Stínová kopie svazku (VSS) ... 72
8.9.25 Služba Stínová kopie svazku (VSS) pro virtuální počítače ... 73
8.9.26 Týdenní zálohování ... 74
8.9.27 Protokol událostí systému Windows ... 74
9 Obnova ... 74
9.1 Shrnutí metod obnovy ... 74
9.2 Tvorba spouštěcího média ... 75
9.3 Obnovení počítače ... 76
9.3.1 Fyzický počítač ... 76
9.3.2 Fyzický počítač na virtuální ... 77
9.3.3 Virtuální počítač ... 78
9.3.4 Obnovení disků pomocí spouštěcích médií ... 80
9.3.5 Použití technologie Universal Restore ... 81
9.4 Obnova souborů ... 83
9.4.1 Obnovení souborů pomocí webového rozhraní ... 83
9.4.2 Stahování souborů z cloudového úložiště ... 84
9.4.3 Podepsání souboru pomocí služby ASign ... 85
9.4.4 Obnova souborů pomocí spouštěcího média ... 86
9.4.5 Extrahování souborů z místních záloh ... 87
9.5 Obnova stavu systému ... 87
9.6 Obnova konfigurace ESXi ... 87
9.7 Možnosti obnovy ... 88
9.7.1 Ověření zálohy ... 89
9.7.2 Zpracování chyb ... 90

9.7.3 Datum a čas pro soubory ... 90
9.7.4 Vyloučení souborů ... 90
9.7.5 Zabezpečení na úrovni souborů ... 90
9.7.6 Flashback ... 91
9.7.7 Obnova úplné cesty ... 91
9.7.8 Přípojné body ... 91
9.7.9 Výkon ... 91
9.7.10 Příkazy před-po ... 91
9.7.11 Změna SID ... 93
9.7.12 Správa napájení virtuálního počítače ... 93
9.7.13 Protokol událostí systému Windows ... 93

10 Obnovení po havárii ... 95

10.1 Softwarové požadavky ... 96

10.2 Konfigurace připojení VPN ... 97

10.2.1 Požadavky na zařízení VPN ... 98
10.2.2 Připojení pomocí zařízení VPN ... 98
10.2.3 Operace se zařízením VPN ... 100
10.2.4 Připojení point-to-site (P2S) ... 100
10.2.5 Parametry připojení point-to-site (P2S) ... 101

10.3 Práce se serverem pro obnovení ... 102

10.3.1 Vytvoření serveru pro obnovení ... 102
10.3.2 Jak funguje převzetí služeb při selhání ... 104
10.3.3 Testování převzetí služeb při selhání ... 105
10.3.4 Provedení převzetí služeb při selhání ... 106
10.3.5 Provedení navrácení služeb po obnovení ... 107

10.4 Práce s primárním serverem ... 108

10.4.1 Vytvoření primárního serveru ... 108
10.4.2 Operace s primárním serverem ... 108

10.5 Zálohování cloudových serverů ... 109

10.6 Používání runbooků ... 109

10.6.1 Vytvoření runbooku ... 110
10.6.2 Operace s runbooky ... 111

11 Operace se zálohami ... 112

11.1 Karta Zálohy ... 112

11.2 Připojování svazků ze zálohy ... 113

11.3 Odstranění záloh ... 114

12 Operace s plány zálohování ... 115

13 Ochrana mobilních zařízení ... 115

14 Ochrana aplikací ... 120

14.1 Předpoklady ... 121

14.2 Zálohování databáze ... 122

14.2.1 Výběr databází SQL ... 122
14.2.2 Výběr dat serveru Exchange ... 122

14.3 Zálohování s podporou aplikací ... 123

14.3.1 Požadovaná uživatelská oprávnění ... 124

14.4 Obnovení databází SQL ... 124

14.4.1 Obnova systémových databází ... 126

14.4.2 Připojení databází serveru SQL ... 126
14.5 Obnova databází Exchange ... 127
14.5.1 Připojení databází aplikace Exchange Server ... 128
14.6 Obnovení poštovních schránek a položek schránek aplikace Exchange ... 128
14.6.1 Obnova schránek ... 129
14.6.2 Obnovení položek poštovní schránky ... 130
14.6.3 Požadovaná uživatelská oprávnění ... 131
15 Ochrana dat v Office 365 ... 132
15.1 Použít místně nainstalovaného agenta pro Office 365. ... 133
15.1.1 Přidání organizace Microsoft Office 365 ... 133
15.1.2 Ochrana poštovních schránek Exchange Online ... 134
15.2 Použít cloudového agenta pro Office 365. ... 136
15.2.1 Přidání organizace Microsoft Office 365 ... 136
15.2.2 Ochrana poštovních schránek Exchange Online ... 136
15.2.3 Ochrana souborů na OneDrivu ... 139
15.2.4 Ochrana webů SharePointu Online ... 142
15.2.5 Upgrade cloudového agenta ... 145
16 Ochrana dat v G Suite ... 146
16.1 Přidání organizace G Suite ... 146
16.2 Ochrana dat v Gmailu ... 147
16.2.1 Výběr poštovních schránek ... 148
16.2.2 Obnovení poštovních schránek a jejich položek ... 149
16.3 Ochrana souborů Disku Google ... 151
16.3.1 Výběr souborů Disku Google ... 152
16.3.2 Obnova Disku Google a souborů Disku Google ... 152
16.4 Ochrana souborů Týmových disků ... 154
16.4.1 Výběr souborů Týmových disků ... 155
16.4.2 Obnova Týmových disků a souborů Týmových disků ... 155
16.5 Notarizace ... 157
16.5.1 Ověřování autenticity souboru pomocí služby Notary ... 157
17 Active Protection ... 158
17.1 Možnosti ochrany ... 160
18 Ochrana webových stránek a hostingových serverů ... 161
18.1 Ochrana webových stránek ... 161
18.1.1 Zálohování webové stránky ... 161
18.1.2 Obnovení webové stránky ... 162
18.2 Ochrana webhostingových serverů ... 163
19 Speciální operace s virtuálními počítači ... 164
19.1 Spuštění virtuálního počítače ze zálohy (funkce okamžitého obnovení) ... 164
19.1.1 Spouštění počítače ... 164
19.1.2 Odstranění počítače ... 165
19.1.3 Dokončení počítače ... 166
19.2 Replikace virtuálních počítačů ... 166
19.2.1 Tvorba plánu replikace ... 167
19.2.2 Testování repliky ... 168
19.2.3 Převzetí služeb při selhání replikou ... 169
19.2.4 Možnosti replikace ... 170

19.2.5 Možnosti navrácení služeb po obnovení ... 170
19.2.6 Naplnění počáteční repliky ... 171
19.3 Správa prostředí pro virtualizaci ... 172
19.4 Migrace počítače ... 172
19.5 Agent pro VMware – zálohování nezávislé na LAN ... 173
19.6 Agent pro VMware – potřebná oprávnění ... 175
19.7 Virtuální počítače Windows Azure a Amazon EC2 ... 178
19.8 Omezení celkového počtu současně zálohovaných virtuálních počítačů ... 178
20 Správa uživatelských účtů a organizačních jednotek ... 179
20.1 Kvóty ... 179
20.1.1 Zálohování ... 179
20.1.2 Obnovení po havárii ... 181
20.2 Upozornění ... 181
20.3 Zprávy o využití ... 182
21 Odstraňování problémů ... 182
22 Slovníček ... 183

1 O službě zálohování

Tato služba umožňuje zálohování a obnovu fyzických a virtuálních počítačů, souborů a databází v rámci místního nebo cloudového úložiště.

Služba je dostupná přes webové rozhraní označované jako konzola pro zálohování.

2 Softwarové požadavky

2.1 Podporované prohlížeče

Webové rozhraní podporuje následující prohlížeče:

- Google Chrome 29 nebo novější,
- Mozilla Firefox 23 nebo novější,
- Opera 16 nebo novější,
- Windows Internet Explorer 10 nebo novější,
- Microsoft Edge 25 nebo novější,
- Safari 8 nebo novější v operačních systémech macOS a iOS.

V ostatních webových prohlížečích (včetně prohlížečů Safari v jiných operačních systémech) se uživatelské rozhraní nemusí správně zobrazovat nebo nemusí být některé funkce dostupné.

2.2 Podporované operační systémy a prostředí

Agent pro Windows

Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)

Windows Server 2003 SP1/2003 R2 a novější – verze Standard a Enterprise (x86, x64)

Windows Small Business Server 2003/2003 R2

Windows Vista – všechny verze

Windows Server 2008 – verze Standard, Enterprise, Datacenter a Web (x86, x64)

Windows Small Business Server 2008

Windows 7 – všechny verze

Windows Server 2008 R2 – verze Standard, Enterprise, Datacenter, Foundation a Web

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011 – všechny verze

Windows 8/8.1 – všechny verze (x86, x64) kromě verzí Windows RT

Windows Server 2012/2012 R2 – všechny verze

Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016

Windows 10 – verze Home, Pro, Education, Enterprise a IoT Enterprise

Windows Server 2016 – všechny možnosti instalace (s výjimkou Nano Serveru)

Windows Server 2019 – všechny možnosti instalace (s výjimkou Nano Serveru)

Agent pro SQL, Agent pro Exchange a Agent pro Active Directory

Všechny tyto agenty lze nainstalovat do počítače s libovolným z výše uvedených operačních systémů a s podporovanou verzí odpovídající aplikace.

Agent pro Office 365

Windows Server 2008 – verze Standard, Enterprise, Datacenter a Web (pouze x64)

Windows Small Business Server 2008

Windows Server 2008 R2 – verze Standard, Enterprise, Datacenter, Foundation a Web

Windows Small Business Server 2011 – všechny verze

Windows 8/8.1 – všechny verze (pouze x64) kromě verzí Windows RT

Windows Server 2012/2012 R2 – všechny verze

Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (pouze x64)

Windows 10 – verze Home, Pro, Education a Enterprise (pouze x64)

Windows Server 2016 – všechny možnosti instalace (pouze x64) s výjimkou Nano Serveru

Agent pro Linux

Linux s jádrem verze 2.6.9 až 4.19.8 a knihovnou glibc verze 2.3.4 nebo novější

Různé distribuce systému Linux x86 + x86_64 včetně:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29
- SUSE Linux Enterprise Server 10 a 11
- SUSE Linux Enterprise Server 12 – podporováno v systémech souborů kromě Btrfs
- Debian 4, 5, 6, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8
- CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6 – Unbreakable Enterprise Kernel i Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5
- ClearOS 5.x, 6.x, 7, 7.1, 7.4
- ALT Linux 7.0

Před instalací produktu v distribuci systému Linux, která nepoužívá RPM (jako je například Ubuntu), musíte nainstalovat RPM ručně: **`apt-get install rpm`**

Agent pro Mac

OS X Mavericks 10.9

OS X Yosemite 10.10

OS X El Capitan 10.11

macOS Sierra 10.12

macOS High Sierra 10.13

macOS Mojave 10.14

Agent pro VMware (Virtual Appliance)

Tento agent je dodáván jako virtuální zařízení pro spouštění na hostiteli ESXi.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7

Agent pro VMware (Windows)

Tento agent je dodáván jako aplikace pro Windows a s následujícími výjimkami je funkční v libovolném výše uvedeném operačním systému pro Agenta pro Windows:

- Nejsou podporovány 32bitové operační systémy.
- Nejsou podporovány systémy Windows XP, Windows Server 2003/2003 R2 a Windows Small Business Server 2003/2003 R2.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7

Agent pro Hyper-V

Windows Server 2008 (pouze x64) s technologií Hyper-V

Windows Server 2008 R2 s Hyper-V

Microsoft Hyper-V Server 2008/2008 R2

Windows Server 2012/2012 R2 s Hyper-V

Microsoft Hyper-V Server 2012/2012 R2

Windows 8, 8.1 (pouze x64) s technologií Hyper-V

Windows 10 – verze Pro, Education a Enterprise s Hyper-V

Windows Server 2016 s Hyper V – všechny možnosti instalace (s výjimkou Nano Serveru)

Microsoft Hyper-V Server 2016

Agent pro Virtuozzo

Virtuozzo 6.0.10, 6.0.11, 6.0.12

2.3 Podporované verze serveru Microsoft SQL Server

- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

2.4 Podporované verze Microsoft Exchange Server

- **Microsoft Exchange Server 2016** – všechny verze.
- **Microsoft Exchange Server 2013** – všechny verze, kumulativní aktualizace 1 (CU1) a novější.
- **Microsoft Exchange Server 2010** – všechny verze, všechny aktualizace Service Pack. Obnovení poštovních schránek a jejich položek je podporováno počínaje aktualizací Service Pack 1 (SP1).
- **Microsoft Exchange Server 2007** – všechny verze, všechny aktualizace Service Pack. Obnovení poštovních schránek a jejich položek není podporováno.

2.5 Podporované verze služby Microsoft SharePoint

Backup Service podporuje následující verze služby SharePoint:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1

- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

*Pro správné fungování aplikace SharePoint Explorer s těmito verzemi je nutné mít farmu SharePoint určenou k obnovování, ke které budou připojeny databáze.

Zálohy nebo databáze, ze kterých se mají extrahovat data, musí pocházet ze stejné verze serveru SharePoint jako je ta, kde je nainstalována aplikace SharePoint Explorer.

2.6 Podporované virtualizační platformy

Následující tabulka shrnuje podporu různých virtualizačních platforem.

Platforma	Zálohování na úrovni hypervizoru (zálohování bez agenta)	Zálohování zevnitř hostujícího operačního systému
VMware		
Verze VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 **Verze VMware vSphere:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (Bezplatné ESXi)**		+
VMware Server (Virtuální server VMware) VMware Workstation VMware ACE VMware Player		+
Microsoft		
Windows Server 2008 64bitová verze s Hyper-V Windows Server 2008 R2 s Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 s Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8 a 8.1 (x64) s technologií Hyper-V Windows 10 s Hyper-V Windows Server 2016 s Hyper V – všechny možnosti instalace (s výjimkou Nano Serveru) Microsoft Hyper-V Server 2016	+	+

Platforma	Zálohování na úrovni hypervizoru (zálohování bez agenta)	Zálohování zevnitř hostujícího operačního systému
Microsoft Virtual PC 2004 a 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5		Pouze plně virtualizovaní (neboli HVM) hosté
Red Hat a Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1		+
Virtuální počítače založené na jádře (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Pouze plně virtualizovaní (neboli HVM) hosté
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x až 20180425.x		+
Virtuozzo		
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	(Pouze virtuální počítače. Kontejnery nejsou podporovány.)
Amazon		
Instance Amazon EC2		+
Microsoft Azure		
Virtuální počítače Azure		+

* V těchto verzích je přenos HotAdd pro virtuální disky podporován v softwaru vSphere 5.0 a novějším. Ve verzi 4.1 může zálohování probíhat pomaleji.

** Zálohování na úrovni hypervizoru není pro vSphere Hypervisor podporováno, protože tento produkt omezuje přístup k rozhraní vzdáleného příkazového řádku (RCLI) na režim pouze ke čtení. Tento agent pracuje v průběhu zkušební doby vSphere Hypervisor bez zadání sériového klíče. Po zadání sériového klíče agent přestane pracovat.

Omezení

- **Počítače odolné vůči chybám**

Agent pro VMware zálohuje počítače odolné vůči chybám, pouze pokud byla odolnost vůči chybám povolena v softwaru VMware vSphere 6.0 a novějším. Pokud jste upgradovali ze starší verze vSphere, postačí zakázat a povolit odolnost proti chybám na jednotlivých počítačích. Jestliže používáte starší verzi vSphere, nainstalujte agenta v hostovaném operačním systému.

- **Nezávislé disky a disky RDM**

  Agent pro VMware nezálohuje nezávislé disky a disky RDM (Raw Device Mapping) v režimu fyzické kompatibility. Agent tyto disky přeskočí a přidá upozornění do protokolového souboru. Nechcete-li upozornění zobrazovat, vynechte nezávislé disky a disky RDM v režimu fyzické kompatibility z plánu zálohování. Pokud si tyto disky nebo data na těchto discích přejete zálohovat, nainstalujte agenta v hostovaném operačním systému.

- **Průchozí disky**

  Agent pro Hyper-V nezálohuje průchozí disky. Během zálohování agent tyto disky přeskočí a přidá upozornění do protokolového souboru. Nechcete-li upozornění zobrazovat, vynechte průchozí disky z plánu zálohování. Pokud si tyto disky nebo data na těchto discích přejete zálohovat, nainstalujte agenta v hostovaném operačním systému.

- **Připojení iSCSI v rámci hostovaného systému**

  Agent pro VMware a Agent pro Hyper-V nezálohují svazky LUN připojené pomocí spouštěče iSCSI, který běží v rámci hostovaného operačního systému. Protože hypervizory ESXi a Hyper-V nemají o těchto svazcích informace, nejsou tyto svazky součástí snímků na úrovni hypervizorů a jsou bez upozornění vynechány ze zálohování. Pokud si tyto svazky nebo data na těchto svazcích přejete zálohovat, nainstalujte agenta v hostovaném operačním systému.

- **Clustering hosta Hyper-V**

  Agent pro Hyper-V nepodporuje zálohování virtuálních počítačů Hyper-V, které jsou uzly clusteru Windows Server Failover Cluster. Snímek VSS na úrovni hostitele může dokonce dočasně odpojit disk externího kvora z clusteru. Pokud si tyto počítače přejete zálohovat, nainstalujte agenta do hostujícího operačního systému.

- **Počítače se systémem Linux s logickými svazky (LVM)**

  Agent pro VMware a Agent pro Hyper-V nepodporují následující operace v počítačích se systémem Linux s LVM:

  - Migrace P2V, migrace V2P a migrace V2V z Virtuozzo. Použití Agenta pro Linux k vytvoření zálohy a spouštěcího média pro obnovení.
  - Spuštění virtuálního počítače ze zálohy vytvořené Agentem pro Linux.

- **Šifrované virtuální počítače** (zavedeno ve verzi VMware vSphere 6.5)
  - Šifrované virtuální počítač jsou zálohovány v nešifrovaném stavu. Pokud je pro vás šifrování důležité, povolte při vytváření plánu zálohování (str. 53) šifrování záloh.
  - Obnovené virtuální počítače jsou vždy nešifrované. Po dokončení obnovení můžete šifrování ručně povolit.
  - Jestliže zálohujete šifrované virtuální počítače, doporučujeme zašifrovat také virtuální počítač, na kterém je spuštěn Agent pro VMware. V opačném případě mohou být operace se šifrovanými počítači pomalejší, než je očekáváno. Pro počítač s agentem použijte **zásady šifrování virtuálního počítače** ve webovém klientu vSphere.
  - Šifrované virtuální počítače budou zálohovány prostřednictvím sítě LAN, a to i v případě, že pro agenta nakonfigurujete transportní režim SAN. Agent se vrátí do transportního režimu NBD, protože VMware nepodporuje transportní režim SAN k zálohování šifrovaných virtuálních disků.
- **Secure Boot** (zavedeno ve verzi VMware vSphere 6.5)

Když je virtuální počítač obnovován jako nový virtuální počítač, je oddíl **Secure Boot** zakázán. Po dokončení obnovení můžete tuto možnost ručně povolit.

- **Zálohování konfigurace ESXi** není pro VMware vSphere 6.7 podporováno.

2.7 Kompatibilita se šifrovacím softwarem

Pro zálohování a obnovování dat šifrovaných softwarem *na úrovni souborů* neexistují žádná omezení.

Software pro *šifrování disků* šifruje data za běhu, proto data obsažená v záloze nejsou šifrována. Software pro šifrování disků často provádí změny v systémových oblastech: spouštěcí záznamy, tabulky oddílů nebo tabulky souborového systému. Tyto faktory ovlivňují zálohu a obnovu na úrovni disku, schopnost obnoveného systému spustit se a přístup k oddílu Secure Zone.

Zálohovat lze data šifrovaná pomocí následujících programů pro šifrování disků:

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption.

Chcete-li zajistit spolehlivou obnovu na úrovni disku, dodržujte obecná pravidla a doporučení pro konkrétní software.

Běžné pravidlo instalace

Důrazně doporučujeme nainstalovat šifrovací software před instalací agentů pro zálohování.

Způsob používání Secure Zone

Oddíl Secure Zone nesmí být šifrován na úrovni disku. Jediný způsob použití Secure Zone je následující:

1. Nainstalujte šifrovací software, poté nainstalujte agenta.
2. Vytvořte oddíl Secure Zone.
3. Při šifrování disku nebo svazků nezahrnujte oddíl Secure Zone.

Běžné pravidla zálohování

V operačním systému můžete provádět zálohování na úrovni disku.

Postupy obnovení pro konkrétní software

Microsoft BitLocker Drive Encryption

Jak provést obnovu systému, který byl zašifrován programem BitLocker:

1. Spusťte systém ze spouštěcího média.
2. Obnovte systém. Obnovená data nebudou šifrována.
3. Restartujte obnovený systém.
4. Spusťte BitLocker.

Pokud potřebujete obnovit pouze jeden diskový oddíl z disku s více diskovými oddíly, obnovte jej v operačním systému. Obnovení pomocí spouštěcího média může způsobit nezjistitelnost obnoveného diskového oddílu pro systém Windows.

McAfee Endpoint Encryption a PGP Whole Disk Encryption

Šifrovaný systémový diskový oddíl můžete obnovit pouze pomocí spouštěcích médií.

Pokud se obnovený systém nepodaří spustit, vytvořte znovu hlavní spouštěcí záznam podle článku znalostní databáze Microsoft: https://support.microsoft.com/kb/2622803.

3 Podporované systémy souborů

Zálohovací agent může zálohovat jakýkoli systém souborů, který je přístupný z operačního systému, v němž je agent nainstalován. Agent pro Windows například může zálohovat a obnovit systém souborů ext4, pokud je v systému Windows nainstalován odpovídající ovladač.

Následující tabulka obsahuje souhrnný přehled systémů souborů, které je možné zálohovat a obnovovat (spouštěcí médium podporuje pouze obnovení). Omezení se vztahují na agenty i spouštěcí médium.

<table>
<tr><th rowspan="2">Systém souborů</th><th colspan="3">Podporováno</th><th rowspan="2">Omezení</th></tr>
<tr><th>Agenti</th><th>Spouštěcí médium pro systémy Windows a Linux</th><th>Spouštěcí médium pro systém Mac</th></tr>
<tr><td>FAT16/32</td><td rowspan="3">Všichni agenti</td><td>+</td><td>+</td><td rowspan="4">Bez omezení</td></tr>
<tr><td>NTFS</td><td>+</td><td>+</td></tr>
<tr><td>ext2/ext3/ext4</td><td>+</td><td>-</td></tr>
<tr><td>HFS+</td><td rowspan="2">Agent pro Mac</td><td>-</td><td>+</td></tr>
<tr><td>APFS</td><td>-</td><td>+</td><td>▪ Podporováno od systému macOS High Sierra 10.13
▪ Pokud obnovu provádíte na jiný než původní počítač nebo na počítač bez operačního systému, měli byste znovu ručně vytvořit konfiguraci disků.</td></tr>
<tr><td>JFS</td><td rowspan="3">Agent pro Linux</td><td>+</td><td>-</td><td rowspan="2">Ze zálohy disku nelze vyloučit soubory</td></tr>
<tr><td>ReiserFS3</td><td>+</td><td>-</td></tr>
<tr><td>ReiserFS4</td><td>+</td><td>-</td><td rowspan="3">▪ Ze zálohy disku nelze vyloučit soubory
▪ Během obnovení nelze změnit velikost svazků.</td></tr>
<tr><td>ReFS</td><td rowspan="2">Všichni agenti</td><td>+</td><td>+</td></tr>
<tr><td>XFS</td><td>+</td><td>+</td></tr>
</table>

Systém souborů	Podporováno			Omezení
	Agenti	Spouštěcí médium pro systémy Windows a Linux	Spouštěcí médium pro systém Mac	
Linux swap	Agent pro Linux	+	-	Bez omezení
exFAT	Všichni agenti	+ Spouštěcí médium nelze použít k obnovení, pokud *je záloha uložena v systému* exFAT	+	▪ Jsou podporovány pouze zálohy disků/svazků. ▪ Ze zálohy nelze vyloučit soubory. ▪ Ze zálohy nelze obnovit jednotlivé soubory.

Software automaticky zapne režim sektor po sektoru při zálohování disků s nerozpoznanými nebo nepodporovanými systémy souborů. Zálohování sektor po sektoru je možné použít pro jakýkoli systém souborů, který:

- je založený na blocích,
- je rozložen pouze na jednom disku,
- používá standardní schéma rozdělení oddílů MBR/GPT.

Jestliže systém neodpovídá těmto požadavkům, zálohování se nezdaří.

4 Aktivace účtu

Jakmile správce vytvoří váš účet, na vaši e-mailovou adresu se odešle e-mail. E-mail obsahuje následující informace:

- **Odkaz aktivace účtu.** Klikněte na odkaz a nastavte heslo účtu. Zapamatujte si vaše přihlašovací jméno, který se zobrazuje na stránce aktivace účtu.
- **Odkaz na stránku pro přihlášení ke konzole zálohování.** Pomocí tohoto odkazu přistoupíte ke konzole v budoucnu. Přihlašovací jméno a heslo jsou stejné jako v předchozím kroku.

5 Přístup ke službě zálohování

Do služby zálohování se můžete přihlásit, pokud jste si aktivovali účet.

Jak se přihlásit ke službě zálohování

1. Přejděte na přihlašovací stránku služby zálohování. Adresa přihlašovací stránky je uvedena v aktivačním e-mailu.
2. Zadejte přihlašovací jméno a potom klikněte na tlačítko **Pokračovat**.
3. Zadejte heslo a potom klikněte na tlačítko **Přihlásit**.
4. Pokud máte ve službě zálohování roli správce, klikněte na položku **Zálohování a obnovení po havárii**.

Uživatelé, kteří nemají roli správce, se přihlašují přímo ke konzoli pro zálohování.

Jazyk webového rozhraní můžete změnit, když kliknete na ikonu účtu v pravém horním rohu.

Pokud služba **Zálohování a obnovení po havárii** není jedinou službou, ke které jste přihlášeni, můžete k přepínání služeb použít  ikonu v pravém horním rohu. Správci mohou tuto ikonu také použít, když chtějí přejít na portál pro správu.

6 Instalace softwaru

6.1 Příprava

Krok 1

Agenta volte podle toho, co se chystáte zálohovat. Rozhodnout se můžete podle informací shrnutých v následující tabulce.

Mějte na paměti, že Agent pro Windows se instaluje s Agentem pro Exchange, Agentem pro SQL, Agentem pro VMware, Agentem pro Hyper-V a Agentem pro Active Directory. Pokud například nainstalujete Agenta pro SQL, bude také možné zálohovat celý počítač, kde je agent nainstalován.

Co chcete zálohovat?	Jakého agenta nainstalovat?	Kam se má nainstalovat?
Fyzické počítače		
Fyzické počítače se systémem Windows	Agent pro Windows	Do počítače, který se bude zálohovat.
Fyzické počítače se systémem Linux	Agent pro Linux	
Fyzické počítače se systémem macOS	Agent pro Mac	
Aplikace		
Databáze SQL	Agent pro SQL	Do počítače, kde běží Microsoft SQL Server
Databáze Exchange	Agent pro Exchange	Do počítače, kde běží Microsoft Exchange Server s rolí poštovní schránky
Poštovní schránky Microsoft Office 365	Zálohovací agent pro Office 365	Do počítače se systémem Windows, který je připojen k internetu V závislosti na požadované funkčnosti můžete nebo nemusíte instalovat Agenta pro Office 365. Další informace najdete v tématu o ochraně dat v Office 365 (str. 132).
Soubory na Microsoft Office 365 OneDrivu a na webech služby SharePoint Online	—	K zálohování těchto dat můžete použít jenom agenta, který je nainstalovaný v cloudu. Další informace najdete v tématu o ochraně dat v Office 365 (str. 132).
Poštovní schránky Gmail služby G Suite, soubory disku Google a soubory Týmových disků	—	K zálohování těchto dat můžete použít jenom agenta, který je nainstalovaný v cloudu. Další informace najdete v tématu Ochrana služby G Suite (str. 146).

<table>
<tr><th>Co chcete zálohovat?</th><th>Jakého agenta nainstalovat?</th><th>Kam se má nainstalovat?</th></tr>
<tr><td>Počítače, na kterých běží doménové služby Active Directory</td><td>Agent pro Active Directory</td><td>Do řadiče domény</td></tr>
<tr><td colspan="3">Virtuální počítače</td></tr>
<tr><td rowspan="2">Virtuální počítače VMware ESXi</td><td>Agent pro VMware (Windows)</td><td>Do počítače se systémem Windows, který má síťový přístup k serveru vCenter a k úložišti virtuálních počítačů*</td></tr>
<tr><td>Agent pro VMware (Virtual Appliance)</td><td>Do hostitele ESXi</td></tr>
<tr><td>Virtuální počítače Hyper-V</td><td>Agent pro Hyper-V</td><td>Do hostitele Hyper-V</td></tr>
<tr><td>Virtuální počítače a kontejnery Virtuozzo</td><td>Agent pro Virtuozzo</td><td>Virtuální počítače a kontejnery Virtuozzo</td></tr>
<tr><td>Virtuální počítače hostované v systému Amazon EC2</td><td rowspan="7">Stejného jako u fyzických počítačů**</td><td rowspan="7">Do počítače, který se bude zálohovat.</td></tr>
<tr><td>Virtuální počítače hostované v systému Windows Azure</td></tr>
<tr><td>Virtuální počítače Citrix XenServer</td></tr>
<tr><td>Red Hat Virtualization (RHV/RHEV)</td></tr>
<tr><td>Virtuální počítače založené na jádře (KVM)</td></tr>
<tr><td>Virtuální počítače Oracle</td></tr>
<tr><td>Virtuální počítače Nutanix AHV</td></tr>
<tr><td colspan="3">Mobilní zařízení</td></tr>
<tr><td>Mobilní zařízení se systémem Android</td><td>Mobilní aplikace pro Android</td><td rowspan="2">Do mobilního zařízení, které se bude zálohovat.</td></tr>
<tr><td>Mobilní zařízení se systémem iOS</td><td>Mobilní aplikace pro iOS</td></tr>
</table>

Pokud ESXi používá úložiště připojené pomocí sítě SAN, nainstalujte agenta do počítače připojeného ke stejné síti SAN. Agent bude zálohovat virtuální počítače přímo z úložiště a ne pomocí hostitele ESXi a LAN. Podrobné informace naleznete v tématu Agent pro VMware - zálohování nezávislé na síti LAN (str. 173).

**Virtuální počítač se považuje za virtuální, pokud jej zálohuje externí agent. Pokud je agent nainstalován v hostovaném systému, budou operace zálohování a obnovy stejné jako u fyzického počítače. Když ale budete nastavovat limit počtu počítačů, bude tento počítač stále považován za virtuální.

Krok 2

Zkontrolujte systémové požadavky pro agenty.

Agent	Místo na disku obsazené agenty
Agent pro Windows	550 MB
Agent pro Linux	500 MB
Agent pro Mac	450 MB
Agent pro SQL	600 MB (50 MB + 550 MB Agent pro Windows)
Agent pro Exchange	750 MB (200 MB + 550 MB Agent pro Windows)
Zálohovací agent pro Office 365	550 MB
Agent pro Active Directory	600 MB (50 MB + 550 MB Agent pro Windows)
Agent pro VMware	700 MB (150 MB + 550 MB Agent pro Windows)
Agent pro Hyper-V	600 MB (50 MB + 550 MB Agent pro Windows)
Agent pro Virtuozzo	500 MB

Obvyklá spotřeba paměti je 300 MB nad požadavky operačního systému a spuštěných aplikací. Ve špičce může využití paměti dosáhnout 2 GB (podle množství a typu dat, která agenti zpracovávají).

Obnovení spouštěcího média nebo disku s restartem vyžaduje alespoň 1 GB paměti.

Krok 3

Stáhněte si instalační program. Odkazy ke stažení zobrazíte kliknutím na **Všechna zařízení** > **Přidat**.

Stránka **Přidat zařízení** obsahuje webové instalátory všech agentů, které lze nainstalovat do Windows. Webový instalátor je malý spustitelný soubor, který stáhne hlavní instalační program z internetu a uloží jej jako dočasný soubor. Tento soubor se okamžitě po instalaci smaže.

Pokud chcete instalační programy ukládat lokálně, stáhněte si balíček obsahující všechny agenty pro instalaci ve Windows pomocí odkazu na konci stránky **Přidat zařízení**. Dostupné jsou 32bitové i 64bitové balíčky. Tyto balíčky umožňují přizpůsobení seznamu instalovaných komponent. Je pomocí nich možné také provést bezobslužnou instalaci, například prostřednictvím zásad skupiny. Tento pokročilý scénář je popsán v části Nasazení agentů pomocí zásad skupiny.

Chcete-li stáhnout instalační program Agenta pro Office 365, klikněte na ikonu účtu v pravém horním rohu stránky a potom klikněte na **Stažené soubory** > **Agent pro Office 365**.

Instalace v systémech Linux a macOS se provádí pomocí běžných instalačních programů.

Všechny instalační programy vyžadují připojení k internetu pro registraci počítače ve službě zálohování. Pokud není připojení k internetu k dispozici, instalace se nezdaří.

Krok 4

Před instalací zkontrolujte, že vaše firewally a ostatní komponenty zabezpečení sítě (například proxy server) umožňují příchozí i odchozí spojení přes následující porty TCP:

- **443** a **8443**: Tyto porty se používají pro přístup ke konzoly zálohování, pro registraci agentů, stahování certifikátů, autorizaci uživatelů a stahování souborů z cloudového úložiště.
- **7770...7800**:
- **44445**: Agenti používají tento port pro přenos dat při zálohování a obnově.

Pokud vaše síť používá proxy server, přečtěte si část Nastavení proxy serveru (str. 19), ve které zjistíte, zda je nutné tato nastavení konfigurovat v každém počítači, kde je spuštěn agent pro zálohování.

Ke správě agenta v cloudu potřebujete připojení k internetu o rychlosti minimálně 1 Mbit/s (nezaměňovat s přenosovou rychlostí, která je přijatelná pro zálohování do cloudu). Myslete na to hlavně, pokud používáte k připojení technologii s malou šířkou pásma, jako je ADSL.

6.2 Nastavení proxy serveru

Agenti pro zálohování mohou přenést data přes HTTP/HTTPS proxy server. Server musí komunikovat přes tunel HTTP bez skenování provozu HTTP nebo interference s tímto provozem. Proxy typu MITM (man-in-the-middle) nejsou podporované.

Vzhledem k tomu, že agent se během instalace registruje v cloudu, musí být nastavení proxy serveru dostupné před instalací nebo během ní.

Ve Windows

Pokud je proxy server nakonfigurován v systému Windows (**Ovládací panely** > **Možnosti Internetu** > **Připojení**), instalační program přečte nastavení proxy serveru z registru a automaticky je použije. Nastavení proxy serveru můžete provést také před instalací nebo během ní pomocí níže popsaného postupu. Pokud byste chtěli nastavení proxy serveru změnit po instalaci, použijte stejný postup.

Nastavení proxy v systému Windows

1. Vytvořte nový textový dokument a otevřete jej v textovém editoru, například Poznámkový blok.
2. Zkopírujte a vložte do souboru následující řádky:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. Výraz `proxy.company.com` nahraďte názvem hostitele nebo IP adresou vašeho proxy serveru a výraz `000001bb` nahraďte hexadecimální hodnotou čísla portu. Například `000001bb` je port 443.
4. Pokud proxy server vyžaduje ověřování, nahraďte hodnoty `proxy_login` a `proxy_password` přihlašovacími údaji proxy serveru. Jinak tyto řádky ze souboru odstraňte.
5. Uložte soubor pod názvem **proxy.reg**.
6. Spusťte soubor jako správce.
7. Potvrďte, že chcete upravit registr systému Windows.
8. Pokud ještě není nainstalován agent zálohování, je možné jej nainstalovat teď. Jinak proveďte následující úkony k restartu agenta:
   a. V nabídce **Start** klikněte na příkaz **Spustit** a zadejte **cmd**.
   b. Klikněte na tlačítko **OK**.
   c. Spusťte následující příkazy:

```
net stop mms
net start mms
```

V systému Linux

Spusťte instalační soubor s parametry **`--http-proxy-host`**=ADDRESS **`--http-proxy-port`**=PORT **`--http-proxy-login`**=LOGIN **`--http-proxy-password`**=PASSWORD. Pokud byste chtěli nastavení proxy serveru změnit po instalaci, použijte postup popsaný níže.

Nastavení proxy v systému Linux

1. Otevřete soubor **/etc/Acronis/Global.config** v textovém editoru.
2. Proveďte jeden z následujících úkonů:

- Pokud bylo nastavení serveru proxy zadáno při instalaci agenta, najděte následující část:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- V opačném případě zkopírujte výše uvedené řádky a vložte je do souboru mezi značky **<registry name="Global">...</registry>**.

3. Výraz v části ADRESA nahraďte novým názvem hostitele nebo IP adresou vašeho proxy serveru a výraz PORT nahraďte desítkovou hodnotou čísla portu.
4. Pokud proxy server vyžaduje ověřování, nahraďte LOGIN a PASSWORD přihlašovacími údaji serveru proxy. Jinak tyto řádky ze souboru odstraňte.
5. Uložte soubor.
6. Restartujte agenta provedením následujícího příkazu v libovolném adresáři:

```
sudo service acronis_mms restart
```

V systému macOS

Proxy server můžete nastavit při instalaci nebo předem níže uvedeným postupem. Pokud byste chtěli nastavení proxy serveru změnit po instalaci, použijte stejný postup.

Nastavení proxy v systému macOS

1. Vytvořte soubor **/Library/Application Support/Acronis/Registry/Global.config** a otevřete jej v textovém editoru, například Text Edit.
2. Zkopírujte a vložte do souboru následující řádky:

```
<?xml version="1.0" ?>
<registry name="Global">
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
        <value name="Host" type="TString">"proxy.company.com"</value>
        <value name="Port" type="Tdword">"443"</value>
        <value name="Login" type="TString">"proxy_login"</value>
        <value name="Password" type="TString">"proxy_password"</value>
    </key>
</registry>
```

3. Výraz proxy.company.com nahraďte názvem hostitele nebo adresou IP vašeho proxy serveru a hodnotu 443 nahraďte desítkovou hodnotou čísla portu.
4. Pokud proxy server vyžaduje ověřování, nahraďte hodnoty proxy_login a proxy_password přihlašovacími údaji proxy serveru. Jinak tyto řádky ze souboru odstraňte.
5. Uložte soubor.
6. Pokud ještě není nainstalován agent zálohování, je možné jej nainstalovat teď. Jinak proveďte následující úkony k restartu agenta:
   a. Přejděte do umístění **Aplikace** > **Nástroje** > **Terminál**.
   b. Spusťte následující příkazy:

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

6.3 Linuxové balíky

Chcete-li přidat potřebné moduly do linuxového jádra, potřebuje instalační program následující balíčky systému Linux:

- Balíček se soubory hlaviček jádra nebo zdrojovými soubory jádra Verze balíčku musí odpovídat verzi jádra.
- Kompilační systém GNU Compiler Collection (GCC). Verze GCC musí být ta, ve které bylo jádro zkompilováno.
- Nástroj pro tvorbu.
- Překladač jazyka Perl
- Knihovny **`libelf-dev`**, **`libelf-devel`** nebo **`elfutils-libelf-devel`**, které od verze 4.15 slouží k vytváření jader a jsou nakonfigurované pomocí CONFIG_UNWINDER_ORC=y. V některých distribucích, jako je Fedora 28, je potřeba je nainstalovat odděleně od hlaviček jádra.

Názvy těchto balíčků se budou lišit podle distribuce systému Linux.

V systémech Red Hat Enterprise Linux, CentOS a Fedora budou balíčky v normálním případě nainstalovány instalačním programem. V jiných distribucích je nutné balíčky nainstalovat, pokud nainstalovány nejsou nebo pokud nemají vyžadované verze.

Jsou vyžadované balíčky již nainstalovány?

Chcete-li zkontrolovat, zda jsou již balíčky nainstalovány, postupujte následovně:

1. Spuštěním následujícího příkazu zjistěte verzi jádra a požadovanou verzi GCC:

   ```
   cat /proc/version
   ```

   Příkaz vrátí řádky podobné těmto: **`Linux version 2.6.35.6`** a **`gcc version 4.5.1`**.
2. Spuštěním následujícího příkazu zkontrolujete, zda je nainstalován nástroj pro tvorbu a kompilátor GCC:

   ```
   make -v
   gcc -v
   ```

   U **gcc** zkontrolujte, zda je verze vrácená příkazem stejná jako verze **`gcc version`** v kroku 1.
   U **make** stačí zkontrolovat, že se příkaz spustil.
3. Zkontrolujte, zda je nainstalována správná verze balíčků pro tvorbu modulů jádra:
   - V systémech Red Hat Enterprise Linux, CentOS a Fedora spusťte následující příkaz:

     ```
     yum list installed | grep kernel-devel
     ```
   - V systému Ubuntu spusťte následující příkazy:

     ```
     dpkg --get-selections | grep linux-headers
     dpkg --get-selections | grep linux-image
     ```

   V každém případě zkontrolujte, zda jsou verze balíčků stejné jako ve verzi **`Linux version`** v kroku 1.
4. Spuštěním následujícího příkazu zkontrolujete, zda je nainstalován překladač jazyka Perl:

   ```
   perl --version
   ```

   Zobrazí-li se informace o verzi jazyka Perl, překladač je nainstalován.
5. V systémech Red Hat Enterprise Linux, CentOS a Fedora spusťte následující příkaz, kterým zkontrolujete, jestli je **`elfutils-libelf-devel`** nainstalovaný:

   ```
   yum list installed | grep elfutils-libelf-devel
   ```

   Pokud se zobrazí informace o verzi knihovny, znamená to, že je nainstalovaná.

Instalace balíčků z úložiště

Následující tabulka uvádí způsoby instalace vyžadovaných balíčků v různých distribucích systému Linux.

Distribuce systému Linux	Názvy balíčků	Postup instalace
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Instalační program stáhne a nainstaluje balíčky automaticky v rámci předplatného Red Hat.
	perl	Spusťte následující příkaz: `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Instalační program stáhne a nainstaluje balíčky automaticky.
	perl	Spusťte následující příkaz: `yum install perl`
Ubuntu Debian	**linux-headers** **linux-image** **gcc** **make** **perl**	Spusťte následující příkazy: `sudo apt-get update` `sudo apt-get install linux-headers-`uname -r`` `sudo apt-get install linux-image-`uname -r`` `sudo apt-get install gcc-<package version>` `sudo apt-get install make` `sudo apt-get install perl`

SUSE Linux
OpenSUSE
	kernel-source
	gcc
	make
	perl
		`sudo zypper install kernel-source`
		`sudo zypper install gcc`
		`sudo zypper install make`
		`sudo zypper install perl`

Balíčky budou staženy z úložiště distribuce a nainstalovány.

U ostatních distribucí systému Linux naleznete způsoby instalace těchto balíčků a jejich přesné názvy v jejich příslušných dokumentacích.

Ruční instalace balíčků

Balíčky může být nutné nainstalovat **ručně** v těchto případech:

- Počítač nemá aktivní předplatné Red Hat nebo připojení k internetu.
- Instalační program nemůže najít verzi **kernel-devel** nebo **gcc** odpovídající verzi jádra. Pokud je dostupný **kernel-devel** novější než vaše jádro, je nutné jádro aktualizovat nebo nainstalovat odpovídající verzi **kernel-devel** ručně.
- Požadované balíčky se nachází v místní síti a nechcete ztrácet čas automatickým vyhledáváním a stahováním.

Získejte balíčky z místní sítě nebo důvěryhodné webové stránky třetí strany a nainstalujte je následujícím způsobem:

- V systémech Red Hat Enterprise Linux, CentOS nebo Fedora spusťte následující příkaz jako uživatel root:

```
rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

- V systému Ubuntu spusťte následující příkaz:

```
sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

Příklad: Ruční instalace balíčků v systému Fedora 14

Pomocí tohoto postupu nainstalujete vyžadované balíčky v systému Fedora 14 na 32bitovém počítači:

1. Spuštěním následujícího příkazu zjistěte verzi jádra a požadovanou verzi GCC:

   ```
   cat /proc/version
   ```

   Výstup tohoto příkazu zahrnuje následující:

   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

2. Získejte balíčky **kernel-devel** a **gcc**, které odpovídají této verzi jádra:

   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```

3. Získejte balíček **make** pro systém Fedora 14:

   ```
   make-3.82-3.fc14.i686
   ```

4. Nainstalujte balíčky spuštěním následujících příkazů jako uživatel root:

   ```
   rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
   rpm -ivh gcc-4.5.1.fc14.i686.rpm
   rpm -ivh make-3.82-3.fc14.i686
   ```

   Všechny tyto balíčky lze zadat jediným příkazem **rpm**. Při instalaci těchto balíčků může být nutné nainstalovat další balíčky kvůli vyřešení závislostí.

6.4 Instalace agentů

Ve Windows

1. Zkontrolujte, že je počítač připojen k internetu.
2. Přihlaste se jako správce a spusťte instalační program.
3. [Volitelné] Klikněte na možnost **Přizpůsobit nastavení instalace** a proveďte příslušné změny, pokud chcete:
   - Ověřit nebo změnit název hostitele nebo IP adresu, port a přihlašovací údaje proxy serveru. Pokud je proxy server povolen ve Windows, automaticky se detekuje a použije.
   - Změnit instalační cestu.
   - Změnit účet pro službu agenta.
4. Klikněte na **Instalovat**.
5. [Pouze při instalaci Agenta pro VMware] Zadejte adresu a pověření k přístupu pro server vCenter nebo samostatného hostitele ESXi, jehož virtuální počítače bude agent zálohovat, a potom klikněte na tlačítko **Hotovo**. Doporučujeme používat účet, který má přiřazenou roli **Správce**. V opačném případě použijte účet, který má potřebná oprávnění (str. 175) na vCenter Serveru nebo v ESXi.
6. [Pouze při instalaci na řadiči domény] Zadejte uživatelský účet, ve kterém bude služba agenta spuštěna, a potom klikněte na tlačítko **Hotovo**. Z bezpečnostních důvodů instalační program automaticky nevytváří nové účty na řadiči domény.
7. Počkejte, až se zobrazí registrační obrazovka.
8. Proveďte jeden z následujících úkonů:

- Klikněte na **Zaregistrovat počítač**. V otevřeném okně prohlížeče se přihlaste do konzoly pro zálohování, zkontrolujte registrační údaje a potom klikněte na možnost **Potvrdit registraci**.
- Klikněte na možnost **Zobrazit informace o registraci**. Instalační program zobrazí registrační odkaz a registrační kód. Můžete je zkopírovat a provést registrační kroky na jiném počítači. V takovém případě budete muset zadat registrační kód do registračního formuláře. Registrační kód je platný jednu hodinu.

Registrační formulář můžete také zobrazit tak, že kliknete na možnost **Všechna zařízení** > **Přidat**, přejdete dolů na možnost **Registrace pomocí kódu** a poté kliknete na možnost **Registrovat**.

Tip *Neukončujte instalační program, dokud nepotvrdíte registraci. Pokud chcete zopakovat registraci, znovu spusťte instalační program a pak klikněte na* ***Zaregistrovat počítač****.*

Počítač poté bude přiřazen k účtu, který byl použit pro přihlášení ke konzole pro zálohování.

V systému Linux

1. Zkontrolujte, že je počítač připojen k internetu.
2. Jako uživatel root spusťte instalační soubor.

   Pokud je při spuštění souboru v síti zapnutý proxy server, zadejte název hostitele / IP adresu a port serveru v následujícím formátu: `--http-proxy-host=`ADDRESS `--http-proxy-port=`PORT `--http-proxy-login=`LOGIN `--http-proxy-password=`PASSWORD.
3. Zaškrtněte políčka pro agenty, které chcete nainstalovat. Dostupní jsou následující agenti:
   - **Agent pro Linux**
   - **Agent pro Virtuozzo**

   Agenta pro Virtuozzo nelze instalovat bez Agenta pro Linux.
4. Počkejte, až se zobrazí registrační obrazovka.
5. Proveďte jeden z následujících úkonů:
   - Klikněte na **Zaregistrovat počítač**. V otevřeném okně prohlížeče se přihlaste do konzoly pro zálohování, zkontrolujte registrační údaje a potom klikněte na možnost **Potvrdit registraci**.
   - Klikněte na možnost **Zobrazit informace o registraci**. Instalační program zobrazí registrační odkaz a registrační kód. Můžete je zkopírovat a provést registrační kroky na jiném počítači. V takovém případě budete muset zadat registrační kód do registračního formuláře. Registrační kód je platný jednu hodinu.

   Registrační formulář můžete také zobrazit tak, že kliknete na možnost **Všechna zařízení** > **Přidat**, přejdete dolů na možnost **Registrace pomocí kódu** a poté kliknete na možnost **Registrovat**.

Tip *Neukončujte instalační program, dokud nepotvrdíte registraci. Chcete-li znovu zahájit registraci, budete muset znovu spustit instalační program a opakovat proces instalace.*

Počítač poté bude přiřazen k účtu, který byl použit pro přihlášení ke konzole pro zálohování.

Informace o řešení problémů jsou uvedeny v souboru:
/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL

V systému macOS

1. Zkontrolujte, že je počítač připojen k internetu.
2. Klikněte dvakrát na instalační soubor (.dmg).
3. Počkejte, až operační systém připojí obraz instalačního disku.
4. Klikněte dvakrát na tlačítko **Instalovat**.

5. Pokud je v síti zapnutý proxy server, klikněte na řádku nabídek na **Agent pro zálohování**, klikněte na **Nastavení proxy serveru** a zadejte název hostitele / IP adresu, port a přihlašovací údaje proxy serveru.
6. Pokud se zobrazí výzva, zadejte pověření správce.
7. Klikněte na možnost **Pokračovat**.
8. Počkejte, až se zobrazí registrační obrazovka.
9. Proveďte jeden z následujících úkonů:
   - Klikněte na **Zaregistrovat počítač**. V otevřeném okně prohlížeče se přihlaste do konzoly pro zálohování, zkontrolujte registrační údaje a potom klikněte na možnost **Potvrdit registraci**.
   - Klikněte na možnost **Zobrazit informace o registraci**. Instalační program zobrazí registrační odkaz a registrační kód. Můžete je zkopírovat a provést registrační kroky na jiném počítači. V takovém případě budete muset zadat registrační kód do registračního formuláře. Registrační kód je platný jednu hodinu.

   Registrační formulář můžete také zobrazit tak, že kliknete na možnost **Všechna zařízení** > **Přidat**, přejdete dolů na možnost **Registrace pomocí kódu** a poté kliknete na možnost **Registrovat**.

   Tip *Neukončujte instalační program, dokud nepotvrdíte registraci. Chcete-li znovu zahájit registraci, budete muset znovu spustit instalační program a opakovat proces instalace.*

Počítač poté bude přiřazen k účtu, který byl použit pro přihlášení ke konzole pro zálohování.

6.5 Nasazení Agenta pro VMware (Virtual Appliance) z šablony OVF

6.5.1 Než začnete

Systémové požadavky agenta

Ve výchozím nastavení má virtuální zařízení přiřazeny 4 GB paměti RAM a 2 procesory vCPU, což je optimální a dostatečný počet pro většinu operací. Pokud předpokládáte, že šířka pásma při zatížení zálohováním překročí 100 MB za sekundu (například u 10gigabitových sítí), a chcete při zálohování zlepšit výkon, doporučujeme použít 8 GB paměti RAM a 4 procesory vCPU.

Vlastní virtuální disky zařízení nezabírají více než 6 GB. Tlustý nebo tenký formát disku není důležitý, protože neovlivňuje výkon zařízení.

Kolik agentů potřebuji?

Jedno virtuální zařízení sice dokáže chránit celé prostředí vSphere, ale osvědčený postup je nasadit na každý cluster vSphere (nebo na hostitele, neexistují-li clustery) jedno virtuální zařízení. Zálohování tak bude rychlejší, protože zařízení může k připojení zálohovaných disků použít přenos HotAdd, kdy zatížení při zálohování bude směrované z jednoho místního disku na druhý.

Normálně můžete současně používat virtuální zařízení i agenta pro VMware (Windows), pokud se připojují ke stejnému serveru vCenter Server *nebo* jsou připojeni k různým hostitelům ESXi. Nepoužívejte způsob, kdy je jeden agent připojený přímo k ESXi a druhý k serveru vCenter Server, který spravuje ESXi.

Pokud máte více agentů, nedoporučujeme používat místně připojené úložiště (tzn. ukládat zálohy na virtuální disky přidané do virtuálního zařízení). Další informace najdete v článku Použití místně připojeného úložiště (str. 27).

Vypnutí automatického nástroje DRS u agenta

Pokud je virtuální zařízení nasazeno v clusteru vSphere, nezapomeňte mu vypnout automatickou komponentu vMotion. V nastavení nástroje DRS clusteru povolte individuální úrovně automatizace virtuálního počítače a potom nastavte **úroveň automatizace** virtuálního zařízení na **Vypnuto**.

6.5.2 Nasazení šablony OVF

1. Klikněte na **Všechna zařízení** > **Přidat** > **VMware ESXi** > **Virtuální zařízení (OVF)**.

   Do vašeho počítače se stáhne archiv .zip.
2. Rozbalte archiv .zip. Složka obsahuje jeden soubor OVF a dva soubory VMDK.
3. Zajistěte, aby byl k těmto souborům přístup z počítače s klientem vSphere.
4. Spusťte klienta vSphere a přihlaste se na server vCenter.
5. Nasaďte šablonu OVF.
   - Při konfiguraci úložiště vyberte sdílené datové úložiště, pokud existuje. Tlustý nebo tenký formát disku není důležitý, protože neovlivňuje výkon zařízení.
   - Při konfiguraci síťových připojení nezapomeňte vybrat síť, která umožňuje internetové připojení, aby se agent mohl řádně zaregistrovat v cloudu.

6.5.3 Konfigurace virtuálního zařízení

1. **Spuštění virtuálního zařízení**

   V klientovi vSphere zobrazte **Inventář**, klikněte pravým tlačítkem na název virtuálního zařízení a poté vyberte možnost **Napájení** > **Zapnout**. Vyberte kartu **Console**.
2. **Proxy server**

   Pokud máte v síti zapnutý proxy server:

   a. Pokud chcete spustit prostředí příkazového řádku, stiskněte v uživatelském rozhraní virtuálního zařízení CTRL+ALT+F2.

   b. Otevřete soubor **/etc/Acronis/Global.config** v textovém editoru.

   c. Najděte následující oddíl:

   ```
   <key name="HttpProxy">
       <value name="Enabled" type="Tdword">"0"</value>
       <value name="Host" type="TString">"ADDRESS"</value>
       <value name="Port" type="Tdword">"PORT"</value>
       <value name="Login" type="TString">"LOGIN"</value>
       <value name="Password" type="TString">"PASSWORD"</value>
   </key>
   ```

   d. Nahraďte **0** hodnotou **1**.

   e. Výraz v části ADRESA nahraďte novým názvem hostitele nebo IP adresou vašeho proxy serveru a výraz PORT nahraďte desítkovou hodnotou čísla portu.

   f. Pokud proxy server vyžaduje ověřování, nahraďte LOGIN a PASSWORD přihlašovacími údaji serveru proxy. Jinak tyto řádky ze souboru odstraňte.

   g. Uložte soubor.

   h. Spusťte příkaz **reboot**.

   Jinak tento krok přeskočte.
3. **Nastavení sítě**

Síťové připojení agenta se konfiguruje automaticky pomocí protokolu DHCP (Dynamic Host Configuration Protocol). Chcete-li výchozí konfiguraci změnit, klikněte pod položkou **Možnosti agenta** v poli **eth0** na možnost **Změnit** a zadejte požadované síťové nastavení.

4. **vCenter/ESX(i)**

   Pod položkou **Možnosti agenta** v serveru **vCenter/ESX(i)** klikněte na **Změnit** a zadejte název nebo IP adresu serveru vCenter. Agent bude moci zálohovat a obnovovat virtuální počítače spravované serverem vCenter.

   Pokud nepoužijete server vCenter, zadejte název nebo IP adresu hostitele ESXi, jehož virtuální počítače chcete zálohovat a obnovovat. Většinou zálohování funguje rychleji, pokud agent zálohuje virtuální počítače hostované na svém vlastním hostiteli.

   Zadejte pověření, která budou agenti používat pro připojení k serveru vCenter nebo hostiteli ESXi. Doporučujeme používat účet, který má přiřazenou roli **Správce**. V opačném případě použijte účet, který má potřebná oprávnění (str. 175) na vCenter Serveru nebo v ESXi.

   Můžete kliknout na **Zkontrolovat spojení**, abyste zjistili, zda jsou pověření k přístupu správná.

5. **Server pro správu**

   a. V části **Možnosti agenta** u položky **Server pro správu** klikněte na **Změnit**.

   b. V poli **Název/IP serveru** vyberte **Cloud**. Software zobrazí adresu zálohovací služby. Tuto adresu neměňte, pokud jste nedostali jiný pokyn.

   c. Do polí **Uživatelské jméno** a **Heslo** zadejte uživatelské jméno a heslo zálohovací služby. Pod tímto účtem se zaregistruje agent i jím spravované virtuální počítače.

6. **Časové pásmo**

   Pod položkou **Virtuální počítač**, v části **Časové pásmo**, klikněte na **Změnit**. Vyberte časové pásmo vašeho umístění, aby se naplánované operace spouštěly ve správný čas.

7. **[Volitelné] Místní úložiště**

   K virtuálnímu zařízení můžete připojit další disk, aby Agent pro VMware mohl zálohovat do tohoto místně připojeného umístění.

   Úpravou nastavení virtuálního počítače přidejte disky a klikněte na **Aktualizovat**. Zpřístupní se odkaz **Vytvořit úložiště**. Klikněte na tento odkaz, vyberte disk a zadejte jeho jmenovku.

6.5.4 Použití místně připojeného úložiště

K Agentovi pro VMware (Virtual Appliance) můžete připojit další disk tak, aby agent mohl zálohovat do tohoto místně připojeného umístění. Tento přístup eliminuje síťový provoz mezi agentem a umístěním zálohy.

Virtuální zařízení, které běží na stejném hostiteli nebo clusteru se zálohovanými virtuálními počítači, má přímý přístup k datovým úložištím, kde jsou tyto počítače umístěny. To znamená, že zařízení může připojit zálohované disky pomocí přenosu HotAdd, a proto je zatížení sítě při zálohování směrováno z jednoho lokálního disku na druhý. Jestliže je datové úložiště připojeno jako **Disk/LUN**, nikoli jako **NFS**, bude zálohování zcela nezávislé na síti LAN. V případě datového úložiště NFS bude mezi datovým úložištěm a hostitelem probíhat síťový provoz.

Použití místně připojeného úložiště předpokládá, že agent vždy zálohuje stejné počítače. Jinak, pokud budou počítače znovu distribuovány mezi agenty serverem pro správu, zálohy jednoho počítače mohou být rozprostřeny na více úložišť. Pokud máte více agentů, nedoporučujeme používat místně připojené úložiště.

Úložiště můžete přidat již fungujícímu agentovi nebo při nasazení agenta ze šablony OVF (str. 26).

Jak připojit úložiště k již fungujícímu agentu

1. V inventáři VMware vSphere klikněte pravým tlačítkem na Agenta pro VMware (Virtual Appliance).
2. Úpravou nastavení virtuálního počítače přidejte disk. Velikost disku musí být alespoň 10 GB.

   Upozornění *Při přidávání již existujícího disku postupujte opatrně. Jakmile je úložiště vytvořeno, všechna data, která disk obsahoval, budou ztracena.*
3. Přejděte do konzoly virtuální zařízení. Odkaz **Vytvořit úložiště** je dostupný v dolní části stránky. Pokud tomu tak není, klikněte na **Aktualizovat**.
4. Klikněte na odkaz **Vytvořit úložiště**, vyberte disk a zadejte jeho jmenovku. Délka jmenovky je kvůli omezení systému souborů omezena na 16 znaků.

Jak vybrat místně připojené úložiště jako cíl zálohování

Při vytváření plánu zálohování (str. 33) v dialogovém okně **Kam se má zálohovat** vyberte položku **Místní složky** a pak zadejte písmeno odpovídající místně připojenému úložišti, například **D:**.

6.6 Instalace agentů pomocí zásad skupiny

Agenta pro Windows můžete centrálně instalovat (nasadit) do počítačů, které jsou členy domény Active Directory, pomocí zásad skupiny.

V této části se dozvíte, jak nastavit objekt zásad skupiny pro instalaci agentů do počítačů v celé doméně nebo v její organizační jednotce.

Při každém přihlášení počítače do domény výsledný objekt zásad skupiny zajistí instalaci a registraci agenta.

Předpoklady

Než budete pokračovat s instalací agentů, ujistěte se, že:

- Máte doménu Active Directory s doménovým řadičem na němž běží Microsoft Windows Server 2003 nebo vyšší.
- Jste v doméně členem skupiny **Domain Admins**.
- Stáhli jste si instalační program **Všichni agenti pro instalaci v systému Windows**. Odkaz ke stažení je dostupný na stránce **Přidat zařízení** v konzole zálohování.

Krok 1: Vygenerování registračního tokenu

Registrační token předává vaši identitu instalačnímu programu bez uložení přihlašovacího jména a hesla pro konzolu pro zálohování. Díky tomu můžete zaregistrovat libovolný počet počítačů pod svým účtem. Z důvodu zabezpečení má token omezenou dobu platnosti.

Jak vygenerovat registrační token

1. Přihlaste se ke konzole pro zálohování zadáním přihlašovacích údajů k účtu, ke kterému mají být počítače přiřazeny.
2. Klikněte na **Všechna zařízení** > **Přidat**.
3. Posuňte se dolů na možnost **Registrační token** a potom klikněte na možnost **Generovat**.
4. Zadejte dobu platnosti tokenu a poté klikněte na možnost **Generovat token**.
5. Zkopírujte token nebo si jej zapište.

   Kliknutím na možnost **Spravovat aktivní tokeny** můžete zobrazit a spravovat již vygenerované tokeny.

Krok 2: Vytvoření souboru transformace .mst a extrahování instalačního balíčku

1. Přihlaste se jako správce na libovolném počítači v doméně.
2. Vytvořte sdílenou složku, která bude obsahovat instalační balíčky. Zkontrolujte, zda mají uživatelé domény ke sdílené složce přístup – například ponechte výchozí nastavení sdílení pro skupinu **Everyone** (Všichni).
3. Spusťte instalační program.
4. Klikněte na možnost **Vytvořit soubory MST a MSI pro bezobslužnou instalaci**.
5. Vedle možnosti **Registrační token** klikněte na **Zadat** a potom zadejte token, který jste vygenerovali.
6. Zkontrolujte nebo upravte nastavení instalace, která se přidají do souboru MST, a potom klikněte na **Pokračovat**.
7. V části **Uložit soubory do** určete cestu k vytvořené složce.
8. Klikněte na možnost **Generovat**.

Vygeneruje se soubor transformace .mst a instalační balíčky .msi a .cab se extrahují do vytvořené složky.

Krok 3: Nastavení objektů zásad skupiny

1. Přihlaste se k řadiči domény jako správci domény; pokud má doména více řadičů domény, přihlaste se k některému z nich jako správce domény.
2. Pokud plánujete instalaci agenta v organizační jednotce, ujistěte se, že organizační jednotka v doméně existuje. Jinak tento krok přeskočte.
3. V nabídce **Start** vyberte položku **Nástroje pro správu** a klikněte na příkaz **Uživatelé a počítače služby Active Directory** (v systému Windows Server 2003) nebo **Správa zásad skupiny** (v systému Windows Server 2008 a novějším).
4. V systému Windows Server 2003:
   - Klikněte pravým tlačítkem myši na název domény nebo organizační jednotky a potom klikněte na příkaz **Vlastnosti**. V dialogovém okně klikněte na kartu **Zásady skupiny** a klikněte na tlačítko **Nový**.

   V systému Windows Server 2008 a novějším:
   - Klikněte pravým tlačítkem myši na název domény nebo organizační jednotky a potom klikněte na příkaz **Zde vytvořit a propojit objekt zásad skupiny**.
5. Pojmenujte nový objekt zásad skupiny **Agent pro Windows**.
6. Objekt zásad skupiny **Agent pro Windows** pro úpravy otevřete následujícím způsobem:
   - V systému Windows Server 2003 klikněte na objekt zásad skupiny a potom klikněte na **Upravit**.
   - V systému Windows Server 2008 a novějším v části **Objekty zásad skupiny** klikněte pravým tlačítkem myši na objekt zásad skupiny a klikněte na příkaz **Upravit**.
7. V modulu snap-in editoru objektů zásad skupiny rozbalte položku **Konfigurace počítače**.
8. V systému Windows Server 2003 a Windows Server 2008:
   - Rozbalte položku **Nastavení softwaru**.

   V systému Windows Server 2012 a novějším:
   - Rozbalte položku **Zásady** > **Nastavení softwaru**.
9. Pravým tlačítkem klikněte na položku **Instalace softwaru**, vyberte nabídku **Nový** a klikněte na položku **Balíček**.

10. Vyberte instalační balíček MSI agenta ve sdílené složce, kterou jste vytvořili, a klikněte na možnost **Otevřít**.
11. V dialogovém okně **Nasazení softwaru** klikněte na tlačítko **Pokročilé** a potom na tlačítko **OK**.
12. Na kartě **Úpravy** klikněte na možnost **Přidat** a vyberte soubor transformace MST, který jste vytvořili.
13. Kliknutím na tlačítko **OK** zavřete dialogové okno **Nasazení softwaru**.

6.7 Aktualizace agentů

Agenty od uvedených verzí dále je možné aktualizovat pomocí webového rozhraní:

- Agent pro Windows, Agent pro VMware (Windows), Agent pro Hyper-V: verze 11.9.191 a novější
- Agent pro Linux: verze 11.9.179 a novější
- Další agenti: aktualizovat lze všechny verze

Chcete-li zjistit verzi agenta, vyberte počítač a klikněte na možnost **Přehled**.

Chcete-li provést aktualizaci ze starších verzí agentů, stáhněte a nainstalujte nejnovějšího agenta ručně. Odkazy ke stažení zobrazíte kliknutím na **Všechna zařízení** > **Přidat**.

Jak aktualizovat agenta pomocí webového rozhraní

1. Klikněte na možnost **Nastavení** > **Agenti**.

   Software zobrazí seznam počítačů. Počítače s neaktuálními verzemi agentů jsou označeny oranžovým vykřičníkem.
2. Vyberte počítače, ve kterých chcete agenty aktualizovat. Počítače musí být online.
3. Klikněte na možnost **Aktualizovat agenta**.

Aktualizace Agenta pro VMware (Virtual Appliance)

1. Odeberte Agenta pro VMware (Virtual Appliance) způsobem popsaným v části Odinstalace agentů (str. 31). V kroku 5 odstraňte agenta z **Nastavení** > **Agenti**, a to i tehdy, pokud agenta plánujete znovu nainstalovat.
2. Nasaďte Agenta pro VMware (Virtual Appliance), jak je popsáno v části Nasazení šablony OVF (str. 26).
3. Konfigurujte Agenta pro VMware (Virtual Appliance) způsobem popsaným v části Konfigurace virtuálního zařízení (str. 26).

   Pokud chcete obnovit místně připojené úložiště, proveďte v kroku 7 následující akce:

   a. Přidejte disk obsahující místní úložiště k virtuálnímu zařízení.
   b. Klikněte na **Aktualizovat** > **Vytvořit úložiště** > **Připojit**.
   c. Software zobrazí původní **písmeno** a **jmenovku** disku. Neměňte je.
   d. Klikněte na tlačítko **OK**.

   Výsledkem je, že plány zálohování, které byly použity pro starého agenta, jsou automaticky znovu použity pro nového agenta.
4. Plány s povoleným zálohováním s podporou aplikací vyžadují opětovné zadání pověření hostujícího operačního systému. Upravte tyto plány a znovu zadejte pověření.
5. U plánů, které zálohují konfiguraci ESXi, je nutné znovu zadat heslo účtu root. Upravte tyto plány a znovu zadejte heslo.

6.8 Odinstalování agentů

Ve Windows

Pokud chcete odebrat jednotlivé součásti produktu (například jednoho z agentů nebo Sledování záloh), spusťte instalační program **Všichni agenti pro instalaci v systému Windows**, zvolte možnost úpravy produktu a zrušte výběr součástí, které chcete odebrat. Odkaz na instalační program se nachází na stránce **Stažené soubory** (klikněte na ikonu účtu v pravém horním rohu stránky > **Stažené soubory**).

Chcete-li z počítače odebrat všechny součásti produktu, použijte níže uvedený postup.

1. Přihlaste se jako správce.
2. Otevřete **Ovládací panely** a vyberte možnosti **Programy a funkce** (**Přidat nebo odebrat programy** ve Windows XP) > **Acronis Backup Agent** > **Odinstalovat**.
3. [Volitelné] Zaškrtněte políčko **Odstranit protokoly a konfigurační nastavení**.

   Pokud agenta plánujete znovu nainstalovat, ponechte toto zaškrtávací políčko prázdné. Pokud toto políčko zaškrtnete, počítač může být v konzole pro zálohování duplikován a zálohy starého počítače nemusí být spojeny s novým počítačem.
4. Potvrďte své rozhodnutí.
5. Pokud agenta plánujete znovu nainstalovat, tento krok přeskočte. V opačném případě v konzoli pro zálohování klikněte na **Nastavení** > **Agenti**, vyberte počítač, kde byl agent nainstalován, a poté klikněte na **Odstranit**.

V systému Linux

1. Jako uživatel root spusťte **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.
2. [Volitelné] Zaškrtněte políčko **Smazat všechny stopy produktu (odstranit jeho protokolové soubory, úlohy, úložiště a nastavení konfigurace)**.

   Pokud agenta plánujete znovu nainstalovat, ponechte toto zaškrtávací políčko prázdné. Pokud toto políčko zaškrtnete, počítač může být v konzole pro zálohování duplikován a zálohy starého počítače nemusí být spojeny s novým počítačem.
3. Potvrďte své rozhodnutí.
4. Pokud agenta plánujete znovu nainstalovat, tento krok přeskočte. V opačném případě v konzoli pro zálohování klikněte na **Nastavení** > **Agenti**, vyberte počítač, na který byl agent nainstalován, a klikněte na **Odstranit**.

V systému macOS

1. Klikněte dvakrát na instalační soubor (.dmg).
2. Počkejte, až operační systém připojí obraz instalačního disku.
3. V obrazu klikněte dvakrát na možnost **Odinstalovat**.
4. Pokud se zobrazí výzva, zadejte pověření správce.
5. Potvrďte své rozhodnutí.
6. Pokud agenta plánujete znovu nainstalovat, tento krok přeskočte. V opačném případě v konzoli pro zálohování klikněte na **Nastavení** > **Agenti**, vyberte počítač, kde byl agent nainstalován, a poté klikněte na **Odstranit**.

Odebrání Agenta pro VMware (Virtual Appliance)

1. Spusťte klienta vSphere a přihlaste se na server vCenter.
2. Po zapnutí virtuálního zařízení na něj klikněte pravým tlačítkem a poté klikněte na **Napájení** > **Vypnout**. Potvrďte své rozhodnutí.

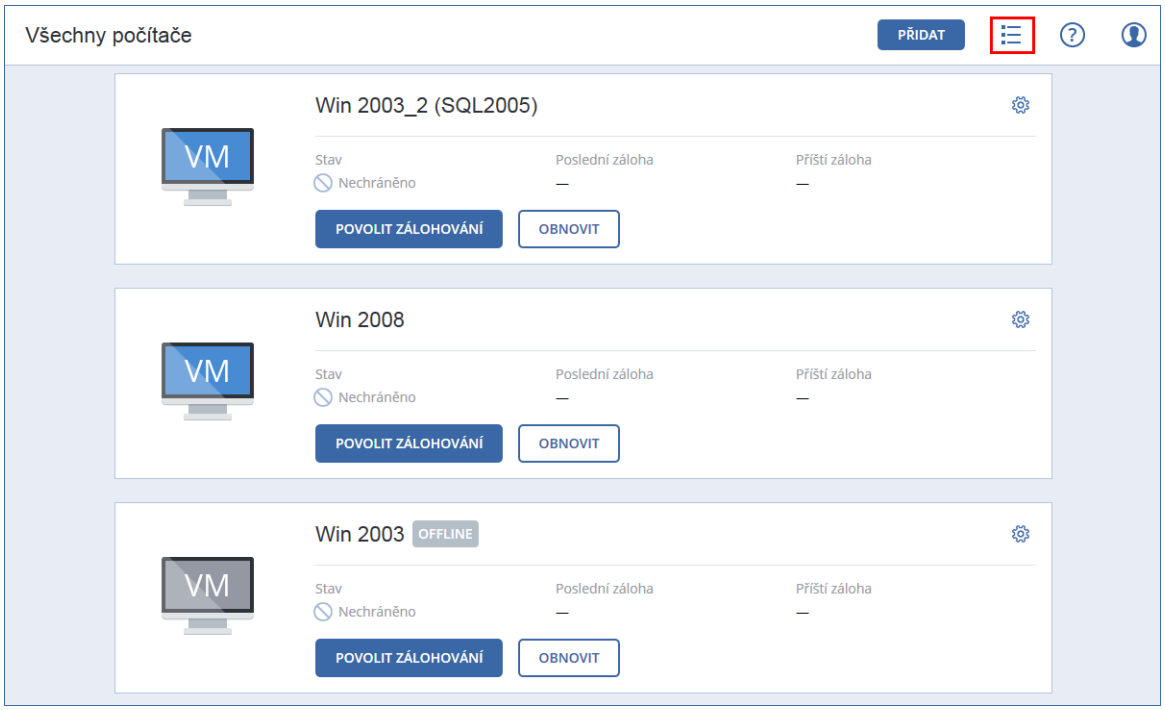
3. Pokud virtuální zařízení používá místně připojené úložiště na virtuálním disku a chcete na tomto disku zachovat data, postupujte následovně:
   a. Pravým tlačítkem klikněte na VA a potom na položku **Upravit nastavení**.
   b. Vyberte disk s úložištěm a potom klikněte na příkaz **Odstranit**. Pod položkou **Možnosti odstranění** klikněte na příkaz **Odstranit z virtuálního počítače**.
   c. Klikněte na tlačítko **OK**.

   Výsledkem je, že disk zůstane v úložišti dat. Disk můžete připojit k jinému VA.
4. Pravým tlačítkem klikněte na VA a potom na položku **Odstranit z disku**. Potvrďte své rozhodnutí.
5. Pokud agenta plánujete znovu nainstalovat, tento krok přeskočte. Jinak v konzoli pro zálohování postupujte takto:
   a. Klikněte na **Nastavení** > **Agenti**, vyberte virtuální zařízení a klikněte na **Odstranit**.
   b. Klikněte na **Zálohy** > **Umístění** a odstraňte umístění, které odpovídá místně připojenému úložišti.

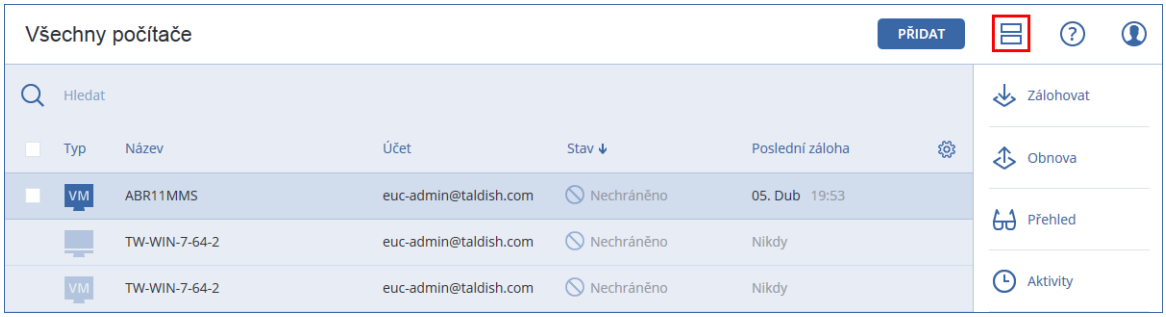
7 Zobrazení konzoly pro zálohování

Konzola pro zálohování má dvě zobrazení: jednoduché zobrazení a tabulkové zobrazení. Chcete-li přepnout mezi zobrazeními, klikněte na odpovídající ikonu v pravém horním rohu.

Jednoduché zobrazení podporuje malé množství počítačů.



Tabulkové zobrazení se automaticky zapne v případě, že bude množství počítačů velké.



Obě zobrazení zprostředkovávají přístup ke stejným funkcím a operacím. Tento dokument popisuje přístup k operacím z tabulkového zobrazení.

8 Zálohování

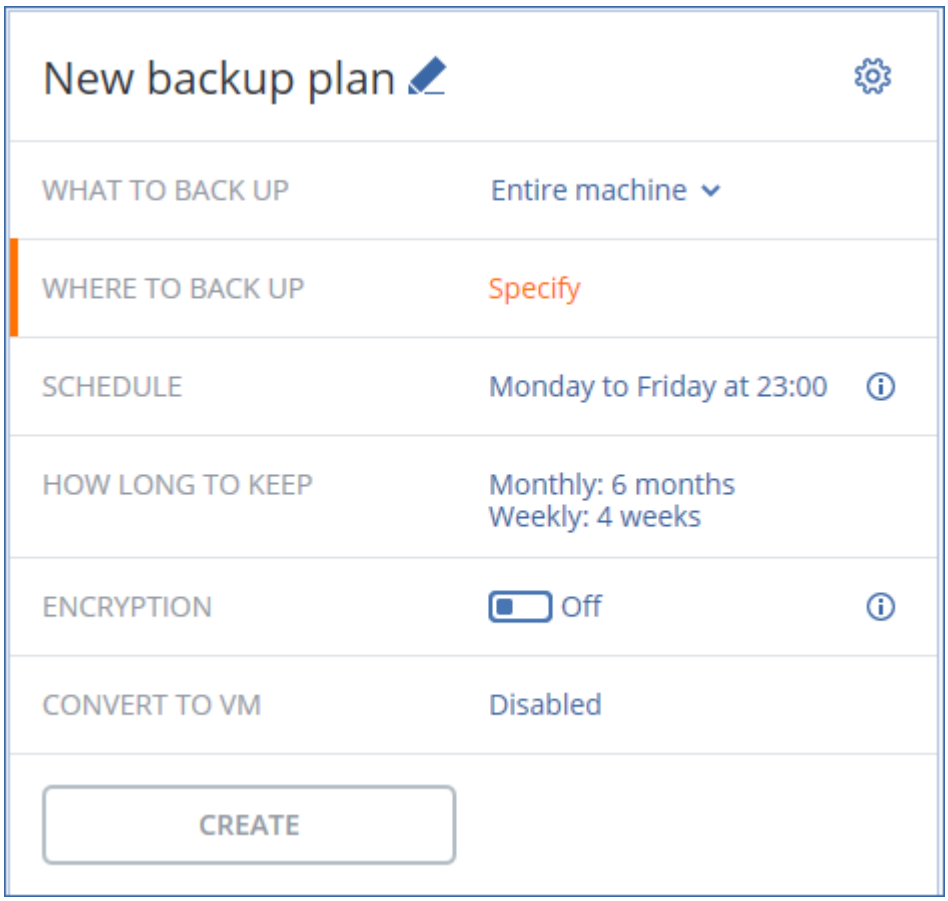
Plán zálohování je soubor pravidel, která určují, jak jsou v daném počítači chráněna data.

Plán zálohování je možné použít pro několik počítačů hned při jeho vytvoření nebo později.

Jak vytvořit první plán zálohování

1. Vyberte počítače, které chcete zálohovat.
2. Klikněte na možnost **Zálohovat**.

   Software zobrazí šablonu nového plánu zálohování.



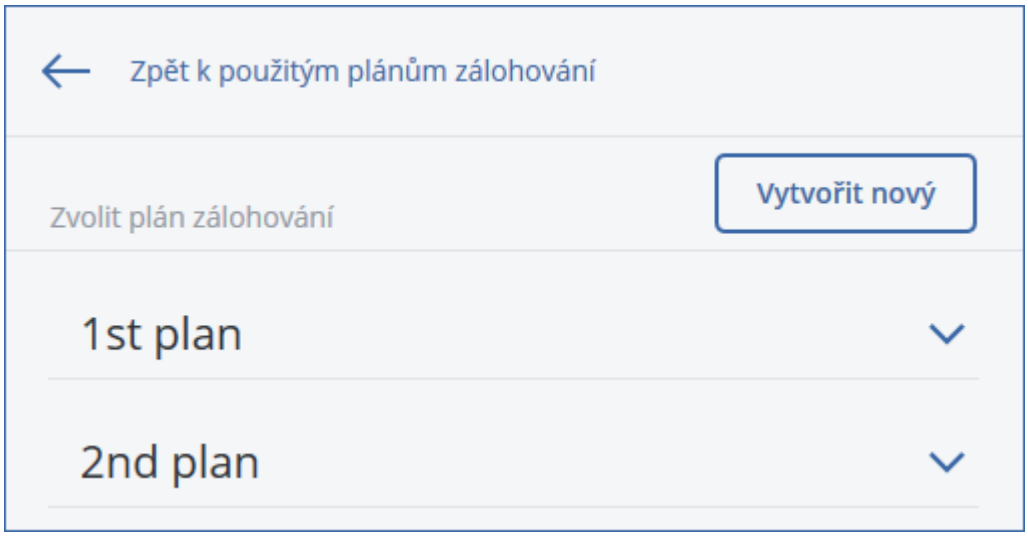
3. [Volitelné] Pokud chcete upravit název plánu zálohování, klikněte na výchozí název.

4. [Volitelné] Chcete-li upravit parametry plánu, klikněte na odpovídající část panelu plánu zálohování.
5. [Volitelné] Pokud chcete upravit název možnosti zálohování, klikněte na ikonu ozubeného kola.
6. Klikněte na tlačítko **Vytvořit**.

Jak použít existující plán zálohování

1. Vyberte počítače, které chcete zálohovat.
2. Klikněte na možnost **Zálohovat**. Pokud se na vybraných počítačích již používá společný plán zálohování, klikněte na možnost **Přidat plán zálohování**.

   Software zobrazí dříve vytvořené plány zálohování.



3. Vyberte plán zálohování, který chcete použít.
4. Klikněte na tlačítko **Použít**.

8.1 Shrnutí plánu zálohování

V následující tabulce jsou shrnuty dostupné parametry plánu zálohování. Pomocí této tabulky si můžete nastavit plán zálohování, který vám nejlépe vyhovuje.

CO ZÁLOHOVAT	ZÁLOHOVANÉ POLOŽKY Metody výběru	KAM ZÁLOHOVAT	PLÁN Schémata zálohování (neplatí pro cloud)	JAK DLOUHO UCHOVÁVAT
Disky/svazky (fyzické počítače)	Přímý výběr (str. 36) Pravidla zásad (str. 36) Filtry souborů (str. 63)	Cloud (str. 41) Místní složka (str. 41) Síťová složka (str. 41) NFS (str. 41)* Secure Zone (str. 41)**	Vždy přírůstková (jeden soubor) (str. 43) Vždy plná (str. 43) Týdenní plná, denní přírůstková (str. 43) Vlastní (F-D-I) (str. 43)	Podle stáří zálohy (jedno pravidlo/na sadu záloh) (str. 52) Podle počtu záloh (str. 52) Zachovat natrvalo (str. 52)
Disky/svazky (virtuální počítače)	Pravidla zásad (str. 36) Filtry souborů (str. 63)	Cloud (str. 41) Místní složka (str. 41) Síťová složka (str. 41) NFS (str. 41)*		

CO ZÁLOHOVAT		ZÁLOHOVANÉ POLOŽKY Metody výběru	KAM ZÁLOHOVAT	PLÁN Schémata zálohování (neplatí pro cloud)	JAK DLOUHO UCHOVÁVAT
Soubory (pouze fyzické počítače)		Přímý výběr (str. 38) Pravidla zásad (str. 38) Filtry souborů (str. 63)	Cloud (str. 41) Místní složka (str. 41) Síťová složka (str. 41) NFS (str. 41)* Secure Zone (str. 41)**	Vždy plná (str. 43) Týdenní plná, denní přírůstková (str. 43) Vlastní (F-D-I) (str. 43)	
Konfigurace ESXi		Přímý výběr (str. 40)	Místní složka (str. 41) Síťová složka (str. 41) NFS (str. 41)*		
Webové stránky (soubory a databáze MySQL)		Přímý výběr (str. 161)	Cloud (str. 41)	—	
Stav systému		Přímý výběr (str. 40)	Cloud (str. 41) Místní složka (str. 41) Síťová složka (str. 41)	Vždy plná (str. 43) Týdenní plná, denní přírůstková (str. 43) Vlastní (F-I) (str. 43)	
Databáze SQL		Přímý výběr (str. 122)			
Databáze Exchange		Přímý výběr (str. 122)			
Microsoft Office 365	Poštovní schránky (místní agent pro Office 365)	Přímý výběr (str. 134)	Cloud (str. 41) Místní složka (str. 41) Síťová složka (str. 41)	Vždy přírůstková (jeden soubor) (str. 43)	
	Poštovní schránky (cloudový agent pro Office 365)	Přímý výběr (str. 137)	Cloud (str. 41)	—	
	Soubory na OneDrivu	Přímý výběr (str. 140) Pravidla zásad (str. 140)			
	Data v SharePointu Online	Přímý výběr (str. 143) Pravidla zásad (str. 143)			
G Suite	Schránky Gmail	Přímý výběr (str. 148)	Cloud (str. 41)	—	
	Soubory Disku Google	Přímý výběr (str. 152) Pravidla zásad (str. 152)			

CO ZÁLOHOVAT		ZÁLOHOVANÉ POLOŽKY Metody výběru	KAM ZÁLOHOVAT	PLÁN Schémata zálohování (neplatí pro cloud)	JAK DLOUHO UCHOVÁVAT
	Soubory Týmových disků	Přímý výběr (str. 155) Pravidla zásad (str. 155)			

* Zálohování do sdílených úložišť NFS není v systému Windows dostupné.

** Oddíl Secure Zone nelze vytvořit v počítačích Mac.

8.2 Výběr dat pro zálohování

8.2.1 Výběr disků nebo svazků

Záloha na úrovni disků obsahuje kopii disku nebo svazku v komprimované podobě. Ze zálohy na úrovni disků je možné obnovit jednotlivé disky, svazky nebo soubory. Záloha celého počítače je zálohou všech jeho disků.

Existují dva způsoby výběru disků nebo svazků: přímo na každém počítači nebo pomocí pravidel zásad. Je možné vyloučit soubory ze zálohy disku nastavením funkce Filtry souborů (str. 63).

Přímý výběr

Přímý výběr je dostupný jen u fyzických počítačů.

1. V okně **Co se má zálohovat** vyberte možnost **Disky/svazky**.
2. Klikněte na možnost **Položky k zálohování**.
3. V části **Vybrat položky pro zálohování** vyberte možnost **Přímo**.
4. U každého počítače zahrnutého do plánu zálohování zaškrtněte políčka vedle disků nebo svazků, které se mají zálohovat.
5. Klikněte na tlačítko **Hotovo**.

Použití pravidel zásad

1. V okně **Co se má zálohovat** vyberte možnost **Disky/svazky**.
2. Klikněte na možnost **Položky k zálohování**.
3. V části **Vybrat položky pro zálohování** vyberte možnost **Pomocí pravidel zásad**.
4. Vyberte některé předem definované pravidlo, zadejte vlastní nebo použijte obojí.

   Pravidla se použijí pro všechny počítače v plánu zálohování. Pokud nebudou v počítači při spuštění zálohování nalezena žádná data splňující alespoň jedno pravidlo, záloha na tomto počítači bude neúspěšná.
5. Klikněte na tlačítko **Hotovo**.

Pravidla pro Windows, Linux a OS X

- `[All volumes]` vybere všechny svazky se systémem Windows a všechny připojené svazky na počítačích se systémem Linux nebo OS X.

Pravidla pro Windows

- Písmeno jednotky (například **C:**) vybere svazek s určeným písmenem jednotky.
- **[Fixed Volumes (Physical machines)]** vybere všechny svazky fyzických počítačů jiné než vyměnitelné médium. Pevné svazky zahrnují svazky na zařízeních SCSI, ATAPI, ATA, SSA, SAS a SATA a také svazky v polích RAID.
- **[BOOT+SYSTEM]** vybere systémové a spouštěcí svazky. Kombinace je minimální množina dat, která zajišťuje obnovu operačního systému ze zálohy.
- **[Disk 1]** vybere první disk v počítači včetně všech svazků na tomto disku. Chcete-li vybrat jiný disk, zadejte odpovídající číslo.

Pravidla pro Linux

- **/dev/hda1** vybere první svazek na prvním pevném disku IDE.
- **/dev/sda1** vybere první svazek na prvním pevném disku SCSI.
- **/dev/md1** vybere první softwarový pevný disk RAID.

Chcete-li vybrat další základní svazky, určete vzorec **/dev/xdyN**, kde:

- "x" odpovídá typu disku,
- "y" odpovídá číslu disku (a pro první disk, b pro druhý disk atd.),
- "N" je číslo svazku.

Chcete-li vybrat logický svazek, zadejte jeho název společně s názvem skupiny svazků. Například u zálohování dvou logických svazků, **lv_root** a **lv_bin**, přičemž oba náleží do skupiny svazků **vg_mymachine**, zadejte:

```
/dev/vg_mymachine/lv_root
/dev/vg_mymachine/lv_bin
```

Pravidla pro OS X

- **[Disk 1]** Vybere první disk v počítači včetně všech svazků na tomto disku. Chcete-li vybrat jiný disk, zadejte odpovídající číslo.

8.2.1.1 Co ukládá záloha disku nebo svazku?

Záloha disku nebo svazku ukládá **systém souborů** disku nebo svazku jako celek spolu s informacemi potřebnými ke spuštění operačního systému. Z takových záloh je možné obnovit disky nebo svazky jako celek nebo i jednotlivé složky či soubory.

Se zapnutou možností zálohování (str. 72) **sektor po sektoru** obsahuje záloha disku všechny sektory disku. Zálohování sektor po sektoru lze použít k zálohování disků s nerozpoznaným nebo nepodporovaným systémem souborů a dalších vlastních datových formátů.

Windows

Záloha svazku ukládá všechny soubory a složky nezávisle na jejich atributech (včetně skrytých a systémových souborů), spouštěcí záznam, (pokud existuje) tabulku FAT, kořenový adresář a nultou stopu pevného disku s hlavním spouštěcím záznamem (MBR).

Záloha disku ukládá všechny svazky vybraného disku (včetně skrytých svazků jako je servisní diskový oddíl výrobce) a nultou stopu s hlavním spouštěcím záznamem (MBR).

Následující položky *nejsou* zahrnuty v záloze disku nebo svazku (ani v záloze na úrovni souborů):

- Odkládací soubor (pagefile.sys) a soubor hiberfil.sys, který při hibernaci uchovává obsah paměti RAM. Po obnově se na odpovídajícím místě tyto soubory znovu vytvoří s nulovou velikostí.
- Záloha provedená v rámci operačního systému (na rozdíl od spouštěcího média nebo zálohování virtuálních počítačů na úrovni hypervizoru):
  - Stínová kopie svazku systému Windows. Cesta je určená hodnotou registru **VSS Default Provider**, kterou lze nalézt v klíči registru **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. To znamená, že v operačních systémech počínaje systémem Windows Vista se body obnovení nezálohují.
  - Je-li možnost zálohování (str. 72) **Služba Stínová kopie svazku (VSS)** zapnutá, soubory a složky uvedené v klíči registru **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** se nezálohují.

Linux

Záloha svazku obsahuje všechny soubory a složky vybraného svazku nezávisle na jejich atributech, spouštěcí záznam a superblok systému souborů.

Záloha disku obsahuje všechny svazky disku i nulovou stopu s hlavním spouštěcím záznamem (MBR).

Mac

Záloha disku nebo svazku obsahuje nejen všechny soubory a adresáře vybraného disku nebo svazku, ale i popis rozvržení svazků.

Následující položky jsou vyloučeny:

- Systémová metadata, jako je žurnál systému souborů a index Spotlightu.
- Koš
- Zálohy Time machine

Disky a svazky jsou na Macu zálohované na úrovni souborů. Obnova na zcela nový počítač je sice ze záloh disku a svazku možná, ale záloha sektor po sektoru k dispozici není.

8.2.2 Výběr souborů a složek

Záloha na úrovni souborů je dostupná pouze u fyzických počítačů.

Zálohování na úrovni souborů není dostatečné pro obnovu operačního systému. Zálohování souborů vyberte v případě, že chcete zabezpečit pouze určitá data (například aktuální projekt). Tím se sníží velikost archivu a ušetří se prostor úložiště.

Soubory lze vybrat dvěma způsoby: přímo na každém počítači nebo pomocí pravidel zásad. Obě metody umožňují další zpřesnění výběru pomocí filtrů souborů (str. 63).

Přímý výběr

1. V části **Co se má zálohovat** vyberte možnost **Soubory/složky**.
2. Klikněte na příkaz **Položky k zálohování**.
3. V části **Vybrat položky pro zálohování** vyberte možnost **Přímo**.
4. U každého počítače zahrnutého do plánu zálohování:
   a. Klikněte na možnost **Vybrat soubory a složky**.
   b. Klikněte na možnost **Místní složka** nebo **Síťová složka**.

Sdílené umístění musí být na vybraném počítači dostupné.

c. Vyhledejte požadované soubory a složky nebo cestu zadejte a klikněte na tlačítko s šipkou. Při zobrazení žádosti zadejte pro složku uživatelské jméno a heslo.

   Zálohování složky s anonymním přístupem není podporováno.

d. Vyberte požadované soubory a složky.

e. Klikněte na tlačítko **Hotovo**.

Použití pravidel zásad

1. V části **Co se má zálohovat** vyberte možnost **Soubory/složky**.
2. Klikněte na příkaz **Položky k zálohování**.
3. V části **Vybrat položky pro zálohování** vyberte možnost **Pomocí pravidel zásad**.
4. Vyberte některé předem definované pravidlo, zadejte vlastní nebo použijte obojí.

   Pravidla se použijí pro všechny počítače v plánu zálohování. Pokud nebudou v počítači při spuštění zálohování nalezena žádná data splňující alespoň jedno pravidlo, záloha na tomto počítači bude neúspěšná.
5. Klikněte na tlačítko **Hotovo**.

Výběrová pravidla pro Windows

- Úplná cesta k souboru nebo složce, například **D:\Práce\Text.doc** nebo **C:\Windows**.
- Šablony:
  - **`[All Files]`** vybere všechny soubory na všech svazcích v počítači.
  - **`[All Profiles Folder]`** vybere složku, kde jsou umístěny všechny uživatelské profily (obvykle **C:\Users** nebo **C:\Documents and Settings**).
- Proměnné prostředí:
  - **`%ALLUSERSPROFILE%`** vybere složku, kde jsou umístěna společná data všech uživatelských profilů (obvykle **C:\ProgramData** nebo **C:\Documents and Settings\All Users**).
  - **`%PROGRAMFILES%`** vybere složku Program Files (například **C:\Program Files**).
  - **`%WINDIR%`** vybere složku systému Windows (například **C:\Windows**).

  Můžete používat i další proměnné prostředí nebo kombinaci proměnných a textu. Chcete-li například vybrat složku Java ve složce Program Files, zadejte: **%PROGRAMFILES%\Java**.

Výběrová pravidla pro Linux

- Úplná cesta k souboru nebo adresáři. Například pokud chcete zálohovat **soubor.txt** ve svazku **/dev/hda3** připojeném k **/home/usr/docs**, zadejte **/dev/hda3/soubor.txt** nebo **/home/usr/docs/soubor.txt**.
  - **`/home`** vybere domovský adresář běžných uživatelů.
  - **`/root`** vybere domovský adresář uživatele root.
  - **`/usr`** vybere adresář všech aplikací týkajících se uživatele.
  - **`/etc`** vybere adresář systémových konfiguračních souborů.
- Šablony:
  - **`[All Profiles Folder]`** vybere složku **/home**. Jedná se o složku, kde jsou ve výchozím nastavení umístěny všechny uživatelské profily.

Výběrová pravidla pro macOS

- Úplná cesta k souboru nebo adresáři.
- Šablony:

- **`[All Profiles Folder]`** vybere složku **/Users**. Jedná se o složku, kde jsou ve výchozím nastavení umístěny všechny uživatelské profily.

Příklady:

- Pokud chcete zálohovat **soubor.txt** na ploše,zadejte **/Users/**<uživatelské jméno>/Desktop/soubor.txt, kde <uživatelské jméno> je vaše uživatelské jméno.
- Chcete-li zálohovat domovské adresáře všech uživatelů, zadejte **/Users**.
- Chcete-li zálohovat adresář, kde jsou nainstalovány aplikace, zadejte **/Applications**.

8.2.3 Výběr stavu systému

Záloha stavu systému je dostupná u počítačů vybavených systémem Windows Vista nebo novějším.

Chcete-li zálohovat stav systému, v okně **Co se má zálohovat** vyberte **Stav systému**.

Záloha stavu systému se skládá z následujících souborů:

- Konfigurace plánovače úloh.
- Úložiště metadat VSS.
- Konfigurační informace čítače výkonu.
- Služba MSSearch.
- Služba BITS (Background Intelligent Transfer Service)
- Registr
- Windows Management Instrumentation (WMI)
- Registrační databáze tříd služeb součástí

8.2.4 Výběr konfigurace ESXi

Záloha konfigurace hostitele ESXi vám umožní obnovit hostitele ESXi na holé železo. Obnova se provede pomocí spouštěcího média.

Virtuální počítače běžící na hostiteli nejsou zahrnuty do zálohy. Je možné je zálohovat a obnovovat samostatně.

Záloha konfigurace hostitele ESXi zahrnuje následující položky:

- Zavaděč a oddíly se spouštěcí bankou.
- Stav hostitele (konfigurace virtuální sítě a úložiště, klíče SSL, nastavení sítě serveru a informace o místním uživateli).
- Rozšíření a opravy nainstalované nebo rozfázované v hostiteli.
- Soubory protokolu.

Předpoklady

- V položce **Bezpečnostní profil** konfigurace hostitele ESXi musí být povoleno SSH.
- Je nutné znát heslo k účtu "root" na hostiteli ESXi.

Omezení

- Zálohování konfigurace ESXi není pro VMware vSphere 6.7 podporováno.
- Konfiguraci ESXi nelze zálohovat do cloudového úložiště.

Jak vybrat konfiguraci ESXi

1. Přejděte na **VMware** > **Hostitel a clustery**.

2. Přejděte k hostitelům ESXi, které chcete zálohovat.
3. Vyberte hostitele ESXi a klikněte na možnost **Zálohovat**.
4. V okně **Co se má zálohovat** vyberte možnost **Konfigurace ESXi**.
5. Do pole **Heslo účtu root ESXi** zadejte heslo účtu root každého z vybraných hostitelů nebo použijte stejné heslo u všech hostitelů.

8.3 Výběr cíle

Klikněte na možnost **Kam zálohovat** a potom vyberte jednu z těchto možností:

- **Cloudové úložiště**

  Zálohy se budou ukládat do cloudového datového centra.

- **Místní složky**

  Pokud je vybrán jeden počítač, vyhledejte složku nebo k ní zadejte cestu.

  Pokud je vybráno více počítačů, zadejte cestu. Zálohy se budou ukládat do zadané složky v každém vybraném fyzickém počítači nebo v počítači, kde je nainstalován agent pro virtuální počítače. Pokud složka neexistuje, bude vytvořena.

- **Síťová složka**

  Toto je složka sdílená pomocí SMB/CIFS/DFS.

  Vyhledejte požadovanou sdílenou složku nebo zadejte cestu v následujícím formátu:

  - Sdílené složky SMB/CIFS: `\\<název hostitele>\<cesta>\` nebo `smb://<název hostitele>/<cesta>/`
  - Sdílené složky DFS: `\\<úplný název domény DNS>\<kořen DFS>\<cesta>`

    Příklad: `\\example.company.com\shared\files`

  Potom klikněte na tlačítko s šipkou. Při zobrazení žádosti zadejte pro složku uživatelské jméno a heslo.

  Zálohování složky s anonymním přístupem není podporováno.

- **Složka NFS** (dostupné pro počítače se systémy Linux nebo macOS)

  Vyhledejte požadovanou složku NFS nebo zadejte cestu v následujícím formátu:

  `nfs://<název hostitele>/<exportovaná složkar>:/<podsložka>`

  Potom klikněte na tlačítko s šipkou.

  Složky NFS chráněné heslem nelze zálohovat.

- **Secure Zone** (dostupné, pokud se nachází v každém vybraném počítači)

  Secure Zone je zabezpečený oddíl na disku zálohovaného počítače. Tento oddíl je nutné před konfigurací zálohy ručně vytvořit. Informace o tom, jak oddíl Secure Zone vytvořit a o jeho výhodách a omezeních naleznete v tématu O službě Secure Zone (str. 41).

8.3.1 O službě Secure Zone

Secure Zone je zabezpečený oddíl na disku zálohovaného počítače. Může obsahovat zálohy disků nebo souborů tohoto počítače.

Pokud dojde k havárii fyzického disku, zálohy uložené v Secure Zone mohou být ztraceny. To je důvod, proč by oddíl Secure Zone neměl být jediným umístěním pro ukládání záloh. V prostředí podniku je možné oddíl Secure Zone považovat za přechodné umístění záloh používané v případě, když je běžné umístění dočasně nedostupné nebo když je připojení pomalé nebo obsazené.

Proč použít Secure Zone?

Secure Zone:

- Umožňuje obnovení disku na stejný disk, kde je umístěna záloha disku.
- Nabízí cenově efektivní a šikovnou metodu zabezpečení dat před vadným softwarem, útokem viru a chybami obsluhy.
- Odstraňuje potřebu samostatných médií nebo síťového připojení pro zálohování nebo obnovu dat. To je zvláště praktické pro mobilní uživatele.
- Může sloužit jako primární umístění při použití replikace záloh.

Omezení

- Oddíl Secure Zone nelze vytvořit na počítači Mac.
- Secure Zone je oddíl na základním disku. Nelze ho vytvořit na dynamickém disku nebo jako logický svazek (spravovaný službou LVM).
- Secure Zone se formátuje se systémem souborů FAT32. Protože FAT32 má pro velikost souborů limit 4 GB, větší zálohy se při uložení do oddílu Secure Zone rozdělují. Na proces a rychlost obnovy to nemá vliv.
- Secure Zone nepodporuje jednosouborový formát záloh (str. 183). Když změníte cíl na Secure Zone v plánu zálohování s metodou **Vždy přírůstková (jeden soubor)**, změní se tato metoda na **Týdenní plná, denní přírůstková**.

Jak vytvořit oddíl Secure Zone

1. Rozhodněte, na který disk chcete oddíl Secure Zone umístit.
2. Spusťte příkazový řádek a zadáním příkazu **`acrocmd list disks`** zobrazte seznam čísel disků.
3. Použijte příkaz **`create asz`** nástroje **`acrocmd`**. Příkaz nejdříve použije nepřidělené místo na tomto disku a pokud není dostatečně velké, použije vybrané místo z vybraných svazků. Podrobnosti naleznete níže v tématu Jak tvorba oddílu Secure Zone transformuje disk.

   Příklady:

   - Vytváření oddílu Secure Zone na disku 1 místního počítače. Oddíl Secure Zone se vytvoří s výchozí velikostí, která odpovídá průměru mezi maximální (veškeré nepřidělené místo) a minimální (přibližně 50 MB) hodnotou.

     ```
     acrocmd create asz --disk=1
     ```

   - Vytváření oddílu Secure Zone chráněného heslem o velikosti 100 GB na disku 2 místního počítače. Pokud není dostatek nepřiděleného místa na disku, místo bude odebráno z druhého svazku daného disku.

     ```
     acrocmd create asz --disk=2 --volume=2-2 --asz_size=100gb --password=abc12345
     ```

   - Vytváření oddílu Secure Zone o velikosti 20 GB na disku 1 vzdáleného počítače.

     ```
     acrocmd create asz --host=192.168.1.2 --credentials=john,pass1 --disk=1
     --asz_size=20gb
     ```

   Podrobný popis příkazu **`create asz`** naleznete v referenční příručce pro příkazový řádek.

Jak tvorba oddílu Secure Zone transformuje disk.

- Oddíl Secure Zone se vytváří vždy na konci pevného disku. Při výpočtu konečného rozvržení svazků aplikace využije nejprve nepřidělené místo na konci.
- Pokud není na konci disku dostatek nepřiděleného místa, ale existuje nepřidělené místo mezi svazky, budou svazky přesunuty tak, aby se nepřidělené místo vyskytovalo na konci.

- Jestliže již bylo všechno nepřidělené místo shromážděno, ale stále to nestačí, aplikace využije volné místo ve vybraných svazcích a proporcionálně zmenší jejich velikost. Změna velikosti uzamknutých svazků vyžaduje restartování.
- Ve svazku však musí být volné místo, aby mohl fungovat operační systém a aplikace (například kvůli tvorbě dočasných souborů). Aplikace nebude zmenšovat svazky, kde volné místo tvoří méně než 25 % celkové velikosti svazku. Aplikace bude pokračovat v proporcionálním zmenšování svazků teprve tehdy, když budou všechny svazky na disku mít 25 % volného místa nebo méně.

Jak je z výše uvedeného patrné, nastavení maximální možné velikosti oddílu Secure Zone není doporučeno. Důsledkem by byl nedostatek volného místa ve všech svazcích, a to by pravděpodobně způsobilo nestabilitu nebo dokonce neschopnost spuštění systému nebo aplikací.

8.4 Plán

Plán používá nastavení času (včetně časového pásma) operačního systému, ve kterém je agent nainstalován. Časové pásmo Agenta pro VMware (Virtual Appliance) lze nakonfigurovat v rozhraní agenta (str. 26).

Pokud je například spuštění plánu zálohování naplánováno na 21:00 a použije se na několik počítačů umístěných v různých časových pásmech, zálohování se spustí na každém počítači ve 21:00 místního času.

Parametry plánu závisí na cíli zálohy.

Při zálohování do cloudového úložiště

Ve výchozím nastavení se zálohy provádí denně (od pondělí do pátku). Čas spuštění zálohy si můžete vybrat.

Pokud chcete změnit frekvenci záloh, posuňte posuvník a zadejte plán.

Zálohy lze naplánovat tak, aby se spouštěly na základě událostí a ne na základě času. To provedete výběrem typu události v nástroji pro výběr plánu. Další informace najdete v části Plánování podle událostí (str. 45).

Důležité *První záloha je plná a trvá tedy nejdéle. Všechny další zálohy jsou přírůstkové a trvají mnohem kratší dobu.*

Při zálohování do jiných úložišť

Můžete si vybrat jedno z předem definovaných schémat zálohování nebo si vytvořit vlastní. Schéma zálohování je součástí plánu zálohování, které zahrnuje plán a metody zálohování.

V části **Schéma zálohování** vyberte jednu z následujících možností:

- [Pouze pro zálohy na úrovni disku] **Vždy přírůstková (jeden soubor)**

  Ve výchozím nastavení se zálohy provádí denně (od pondělí do pátku). Čas spuštění zálohy si můžete vybrat.

  Pokud chcete změnit frekvenci záloh, posuňte posuvník a zadejte plán.

  Zálohy používají nový jednosouborový formát (str. 183).

  Nedostupné při zálohování na pásku nebo do oddílu Secure Zone.
- **Vždy plná**

  Ve výchozím nastavení se zálohy provádí denně (od pondělí do pátku). Čas spuštění zálohy si můžete vybrat.

Pokud chcete změnit frekvenci záloh, posuňte posuvník a zadejte plán.

Všechny zálohy jsou plné.

- **Týdenní plná, denní přírůstková**

  Ve výchozím nastavení se zálohy provádí denně (od pondělí do pátku). Dny v týdnu a čas spuštění zálohy si můžete vybrat.

  Jednou za týden se vytvoří plná záloha. Všechny ostatní zálohy jsou přírůstkové. Den, kdy se vytvoří plná záloha, je určen možností **Týdenní zálohování** (klikněte na ikonu ozubeného kola a potom na možnost **Možnosti zálohování** > **Týdenní zálohování**).

- **Vlastní**

  Určete plány pro plné, rozdílové a přírůstkové zálohy.

  Rozdílové zálohy nejsou dostupné při zálohování dat SQL či Exchange nebo dat o stavu systému.

U všech schémat zálohování lze naplánovat, aby se zálohy spouštěly na základě událostí a ne na základě času. To provedete výběrem typu události v nástroji pro výběr plánu. Další informace najdete v tématu Plánování podle událostí (str. 45).

Další možnosti plánování

U každého cíle můžete provést toto:

- Zadejte podmínky spuštění zálohy, aby se naplánovaná záloha provedla pouze při splnění těchto podmínek. Další informace najdete v části Podmínky spuštění (str. 46).
- Nastavte období, pro které plán platí. Zaškrtněte políčko **Spustit plán v časovém rozsahu** a zadejte období.
- Vypněte použití plánu. Když je plán vypnutý, pravidla zachování se nepoužijí (pokud nebyla záloha spuštěna ručně).
- Nastavte zpoždění oproti naplánovanému času. Hodnota zpoždění u každého počítače se vybere náhodně a může být v rozsahu od nuly do maximální zadané hodnoty. Toto nastavení možná budete chtít použít při zálohování více počítačů do síťového umístění, abyste se vyhnuli nadměrnému zatížení sítě.

  Klikněte na ikonu ozubeného kola a potom na možnost **Možnosti zálohování** > **Plán**. Zaškrtněte políčko **Rozložit čas spuštění do časového rámce** a zadejte maximální zpoždění. Hodnota zpoždění každého počítače se určí po nasazení plánu zálohování do počítače a zůstane stejná, dokud neupravíte plán zálohování a nezměníte maximální hodnotu zpoždění.

  Poznámka: *Tato možnost je ve výchozím nastavení zapnutá a maximální zpoždění je nastaveno na 30 minut.*

- Kliknutím na **Zobrazit více** zobrazte následující možnosti:
  - **Pokud je počítač vypnutý, vynechané úlohy se spustí při spuštění počítače.** (ve výchozím nastavení vypnuto)
  - **Zabránit režimu spánku nebo hibernace při zálohování** (ve výchozím nastavení zapnuto)

    Tato možnost má vliv pouze v počítačích se systémem Windows.
  - **Probudit z režimu spánku nebo hibernace při spuštění naplánované zálohy** (ve výchozím nastavení vypnuto)

    Tato možnost má vliv pouze v počítačích se systémem Windows. Tato možnost není účinná, pokud je počítač vypnut. V takovém případě tato možnost nevyvolá funkci Wake-on-LAN.

8.4.1 Plánování podle událostí

Při nastavování časového plánu pro plán zálohování můžete vybrat typ události v nástroji pro výběr plánu. Zálohování bude zahájeno, jakmile nastane daná událost.

Můžete si vybrat některou z následujících událostí:

- **Po uplynutí času od poslední zálohy**

  Jde o dobu od dokončení poslední úspěšné zálohy v rámci stejného plánu zálohování. Můžete zadat časový interval.
- **Když se uživatel přihlásí do systému**

  Ve výchozím nastavení se při přihlášení libovolného uživatele spustí zálohování. Libovolného uživatele můžete změnit na účet konkrétního uživatele.
- **Když se uživatel odhlásí od systému**

  Ve výchozím nastavení se při odhlášení libovolného uživatele spustí zálohování. Libovolného uživatele můžete změnit na účet konkrétního uživatele.

  Poznámka: *Zálohování neprobíhá při vypnutí systému, protože vypnutí není totéž jako odhlášení.*
- **Při spuštění systému**
- **Při vypnutí systému**
- **Při události v protokolu událostí systému Windows**

  Musíte zadat vlastnosti události (str. 45).

V následující tabulce je uveden seznam událostí, které jsou k dispozici pro různá data v systémech Windows, Linux a macOS.

CO ZÁLOHOVAT	Po uplynutí času od poslední zálohy	Když se uživatel přihlásí do systému	Když se uživatel odhlásí od systému	Při spuštění systému	Při vypnutí systému	Při události v protokolu událostí systému Windows
Disky/svazky nebo soubory (fyzické počítače)	Windows, Linux, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Disky/svazky (virtuální počítače)	Windows, Linux	–	–	–	–	–
Konfigurace ESXi	Windows, Linux	–	–	–	–	–
Poštovní schránky Office 365	Windows	–	–	–	–	Windows
Databáze a poštovní schránky Exchange	Windows	–	–	–	–	Windows
Databáze SQL	Windows	–	–	–	–	Windows

8.4.1.1 Při události v protokolu událostí systému Windows

Je možné naplánovat, aby se zálohování spustilo v případě, že je v některém z protokolů Windows (protokol **Aplikace**, **Zabezpečení** nebo **Systém**) zaznamenána určitá událost.

Je například možné nastavit plán zálohování tak, aby byla provedena nouzová plná záloha vašich dat, jakmile systém Windows zjistí, že hrozí havárie pevného disku.

K procházení událostí a zobrazení vlastností událostí použijte doplněk **Prohlížeč událostí** dostupný v konzole **Správa počítače**. Abyste mohli otevřít protokol **Zabezpečení**, musíte být členem skupiny **Administrators**.

Vlastnosti události

Název logu (protokolového souboru)

Určuje jméno logu. Vyberte název standardního protokolu (**Aplikace**, **Zabezpečení** nebo **Systém**) ze seznamu, nebo napište například: **Microsoft Office Sessions**

Zdroj události

Určuje zdroj události, který typicky indikuje program nebo součást systému, která způsobila událost - například: **disk**

Typ události

Určuje typ události: **Chyba**, **Upozornění**, **Informace**, **Úspěšný audit** nebo **Neúspěšný audit**.

ID události

Určuje číslo události, které typicky identifikuje konkrétní typ událostí mezi událostmi ze stejného zdroje.

Například, událost **Chyba** se Zdrojem události **disk** a Událost ID **7** se objeví, když Windows na disku objeví vadný blok, zatímco událost **Chyba** se Zdrojem události **disk** a Událost ID **15** se objeví, když disk ještě není připraven pro přístup.

Příklad: Nouzová záloha při zjištění vadného bloku

Jeden nebo více vadných bloků, které se najednou objevily na pevném disku, obvykle značí, že pevný disk brzy selže. Řekněme, že chcete vytvořit plán zálohování, který zazálohuje data z disku, jakmile k takové situaci dojde.

Když systém Windows zjistí vadný blok na pevném disku, zaznamená událost se zdrojem události **disk** a číslem události **7** do protokolu **Systém**. Typ události je **Chyba**.

Při vytváření plánu v sekci **Naplánovat** zadejte nebo zvolte následující:

- **Název protokolu**: **Systém**
- **Zdroj události**: **disk**
- **Typ události**: **Chyba**
- **ID události**: **7**

Důležité *Aby se zaručilo, že se taková záloha dokončí navzdory přítomnosti vadných boků, musíte nastavit, aby zálohování vadné bloky ignorovalo. To uděláte tak, že v* ***Možnostech zálohování*** *přejdete na* ***Zpracování chyb*** *a zaškrtnete políčko* ***Ignorovat chybné sektory****.*

8.4.2 Podmínky spuštění

Tato nastavení rozšiřují plánovač o další možnosti, které umožní provést zálohování podle určitých podmínek. V případě více podmínek musí být pro povolení spuštění zálohy splněny všechny podmínky současně. Podmínky spuštění nemají vliv v případě, že je zálohování spuštěno ručně.

K těmto nastavením se dostanete tak, že při nastavování časového plánu pro plán zálohování kliknete na možnost **Zobrazit více**.

Chování plánovače v případě, že podmínka (nebo více podmínek) není splněna, určuje možnost zálohy Podmínky spuštění zálohování (str. 61). Pro řešení situace, kdy podmínky nejsou splněny příliš

dlouho a další odklad zálohování se stává rizikovým, můžete nastavit časový interval, po jehož uplynutí bude zálohování spuštěno bez ohledu na podmínku.

V následující tabulce je uveden seznam podmínek spuštění, které jsou k dispozici pro různá data v systémech Windows, Linux a macOS.

CO ZÁLOHOVAT	Disky/svazky nebo soubory (fyzické počítače)	Disky/svazky (virtuální počítače)	Konfigurace ESXi	Poštovní schránky Office 365	Databáze a poštovní schránky Exchange	Databáze SQL
Uživatel je nečinný (str. 47)	Windows	–	–	–	–	–
Hostitel umístění zálohy je dostupný (str. 48)	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Uživatelé se odhlásili (str. 48)	Windows	–	–	–	–	–
Vyhovuje časovému intervalu (str. 49)	Windows, Linux, macOS	Windows, Linux	–	–	–	–
Šetřit baterii (str. 49)	Windows	–	–	–	–	–
Nespouštět při připojení účtovaném podle objemu dat (str. 50)	Windows	–	–	–	–	–
Nespouštět při připojení k následujícím sítím Wi-Fi (str. 50)	Windows	–	–	–	–	–
Kontrolovat IP adresu zařízení (str. 51)	Windows	–	–	–	–	–

8.4.2.1 Uživatel je nečinný

Hláška „Uživatel je nečinný“ znamená, že je na počítači spuštěn spořič obrazovky nebo je počítač uzamčený.

Příklad

Spustit zálohování počítače každý den ve 21:00, nejlépe když je uživatel nečinný. Ve 23:00 spustit zálohování, i kdyby byl uživatel stále aktivní.

- Plánování: Denně, spouštět každý den. Spustit při: **21:00**.
- Podmínka: **Uživatel je nečinný**.
- Podmínky spuštění zálohování: **Čekat, než budou splněny podmínky. Po 2** hodinách **spustit zálohování bez ohledu na splnění podmínky**.

Výsledek

(1) Bude-li uživatel před 21:00 nečinný, zálohování se spustí ve 21:00.

(2) Stane-li se uživatel nečinný mezi 21:00 a 23:00 , zálohování se spustí okamžitě, jakmile se uživatel stane nečinný.

(3) Bude-li uživatel ve 23:00 stále aktivní, zálohování se spustí bez ohledu na jeho stav.

8.4.2.2 Hostitel umístění zálohy je dostupný

Hláška „Hostitel umístění zálohy je dostupný“, znamená, že počítač, který je hostitelem cílového umístění pro ukládání záloh, je prostřednictvím sítě dostupný.

Tato podmínka platí pro síťové složky, cloudové úložiště a umístění spravované uzlem úložišť.

Tato podmínka nezaručuje dostupnost samotného umístění, zaručuje pouze dostupnost hostitele. Například když je hostitel dostupný, ale síťová složka u tohoto hostitele není sdílená nebo pověření k této složce již nejsou platná, je podmínka přesto považovaná za splněnou.

Příklad

Data se zálohují do síťové složky každý pracovní den ve 21:00. Není-li počítač, který je hostitelem této složky, v té době dostupný (například kvůli údržbě), chcete tuto zálohu přeskočit a počkat s naplánovaným spuštěním do dalšího pracovního dne.

- Plánování: Denně, spouštět od pondělí do pátku. Spustit při: **21:00**.
- Podmínka: **Hostitel umístění zálohy je dostupný**.
- Podmínky spuštění zálohování: **Přeskočit naplánovanou zálohu**

Výsledek:

(1) Pokud je 21:00 a hostitel je dostupný, zálohování začne okamžitě.

(2) Pokud je 21:00, ale hostitel není dostupný, zálohování se spustí další pracovní den (jestliže bude hostitel dostupný).

(3) Nebude-li hostitel v žádný pracovní den ve 21:00 dostupný, zálohování se nespustí nikdy.

8.4.2.3 Uživatelé se odhlásili

Umožňuje oddálit zálohování, dokud se všichni uživatelé ze systému Windows neodhlásí.

Příklad

Spustit zálohování každý pátek ve 20:00, nejlépe když jsou všichni uživatelé odhlášeni. Ve 23:00 spustit zálohování, i kdyby byl jeden z uživatelů stále přihlášen.

- Plánování: Týdně, vždy v pátek. Spustit při: **20:00**.
- Podmínka: **Uživatelé jsou odhlášeni**.
- Podmínky spuštění zálohování: **Čekat, než budou splněny podmínky**. **Po 3** hodinách **spustit zálohování bez ohledu na splnění podmínky**.

Výsledek:

(1) Budou-li ve 20:00 všichni uživatelé odhlášeni, zálohování začne ve 20:00.

(2) Odhlásí-li se poslední uživatel mezi 20:00 a 23:00 , zálohování se spustí okamžitě, jakmile se uživatel odhlásí.

(3) Bude-li uživatel ve 23:00 stále přihlášený, zálohování se spustí bez ohledu na jeho stav.

8.4.2.4 Vyhovuje časovému intervalu

Omezí čas spuštění zálohování na zadaný interval.

Příklad

Společnost používá různá umístění ve stejném úložišti připojeném k síti k zálohování dat uživatelů a serverů. Pracovní den začíná v 8:00 a končí v 17:00. Data uživatelů by se měla zálohovat, jakmile se uživatelé odhlásí, ale nejdříve v 16:30. Servery společnosti se zálohují každý den ve 23:00. Data uživatelů by se proto měla zálohovat nejlépe před tímto časem, aby se uvolnila šířka pásma sítě. Předpokládá se, že zálohování dat uživatelů nezabere více než jednu hodinu, proto je poslední čas spuštění zálohování 22:00. Pokud je uživatel v zadaném časovém intervalu stále přihlášený nebo se odhlásí kdykoli jindy – nezálohovat data uživatele, tj. přeskočit provedení zálohy.

- Akce: **Když se uživatel odhlásí od systému.** Zadejte uživatelský účet: **Libovolný uživatel**.
- Podmínka: **Vyhovuje časovému intervalu** od **16:30** do **22:00**.
- Podmínky spuštění zálohování: **Přeskočit naplánovanou zálohu**

Výsledek:

(1) Odhlásí-li se uživatel mezi 16:30 a 22:00, zálohování se spustí okamžitě po odhlášení.

(2) Odhlásí-li se uživatel kdykoli jindy, zálohování se přeskočí.

8.4.2.5 Šetřit baterii

Zabrání zálohování, pokud není zařízení (přenosný počítač nebo tablet) připojené k napájecímu zdroji. Podle hodnoty možnosti zálohování Podmínky spuštění zálohování (str. 61) se vynechané zálohování spustí nebo nespustí po připojení zařízení k napájecímu zdroji. Dostupné jsou následující možnosti:

- **Nespouštět při napájení z baterie**

  Zálohování začne, pouze pokud je zařízení připojené k napájecímu zdroji.
- **Spustit při napájení z baterie, když je nabití baterie vyšší než**

  Zálohování začne, pouze pokud je zařízení připojené k napájecímu zdroji nebo je nabití baterie vyšší než zadaná hodnota.

Příklad

Data se zálohují každý den ve 21:00. Jestliže není zařízení připojené k napájecímu zdroji (například když má uživatel pozdní schůzku), je vhodné vynechat zálohování, ušetřit nabitou baterii a počkat, až uživatel připojí zařízení k napájecímu zdroji.

- Plánování: Denně, spouštět od pondělí do pátku. Spustit při: 21:00.
- Podmínka: **Šetřit baterii**, **Nespouštět při napájení z baterie**.
- Podmínky spuštění zálohování: **Čekat, než budou splněny podmínky**.

Výsledek:

(1) Pokud je 21:00 a zařízení je připojené k napájecímu zdroji, začne ihned zálohování.

(2) Pokud je 21:00 a zařízení se napájí z baterie, začne zálohování, jakmile se zařízení připojí k napájecímu zdroji.

8.4.2.6 Nespouštět při připojení účtovaném podle objemu dat

Zabrání zálohování (včetně zálohování na místní disk), je-li zařízení připojené k internetu pomocí připojení nastaveného v systému Windows jako účtované podle objemu dat. Další informace o připojeních účtovaných podle objemu dat naleznete na stránce https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

Další opatření, které zabrání zálohování přes mobilní hotspoty, je automatické zapnutí podmínky **Nespouštět při připojení k následujícím sítím Wi-Fi** zároveň se zapnutím podmínky **Nespouštět při připojení účtovaném podle objemu dat**. Ve výchozím nastavení se zadávají následující síťové názvy: „android“, „telefon“, „mobil“, a „modem“. Tyto názvy můžete ze seznamu odstranit kliknutím na znak X.

Příklad

Data se zálohují každý den ve 21:00. Je-li zařízení připojené k internetu pomocí připojení účtovaného podle objemu dat (například když je uživatel na služební cestě), je vhodné vynecháním zálohování snížit provoz sítě a počkat na plánované spuštění následující pracovní den.

- Plánování: Denně, spouštět od pondělí do pátku. Spustit při: 21:00.
- Podmínka: **Nespouštět při připojení účtovaném podle objemu dat**.
- Podmínky spuštění zálohování: **Přeskočit naplánovanou zálohu**

Výsledek:

(1) Pokud je 21:00 a zařízení není připojené k internetu pomocí připojení účtovaného podle objemu dat, začne ihned zálohování.

(2) Pokud je 21:00 a zařízení je připojené k internetu pomocí připojení účtovaného podle objemu dat, zálohování se spustí další pracovní den.

(3) Pokud je zařízení v pracovní dny ve 21:00 neustále připojené k internetu pomocí připojení účtovaného podle objemu dat, zálohování se nespustí nikdy.

8.4.2.7 Nespouštět při připojení k následujícím sítím Wi-Fi

Zabrání zálohování (včetně zálohování na místní disk), je-li zařízení připojené k jakékoli z uvedených bezdrátových sítí. Můžete zadat síťové názvy bezdrátových sítí Wi-Fi známých také jako SSID (Service Set Identifiers).

Toto omezení platí pro všechny sítě obsahující zadaný název jako podřetězec názvu bez rozlišení velikosti písmen. Zadáte-li například jako název sítě „telefon“, zálohování se nespustí, pokud je zařízení připojené k libovolné z následujících sítí: „Petrův telefon“, „telefon_wifi“ nebo „můj_wifi_telefon“.

Tato podmínka pomáhá zabránit zálohování, je-li zařízení připojené k internetu pomocí mobilního hotspotu.

Další opatření, které zabrání zálohování přes mobilní hotspoty, je automatické zapnutí podmínky **Nespouštět při připojení k následujícím sítím Wi-Fi** zároveň se zapnutím podmínky **Nespouštět při připojení účtovaném podle objemu dat**. Ve výchozím nastavení se zadávají následující síťové názvy:

„android“, „telefon“, „mobil“, a „modem“. Tyto názvy můžete ze seznamu odstranit kliknutím na znak X.

Příklad

Data se zálohují každý den ve 21:00. Je-li zařízení připojené k internetu pomocí mobilního hotspotu (například když je přenosný počítač připojený sdílením internetového připojení), je vhodné vynechat zálohování a počkat na plánované spuštění následující pracovní den.

- Plánování: Denně, spouštět od pondělí do pátku. Spustit při: 21:00.
- Podmínka: **Nespouštět při připojení k následujícím sítím**, **Název sítě**: `<SSID sítě hotspotu>`.
- Podmínky spuštění zálohování: **Přeskočit naplánovanou zálohu**

Výsledek:

(1) Pokud je 21:00 a počítač není připojený k dané síti, začne ihned zálohování.

(2) Pokud je 21:00 a počítač je připojený k dané síti, začne zálohování následující pracovní den.

(3) Pokud je počítač v pracovní dny ve 21:00 neustále připojený k dané síti, zálohování se nespustí nikdy.

8.4.2.8 Kontrolovat IP adresu zařízení

Zabrání zálohování (včetně zálohování na místní disk), spadá-li některá z IP adres zařízení do určeného rozsahu IP adres nebo je mimo něj. Dostupné jsou následující možnosti:

- **Spouštět vně rozsahu IP**
- **Spouštět uvnitř rozsahu IP**

V rámci každé možnosti lze určit více rozsahů. Jsou podporovány pouze adresy IPv4.

Tato podmínka pomůže vyhnout se vysokým poplatkům za přenos dat, pokud je uživatel v zahraničí. Pomáhá také zabránit zálohování přes připojení VPN (Virtual Private Network).

Příklad

Data se zálohují každý den ve 21:00. Je-li zařízení připojené k firemní síti pomocí tunelového připojení sítě VPN (například když uživatel pracuje z domu), je vhodné vynechat zálohování a počkat, až uživatel přinese zařízení do kanceláře.

- Plánování: Denně, spouštět od pondělí do pátku. Spustit při: 21:00.
- Podmínka: **Kontrolovat IP adresu zařízení**, **Spouštět vně rozsahu IP**, **Od**: `<začátek rozsahu IP adres sítě VPN>`, **Do**: `<konec rozsahu IP adres sítě VPN>`.
- Podmínky spuštění zálohování: **Čekat, než budou splněny podmínky**.

Výsledek:

(1) Pokud je 21:00 a IP adresa počítače není v zadaném rozsahu, začne ihned zálohování.

(2) Pokud je 21:00 a IP adresa počítače je v zadaném rozsahu, zálohování začne, jakmile zařízení získá IP adresu mimo síť VPN.

(3) Je-li v pracovní dny ve 21:00 IP adresa počítače neustále v zadaném rozsahu, zálohování se nespustí nikdy.

8.5 Pravidla zachování

1. Klikněte na možnost **Jak dlouho uchovávat**.
2. V okně **Vyčištění** vyberte jednu z následujících možností:
   - **Podle stáří zálohy** (výchozí)

     Určete, jak dlouho budou zálohy vytvořené plánem zálohování uchovány. Ve výchozím nastavení jsou pravidla zachování určena pro každou sadu záloh (str. 183) samostatně. Pokud chcete použít pro všechny zálohy jedno pravidlo, klikněte na možnost **Přepnout na jedno pravidlo pro všechny sady záloh**.
   - **Podle počtu záloh**

     Určete maximální počet záloh, které zůstanou zachovány.
   - **Zachovat zálohy na neurčito**

Co ještě potřebujete vědět

- Pokud je každá záloha uložená jako samostatný soubor podle schématu zálohování a formátu zálohy, nelze tento soubor odstranit, dokud nevyprší životnost všech závislých záloh (přírůstkových i rozdílových). Toto vyžaduje další prostor k ukládání záloh, jejichž odstranění je odloženo. Taktéž stáří zálohy a počet nebo velikost záloh může přesáhnout hodnoty, které jste určili.

  Toto chování je možné změnit pomocí možnosti zálohy Slučování záloh (str. 58).
- Pravidla zachování jsou součástí plánu zálohování. Přestanou pro zálohy počítače fungovat, jakmile je plán zálohování odejmut nebo odstraněn z počítače, nebo je ze zálohovací služby odstraněn samotný počítač. Pokud už nepotřebujete zálohy vytvořené podle plánu, odstraňte je podle pokynů v části Odstranění záloh (str. 114).

8.6 Replikace

Pokud povolíte replikaci záloh, každá záloha se ihned po vytvoření zkopíruje do druhého umístění. Pokud předchozí zálohy nebyly replikovány (například došlo ke ztrátě síťového spojení), aplikace replikuje také všechny zálohy, které se objevily po poslední úspěšné replikaci.

Replikované zálohy nezávisí na zbývajících zálohách v původním umístění a naopak. Je možné obnovit data z libovolné zálohy bez přístupu k dalším umístěním.

Příklady použití

- **Spolehlivá obnova po havárii**

  Ukládejte zálohy jak na místě (pro okamžitou obnovu) tak na jiném místě (pro ochranu záloh při selhání místního úložiště nebo při přírodní katastrofě).
- **Použití cloudového úložiště k ochraně dat při přírodní katastrofě**

  Replikujte zálohy do cloudového úložiště pouhým přenesením změn v datech.
- **Zachování pouze posledních bodů obnovy**

  Odstraněním starších záloh z rychlého úložiště podle pravidel zachování zabráníte přílišnému používání drahého prostoru úložiště.

Podporovaná umístění

Zálohu je možné replikovat *z* libovolného z následujících umístění:

- místní složka,
- síťová složka,

- Secure Zone

Zálohu je možné replikovat *do* libovolného z následujících umístění:

- místní složka,
- síťová složka,
- cloudové úložiště.

Jak povolit replikaci záloh

1. Na panelu plánu zálohování zapněte přepínač **Replikovat zálohy**.

   Tento přepínač se zobrazí, pouze pokud je replikace podporována z umístění vybraného v nabídce **Kam zálohovat**.
2. V okně **Kam replikovat** určete umístění replikace podle postupu popsaného v tématu "Výběr umístění" (str. 41).
3. V okně **Jak dlouho uchovávat** určete pravidla zachování podle postupu popsaného v tématu "Pravidla zachování" (str. 52).

8.7 Šifrování

Doporučujeme šifrovat všechny zálohy uložené v cloudovém úložišti, zvlášť pokud se na vaši společnost vztahují právní předpisy.

Důležité *Neexistuje žádný způsob, jak obnovit šifrované zálohy v případě ztráty hesla.*

Šifrování v plánu zálohování

Chcete-li povolit šifrování, určete nastavení šifrování při tvorbě plánu zálohování. Poté, co se plán zálohování použije, není možné upravit nastavení šifrování. Chcete-li použít jiná nastavení šifrování, vytvořte nový plán zálohování.

Jak určit nastavení šifrování v plánu zálohování

1. Na panelu plánu zálohování povolte přepínač **Šifrování**.
2. Určete a potvrďte heslo šifrování.
3. Vyberte jeden z následujících algoritmů šifrování:
   - **AES 128** – zálohy se šifrují pomocí algoritmu AES (Advanced Encryption Standard) se 128bitovým klíčem.
   - **AES 192** – zálohy se šifrují pomocí algoritmu AES se 192bitovým klíčem.
   - **AES 256** – zálohy se šifrují pomocí algoritmu AES s 256bitovým klíčem.
4. Klikněte na tlačítko **OK**.

Šifrování jako vlastnost počítače

Tato možnost je určena pro správce, kteří zpracovávají zálohy více počítačů. Pokud potřebujete u každého počítače jedinečné heslo šifrování nebo pokud potřebujete vynutit šifrování záloh bez ohledu na nastavení šifrování plánů zálohování, uložte nastavení šifrování jednotlivě na každém počítači. Zálohy se šifrují pomocí algoritmu AES s 256bitovým klíčem.

Uložení nastavení šifrování na počítači ovlivní plány zálohování následujícím způsobem:

- **Plány zálohování, které již byly na počítači použity.** Pokud je nastavení šifrování v plánu zálohování odlišné, zálohování se nezdaří.

- **Plány zálohování, které teprve budou na počítači použity.** Nastavení šifrování uložené na počítači přepíše nastavení šifrování v plánu zálohování. Všechny vytvořené zálohy budou šifrovány, a to i v případě, že je šifrování v nastavení plánu zálohování zakázáno.

Tuto možnost je možné použít na počítači, na kterém běží agent pro VMware. Postupujte však obezřetně v případě, kdy je ke stejnému serveru vCenter připojených o více agentů pro VMware. Pro všechny agenty je potřeba použít stejné nastavení šifrování, protože mezi nimi funguje určitý způsob vyrovnávání zatížení.

Po uložení nastavení šifrování lze tato nastavení podle níže uvedeného popisu měnit nebo obnovovat.

Důležité: *Pokud již plán zálohování běžící v tomto počítači vytvořil zálohy, změna nastavení šifrování způsobí, že se tento plán nezdaří. Chcete-li pokračovat v zálohování, vytvořte nový plán.*

Jak uložit nastavení šifrování na počítači

1. Přihlaste se k účtu správce (v systému Windows) nebo účtu root (v systému Linux).
2. Spusťte následující skript:
   - V systému Windows: `<installation_path>`**\PyShell\bin\acropsh.exe -m manage_creds --set-password** `<encryption_password>`

     `<installation_path>` je zde cestou instalace agenta zálohování. Ve výchozím nastavení je to **%ProgramFiles%\BackupClient**.
   - V systému Linux: **/usr/sbin/acropsh -m manage_creds --set-password** `<encryption_password>`

Jak resetovat nastavení šifrování na počítači

1. Přihlaste se k účtu správce (v systému Windows) nebo účtu root (v systému Linux).
2. Spusťte následující skript:
   - V systému Windows: `<installation_path>`**\PyShell\bin\acropsh.exe -m manage_creds --reset**

     `<installation_path>` je zde cestou instalace agenta zálohování. Ve výchozím nastavení je to **%ProgramFiles%\BackupClient**.
   - V systému Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Změna nastavení šifrování pomocí Sledování záloh

1. Přihlaste se v systému Windows nebo macOS jako správce.
2. V oznamovací oblasti (ve Windows) nebo na řádku nabídek (v macOS) klikněte na ikonu **Sledování záloh**.
3. Klikněte na ikonu ozubeného kola.
4. Klikněte na **Šifrování**.
5. Proveďte jeden z následujících úkonů:
   - Vyberte možnost **Nastavit konkrétní heslo pro tento počítač**. Určete a potvrďte heslo šifrování.
   - Vyberte možnost **Použít nastavení šifrování zadaná v plánu zálohování**.
6. Klikněte na tlačítko **OK**.

Jak funguje šifrování

Šifrovací algoritmus AES pracuje v režimu zřetězení číselných bloků (CBC) a používá náhodně generovaný klíč s uživatelem definovanou velikostí 128, 192 nebo 256 bitů. Čím větší je velikost klíče, tím déle bude programu trvat šifrování záloh a vaše data budou tím bezpečnější.

Šifrovací klíč je poté šifrován s algoritmem AES-256 pomocí hodnoty hashovací funkce SHA-256 hesla jako klíče. Samotné heslo není uloženo nikde na disku nebo v zálohách; hash hesla se používá pouze k ověřovacím účelům. S tímto dvouúrovňovým zabezpečením jsou data chráněna před neautorizovaným přístupem, ale obnovení ztraceného hesla není možné.

8.8 Spouštění zálohy ručně

1. Vyberte počítač, který má alespoň jeden použitý plán zálohování.
2. Klikněte na možnost **Zálohovat**.
3. Pokud je použito více plánů zálohování, vyberte plán zálohování.
4. Klikněte na možnost **Spustit** na panelu plánu zálohování.

Postup zálohy se zobrazuje ve sloupci **Stav** u daného počítače.

8.9 Možnosti zálohování

Chcete-li upravit možnosti zálohování, klikněte na ikonu ozubeného kola vedle názvu plánu zálohování a potom klikněte na možnost **Možnosti zálohování**.

Dostupnost možností zálohování

Sada dostupných možností zálohování závisí na:

- Prostředí, ve kterém agent pracuje (Windows, Linux, macOS)
- Typu zálohovaných dat (disky, soubory, virtuální počítače, data aplikací).
- Cílovému umístění zálohy (cloudové úložiště, místní nebo síťová složka).

Následující tabulka shrnuje dostupnost možností zálohování.

	Záloha na úrovni disku			**Zálohy na úrovni souborů**			**Virtuální počítače**			**SQL a Exchange**
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Výstrahy (str. 58)	+	+	+	+	+	+	+	+	+	+
Slučování záloh (str. 58)	+	+	+	+	+	+	+	+	+	-
Formát zálohy (str. 59)	+	+	+	+	+	+	+	+	+	+
Ověření zálohy (str. 60)	+	+	+	+	+	+	+	+	+	+
Podmínky spuštění zálohování (str. 61)	+	+	-	+	+	-	+	+	+	+

	Záloha na úrovni disku			Zálohy na úrovni souborů			Virtuální počítače			SQL a Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Sledování změněných bloků (CBT) (str. 61)	+	-	-	-	-	-	+	+	-	-
Úroveň komprese (str. 61)	+	+	+	+	+	+	+	+	+	+
Zpracování chyb (str. 62)										
Pokud dojde k chybě, pokusit se znovu	+	+	+	+	+	+	+	+	+	+
Při zpracování nezobrazovat zprávy a dialogová okna (tichý režim)	+	+	+	+	+	+	+	+	+	+
Ignorovat chybné sektory	+	+	+	+	+	+	+	+	+	-
Pokud dojde k chybě, pokusit se znovu při vytváření snímku virtuálního počítače	-	-	-	-	-	-	+	+	+	-
Rychlá přírůstková/rozdílová záloha (str. 63)	+	+	+	-	-	-	-	-	-	-
Snímky záloh na úrovni souborů (str. 64)	-	-	-	+	+	+	-	-	-	-
Filtry souborů (str. 63)	+	+	+	+	+	+	+	+	+	-
Zkrácení protokolu (str. 65)	-	-	-	-	-	-	+	+	-	Pouze SQL

	Záloha na úrovni disku			Zálohy na úrovni souborů			Virtuální počítače			SQL a Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Zachycování snímků LVM (str. 65)	-	+	-	-	-	-	-	-	-	-
Přípojné body (str. 65)	-	-	-	+	-	-	-	-	-	-
Snímek více svazků (str. 66)	+	+	-	+	+	-	-	-	-	-
Výkon (str. 66)	+	+	+	+	+	+	+	+	+	+
Odesílání fyzických dat (str. 67)	+	+	+	+	+	+	+	+	+	-
Příkazy před-po (str. 68)	+	+	+	+	+	+	+	+	+	+
Příkazy před/po získání dat (str. 69)	+	+	+	+	+	+	-	-	-	+
Plánování (str. 71)										
Rozložit čas spuštění do časového rámce	+	+	+	+	+	+	+	+	+	+
Omezení počtu souběžně spuštěných záloh	-	-	-	-	-	-	+	+	+	-
Zálohování sektor po sektoru (str. 72)	+	+	-	-	-	-	+	+	+	-
Rozdělování (str. 72)	+	+	+	+	+	+	+	+	+	+
Zpracování selhání úlohy (str. 72)	+	+	+	+	+	+	+	+	+	+
Služba Stínová kopie svazku (VSS) (str. 72)	+	-	-	+	-	-	-	+	-	+

	Záloha na úrovni disku			Zálohy na úrovni souborů			Virtuální počítače			SQL a Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Služba Stínová kopie svazku (VSS) pro virtuální počítače (str. 73)	-	-	-	-	-	-	+	+	-	-
Týdenní zálohování (str. 74)	+	+	+	+	+	+	+	+	+	+
Protokol událostí systému Windows (str. 74)	+	-	-	+	-	-	+	+	-	+

8.9.1 Výstrahy

Žádné úspěšné zálohy po určený počet po sobě jdoucích dní

Výchozí nastavení: **Zakázáno**.

Tato možnost určuje, zda bude generována výstraha v případě, že po zadané období nebudou v rámci plánu zálohování vytvořeny žádné úspěšné zálohy. Kromě nezdařených záloh software započítává také zálohy, které neproběhly podle plánu (chybějící zálohy).

Výstrahy jsou generovány pro jednotlivé počítače a jsou zobrazeny na kartě **Výstrahy**.

Můžete zadat počet po sobě jdoucích dnů bez zálohování, po kterém je generována výstraha.

8.9.2 Slučování záloh

Tato možnost určuje, zda zálohy během čištění slučovat nebo zda celé řetězce záloh odstraňovat.

Výchozí nastavení: **Zakázáno**.

Slučování je proces spojení dvou nebo více následných záloh do jedné.

Pokud tuto možnost zapnete, zálohy, které by se měly při čištění odstranit, se sloučí s další závislou zálohou (přírůstkovou nebo rozdílovou).

Jinak se záloha zachová až do chvíle, kdy budou všechny závislé zálohy označeny k odstranění. Tento režim zabraňuje potenciálně časově náročnému slučování, ale vyžaduje místo navíc pro ukládání záloh, jejichž odstranění je odloženo. Číslo nebo stáří záloh může překročit hodnoty určené v pravidlech pro zachování.

Důležité: *Mějte na paměti, že slučování je jen metodou odstranění a není alternativou k odstranění. Výsledná záloha nebude obsahovat data, která byla obsažena v odstraněné záloze a chyběla v zachovaných přírůstkových nebo rozdílových zálohách.*

Tato možnost *není* účinná, pokud:

- Cílem zálohy je cloudové úložiště.
- Schéma zálohování je nastaveno na možnost **Vždy přírůstkový (jeden soubor)**.
- Formát zálohy (str. 59) je nastavený na **Verze 12**.

Zálohy uložené v cloudovém úložišti a jednosouborové zálohy (ve formátech verzí 11 a 12) se vždy slučují, protože jejich vnitřní struktura umožňuje rychlé a snadné sloučení.

Při použití formátu verze 12 za přítomnosti více řetězců záloh (s každým řetězcem uloženým do samostatného souboru TIBX) bude sloučení fungovat pouze u posledního řetězce. Každý další řetězec bude celý odstraněn s výjimkou prvního, který se zmenší na minimální velikost, aby byla zachována metainformace (~12 kB). Tato metainformace je nutná k zajištění konzistence dat během souběžných operací čtení a zápisu. Zálohy zahrnuté v těchto řetězcích zmizí z GUI ihned po použití pravidla zachování, i když fyzicky existují, dokud není odstraněn celý řetězec.

Ve všech ostatních případech budou zálohy s odloženým odstraněním v GUI označeny ikonou odpadkového koše (). Pokud takovou zálohu odstraníte kliknutím na znak X, proběhne sloučení.

8.9.3 Formát zálohy

Tato možnost určuje formát záloh vytvořených plánem zálohování. Můžete se rozhodnout mezi novým formátem (**Verze 12**) navrženým pro rychlejší zálohování a obnovení a starším formátem (**Verze 11**) zachovaným za účelem zpětné kompatibility a pro speciální případy.

Tato možnost *není* dostupná pro zálohování webů, dat Office 365 a dat G Suite. Tyto zálohy budou mít vždy nový formát.

Výchozí nastavení: **Automatický výběr**.

Je možné vybrat jednu z následujících možností:

- **Automatický výběr**

  Pokud plán zálohování nepřipojuje zálohy k zálohám vytvořeným staršími verzemi produktu, bude použita verze 12.
- **Verze 12**

  Ve většině případů je v zájmu rychlého zálohování a obnovování doporučen nový formát. Každý řetězec záloh se uloží do jednoho souboru TIBX pro každý řetězec záloh (plná nebo rozdílová záloha a všechny závislé přírůstkové zálohy).
- **Verze 11**

  Starší formát se bude používat v novém plánu zálohování, který připojuje zálohy k zálohám vytvořeným staršími verzemi produktu.

  Tento formát také používejte (s libovolným schématem zálohování vyjma formátu **Vždy přírůstkový (jeden soubor)**, pokud chcete, aby plné, přírůstkové a rozdílové zálohy byly samostatné soubory.

Formát a soubory záloh

U umístění záloh, které je možné procházet pomocí správce souborů (například místní nebo síťové složky), určuje formát záloh počet souborů a jejich přípony. Následující tabulka uvádí soubory, které může vytvořit počítač nebo poštovní schránka.

	Vždy přírůstkový (jeden soubor)	**Jiná schémata zálohování**
Formát zálohy **Verze 11**	Jeden soubor TIB a jeden soubor metadat XML	Několik souborů TIB a jeden soubor metadat XML (běžný formát)
Formát zálohy **Verze 12**	Jeden soubor TIBX pro každý řetězec záloh (plná nebo rozdílová záloha a všechny závislé přírůstkové zálohy)	

Změna formátu zálohy

Zálohy na úrovni disku: Poté, co se použije plán zálohování, není možné formát zálohy změnit.

Zálohy na úrovni souborů a zálohy databází: Poté, co se použije plán zálohování, je možné změnit formát zálohy z **verze 11** na **verzi 12**. Reverzní operace není možná.

Pokud změníte formát zálohy:

- Další záloha bude plná.
- U umístění záloh, které je možné procházet pomocí správce souborů (například místní nebo síťové složky), bude vytvořen nový soubor s příponou .tibx. Nový soubor zálohy bude mít stejný název jako původní soubor, ale s příponou **_v12A**.
- Pravidla zachování a replikace se použijí pouze u nových záloh.
- Staré zálohy nebudou odstraněny. Budou nadále dostupné na kartě **Zálohy**. V případě potřeby je můžete odstranit ručně.
- Staré cloudové zálohy nebudou spotřebovávat **kvótu cloudového úložiště**.
- Staré místní zálohy budou spotřebovávat **kvótu místních záloh**, dokud je ručně neodstraníte.

8.9.4 Ověření zálohy

Ověřování je operace, která kontroluje možnost obnovy dat ze zálohy. Když je tato možnost zapnutá, každá záloha vytvořená v rámci plánu se po vytvoření okamžitě ověří.

Výchozí nastavení: **Zakázáno**.

Ověřování vypočítá kontrolní součet pro každý datový blok, který lze ze zálohy obnovit. Jedinou výjimkou je ověřování záloh na úrovni souborů, které jsou umístěny v cloudovém úložišti. Tyto zálohy se ověřují tak, že se zkontroluje konzistence metadat uložených v záloze.

Ověřování je časově náročný proces, a to i u přírůstkových nebo rozdílových záloh, které jsou malé. To proto, že operace ověří nejen data fyzicky obsažená v záloze, ale také data obnovitelná výběrem zálohy. K tomu je nezbytný přístup k dříve vytvořeným zálohám.

Zatímco úspěšné ověření znamená vysokou pravděpodobnost úspěšné obnovy, nekontrolují se všechny faktory, které ovlivňují proces obnovy. Pokud zálohujete operační systém, doporučujeme provést zkušební obnovení se spouštěcím médiem na náhradní pevný disk nebo spuštění virtuálního počítače z této zálohy (str. 164) v prostředí ESXi nebo Hyper-V.

8.9.5 Podmínky spuštění zálohování

Tato možnost má vliv v operačních systémech Windows a Linux.

Tato možnost určuje chování programu v případě, že má být spuštěna záloha (nastane naplánovaný čas nebo dojde k zadané události v plánu), ale podmínka (nebo více podmínek) není splněna. Další informace o podmínkách najdete v tématu Podmínky spuštění (str. 46).

Výchozí nastavení: **Čekat, než budou splněny podmínky.**

Čekat, než budou splněny podmínky.

V případě tohoto nastavení začne plánovač monitorovat podmínky, a jakmile budou splněny, spustí zálohování. Pokud nebudou podmínky splněny nikdy, nezačne nikdy ani zálohování.

Pro řešení situace, kdy podmínky nejsou splněny příliš dlouho a další odklad zálohování se stává rizikovým, můžete nastavit časový interval, po jehož uplynutí bude zálohování spuštěno bez ohledu na podmínku. Zaškrtněte políčko **Přesto spustit zálohování po** a zadejte časový interval. Zálohování se spustí, jakmile budou splněny podmínky NEBO jakmile uplyne maximální doba prodlevy (podle toho, co nastane jako první).

Přeskočit naplánovanou zálohu

Zpoždění zálohování může být nepřijatelné, pokud například potřebujete zálohovat data v přesně určený čas. V takovém případě může být místo čekání na splnění podmínek vhodnější zálohování přeskočit, a to zejména pokud zálohování probíhá relativně často.

8.9.6 Sledování změněných bloků (CBT)

Tato možnost platí pro zálohy na úrovni disků u virtuálních počítačů a fyzických počítačů se systémem Windows. Platí také pro zálohy databází Microsoft SQL Serveru a databází Microsoft Exchange Serveru.

Výchozí nastavení: **Povoleno**.

Tato možnost určuje, zda se při provádění přírůstkové nebo rozdílové zálohy použije sledování změněných bloků (CBT).

Technologie CBT zrychluje celý proces zálohování. Změny disku nebo obsahu databáze jsou neustále sledovány na úrovni bloků. Když začne zálohování, je možné změny do zálohy okamžitě uložit.

8.9.7 Úroveň komprese

Tato možnost určuje úroveň komprese, která se použije na zálohovaná data. Dostupné jsou následující úrovně: **Žádná**, **Normální**, **Vysoká**.

Výchozí nastavení: **Normální** –

Při vyšší úrovni komprese bude zálohování trvat déle, ale výsledná záloha zabere méně místa.

Optimální úroveň komprese dat závisí na typu dat, která jsou zálohována. Pokud záloha obsahuje komprimované soubory, například ve formátu JPG, PDF nebo MP3, velikost zálohy se příliš nezmenší ani při maximální kompresi. Formáty souborů DOC nebo XLS se však budou komprimovat dobře.

8.9.8 Zpracování chyb

Umožňují určit, jak se mají zpracovat chyby, které se mohou vyskytnou během zálohování.

Pokud dojde k chybě, pokusit se znovu

Výchozí nastavení: **Povoleno. Počet pokusů: 30. Intervaly mezi pokusy: 30 sekund.**

Když dojde k opravitelné chybě, aplikace se znovu pokusí provést neúspěšnou operaci. Je možné nastavit interval a počet pokusů. Pokusy budou ukončeny, jakmile se operace zdaří nebo dojde k vykonání zadaného počtu pokusů, podle toho, co nastane dřív.

Například pokud umístění zálohy v síti není k dispozici nebo není dosažitelné, aplikace se bude pokoušet o přístup k tomuto umístění každých 30 sekund, ale ne více než 30krát. Pokusy budou zastaveny, jakmile se obnoví spojení nebo bude dosaženo zadaného počtu pokusů, v závislosti na tom, co se nastane dříve.

Cloudové úložiště

Pokud jako cíl zálohy vyberete cloudové úložiště, nastaví se hodnota možnosti automaticky na **Povoleno**. **Počet pokusů: 300**. **Interval mezi pokusy: 30 sekund**.

V tomto případě je skutečný počet pokusů neomezený, ale časový limit do selhání zálohování se počítá takto: (300 sekund + **Interval mezi pokusy**) * (**Počet pokusů** + 1).

Příklady:

- Při použití výchozích hodnot selže zálohování po uplynutí (300 sekund + 30 sekund) * (300 + 1) = 99330 sekund, tedy ~27,6 hodin.
- Pokud nastavíte **Počet pokusů** na 1 a **Interval mezi pokusy** na 1 sekundu, selže zálohování po uplynutí (300 sekund + 1 sekunda) * (1 + 1) = 602 sekund, tedy ~10 minut.

Pokud vypočítaný časový limit přesahuje 30 minut a dosud nezačal přenos dat, nastaví se skutečný časový limit na 30 minut.

Při zpracování nezobrazovat zprávy a dialogová okna (tichý režim)

Výchozí nastavení: **Povoleno**.

S povoleným tichým režimem bude aplikace automaticky zpracovávat situace vyžadující zásah uživatele (kromě zpracování vadných sektorů, jenž je definováno jako samostatná možnost). Když operace nemůže bez zásahu uživatele pokračovat, nezdaří se. Podrobnosti o operaci včetně případných chyb lze nalézt v protokolu operace.

Ignorovat chybné sektory

Výchozí nastavení: **Zakázáno**.

Když je tato možnost vypnutá a program najde vadný sektor, přiřadí se aktivitě zálohování stav **Je nutný zásah uživatele**. Chcete-li zálohováním zachránit důležité informace z rychle se poškozujícího disku, zapněte ignorování chybných sektorů. Zbytek dat se zálohuje a vy budete moci připojit výslednou zálohu disku a extrahovat platné soubory na jiný disk.

Pokusit se znovu, pokud dojde k chybě při tvorbě snímku virtuálního počítače

Výchozí nastavení: **Povoleno. Počet pokusů: 3. Intervaly mezi pokusy: 5 minut.**

Když se tvorba snímku virtuálního počítače nezdaří, program se pokusí neúspěšnou operaci provést znovu. Je možné nastavit interval a počet pokusů. Pokusy budou ukončeny, jakmile se operace zdaří nebo dojde k vykonání zadaného počtu pokusů, podle toho, co nastane dřív.

8.9.9 Rychlá přírůstková/rozdílová záloha

Tato možnost platí pro přírůstkové a rozdílové zálohy na úrovni disku.

Výchozí nastavení: **Povoleno**.

Přírůstkové nebo rozdílové zálohy zaznamenávají pouze změny dat. Aby program proces zálohování urychlil, určí to, zda se soubor změnil nebo ne, podle velikosti a data a času poslední úpravy. Vypnutí této funkce způsobí, že program bude muset porovnat celý obsah souboru uloženého v záloze.

8.9.10 Filtry souborů

Filtry souborů definují soubory a složky, které se při zálohování mají přeskakovat.

Jsou dostupné pro zálohy na úrovni disků i souborů, pokud není uvedeno jinak.

Jak zapnout filtry souborů

1. Vyberte data k zálohování.
2. Klikněte na ikonu ozubeného kola vedle názvu plánu zálohování a potom na možnost **Možnosti zálohování**.
3. Vyberte možnost **Filtry souborů**.
4. Použijte některou z níže popsaných možností.

Vyloučit soubory splňující konkrétní kritéria

Existují dvě možnosti, které mají opačný účinek.

- **Zálohovat jen soubory splňující následující kritéria**

  Příklad: Pokud vyberete, že chcete zálohovat celý počítač, a zadáte do kritérií filtru **C:\Soubor.exe**, bude se zálohovat jen tento soubor.

  Poznámka: *Tento filtr nemá vliv na zálohy na úrovni souborů, pokud je jako **formát zálohy** (str. 59) vybrána možnost **Verze 11** a cílové umístění zálohy NENÍ cloudové úložiště.*

- **Nezálohovat soubory splňující následující kritéria**

  Příklad: Jestliže vyberete, že chcete zálohovat celý počítač, a zadáte do kritérií filtru **C:\Soubor.exe**, bude přeskočen jen tento soubor.

Je možné použít obě možnosti zároveň. Druhá možnost přepíše tu první; pokud tedy do obou polí zadáte **C:\Soubor.exe**, bude tento soubor při zálohování přeskočen.

Kritéria

- **Úplná cesta**

  Zadejte úplnou cestu k souboru nebo složce, počínaje písmenem jednotky (při zálohování systému Windows) nebo kořenovým adresářem (při zálohování systému Linux nebo macOS).

  V systémech Windows i Linux/macOS můžete v cestě k souboru nebo složce použít normální lomítka (například **C:/Temp/Soubor.tmp**). V systému Windows můžete také použít tradiční zpětné lomítko (například **C:\Temp\Soubor.tmp**).

- **Název**

Zadejte název souboru nebo složky, například **Dokument.txt**. Vyberou se všechny soubory a složky s tímto názvem.

Kritéria *nerozlišují* velikost písmen. Zadáte-li například **C:\Temp**, vyberou se i položky **C:\TEMP**, **C:\temp** a tak dále.

V kritériu můžete použít jeden nebo více zástupných znaků (*, ** a ?). Tyto znaky lze použít v úplné cestě i v názvu souboru nebo složky.

Znak hvězdičky (*) v názvu souboru nahrazuje nula nebo více znaků. Například kritérium **Doc*.txt** zahrnuje soubory jako **Doc.txt** a **Document.txt**

Dvě hvězdičky (*) v názvu souboru a cestě nahrazuje nula nebo více znaků. Například kritérium ****/Docs/**.txt** zahrnuje všechny soubory txt ve všech podsložkách všech složek **Docs**.

Znak otazníku (?) v názvu souboru nahrazuje přesně jeden znak. Kritérium **Doc?.txt** zahrnuje soubory jako **Doc1.txt** a **Docs.txt**, nikoli však soubory **Doc.txt** nebo **Doc11.txt**

Vyloučit skryté soubory a složky

Zaškrtnutím tohoto políčka lze přeskočit soubory a složky, které mají atribut **skryté** (u systémů souborů, které jsou podporovány systémem Windows) nebo které začínají znakem tečka (.) (u systémů souborů používaných systémem Linux, například Ext2 a Ext3). Pokud je složka skrytá, bude vyloučen veškerý její obsah (včetně souborů, které nejsou skryté).

Vyloučit systémové soubory a složky

Tato možnost platí pouze systémy souborů podporované systémem Windows. Výběrem tohoto zaškrtávacího políčka přeskočíte soubory a složky s nastaveným atributem **Systémový**. Jestliže má složka atribut **systémový**, veškerý její obsah (včetně souborů, které nemají atribut **systémové**) se vyloučí.

Tip *Atributy souboru nebo složky se zobrazují ve vlastnostech souboru nebo složky nebo je lze zobrazit pomocí příkazu attrib. Další informace získáte v Centru pro nápovědu a odbornou pomoc v systému Windows.*

8.9.11 Snímky záloh na úrovni souborů

Tato možnost platí pouze pro zálohy na úrovni souborů.

Definuje, zda se soubory mají zálohovat jeden po druhém nebo pořízením rychlého snímku dat.

Poznámka *Soubory uložené v síťových úložištích se vždy zálohují jeden po druhém.*

Výchozí nastavení:

- Poku jsou pro zálohování vybrány pouze čítače se systémem Linux: **Nevytvářet snímek**
- Ostatní případy: **Vytvořit snímek, pokud je to možné**

Je možné vybrat jednu z následujících možností:

- **Vytvořit snímek, pokud je to možné**

  Pokud získání snímku není možné, soubory se zálohují přímo.
- **Vždy vytvořit snímek**

  Snímek umožňuje zálohování všech souborů včetně souborů otevřených pro výhradní přístup. Soubory budou zálohovány ve stejném okamžiku. Toto nastavení vyberte pouze v případě, že tyto faktory jsou velmi důležité (tedy zálohování souborů bez snímku nedává smysl). Pokud nemůže být snímek získán, záloha se nezdaří.

- **Nevytvářet snímek**

  Soubory se vždy zálohují přímo. Pokus o zálohování souborů, které jsou otevřeny pro výhradní přístup způsobí chybu čtení. Soubory v záloze nemusí být časově konzistentní.

8.9.12 Zkrácení protokolu

Tato možnost platí pro zálohování databází serveru Microsoft SQL Server a pro zálohy na úrovni disku se zapnutým zálohováním aplikací Microsoft SQL Server.

Tato možnost určuje, zda se protokoly transakcí pro SQL Server po úspěšném zálohování zkrátí.

Výchozí nastavení: **Povoleno**.

Když je tato možnost zapnutá, lze databázi obnovit jen do bodu v čase zálohy vytvořené tímto softwarem. Vypněte tuto možnost, pokud zálohujete transakční protokoly pomocí nativního zálohovacího nástroje aplikace Microsoft SQL Server. Transakční protokoly budete moci použít po obnově a obnovit tak databázi do jakéhokoli bodu v čase.

8.9.13 Zachycování snímků LVM

Tato možnost platí pouze pro fyzické počítače.

Tato možnost je platná pro zálohy na úrovni disků při zálohování svazků spravovaných Správcem logických svazků systému Linux (LVM). Takové svazky se také nazývají logické svazky.

Tato možnost definuje způsob pořízení snímku logického svazku. Software může tyto operace provádět sám nebo pomocí Správce logických svazků systému Linux (LVM).

Výchozí nastavení: **Softwarem pro zálohování**.

- **Softwarem pro zálohování**. Data snímku se uchovávají převážně v RAM. Zálohování je rychlejší a nepřidělené místo ve skupině svazků není nutné. Proto doporučujeme měnit přednastavené hodnoty pouze v případě, že se setkáváte s problémy se zálohováním logických svazků.
- **Službou LVM**. Snímek je uložen v nepřiděleném místě ve skupině svazků. Pokud nepřidělené místo chybí, vytvoří snímek software pro zálohování.

8.9.14 Přípojné body

Tato možnost je účinná jen ve Windows pro zálohování zdrojů dat na úrovni souborů, které zahrnují připojené svazky nebo svazky sdílené v clusteru.

Tato možnost je účinná pouze v případě, že pro zálohování vyberete složku, která je v hierarchii složek výše než přípojný bod. (Přípojný bod je složka, ke které je logicky připojen další svazek.)

- Pokud je taková složka (nadřazená složka) vybrána k zálohování a možnost **Přípojné body** je zapnuta, budou všechny soubory umístěné na připojeném svazku zahrnuty do zálohy. Pokud je možnost **Přípojné body** vypnuta, bude v záloze přípojný bod prázdný.

  Obnovení obsahu přípojného bodu během obnovy nadřazené složky závisí na tom, jestli je zapnuta nebo vypnuta možnost obnovy **Přípojné body** (str. 91).
- Pokud vyberete přímo přípojný bod nebo složku v připojeném svazku, budou vybrané složky považovány za běžné složky. Budou zálohovány nezávisle na stavu možnosti **Přípojné body** a obnoveny nezávisle na stavu možnosti obnovy**Přípojné body** (str. 91).

Výchozí nastavení: **Zakázáno**.

Tip: *Zálohu virtuálních počítačů Hyper-V, které se nacházejí na svazku sdíleném v rámci clusteru, můžete provést zálohováním potřebných souborů nebo celého svazku na úrovni souborů. Je třeba pouze vypnout virtuální počítače, aby bylo jisté, že záloha bude provedena v konzistentním stavu.*

Příklad

Předpokládejme, že složka **C:\Data1** je přípojným bodem připojeného svazku. Svazek obsahuje složky **Složka1** a **Složka2**. Vytvoříte plán zálohování pro zálohu vašich dat na úrovni souborů.

Pokud vyberete svazek C a zapnete možnost **Přípojné body**, složka **C:\Data1** v záloze bude obsahovat složky **Složka1** a **Složka2**. Při obnově zálohovaných dat dávejte pozor na správné použití možnosti obnovy **Přípojné body** (str. 91).

Pokud zaškrtnete políčko pro svazek C a zrušíte zaškrtnutí možnosti **Přípojné body**, složka **C:\Data1** v záloze bude prázdná.

Pokud zaškrtnete políčko pro složku **Data1**, **Složka1** nebo **Složka2**, budou vybrané složky zahrnuty do zálohy jako obyčejné složky nezávisle na nastavení možnosti **Přípojné body**.

8.9.15 Snímek více svazků

Tato možnost platí pro zálohy fyzických počítačů se systémem Windows nebo Linux.

Tato možnost platí pro zálohy na úrovni disku. Platí také pro zálohy na úrovni souborů v případě, že jsou prováděny pořízením snímků. (Možnost Snímky záloh na úrovni souborů (str. 64) určuje, zda bude při zálohování na úrovni souborů pořízen snímek.)

Tato možnost určuje, zda se snímky více svazků budou vytvářet zároveň nebo po jednom.

Výchozí nastavení:

- Je-li k zálohování vybrán alespoň jeden počítač se systémem Windows: **Povoleno**.
- Ostatní případy: **Zakázáno**.

Když je tato možnost zapnutá, snímky všech zálohovaných svazků se budou vytvářet současně. Pomocí této možnosti lze vytvořit časově konzistentní zálohu dat rozložených ve více svazcích, například u databáze Oracle.

Pokud je tato možnost vypnutá, snímky svazků se budou vytvářet jeden po druhém. Jestliže jsou tedy data rozložena ve více svazcích, nemusí výsledná záloha být konzistentní.

8.9.16 Výkon

Priorita procesu

Tato možnost definuje prioritu procesu zálohování v operačním systému.

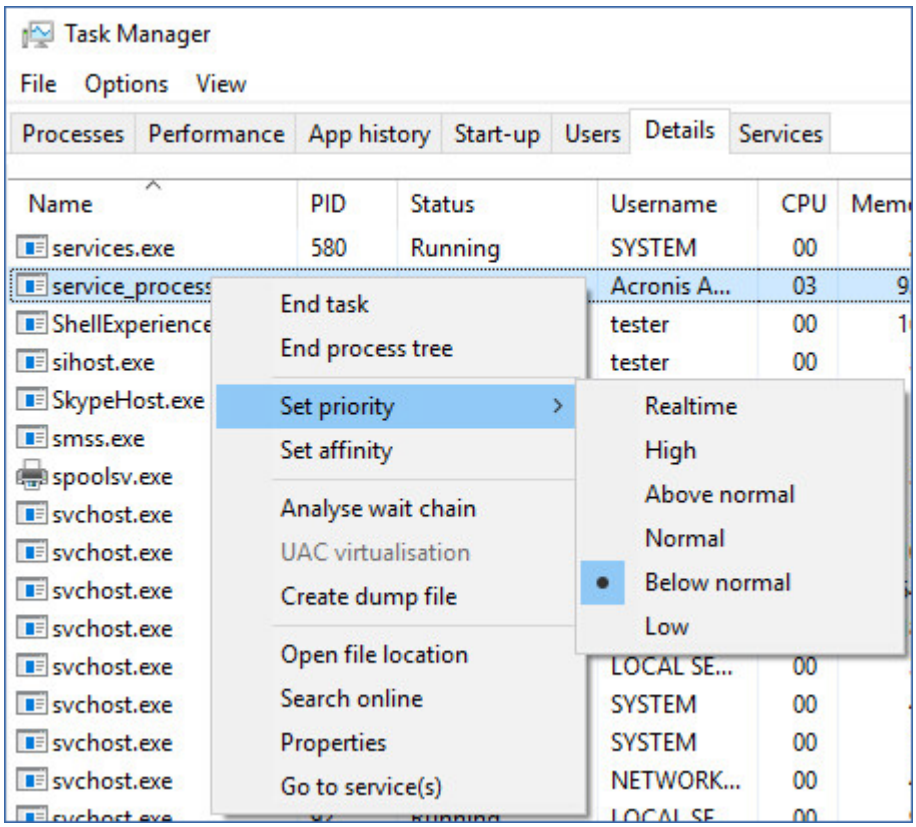
K dispozici jsou následující nastavení: **Nízká**, **Normální**, **Vysoká**.

Výchozí nastavení: **Nízká** (odpovídá nastavení **Nižší než normální** ve Windows).

Priorita procesu běžícího v systému určuje množství CPU a systémových zdrojů poskytnutých procesu. Snížením priority zálohy uvolníte více zdrojů pro další aplikace. Zvýšení priority zálohování může zrychlit proces zálohování žádostí, aby operační systém přidělil zálohovací aplikaci více zdrojů,

například procesor. Výsledek ovšem závisí na celkovém zatížení procesoru a dalších faktorech, například rychlosti čtení/zápisu disku nebo síťovém provozu.

Tato možnost nastavuje prioritu procesu zálohování ve Windows (**service_process.exe)** a v Linuxu a OS X (**service_process)**.



Výstupní rychlost při zálohování

Pomocí této možnosti lze omezit rychlost zápisu pevného disku (při zálohování do lokální složky) nebo rychlost přenosu dat zálohy přes síť (při zálohování do sdíleného síťového nebo cloudového úložiště).

Výchozí nastavení: **Zakázáno**.

Když je tato možnost zapnutá, můžete zadat maximální povolenou výstupní rychlost v kB/s.

8.9.17 Odesílání fyzických dat

Tato možnost je účinná, pokud je cílem umístěním zálohy cloudové úložiště a formát zálohy (str. 59) je nastaven na **verzi 12**.

Tato možnost je platná pro zálohy na úrovni disků a zálohy souborů vytvořené agentem pro Windows, agentem pro Linux, agentem pro Mac, agentem pro VMware, agentem pro Hyper-V a agentem pro Virtuozzo.

Tato možnost určuje, zda bude první plná záloha vytvořená plánem zálohování odeslána do cloudového úložiště na jednotce pevného disku pomocí služby Odesílání fyzických dat. Následující přírůstkové zálohy lze provést prostřednictvím sítě.

Výchozí nastavení: **Zakázáno**.

Informace o službě Odesílání fyzických dat

Webové rozhraní služby Odesílání fyzických dat je k dispozici pouze správcům.

Podrobné pokyny týkající se používání služby Odesílání fyzických dat a nástroje pro vytvoření objednávky naleznete v Příručce pro správce služby Odesílání fyzických dat. Tento dokument zpřístupníte ve webovém rozhraní služby Odesílání fyzických dat kliknutím na ikonu otazníku.

Přehled procesu odesílání fyzických dat

1. Vytvořte nový plán zálohování. V tomto plánu povolte možnost zálohování **Odesílání fyzických dat**.

   Zálohovat můžete přímo na jednotku nebo do místní či síťové složky a poté zálohu zkopírovat nebo přesunout na jednotku.

   Důležité *Po dokončení počáteční plné zálohy musí být následující zálohy provedeny stejným plánem zálohování. Další plán zálohování, a to i se stejnými parametry a pro stejný počítač, bude vyžadovat další cyklus odesílání fyzických dat.*

2. Po dokončení prvního zálohování použijte webové rozhraní služby Odesílání fyzických dat ke stažení nástroje pro vytvoření objednávky a vytvořte objednávku.

   Chcete-li přejít do webového rozhraní, přihlaste se k portálu pro správu, klikněte na kartu **Přehled** > **Použití** a poté klikněte na možnost **Spravovat službu** v části **Odesílání fyzických dat**.

3. Zabalte jednotky a odešlete je do datového centra.

   Důležité *Postupujte podle pokynů k balení uvedené v Příručce pro správce služby Odesílání fyzických dat.*

4. Stav objednávky můžete sledovat prostřednictvím webového rozhraní služby Odesílání fyzických dat. Mějte prosím na paměti, že následující zálohy selžou, dokud nebude počáteční záloha nahrána do cloudového úložiště.

8.9.18 Příkazy před-po

Tato možnost umožňuje určit příkazy, které se provedou automaticky před a po procesu zálohování

Následující schéma znázorňuje, kdy jsou příkazy před/po prováděny.

Příkaz před zálohou	Zálohování	Příkaz po záloze

Příklady, jak můžete používat příkazy před/po záloze:

- odstranit z disku dočasné soubory před spuštěním zálohy,
- nastavit antivirové programy od jiných dodavatelů, aby se spouštěly před spuštěním každé zálohy,
- Selektivně kopírovat zálohy do jiného umístění. Tato možnost může být užitečná, protože replikace nastavená v plánu zálohování kopíruje *každou* zálohu do následujících umístění.

Agent provede replikaci *po* vykonání příkazů, které se spouští po zálohování.

Tento program nepodporuje interaktivní příkazy, tedy příkazy, které vyžadují zásah uživatele (například „pause“).

8.9.18.1 Příkaz před zálohou

Jak zadat příkaz nebo dávkový soubor, který má být proveden před spuštěním procesu zálohování

1. Zapněte přepínač **Spustit příkaz před zálohováním**.

2. Do pole **Příkaz...** zadejte příkaz nebo vyhledejte dávkový soubor. Tento program nepodporuje interaktivní příkazy. To jsou příkazy, které vyžadují zásah uživatele (například "pause").
3. V textovém poli **Pracovní adresář** zadejte cestu k adresáři, kde bude spuštěn příkaz nebo dávkový soubor.
4. Pokud je to nutné, zadejte argumenty spouštěných příkazů do textového pole **Argumenty**.
5. Podle toho, jakého výsledku chcete dosáhnout, vyberte požadované možnosti (popsány jsou v tabulce).
6. Klikněte na tlačítko **Hotovo**.

Zaškrtávací políčko	**Nastavení**			
Nechat selhat úlohu zálohování, pokud selže vykonávání příkazu*	Zaškrtnuto	Nezaškrtnuto	Zaškrtnuto	Nezaškrtnuto
Neprovádět zálohu před dokončením provedení příkazu	Zaškrtnuto	Zaškrtnuto	Nezaškrtnuto	Nezaškrtnuto
Výsledek				
	Přednastaveno Provést zálohu pouze po úspěšném vykonání příkazu. Nechat selhat úlohu zálohování, pokud selže vykonávání příkazu.	Provést zálohu po vykonání příkazu, ať už vykonání příkazů bylo nebo nebylo úspěšné.	N/A	Provést zálohu současně s vykonáváním příkazu a bez ohledu na výsledek provedení příkazu.

Za selhání příkazu se považuje, pokud jeho návratový kód není roven nule.

8.9.18.2 Příkaz po záloze

Jak určit, aby byl příkaz/spustitelný soubor spuštěn po dokončení zálohy

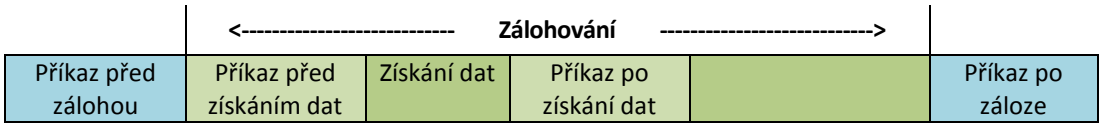
1. Zapněte přepínač **Spustit příkaz po zálohování**.
2. Do pole **Příkaz...** zadejte příkaz nebo vyhledejte dávkový soubor.
3. V textovém poli **Pracovní adresář** zadejte cestu k adresáři, kde bude spuštěn příkaz nebo dávkový soubor.
4. Pokud je to nutné, zadejte argumenty spouštěných příkazů do textového pole **Argumenty**.
5. Pokud je provedení příkazu velmi důležité, zaškrtněte políčko **Nechat selhat úlohu zálohování, pokud selže vykonávání příkazu**. Za selhání příkazu se považuje, pokud jeho ukončovací kód není roven nule. V případě, že provedení příkazu selže, stav zálohy bude nastaven na **Chyba**.

   Jestliže není toto políčko zaškrtnuto, výsledek provedení příkazu neovlivní úspěch nebo selhání zálohy. Výsledky spuštění příkazu můžete sledovat na kartě **Aktivity**.
6. Klikněte na tlačítko **Hotovo**.

8.9.19 Příkazy před/po získání dat

Tato možnost vám umožňuje určit příkazy, které se provedou automaticky před a po získání dat (tedy pořízení snímku dat). Získání dat se provádí na začátku procedury zálohování.

Následující schéma znázorňuje, kdy jsou příkazy před/po získání dat prováděny.



Pokud je zapnutá možnost (str. 72) stínové kopie svazku, spuštění příkazů a akcí VSS bude uspořádáno následovně:

Příkazy „před získáním dat“ -> pozastavení VSS -> získání dat -> obnovení VSS -> příkazy „po získání dat“.

Pomocí příkazů před/po získání dat můžete pozastavit a opět uvést do chodu databázi nebo aplikaci, která není kompatibilní se službou VSS. Protože získání dat trvá jen několik vteřin, bude doba nečinnosti databáze nebo aplikace minimální.

8.9.19.1 Příkaz před získáním dat

Jak zadat příkaz nebo dávkový soubor, který má být proveden před získáním dat

1. Zapněte přepínač **Spustit příkaz před získáním dat**.
2. Do pole **Příkaz...** zadejte příkaz nebo vyhledejte dávkový soubor. Tento program nepodporuje interaktivní příkazy. To jsou příkazy, které vyžadují zásah uživatele (například "pause").
3. V textovém poli **Pracovní adresář** zadejte cestu k adresáři, kde bude spuštěn příkaz nebo dávkový soubor.
4. Pokud je to nutné, zadejte argumenty spouštěných příkazů do textového pole **Argumenty**.
5. Podle toho, jakého výsledku chcete dosáhnout, vyberte požadované možnosti (popsány jsou v tabulce).
6. Klikněte na tlačítko **Hotovo**.

Zaškrtávací políčko	**Nastavení**			
Nechat selhat úlohu zálohování, pokud selže vykonávání příkazu*	Zaškrtnuto	Nezaškrtnuto	Zaškrtnuto	Nezaškrtnuto
Neprovádět získání dat před dokončením provedení příkazu	Zaškrtnuto	Zaškrtnuto	Nezaškrtnuto	Nezaškrtnuto
Výsledek				
	Přednastaveno Provést získání dat pouze po úspěšném vykonání příkazu. Nechat selhat úlohu zálohování, pokud selže vykonávání příkazu.	Provést získání dat po vykonání příkazu, ať už vykonání příkazů bylo nebo nebylo úspěšné.	N/A	Provést získání dat současně s příkazem a to bez ohledu na výsledek provedení příkazu.

Za selhání příkazu se považuje, pokud jeho návratový kód není roven nule.

8.9.19.2 Příkaz po získání dat

Jak zadat příkaz nebo dávkový soubor, který má být proveden po získání dat

1. Zapněte přepínač **Spustit příkaz po získání dat**.
2. Do pole **Příkaz...** zadejte příkaz nebo vyhledejte dávkový soubor. Tento program nepodporuje interaktivní příkazy. To jsou příkazy, které vyžadují zásah uživatele (například "pause").

3. V textovém poli **Pracovní adresář** zadejte cestu k adresáři, kde bude spuštěn příkaz nebo dávkový soubor.
4. Pokud je to nutné, zadejte argumenty spouštěných příkazů do textového pole **Argumenty**.
5. Podle toho, jakého výsledku chcete dosáhnout, vyberte požadované možnosti (popsány jsou v tabulce).
6. Klikněte na tlačítko **Hotovo**.

Zaškrtávací políčko	**Nastavení**			
Nechat selhat úlohu zálohování, pokud selže vykonávání příkazu*	Zaškrtnuto	Nezaškrtnuto	Zaškrtnuto	Nezaškrtnuto
Neprovádět zálohu před dokončením provedení příkazu	Zaškrtnuto	Zaškrtnuto	Nezaškrtnuto	Nezaškrtnuto
Výsledek				
	Přednastaveno Pokračování v záloze pouze po úspěšném vykonání příkazu.	Pokračovat v záloze po vykonání příkazu, ať už vykonání příkazu bylo nebo nebylo úspěšné.	N/A	Pokračování v záloze současně s vykonáváním příkazu, a to bez ohledu na výsledku provedení příkazu.

Za selhání příkazu se považuje, pokud jeho návratový kód není roven nule.

8.9.20 Plánování

Tato možnost určuje, zda se zálohování bude spouštět podle plánu nebo se zpožděním, a kolik virtuálních počítačů se bude zálohovat současně.

Výchozí nastavení: **Rozložit čas spuštění zálohy do časového rámce Maximální prodleva: 30 minut.**

Je možné vybrat jednu z následujících možností:

- **Spustit všechny zálohy přesně podle plánu**

  Zálohování fyzických počítačů začne přesně podle plánu. Virtuální počítače se budou zálohovat po jednom.
- **Rozložit čas spuštění do časového rámce**

  Zálohování fyzických počítačů začne se zpožděním proti naplánovanému času. Hodnota zpoždění u každého počítače se vybere náhodně a může být v rozsahu od nuly do maximální zadané hodnoty. Toto nastavení možná budete chtít použít při zálohování více počítačů do síťového umístění, abyste se vyhnuli nadměrnému zatížení sítě. Hodnota zpoždění každého počítače se určí po nasazení plánu zálohování do počítače a zůstane stejná, dokud neupravíte plán zálohování a nezměníte maximální hodnotu zpoždění.

  Virtuální počítače se budou zálohovat po jednom.
- **Omezit počet souběžně spuštěných záloh na**

  Tato možnost je dostupná pouze v případě, že plán zálohování použijete pro více virtuálních počítačů. Tato možnost určuje, kolik virtuálních počítačů může agent zálohovat současně při provádění daného plánu zálohování.

  Pokud podle plánu zálohování musí agent začít zálohovat více počítačů najednou, vybere dva počítače. (Agent se pokusí porovnat počítače uložené v různých úložištích tak, aby mohl optimalizovat výkon zálohování.) Jakmile je jedna z těchto záloh dokončena, agent vybere třetí počítač atd.

Počet virtuálních počítačů, které bude agent současně zálohovat, lze změnit. Maximální hodnota je 10. Pokud však agent provádí více plánů zálohování, které se překrývají v čase, sčítají se čísla uvedená v jejich možnostech zálohování. Můžete omezit celkový počet virtuálních počítačů (str. 178), které může agent současně zálohovat, bez ohledu na to, kolik plánů zálohování je spuštěno.

Zálohování fyzických počítačů začne přesně podle plánu.

8.9.21 Zálohování sektor po sektoru

Tato možnost má vliv pouze na zálohy na úrovni disku.

Tato možnost definuje, zda se vytvoří přesná kopie disku nebo svazku na fyzické úrovni.

Výchozí nastavení: **Zakázáno**.

Pokud je tato možnost zapnutá, budou se zálohovat všechny sektory disku nebo svazku včetně nepřiděleného místa a volných sektorů. Výsledná záloha bude mít stejnou velikost jako zálohovaný disk (pokud je možnost Úroveň komprese (str. 61) nastavena na **Žádná**). Software automaticky zapne režim sektor po sektoru při zálohování disků s nerozpoznanými nebo nepodporovanými systémy souborů.

8.9.22 Rozdělování

Tato možnost platí pro schémata zálohování **Vždy plná**, **Týdenní plná, denní přírůstková** a **Vlastní**.

Pomocí této možnosti je možné vybrat metodu rozdělování velkých záloh na menší soubory.

Výchozí nastavení: **Automaticky**.

K dispozici jsou následující nastavení:

- **Automaticky**

  Záloha bude rozdělena, pokud překročí maximální velikost souboru podporovanou systémem souborů.
- **Pevná velikost**

  Zadejte požadovanou velikost souboru nebo ji vyberte v rozbalovacím seznamu.

8.9.23 Zpracování selhání úlohy

Tato možnost určuje chování programu při selhání plánovaného provedení plánu zálohování. Tato možnost nemá vliv v případě, že plán zálohování je spuštěn ručně.

Pokud je zapnutá, program se pokusí plán zálohování provést znovu. Počet pokusů a časový interval mezi jednotlivými pokusy můžete určit. Pokusy budou ukončeny, jakmile se operace zdaří NEBO dojde k vykonání zadaného počtu pokusů, podle toho, co nastane dřív.

Výchozí nastavení: **Zakázáno**.

8.9.24 Služba Stínová kopie svazku (VSS)

Tato možnost platí pouze pro operační systémy Windows.

Možnost určuje, zda zprostředkovatel služby VSS musí upozorňovat aplikace se službou VSS, že bude spuštěno zálohování. Tím je zajištěn konzistentní stav dat používaných danou aplikací a zvláště dokončení všech transakcí databáze v okamžiku pořízení snímku dat pomocí softwaru pro zálohování.

Konzistence dat pak zajišťuje, že aplikace bude obnovena do správného stavu a bude funkční okamžitě po obnově.

Výchozí nastavení: **Povoleno**. **Automaticky vybrat zprostředkovatele snímku**.

Je možné vybrat jednu z následujících možností:

- **Automaticky vybrat zprostředkovatele snímku**

  Provede automatický výběr z hardwarových a softwarových zprostředkovatelů snímků a zprostředkovatele stínové kopie svazku Microsoft.
- **Použít zprostředkovatele stínové kopie svazku Microsoft**

  Při zálohování serverů aplikací (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint nebo Active Directory) doporučujeme vybrat tuto možnost.

Vypněte ji, pokud není vaše databáze kompatibilní se službou VSS. Pořizování snímků je rychlejší, ale konzistenci dat aplikací, jejichž operace nejsou dokončeny v čase vytvoření snímku, nelze zaručit. Pokud chcete zajistit zálohování dat v konzistentním stavu, můžete použít příkazy před/po získání dat (str. 69). Například zadejte příkazy před zachycením dat, které pozastaví databázi a vyprázdní všechny mezipaměti, aby bylo zajištěno, že veškeré transakce jsou dokončeny, a zadejte příkazy po zachycení dat, které po pořízení snímku opět spustí operace databáze.

Poznámka: *Je-li tato možnost povolená, soubory a složky uvedené v klíči registru* ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot*** *se nezálohují. Konkrétně se nezálohují offline datové soubory Outlooku (.ost), protože jsou uvedené v hodnotě* ***OutlookOST*** *tohoto klíče.*

Zapnout úplné zálohování služby VSS

Pokud je tato možnost zapnuta, protokoly aplikace Microsoft Exchange Server a ostatních aplikací s podporou VSS (kromě Microsoft SQL Server) se zkrátí po každé plné, přírůstkové nebo rozdílové záloze na úrovni disku.

Výchozí nastavení: **Zakázáno**.

Tuto možnost ponechte zakázanou v následujících případech:

- Jestliže zálohujete data serveru Exchange Server pomocí agenta Agent pro Exchange nebo softwaru třetích stran. To proto, že zkracování protokolů bude kolidovat s následnými zálohami transakčních protokolů.
- Pokud zálohu dat serveru SQL provádíte pomocí softwaru externích dodavatelů: Důvodem je to, že software externích dodavatelů převezme výslednou zálohu na úrovni disku jako „vlastní“ plnou zálohu. Tím způsobí selhání další rozdílové zálohy dat serveru SQL. Zálohy budou selhávat do doby, kdy si software externího dodavatele vytvoří další „vlastní“ plnou zálohu.
- Pokud jsou v počítači spuštěny aplikace s podporou VSS a potřebujete z jakéhokoli důvodu zachovat jejich protokoly.

Povolení této možnosti nezkrátí protokoly aplikace Microsoft SQL Server. Chcete-li po zálohování zkrátit protokol SQL Serveru, zapněte možnost zálohy Zkrácení protokolu (str. 65).

8.9.25 Služba Stínová kopie svazku (VSS) pro virtuální počítače

Tato možnost určuje, kdy se pořizují snímky virtuálních počítačů ve stavu nečinnosti. Při pořizování takového snímku software použije službu VSS ve virtuálním počítači pomocí integračních služeb VMware Tools nebo Hyper-V.

Výchozí nastavení: **Povoleno**.

Pokud je tato možnost zapnutá, provedou se před pořízením snímku transakce všech aplikací s podporou VSS ve virtuálním počítači. Pokud tvorba snímku ve stavu nečinnosti selže po provedených opakovaných pokusech v počtu určeném v možnosti Zpracování chyb (str. 62) a zálohování aplikací je vypnuto, vytvoří se snímek mimo stav nečinnosti. Pokud je zapnuto zálohování aplikací, záloha selže.

Pokud je tato možnost vypnutá, vytvoří se snímek mimo stav nečinnosti. Virtuální počítač se bude zálohovat ve stavu konzistentním s havárií.

8.9.26 Týdenní zálohování

Tato možnost určuje, které zálohy se u pravidel zachování a schémat zálohování považují za týdenní. Týdenní záloha je první záloha vytvořená po začátku týdne.

Výchozí nastavení: **Pondělí**.

8.9.27 Protokol událostí systému Windows

Tato možnost platí pouze pro operační systémy Windows.

Tato možnost určuje, zda má agent zaznamenávat události operací zálohování do protokolu událostí aplikací ve Windows (protokol zobrazíte tak, že spustíte eventvwr.exe nebo vyberete **Ovládací panely** > **Nástroje pro správu** > **Prohlížeč událostí**). Zaznamenávané události můžete filtrovat.

Výchozí nastavení: **Zakázáno**.

9 Obnova

9.1 Shrnutí metod obnovy

V následující tabulce jsou shrnuty dostupné možnosti obnovy. Pomocí této tabulky si můžete vybrat metodu, která vám nejlépe vyhovuje.

Co obnovovat	Metoda obnovení
Fyzický počítač (Windows nebo Linux)	Pomocí webového rozhraní (str. 76) Pomocí spouštěcích médií (str. 80)
Fyzický počítač (Mac)	Pomocí spouštěcích médií (str. 80)
Fyzický počítač (VMware nebo Hyper-V)	Pomocí webového rozhraní (str. 78) Pomocí spouštěcích médií (str. 80)
Virtuální počítač nebo kontejner (Virtuozzo)	Pomocí webového rozhraní (str. 78)
Konfigurace ESXi	Pomocí spouštěcích médií (str. 87)
Soubory/složky	Pomocí webového rozhraní (str. 83) Stahování souborů z cloudového úložiště (str. 84) Pomocí spouštěcích médií (str. 86) Extrahování souborů z místních záloh (str. 87)
Stav systému	Pomocí webového rozhraní (str. 87)
Databáze SQL	Pomocí webového rozhraní (str. 124)
Databáze Exchange	Pomocí webového rozhraní (str. 127)
Poštovní schránky Exchange	Pomocí webového rozhraní (str. 128)

Co obnovovat		Metoda obnovení
Webové stránky		Pomocí webového rozhraní (str. 162)
Microsoft Office 365	Poštovní schránky (místní agent pro Office 365)	Pomocí webového rozhraní (str. 134)
	Poštovní schránky (cloudový agent pro Office 365)	Pomocí webového rozhraní (str. 137)
	Soubory na OneDrivu	Pomocí webového rozhraní (str. 140)
	Data v SharePointu Online	Pomocí webového rozhraní (str. 144)
G Suite	Poštovní schránky	Pomocí webového rozhraní (str. 149)
	Soubory Disku Google	Pomocí webového rozhraní (str. 152)
	Soubory Týmových disků	Pomocí webového rozhraní (str. 155)

Poznámka pro uživatele počítačů Mac

- Počínaje OS X 10.11 El Capitan jsou některé systémové soubory, složky a procesy označeny pomocí rozšířeného souborového atributu com.apple.rootless jako chráněné. Tato funkce se nazývá ochrana integrity systému. Mezi chráněné soubory patří předinstalované aplikace a většina obsahu složek /system, /bin, /sbin, /usr.

  Chráněné soubory a složky se nedají přepsat během obnovy spuštěné z operačního systému. Abyste chráněné soubory mohli přepsat, spusťte obnovu ze spouštěcího média.
- Počínaje macOS Sierra 10.12 mohou být zřídka používané soubory přesunuty do služby iCloud pomocí funkce Store in Cloud (Uložit v cloudu). V souboru systému jsou o těchto souborech uchovávána určitá data. Tato data jsou zálohována místo původních souborů.

  Když je obnovíte data o přesunutém souboru do původního umístění, jsou údaje synchronizovány se službou iCloud a zpřístupní se původní soubor. Když je obnovíte data o přesunutém souboru do jiného umístění, nelze údaje synchronizovat a původní soubor nebude dostupný.

9.2 Tvorba spouštěcího média

Spouštěcí médium je CD, DVD, USB flash disk nebo jiné vyměnitelné médium, které umožňuje spuštění agenta bez operačního systému. Hlavním účelem spouštěcího média je obnovení operačního systému, který nelze spustit.

Důrazně doporučujeme, abyste si vytvořili a otestovali spouštěcí médium, jakmile začnete používat zálohy na úrovni disku. Je také dobré médium znovu vytvořit po každé větší aktualizaci agenta pro zálohování.

Pomocí stejného média je možné obnovit systém Windows i Linux. Chcete-li obnovit systém macOS, vytvořte samostatné médium na počítači se systémem macOS.

Jak vytvořit spouštěcí média v systému Windows nebo Linux

1. Stáhněte si soubor ISO spouštěcího média. Pokud chcete soubor stáhnout, vyberte počítač a klikněte na **Obnovit** > **Více způsobů obnovy...** > **Stáhnout obraz ISO**.
2. [Volitelné] Zkopírujte a vytiskněte si nebo si poznamenejte registrační token, který zobrazí konzola pro zálohování.

   Tento token umožňuje přístup ke cloudovému úložišti ze spouštěcího média bez zadání přihlašovacího jména a hesla. Potřebujete ho, pokud nemáte přímý přístup do cloudu, ale používáte externí ověřování.
3. Proveďte jeden z následujících úkonů:
   - Vypalte CD nebo DVD pomocí souboru ISO.

- Vytvořte spouštěcí USB flash disk pomocí souboru ISO a některého z nástrojů volně dostupných online.

  Použijte nástroj `ISO to USB` nebo RUFUS, pokud chcete spouštět počítač UEFI, nebo `Win32DiskImager` pro počítač, kde je BIOS. V Linuxu je možné použít nástroj `dd`.
- Připojte soubor ISO jako CD nebo DVD jednotku k virtuálnímu počítači, který chcete obnovit.

Vytvoření spouštěcího média v systém macOS

1. Na počítači s nainstalovaným Agentem pro Mac klikněte na **Aplikace** > **Tvůrce záchranných médií**.
2. Software zobrazí připojená vyměnitelná média. Vyberte to, které chcete nastavit jako spouštěcí.

   Upozornění *Všechna data na disku budou smazána.*
3. Klikněte na tlačítko **Vytvořit**.
4. Počkejte, až software spouštěcí médium vytvoří.

9.3 Obnovení počítače

9.3.1 Fyzický počítač

Tato část popisuje obnovu fyzických počítačů pomocí webového rozhraní.

Použijte spouštěcí médium namísto webového rozhraní v případě, že potřebujete obnovit:

- OS X.
- Jakýkoli operační systém na holé železo nebo na počítač ve stavu offline.

Obnova operačního systému vyžaduje restart. Je možné vybrat, zda se má počítač restartovat automaticky, nebo přiřadit stav **Je nutný zásah uživatele**. Obnovený operační systém automaticky přejde do stavu online.

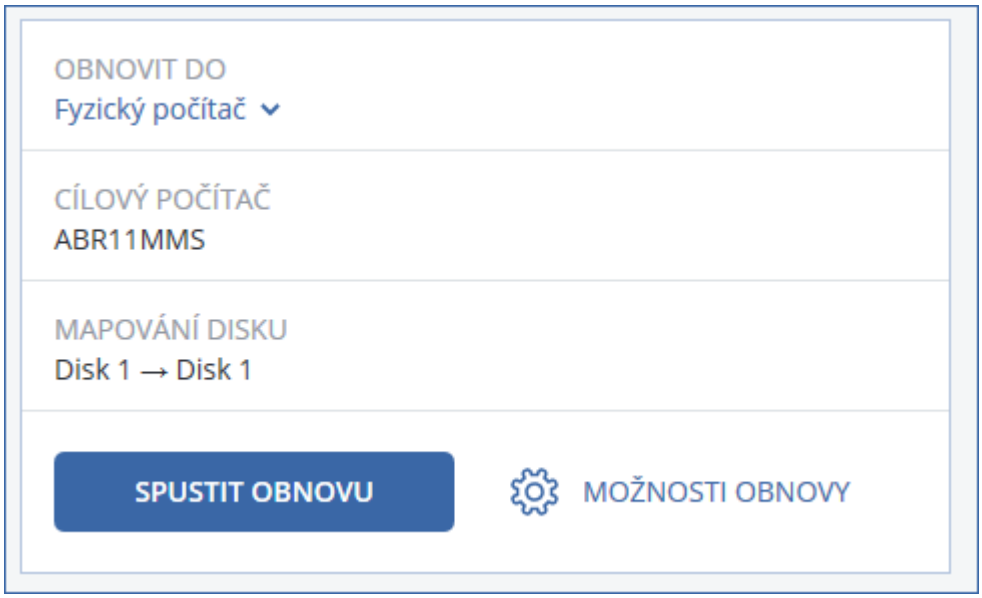
Jak obnovit fyzický počítač

1. Vyberte zálohovaný počítač.
2. Klikněte na možnost **Obnova**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Proveďte jeden z následujících úkonů:
   - Pokud se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte cílový počítač ve stavu online a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Zálohy (str. 112).
   - Obnovte počítač podle postupu popsaného v tématu Obnova disků pomocí spouštěcího média (str. 80).
4. Klikněte na **Obnovit** > **Celý počítač**.

   Software automaticky namapuje disky ze zálohy na disky cílového počítače.
   - Chcete-li obnovit další fyzický počítač, klikněte na možnost **Cílový počítač** a poté vyberte cílový počítač ve stavu online.

- Jestliže mapování disků selže, obnovte počítač podle postupu popsaného v tématu Obnova disků pomocí spouštěcího média (str. 80). Médium vám umožní vybrat disky k obnově a namapovat disky ručně.



5. Klikněte na možnost **Spustit obnovu**.
6. Potvrďte, že chcete přepsat disky jejich zálohovanými verzemi. Vyberte, zda se má počítač automaticky restartovat.

Postup obnovy se zobrazuje na kartě **Aktivity**.

9.3.2 Fyzický počítač na virtuální

Tato část popisuje obnovu fyzického počítače jako virtuálního počítače pomocí webového rozhraní. Tuto operaci je možné provést, pokud je nainstalován a registrován alespoň jeden agent pro VMware nebo agent pro Hyper-V.

Další informace o migraci P2V naleznete v tématu Migrace počítače (str. 172).

Jak obnovit fyzický počítač jako virtuální počítač

1. Vyberte zálohovaný počítač.
2. Klikněte na možnost **Obnova**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Proveďte jeden z následujících úkonů:

   - Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte počítač ve stavu online a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Zálohy (str. 112).
   - Obnovte počítač podle postupu popsaného v tématu Obnova disků pomocí spouštěcího média (str. 80).
4. Klikněte na **Obnovit** > **Celý počítač**.
5. V poli **Obnovit na** vyberte **Virtuální počítač**.
6. Klikněte na možnost **Cílový počítač**.
   a. Vyberte hypervisor (**VMware ESXi** nebo **Hyper-V**).

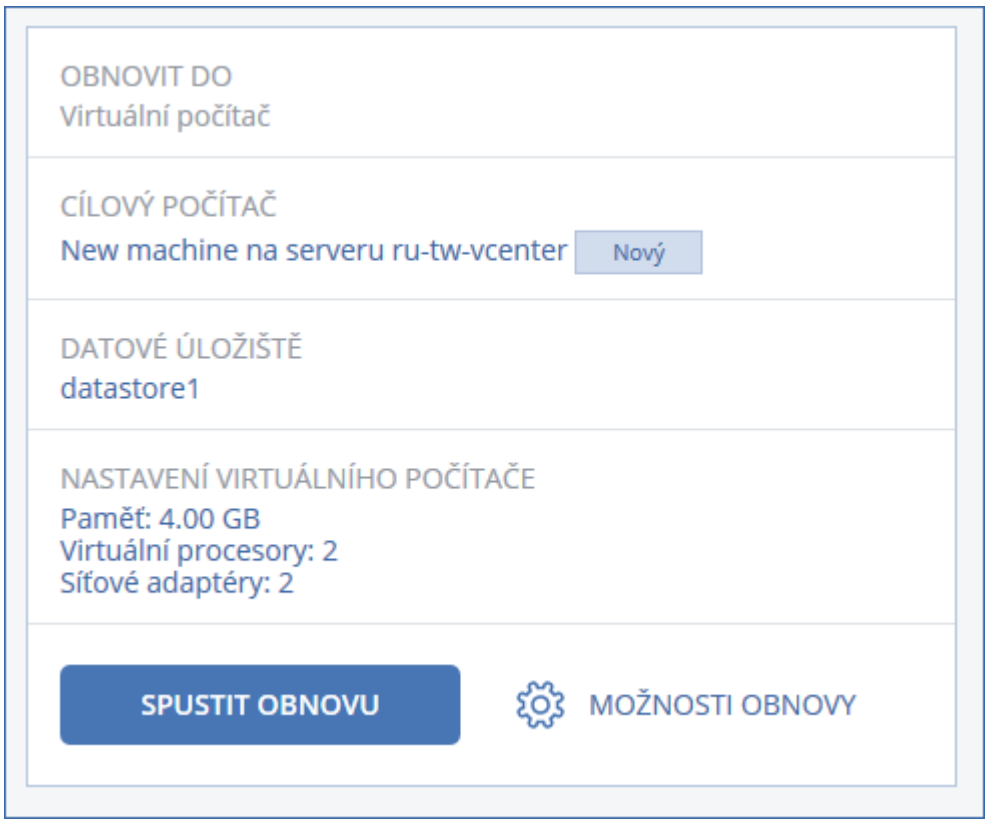
      Je nutné, aby byl nainstalován alespoň jeden agent pro VMware nebo agent pro Hyper-V.

b. Vyberte, zda se má provést obnova na nový, nebo existující počítač. Je doporučena možnost nového počítače, protože nevyžaduje, aby se konfigurace disků cílového počítače přesně shodovala s konfigurací disku v záloze.

c. Vyberte hostitele a určete název nového počítače, případně vyberte existující cílový počítač.

d. Klikněte na tlačítko **OK**.

7. [Volitelné] Při obnově na nový počítač je také možné provést následující úkony:
   - Klikněte na možnost **Datové úložiště** u ESXi nebo na možnost **Cesta** u Hyper-V a poté vyberte datové úložiště virtuálního počítače.
   - Pomocí možnosti **Nastavení virtuálního počítače** změňte velikost paměti, počet procesorů a síťová připojení virtuálního počítače.



8. Klikněte na možnost **Spustit obnovu**.
9. Při obnově na existující virtuální počítač potvrďte, že chcete přepsat disky.

Postup obnovy se zobrazuje na kartě **Aktivity**.

9.3.3 Virtuální počítač

Virtuální počítač je nutné zastavit během obnovy na tento počítač. Software zastaví počítač bez dalších výzev. Jakmile je obnova dokončena, je třeba počítač ručně spustit.

Toto chování je možné změnit pomocí možnosti obnovy Správa napájení VM (klikněte na možnost **Možnosti obnovy** > **Správa napájení VM**).

Jak obnovit virtuální počítač

1. Proveďte jeden z následujících úkonů:
   - Vyberte zálohovaný počítač, klikněte na možnost **Obnova** a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Zálohy (str. 112).

2. Klikněte na možnost **Obnovit**>**Celý počítač**.
3. Pokud chcete obnovit fyzický počítač, vyberte možnost **Fyzický počítač** v okně **Obnovit na**. Jinak tento krok přeskočte.

   Obnova na fyzický počítač je možná pouze, pokud se konfigurace disku cílového počítače přesně shoduje s konfigurací disku v záloze.

   V takovém případě pokračujte krokem 4 v tématu "Fyzický počítač" (str. 76). Jinak doporučujeme provést V2P migraci pomocí spouštěcího média (str. 80).
4. Software automaticky vybere původní počítač jako cílový.

   Chcete-li obnovit další virtuální počítač, klikněte na možnost **Cílový počítač** a poté proveďte následující úkony:

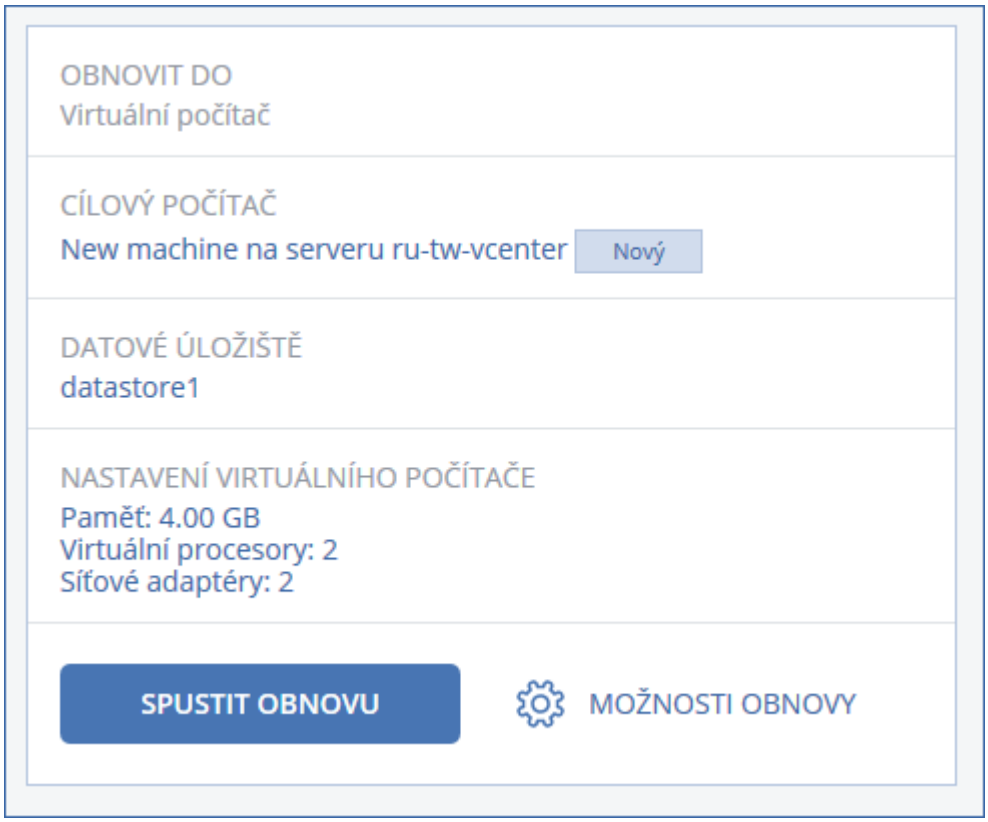
   a. Vyberte hypervisor (**VMware ESXi**, **Hyper-V** nebo **Virtuozzo**).

      Virtuální počítače Virtuozzo je možné obnovit pouze na Virtuozzo. Další informace o V2V migraci naleznete v tématu "Migrace počítače" (str. 172).

   b. Vyberte, zda se má provést obnova na nový, nebo existující počítač.

   c. Vyberte hostitele a určete název nového počítače, případně vyberte existující cílový počítač.

   d. Klikněte na tlačítko **OK**.
5. [Volitelné] Při obnově na nový počítač je také možné provést následující úkony:
   - Klikněte na možnost **Datové úložiště** u ESXi nebo na možnost **Cesta** u Hyper-V a poté vyberte datové úložiště virtuálního počítače.
   - Pomocí možnosti **Nastavení virtuálního počítače** změňte velikost paměti, počet procesorů a síťová připojení virtuálního počítače.



6. Klikněte na možnost **Spustit obnovu**.
7. Při obnově na existující virtuální počítač potvrďte, že chcete přepsat disky.

Postup obnovy se zobrazuje na kartě **Aktivity**.

9.3.4 Obnovení disků pomocí spouštěcích médií

Informace o tvorbě spouštěcích médií naleznete v tématu Tvorba spouštěcího média (str. 75).

Jak obnovit disky pomocí spouštěcích médií

1. Spusťte cílový počítač pomocí spouštěcích médií.
2. [Pouze při obnově počítače Mac] Pokud obnovujete disky/svazky formátu APFS na jiný než původní počítač nebo na počítač bez operačního systému, ručně znovu vytvořte původní konfiguraci disků:
   a. Klikněte na možnost **Nástroj Disk**.
   b. Znovu vytvořte původní konfiguraci disků. Další informace naleznete na stránce https://support.apple.com/guide/disk-utility/welcome.
   c. Klikněte na možnost **Nástroj Disk** > **Ukončit nástroj Disk**.
3. Klikněte na možnost **Místní správa tohoto počítače** nebo dvakrát klikněte na možnost **Spouštěcí záchranná média** (podle typu média, které používáte).
4. Pokud je v síti zapnutý proxy server, klikněte na **Nástroje** > **Proxy server** a zadejte název hostitele nebo IP adresu, port a přihlašovací údaje proxy serveru. Jinak tento krok přeskočte.
5. [Volitelné] Pokud obnovujete systém Windows nebo Linux, klikněte na **Nástroje** > **Zaregistrovat médium ve službě zálohování** a zadejte registrační token, který jste získali při stahování média. Když to uděláte, nebudete muset při přístupu ke cloudovému úložišti zadávat přihlašovací údaje ani registrační kód (viz popis kroku č. 8).
6. V uvítacím okně klikněte na možnost **Obnovit**.
7. Klikněte na **Označit data** a poté klikněte na **Procházet**.
8. Určete umístění zálohy:
   - Chcete-li provést obnovení z cloudového úložiště, vyberte možnost **Cloudové úložiště**. Zadejte pověření k účtu, ke kterému je zálohovaný počítač přiřazen.

     Při obnovení Windows nebo Linuxu můžete požádat o registrační kód a použít ho místo přihlašovacích údajů. Klikněte na **Použijte registrační kód** > **Požádat o kód**. Software zobrazí registrační odkaz a registrační kód. Můžete je zkopírovat a provést registrační kroky na jiném počítači. Registrační kód je platný jednu hodinu.
   - Pokud chcete provést obnovení z místní nebo síťové složky, vyhledejte ji v části **Místní složky** nebo **Síťové složky**.

   Kliknutím na tlačítko **OK** potvrdíte váš výběr.
9. Vyberte zálohu, ze které chcete data obnovit. Pokud se zobrazí výzva, zadejte heslo zálohy.
10. V části **Obsah zálohy** vyberte disky, které chcete obnovit. Kliknutím na tlačítko **OK** potvrdíte váš výběr.
11. V části **Kam obnovit** software automaticky mapuje vybrané disky na cílové disky.

    Pokud nebudete spokojeni s výsledkem mapování nebo se mapování nezdaří, můžete disky znovu mapovat ručně.

    Změna rozvržení disků může ovlivnit schopnost operačního systému se spustit. Pokud si nejste zcela jisti úspěšností operace, použijte původní rozvržení disků.
12. [Při obnově systému Linux] Pokud zálohovaný počítač obsahoval logické svazky (LVM) a chcete reprodukovat původní strukturu LVM:
    a. Zkontrolujte, že počet disků v cílovém počítači a kapacita každého z nich jsou shodné nebo vyšší než v původním počítači, a klikněte na možnost **Použít RAID/LVM**.
    b. Zkontrolujte strukturu svazku a kliknutím na **Použít RAID/LVM** strukturu vytvořte.

13. [Volitelné] Klikněte na možnost **Možnosti obnovy** a určete další nastavení.
14. Kliknutím na tlačítko **OK** spusťte obnovu.

9.3.5 Použití technologie Universal Restore

Nejnovější operační systémy zůstávají spustitelné i při obnovení na odlišném hardwaru včetně platforem VMware či Hyper-V. Jestliže se obnovený operační systém nespustí, aktualizujte pomocí nástroje Universal Restore ovladače a moduly nezbytné pro spuštění operačního systému.

Funkci Universal Restore lze použít v systémech Windows a Linux.

Jak použít funkci Universal Restore

1. Spusťte počítač ze spouštěcího média.
2. Klikněte na možnost **Použít doplněk Universal Restore**.
3. Pokud máte v počítači více operačních systémů, vyberte si jeden z nich, na který se použije nástroj Universal Restore.
4. [Pouze ve Windows] Konfigurujte další nastavení (str. 81).
5. Klikněte na tlačítko **OK**.

9.3.5.1 Nástroj Universal Restore v systému Windows

Příprava

Příprava ovladačů

Před použitím nástroje Universal Restore v operačním systému Windows se ujistěte, že máte k dispozici ovladače pro nový řadič pevného disku a čipovou sadu. Tyto ovladače jsou rozhodující pro spuštění operačního systému. Použijte CD nebo DVD poskytované dodavatelem hardwaru nebo stáhněte ovladače z jeho webových stránek. Soubory ovladačů by měly mít příponu INF. Pokud stáhnete ovladače ve formátu EXE, CAB nebo ZIP, rozbalte je pomocí příslušných aplikací.

Osvědčeným postupem je uchovávat ovladače pro veškerý hardware použitý ve vaší organizaci v jediném úložišti tříděném podle typu zařízení nebo hardwarové konfigurace. Kopii úložiště můžete mít na disku DVD nebo flash disku, můžete vybrat některé ovladače a přidat je na spouštěcí médium, můžete vytvořit vlastní spouštěcí médium s potřebnými ovladači (a požadovanou konfigurací sítě) pro každý ze serverů. Nebo můžete jednoduše při každém použití nástroje Universal Restore zadat cestu k úložišti.

Kontrola přístupu k ovladačům ve spouštěcím prostředí

Zkontrolujte, zda máte při práci ze spouštěcího média přístup k zařízení s ovladači. Jestliže je zařízení k dispozici v systému Windows, ale médium pro systém Linux jej nenalezne, použijte médium pro prostředí WinPE.

Nastavení nástroje Universal Restore

Automatické vyhledání ovladačů

Určete, kde bude aplikace hledat vrstvu HAL (Hardware Abstraction Layer), ovladač řadiče pevného disku a ovladače síťových adaptérů:

- Jestliže jsou ovladače na disku výrobce nebo na jiném vyměnitelném médiu, zapněte možnost **Prohledávat vyměnitelná média**.
- Pokud jsou ovladače umístěny v síťové složce nebo na spouštěcím médiu, klikněte na možnost **Přidat složku** a zadejte cestu ke složce.

Aplikace Universal Restore kromě toho prohledá také výchozí složku úložiště ovladačů systému Windows. Její umístění je určené hodnotou registru **DevicePath**, kterou lze nalézt v klíči registru **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. Touto složkou úložiště je většinou WINDOWS/inf.

Nástroj Universal Restore provede rekurzivní hledání ve všech podsložkách určené složky, vyhledá ve všech dostupných ovladačích nejvhodnější ovladače HAL a řadiče disku a nainstaluje je do systému. Nástroj Universal Restore také hledá ovladač síťového adaptéru. Cestu k nalezeném ovladači potom nástroj přenese do operačního systému. Jestliže má hardware více síťových karet, nástroj Universal Restore se pokusí konfigurovat ovladače všech karet.

V každém případě instalovat ovladače velkokapacitních zařízení

Toto nastavení potřebujete v následujících případech:

- Hardware obsahuje specifický řadič velkokapacitního paměťového zařízení, například RAID (obzvláště NVIDIA RAID) nebo adaptér Fibre Channel.
- Přesunuli jste systém na virtuální počítač, který používá řadič pevného disku SCSI. Použijte ovladače SCSI dodávané s virtualizačním softwarem nebo stáhněte nejnovější verze ovladačů ze stránek výrobce softwaru.
- Pokud automatické vyhledání ovladačů nepomůže spustit systém.

Určete příslušné ovladače kliknutím na možnost **Přidat ovladač**. Zde definované ovladače se nainstalují s příslušným upozorněním i v případě, že aplikace nalezne lepší ovladač.

Proces používání nástroje Universal Restore

Až určíte požadovaná nastavení, klikněte na tlačítko **OK**.

Pokud nástroj Universal Restore nenalezne kompatibilní ovladač v zadaných umístěních, zobrazí výzvu o problémovém zařízení. Proveďte jeden z následujících úkonů:

- Přidejte ovladač do jednoho z dříve zadaných umístění a klikněte na tlačítko **Opakovat**.
- Pokud si nepamatujete umístění, klikněte na tlačítko **Ignorovat**; proces tak bude pokračovat. Pokud výsledek není uspokojivý, použijte nástroj Universal Restore znovu. Při konfiguraci operace zadejte potřebný ovladač.

Po spuštění systému Windows se spustí běžná procedura instalace nového hardwaru. Pokud je ovladač síťového adaptéru podepsán systémem Microsoft Windows, ovladač se nainstaluje na pozadí. Jinak systém Windows požádá o potvrzení, zda nepodepsaný ovladač instalovat.

Potom bude možné konfigurovat síťové připojení a vybrat ovladače pro grafický adaptér, USB a další zařízení.

9.3.5.2 Nástroj Universal Restore v systému Linux

Nástroj Universal Restore lze použít v operačních systémech Linux s verzí jádra 2.6.8 nebo novější.

Pokud je nástroj Universal Restore použit na operační systém Linux, aktualizuje dočasný systém souborů nazývaný počáteční disk RAM (initrd). To zajistí, že bude možné spustit operační systém na novém hardwaru.

Nástroj Universal Restore přidá do počátečního disku RAM moduly pro nový hardware (včetně ovladačů zařízení). Obvykle nalezne potřebné moduly v adresáři **/lib/modules**. Pokud Universal Restore nenalezne potřebný modul, zapíše název souboru modulu do protokolu.

Nástroj Universal Restore může změnit konfiguraci zavaděče GRUB. To může být nutné například pro zajištění spuštění systému, pokud má nový počítač jiné rozvržení svazků než původní počítač.

Nástroj Universal Restore nikdy neupravuje jádro systému Linux.

Návrat k původnímu počátečnímu disku RAM

V případě potřeby se můžete vrátit zpět k původnímu počátečnímu disku RAM.

Počáteční disk RAM je uložen v počítači v souboru. Před první aktualizací počátečního disku RAM uloží nástroj Universal Restore jeho kopii do stejného adresáře. Název kopie je název souboru následovaný příponou **_acronis_backup.img**. Tato kopie bude přepsána v případě, že spustíte Universal Restore více než jednou (například po přidání chybějících ovladačů).

Chcete-li se vrátit k původnímu počátečnímu disku RAM, proveďte některý z následujících úkonů:

- Přejmenujte odpovídajícím způsobem kopii. Například pomocí příkazu podobného následujícímu:

```
mv initrd-2.6.16.60-0.21-default_acronis_backup.img
initrd-2.6.16.60-0.21-default
```

- Zadejte kopii v řádku **initrd** konfigurace zavaděče GRUB.

9.4 Obnova souborů

9.4.1 Obnovení souborů pomocí webového rozhraní

1. Vyberte počítač, který původně obsahoval data, která chcete obnovit.
2. Klikněte na možnost **Obnova**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je vybraný počítač fyzický a je offline, body obnovy se nezobrazí. Proveďte jeden z následujících úkonů:

   - [Doporučeno] Pokud se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte cílový počítač, který je online, a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Zálohy (str. 112).
   - Stáhněte soubory z cloudového úložiště (str. 84).
   - Použijte spouštěcí médium (str. 86).
4. Klikněte na **Obnovit** > **Soubory/složky**.
5. Přejděte do požadované složky nebo pomocí vyhledávání získejte seznam požadovaných souborů a složek.

   Je možné použít více zástupných znaků (* a ?). Více informací o používání zástupných znaků naleznete v části Filtry souborů (str. 63).

   Poznámka: *Vyhledávání není k dispozici pro zálohy na úrovni disku, které jsou uloženy v cloudovém úložišti.*
6. Vyberte soubory, které chcete obnovit.
7. Pokud chcete soubory uložit do souboru .zip, klikněte na **Stáhnout**, vyberte umístění, do kterého se mají data uložit, a klikněte na **Uložit**. Jinak tento krok přeskočte.

   Stahování není dostupné, pokud celková velikost vybraných souborů překračuje 100 MB nebo jsou vybrány i složky.
8. Klikněte na příkaz **Obnovit**.

   V části **Obnovit do** se zobrazí jedna z následujících možností:

- Počítač, který původně obsahoval soubory, jež chcete obnovit (pokud je na počítači nainstalován agent).
- Počítač, kde je nainstalován Agent pro VMware, Agent pro Hyper-V nebo Agent pro Virtuozzo (pokud soubory pocházejí z virtuálního počítače ESXi, Hyper-V nebo Virtuozzo).

Toto je cílový počítač pro obnovu. Pokud je to nutné, můžete vybrat jiný počítač.

9. V části **Cesta** vyberte cílové umístění obnovy. Je možné vybrat jednu z následujících možností:
   - Původní umístění (při obnově na původní počítač)
   - Místní složka v cílovém počítači
   - Síťová složka, která je přístupná z cílového počítače
10. Klikněte na možnost **Spustit obnovu**.
11. Vyberte jednu z možností pro přepis souborů:
    - **Přepsat existující soubory**
    - **Přepsat existující soubor, pokud je starší**
    - **Nepřepisovat existující soubory**

Postup obnovy se zobrazuje na kartě **Aktivity**.

9.4.2 Stahování souborů z cloudového úložiště

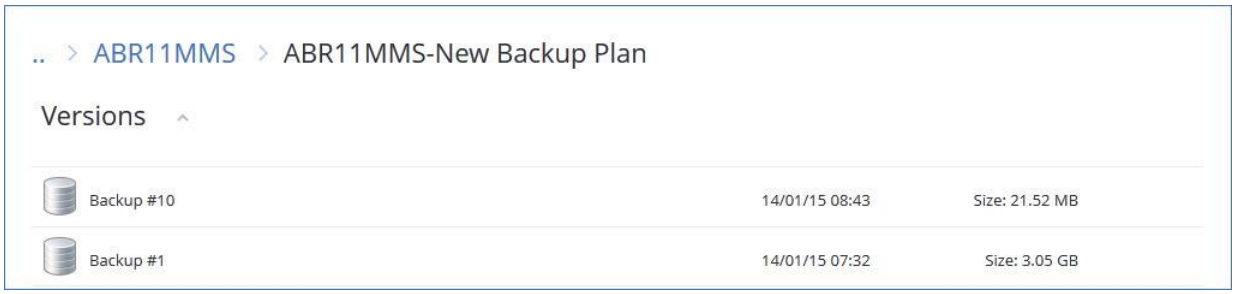
Je možné procházet cloudové úložiště, zobrazovat obsah záloh a stahovat potřebné soubory.

Omezení

- Zálohy stavu systému, databáze SQL a databáze Exchange není možné procházet.
- Pokud chcete zlepšit stahování, nestahujte najednou více než 100 MB dat. Chcete-li rychle načíst větší množství dat z cloudu, použijte postup pro obnovení souborů (str. 83).

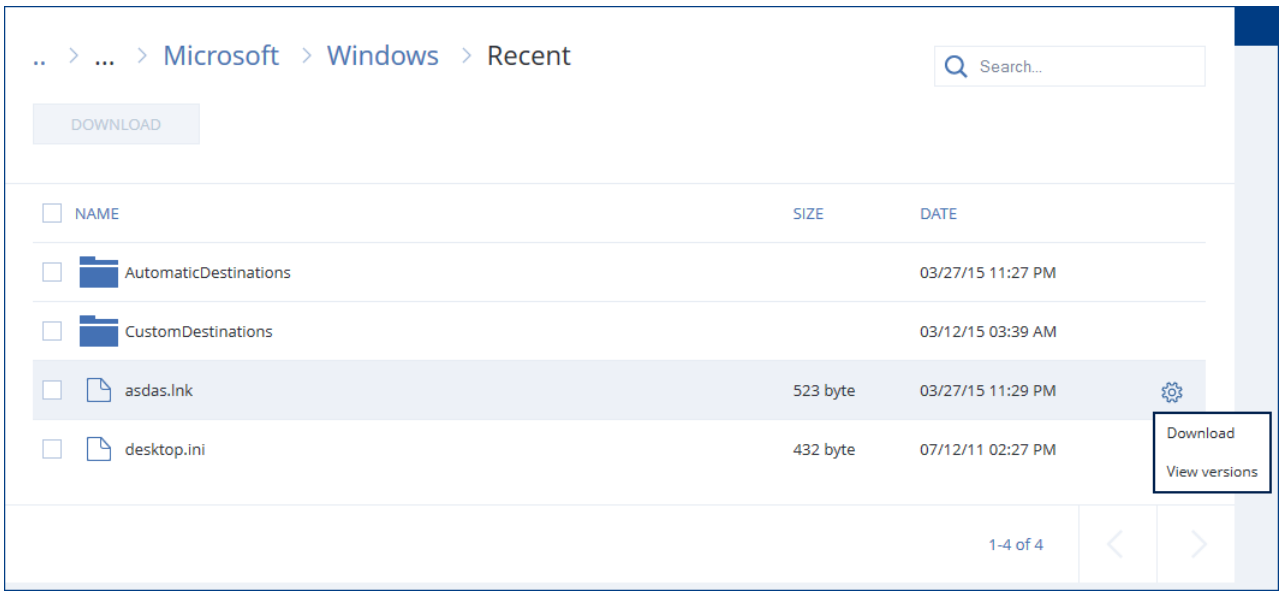
Jak stáhnout soubory z cloudového úložiště

1. Vyberte zálohovaný počítač.
2. Klikněte na **Obnovit** > **Více způsobů obnovy...** > **Stáhnout soubory**.
3. Zadejte pověření k účtu, ke kterému je zálohovaný počítač přiřazen.
4. [Při procházení záloh na úrovni disků] Pod položkou **Verze** klikněte na zálohu, ze které chcete obnovit soubory.



[Při procházení záloh na úrovni souborů] Je možné vybrat datum a čas zálohy v dalším kroku pod tlačítkem ozubeného kola napravo od vybraného souboru. Ve výchozím nastavení se soubory obnoví z nejnovější zálohy.

5. Přejděte do požadované složky nebo pomocí vyhledávání získejte seznam požadovaných souborů.



6. Zaškrtněte políčka u položek, které potřebujete obnovit, a klikněte na **Stáhnout**.

   Pokud vyberete jeden soubor, stáhne se tak, jak je. Jinak se vybraná data archivují do souboru .zip
7. Vyberte umístění k uložení dat a klikněte na tlačítko **Uložit**.

9.4.3 Podepsání souboru pomocí služby ASign

ASign je služba umožňující více lidem elektronicky podepsat zálohovaný soubor. Tato funkce je k dispozici pouze pro zálohy na úrovni souborů uložených v cloudovém úložišti.

Podepsána může být vždy jen jedna verze souboru. Pokud byl soubor zálohován vícekrát, musíte zvolit verzi k podpisu a pouze tato verze bude podepsaná.

Například můžete ASign použít k elektronickému podpisu následujících souborů:

- Dohody o pronájmu
- Kupní smlouvy
- Ujednání o nákupu jmění
- Dohody o půjčce
- Udělení souhlasu
- Finanční dokumenty
- Pojišťovací dokumenty
- Omezení zodpovědnosti
- Zdravotní dokumenty
- Výzkumné studie
- Osvědčení o pravosti výrobku
- Dohody o mlčenlivosti
- Nabídky
- Dohody o utajení
- Dohody s nezávislými dodavateli

Jak podepsat verzi souboru

1. Soubor vyberte podle kroků 1–6 v části Obnovení souborů pomocí webového rozhraní (str. 83).
2. Ověřte, zda je v levém panelu vybráno správné datum a čas.
3. Pokračujte kliknutím na možnost **Podepsat tuto verzi souboru**.
4. Zadejte heslo pro účet cloudového úložiště, ve kterém je záloha uložena. Přihlášení k účtu se zobrazí v okně s výzvou.

   V okně webového prohlížeče se zobrazí rozhraní služby ASign.
5. Přidejte další signatáře zadáním jejich e-mailových adres. Signatáře nelze přidat nebo odebrat po odeslání žádostí o podpis, proto se přesvědčte, že seznam obsahuje všechny osoby, jejichž podpis je vyžadován.
6. Kliknutím na tlačítko **Invite to sign** (Pozvat k podpisu) odešlete žádosti o podpis.

   Každý podepsaný obdrží e-mailovou zprávu s žádostí o podpis. Poté co všichni signatáři podepíší soubor, je soubor notářsky ověřen a podepsán notářskou službou.

   V procesu podepisování obdržíte oznámení o podpisu jednotlivých signatářů a také o dokončení celého procesu. Kliknutím na odkaz **View details** (Zobrazit podrobnosti), který je dostupný v každé přijaté e-mailové zprávě s oznámením, můžete přejít na webovou stránku služby ASign.
7. Po dokončení celého procesu přejděte na webovou stránku služby ASign a kliknutím na tlačítko **Get document** (Získat dokument) stáhněte dokument PDF, který obsahuje následující informace:
   - Stránka certifikátu o podpisu se shromážděnými podpisy
   - Stránka se záznamem pro audit obsahující historii aktivit: kdy byly odeslány pozvánky k podpisu signatářům, kdy každý signatář podepsal soubor atd.

9.4.4 Obnova souborů pomocí spouštěcího média

Informace o tvorbě spouštěcích médií naleznete v tématu Tvorba spouštěcího média (str. 75).

Jak obnovit soubory pomocí spouštěcího média

1. Spusťte cílový počítač pomocí spouštěcího média.
2. Klikněte na možnost **Místní správa tohoto počítače** nebo dvakrát klikněte na možnost **Spouštěcí záchranná média** (podle typu média, které používáte).
3. Pokud je v síti zapnutý proxy server, klikněte na **Nástroje** > **Proxy server** a zadejte název hostitele nebo IP adresu, port a přihlašovací údaje proxy serveru. Jinak tento krok přeskočte.
4. [Volitelné] Pokud obnovujete systém Windows nebo Linux, klikněte na **Nástroje** > **Zaregistrovat médium ve službě zálohování** a zadejte registrační token, který jste získali při stahování média. Když to uděláte, nebudete muset při přístupu ke cloudovému úložišti zadávat přihlašovací údaje ani registrační kód (viz popis kroku č. 7).
5. V uvítacím okně klikněte na možnost **Obnovit**.
6. Klikněte na **Označit data** a poté klikněte na **Procházet**.
7. Určete umístění zálohy:
   - Chcete-li provést obnovení z cloudového úložiště, vyberte možnost **Cloudové úložiště**. Zadejte pověření k účtu, ke kterému je zálohovaný počítač přiřazen.

     Při obnovení Windows nebo Linuxu můžete požádat o registrační kód a použít ho místo přihlašovacích údajů. Klikněte na **Použijte registrační kód** > **Požádat o kód**. Software zobrazí registrační odkaz a registrační kód. Můžete je zkopírovat a provést registrační kroky na jiném počítači. Registrační kód je platný jednu hodinu.
   - Pokud chcete provést obnovení z místní nebo síťové složky, vyhledejte ji v části **Místní složky** nebo **Síťové složky**.

Kliknutím na tlačítko **OK** potvrdíte váš výběr.

8. Vyberte zálohu, ze které chcete data obnovit. Pokud se zobrazí výzva, zadejte heslo zálohy.
9. V okně **Obsah zálohy** vyberte možnost **Složky/soubory**.
10. Vyberte data, která chcete obnovit. Kliknutím na tlačítko **OK** potvrdíte váš výběr.
11. V části **Kam obnovit** určete složku. Volitelně je možné zakázat přepisování nových verzí souborů nebo vyloučit některé soubory z obnovy.
12. [Volitelné] Klikněte na možnost **Možnosti obnovy** a určete další nastavení.
13. Kliknutím na tlačítko **OK** spusťte obnovu.

9.4.5 Extrahování souborů z místních záloh

Můžete procházet obsah záloh a extrahovat z nich soubory, které potřebujete.

Požadavky

- Tato funkce je dostupná jen ve Windows v Průzkumníku souborů.
- Na počítači, na kterém chcete procházet zálohy, musí být nainstalovaný agent pro zálohování.
- Zálohovaný systém souborů musí být v některém z těchto formátů: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS nebo HFS+.
- Záloha musí být uložená v místní složce nebo v síťovém úložišti (SMB/CIFS).

Jak extrahovat soubory ze zálohy

1. V Průzkumníku souborů přejděte do umístění se zálohou.
2. Dvakrát klikněte na soubor zálohy. Názvy souborů se tvoří podle následující šablony:
   `<název počítače> – <GUID plánu zálohování>`.
3. Pokud je záloha zašifrovaná, zadejte šifrovací heslo. Jinak tento krok přeskočte.
   Průzkumník souborů zobrazí body obnovy.
4. Dvakrát klikněte na požadovaný bod obnovy.
   Průzkumník souborů zobrazí zálohovaná data.
5. Přejděte do požadované složky.
6. Zkopírujte požadované soubory do libovolné složky v systému souborů.

9.5 Obnova stavu systému

1. Vyberte počítač, u kterého chcete obnovit stav systému.
2. Klikněte na možnost **Obnova**.
3. Vyberte bod obnovy stavu systému. Body obnovy se filtrují podle umístění.
4. Klikněte na možnost **Obnovit stav systému**.
5. Potvrďte, že chcete přepsat stav systému jeho zálohovanou verzí.

Postup obnovy se zobrazuje na kartě **Aktivity**.

9.6 Obnova konfigurace ESXi

Chcete-li obnovit konfiguraci ESXi, budete potřebovat spouštěcí média systému Linux. Informace o tvorbě spouštěcích médií naleznete v tématu Tvorba spouštěcího média (str. 75).

Pokud obnovujete konfiguraci ESXi do jiného než původního hostitele a původní hostitel ESXi je k serveru vCenter stále připojen, ze serveru jej odeberte, aby při obnově nedocházelo k nečekaným

potížím. Pokud chcete původního hostitele ponechat spolu s obnoveným, můžete jej znovu přidat, až bude obnova dokončena.

Virtuální počítače spuštěné v hostiteli se do zálohy konfigurace ESXi nezahrnují. Je možné je zálohovat a obnovovat samostatně.

Jak obnovit konfiguraci ESXi

1. Spusťte cílový počítač pomocí spouštěcího média.
2. Klikněte na tlačítko **Místní správa tohoto počítače**.
3. V uvítacím okně klikněte na možnost **Obnovit**.
4. Klikněte na **Označit data** a poté klikněte na **Procházet**.
5. Určete umístění zálohy:
   - Vyhledejte složku v části **Místní složky** nebo **Síťové složky**.

   Kliknutím na tlačítko **OK** potvrdíte váš výběr.
6. V části **Zobrazit** vyberte možnost **Konfigurace ESXi**.
7. Vyberte zálohu, ze které chcete data obnovit. Pokud se zobrazí výzva, zadejte heslo zálohy.
8. Klikněte na tlačítko **OK**.
9. V části **Disky, které se použijí pro nová datová úložiště** proveďte následující postup:
   - V části **Obnovit ESXi do** vyberte disk, kam bude obnovena konfigurace hostitele. Pokud obnovujete konfiguraci do původního hostitele, bude jako výchozí vybrán původní disk.
   - [Volitelné] V části **Použít pro nové datové úložiště** vyberte disky, kde budou vytvořena nová datová úložiště. Postupujte opatrně, protože veškerá data na vybraných discích budou ztracena. Chcete-li zachovat virtuální počítače ve stávajících datových úložištích, žádné disky nevybírejte.
10. Pokud vyberete disky pro nová datová úložiště, vyberte metodu tvorby datového úložiště v části **Jak vytvořit nová datová úložiště**: **Vytvořit jedno datové úložiště na každém disku** nebo **Vytvořit jedno datové úložiště na všech vybraných pevných discích**.
11. [Volitelné] V části **Mapování sítě** změňte výsledek automatického mapování virtuálních přepínačů v záloze na fyzické síťové adaptéry.
12. [Volitelné] Klikněte na možnost **Možnosti obnovy** a určete další nastavení.
13. Kliknutím na tlačítko **OK** spusťte obnovu.

9.7 Možnosti obnovy

Možnosti obnovy změníte kliknutím na odkaz **Možnosti obnovy** při konfiguraci.

Dostupnost možností obnovení

Dostupné možnosti obnovení závisí na:

- Prostředí, ve kterém funguje agent, který provádí obnovu (Windows, Linux, macOS nebo spouštěcí médium).
- Typu obnovovaných dat (disky, soubory, virtuální počítače, data aplikací).

Následující tabulka shrnuje dostupnosti možností obnovení.

	Disky	Soubory	Virtuální počítače	SQL a Exchange

	Windows	Linux	Spouštěcí médium	Windows	Linux	macOS	Spouštěcí médium	ESXi, Hyper-V a Virtuozzo	Windows
Ověření zálohy (str. 89)	+	+	+	+	+	+	+	+	+
Datum a čas pro soubory (str. 90)	-	-	-	+	+	+	+	-	-
Zpracování chyb (str. 90)	+	+	+	+	+	+	+	+	+
Vyloučení souborů (str. 90)	-	-	-	+	+	+	+	-	-
Zabezpečení na úrovni souborů (str. 90)	-	-	-	+	-	-	-	-	-
Flashback (str. 91)	+	+	+	-	-	-	-	+	-
Obnova úplné cesty (str. 91)	-	-	-	+	+	+	+	-	-
Přípojné body (str. 91)	-	-	-	+	-	-	-	-	-
Výkon (str. 91)	+	+	-	+	+	+	-	+	+
Příkazy před-po (str. 91)	+	+	-	+	+	+	-	+	+
Změna SID (str. 93)	+	-	-	-	-	-	-	-	-
Správa napájení virtuálního počítače (str. 93)	-	-	-	-	-	-	-	+	-
Protokol událostí systému Windows (str. 93)	+	-	-	+	-	-	-	Pouze Hyper-V	+

9.7.1 Ověření zálohy

Tato možnost určuje, zda se má ověřovat záloha, aby bylo před obnovením dat zajištěno, že záloha není poškozena.

Výchozí nastavení: **Zakázáno**.

Ověření vypočítá kontrolní součet pro každý blok dat uložený v záloze. Jedinou výjimkou je ověřování záloh na úrovni souborů, které jsou umístěny v cloudovém úložišti. Tyto zálohy se ověřují tak, že se zkontroluje konzistence metadat uložených v záloze.

Ověřování je časově náročný proces, a to i u přírůstkových nebo rozdílových záloh, které jsou malé. To proto, že operace ověří nejen data fyzicky obsažená v záloze, ale také data obnovitelná výběrem zálohy. K tomu je nezbytný přístup k dříve vytvořeným zálohám.

9.7.2 Zpracování chyb

Tyto možnosti umožňují určit, jak se mají zpracovat chyby, které se mohou vyskytnou během obnovy.

Pokud dojde k chybě, pokusit se znovu

Výchozí nastavení: **Povoleno. Počet pokusů: 30 Interval mezi pokusy: 30 sekund**.

Když dojde k opravitelné chybě, aplikace se znovu pokusí provést neúspěšnou operaci. Je možné nastavit interval a počet pokusů. Pokusy budou ukončeny, jakmile se operace zdaří nebo dojde k vykonání zadaného počtu pokusů, podle toho, co nastane dřív.

Při zpracování nezobrazovat zprávy a dialogová okna (tichý režim)

Výchozí nastavení: **Zakázáno**.

Když je zapnut tichý režim, aplikace automaticky zpracuje situace vyžadující zásah uživatele, kde je to jen možné. Když operace nemůže bez zásahu uživatele pokračovat, nezdaří se. Podrobnosti o operaci včetně případných chyb lze nalézt v protokolu operace.

9.7.3 Datum a čas pro soubory

Tato možnost je účinná pouze při obnově souborů.

Tato možnost určuje, zda obnovit datum a čas souborů tak, jak je v záloze, nebo zda k nim přiřadit aktuální datum a čas.

Pokud tuto možnost zapnete, souborům se přiřadí aktuální datum a čas.

Výchozí nastavení: **Povoleno**.

9.7.4 Vyloučení souborů

Tato možnost je účinná pouze při obnově souborů.

Tato možnost určuje, které soubory a složky se mají během procesu obnovy vynechat a tím vyloučit ze seznamu obnovených položek.

Poznámka *Výjimky předefinují výběr datových položek k obnovení. Pokud například zvolíte k obnovení soubor Soubor.tmp a vyloučíte všechny soubory .tmp, soubor Soubor.tmp nebude obnoven.*

9.7.5 Zabezpečení na úrovni souborů

Tato možnost je účinná při obnovení souborů ze záloh svazků ve formátu NTFS na úrovni disků a souborů či složek.

Určuje, zda se zároveň se soubory budou obnovovat oprávnění NTFS.

Výchozí nastavení: **Povoleno**.

Můžete určit, zda chcete obnovit oprávnění nebo nechat soubory převzít oprávnění NTFS ze složky, do které se obnovují.

9.7.6 Flashback

Tato možnost je aktivní při obnovování disků a svazků na fyzických a virtuálních počítačích, kromě počítačů Mac.

Tato možnost je funkční pouze tehdy, pokud rozvržení svazků obnovovaného disku přesně odpovídá cílovému disku.

Pokud je tato možnost zapnutá, obnoví se jen rozdíly mezi daty v záloze a na cílovém disku. Zrychluje obnovení fyzických a virtuálních počítačů. Data se porovnávají na úrovni bloků.

Výchozí nastavení při obnově fyzického počítače: **Zakázáno**.

Výchozí nastavení při obnově virtuálního počítače: **Povoleno**.

9.7.7 Obnova úplné cesty

Tato možnost funguje jen při obnově dat ze zálohy na úrovni souborů.

Pokud je zapnutá, v cílovém umístění se vytvoří úplná cesta k souboru.

Výchozí nastavení: **Zakázáno**.

9.7.8 Přípojné body

Tato možnost má vliv jen ve Windows při obnově dat ze zálohy na úrovni souborů.

Tuto možnost zapněte, chcete-li obnovit soubory a složky, které byly uloženy na připojených svazcích a zálohovány se zapnutou možností Přípojné body (str. 65).

Výchozí nastavení: **Zakázáno**.

Tato možnost je účinná pouze v případě, že pro obnovu vyberete složku, která je v hierarchii složek výše než přípojný bod. Pokud vyberete pro obnovu složky v přípojném bodě nebo samotný přípojný bod, obnoví se vybrané položky nezávisle na hodnotě možnosti **Přípojné body**.

Poznámka *Nezapomeňte, že pokud není v okamžiku obnovy svazek připojen, data se obnoví přímo do složky, která byla přípojným bodem v okamžiku zálohy.*

9.7.9 Výkon

Tato možnost definuje prioritu procesu obnovy v operačním systému.

K dispozici jsou následující nastavení: **Nízká**, **Normální**, **Vysoká**.

Výchozí nastavení: **Normální**–

Priorita procesu běžícího v systému určuje množství CPU a systémových zdrojů poskytnutých procesu. Snížením priority obnovy uvolníte více zdrojů pro další aplikace. Pokud zvýšíte prioritu obnovy, může to celý proces urychlit, protože operační systém bude moci přidělit více prostředků aplikaci, která bude obnovu provádět. Výsledek ovšem závisí na celkovém zatížení procesoru a dalších faktorech, například rychlosti čtení/zápisu disku nebo síťovém provozu.

9.7.10 Příkazy před-po

Tato volba vám umožňuje určit příkazy, které se provedou automaticky před a po obnově dat.

Příklad, jak můžete používat příkazy před/po:

- Můžete spustit příkaz **Checkdisk** s cílem najít a opravit logické chyby systému souborů, fyzické chyby nebo vadné sektory před zahájením obnovy nebo po dokončení obnovy.

Tento program nepodporuje interaktivní příkazy. To jsou příkazy, které vyžadují zásah uživatele (například "pause").

Příkazy po obnově nebudou vykonány, pokud obnova pokračuje restartováním.

9.7.10.1 Příkaz před obnovením

Jak zadat příkaz nebo dávkový soubor, který má být proveden před spuštěním procesu obnovení

1. Zapněte přepínač **Spustit příkaz před obnovou**.
2. Do pole **Příkaz...** zadejte příkaz nebo vyhledejte dávkový soubor. Tento program nepodporuje interaktivní příkazy. To jsou příkazy, které vyžadují zásah uživatele (například "pause").
3. V textovém poli **Pracovní adresář** zadejte cestu k adresáři, kde bude spuštěn příkaz nebo dávkový soubor.
4. Pokud je to nutné, zadejte argumenty spouštěných příkazů do textového pole **Argumenty**.
5. Podle toho, jakého výsledku chcete dosáhnout, vyberte požadované možnosti (popsány jsou v tabulce).
6. Klikněte na tlačítko **Hotovo**.

Zaškrtávací políčko	**Nastavení**			
Nechat selhat obnovu, pokud selže vykonávání příkazu*	Zaškrtnuto	Nezaškrtnuto	Zaškrtnuto	Nezaškrtnuto
Neobnovovat před dokončením provedení příkazu	Zaškrtnuto	Zaškrtnuto	Nezaškrtnuto	Nezaškrtnuto
Výsledek				
	Přednastaveno Provést obnovu pouze po úspěšném vykonání příkazu. Nechat selhat obnovu, pokud selže vykonávání příkazu.	Provést obnovu po vykonání příkazu, ať už vykonání příkazů bylo nebo nebylo úspěšné.	N/A	Provést obnovu současně s vykonáváním příkazu a bez ohledu na výsledku provedení příkazu.

Za selhání příkazu se považuje, pokud jeho návratový kód není roven nule.

9.7.10.2 Příkaz po obnovení

Jak zadat příkaz/spustitelný soubor, aby byl spuštěn po dokončení obnovení

1. Zapněte přepínač **Spustit příkaz po obnově**.
2. Do pole **Příkaz...** zadejte příkaz nebo vyhledejte dávkový soubor.
3. V textovém poli **Pracovní adresář** zadejte cestu k adresáři, kde bude spuštěn příkaz nebo dávkový soubor.
4. Pokud je to nutné, zadejte argumenty spouštěných příkazů do textového pole **Argumenty**.
5. Pokud je provedení příkazu velmi důležité, zaškrtněte políčko **Nechat selhat obnovu, pokud selže vykonávání příkazu**. Za selhání příkazu se považuje, pokud jeho ukončovací kód není roven nule. V případě, že provedení příkazu selže, stav obnovy bude nastaven na **Chyba**.

Jestliže není toto políčko zaškrtnuto, výsledek provedení příkazu neovlivní úspěch nebo selhání obnovy. Výsledky spuštění příkazu můžete sledovat na kartě **Aktivity**.

6. Klikněte na tlačítko **Hotovo**.

Poznámka *Příkazy po obnově nebudou vykonány, pokud obnova pokračuje restartováním.*

9.7.11 Změna SID

Tato možnost platí při obnově systému Windows 8.1/Windows Server 2012 R2 nebo staršího.

Tato možnost neplatí, když se provádí obnova na virtuální počítač pomocí Agenta pro VMware nebo Agenta pro Hyper-V.

Výchozí nastavení: **Zakázáno**.

Software umí pro obnovený operační systém vygenerovat unikátní bezpečnostní identifikátor (SID počítače). Tuto možnost potřebujete pouze k zajištění funkčnosti softwaru třetích stran, který závisí na SID počítače.

Společnost Microsoft oficiálně nepodporuje změnu SID na nasazeném nebo obnoveném systému. Tuto možnost proto používejte na svoje vlastní riziko.

9.7.12 Správa napájení virtuálního počítače

Tyto možnosti fungují, když se provádí obnova na virtuální počítač pomocí Agenta pro VMware, Agenta pro Hyper-V nebo Agenta pro Virtuozzo.

Vypnout cílové virtuální počítače při spuštění obnovení

Výchozí nastavení: **Povoleno**.

Obnovení do existující virtuálního počítače není možné, pokud je online, a proto je tento počítač při zahájení obnovy automaticky vypnut. Uživatelé budou od počítače odpojeni a veškerá neuložená data budou ztracena.

Zrušte zaškrtnutí políčka pro toto nastavení, pokud před obnovením preferujete ruční vypnutí virtuálního počítače.

Zapnout cílový virtuální počítač po dokončení obnovení

Výchozí nastavení: **Zakázáno**.

Po obnovení počítače ze zálohy na jiný počítač existuje šance, že se v síti objeví replika existujícího počítače. Bezpečný provoz zajistíte ručním zapnutím obnoveného virtuálního počítače po provedení nezbytných opatření.

9.7.13 Protokol událostí systému Windows

Tato možnost platí pouze pro operační systémy Windows.

Tato možnost určuje, zda má agent zaznamenávat události operací obnovy do protokolu událostí aplikací ve Windows (protokol zobrazíte tak, že spustíte eventvwr.exe nebo vyberete **Ovládací panely** > **Nástroje pro správu** > **Prohlížeč událostí**). Zaznamenávané události můžete filtrovat.

Výchozí nastavení: **Zakázáno**.

10 Obnovení po havárii

Funkce obnovení po havárii vám umožňuje vlastnit virtuální počítač v cloudu. V případě havárie je možné ihned přepnout zatížení (převzít služby) z poškozeného počítače do cloudového virtuálního počítače.

Chcete-li zahrnout cloudový počítač do místní sítě TPC/IP, bude třeba síť rozšířit do cloudu přes zabezpečené tunelové připojení VPN. Lze to snadno provést instalací zařízení VPN, které se dodává ve dvou variantách: pro VMware ESXi a pro Hyper-V.

Po nakonfigurování připojení VPN a vytvoření virtuálního počítače v cloudu můžete k virtuálnímu počítači přistupovat přímo z konzoly pro zálohování. Lze také použít připojení RDP nebo SSH.

Funkce obnovení po havárii jsou k dispozici pouze správcům na úrovni společnosti. Správci jsou zodpovědní za poskytnutí přístupu uživatelům do cloudového virtuálního počítače a za poučení uživatelů o přístupu k tomuto počítači v případě havárie.

Placené prostředky řízené kvótami

Máte-li v cloudu virtuální počítač, nemusíte se starat o náhradní hardware, ale musíte platit za počítačové prostředky spotřebované virtuálním počítačem. K těmto prostředkům patří procesor a paměť RAM, které jsou přepočtené do výpočetních bodů, dále pak prostor datového úložiště obsazený soubory virtuálního počítače a případně veřejná IP adresa.

Prostor datového úložiště se nazývá úložiště obnovení po havárii. Toto rychlé úložiště je dražší než běžné cloudové úložiště, kam se ukládají zálohy. Náklady na úložiště obnovení po havárii také zahrnují výdaje na infrastrukturu požadovanou při obnovení po havárii.

Servery pro obnovení

Cloudový virtuální počítač může být kopií místního serveru založenou na zálohách serveru uložených v cloudu. Tento počítač se nazývá **server pro obnovení**.

Server pro obnovení je po většinu času vypnutý. Spouští se pouze při testování nebo v případě, že je nutné převzetí služeb při selhání. Protože se prostředky procesoru a paměti RAM spotřebovávají po relativně krátkou dobu, platíte hlavně za cloudové úložiště, kam se ukládají zálohy, a za rezervaci úložiště pro případ obnovení po havárii. Následují další výhody serveru pro obnovení:

- Nejsou potřeba hluboké znalosti softwaru nainstalovaného na serveru.
- Data jsou uchována dlouhodobě. Můžete se vrátit do bodu obnovy, který jde roky zpět a zobrazit změny dat nebo zpřístupnit odstraněná data.
- Další možnosti obnovení. Můžete obnovit počítač nebo provést granulární obnovu ze stejné zálohy, která se používá k obnovení po havárii.

Primární servery

Dalším typem cloudového virtuálního počítače je **primární server**. Je to prostě další server ve vaší síti. Služba vám umožňuje vytvořit virtuální počítač na základě poskytnutých šablon. Další údržba serveru je na vaši odpovědnost.

Obvykle se primární server používá k replikaci dat v reálném čase mezi servery, na kterých běží klíčové aplikace. Replikaci si nastavujete sami s využitím nativních nástrojů aplikace. Například replikaci služby Active Directory nebo SQL lze nakonfigurovat mezi místními servery a primárním serverem.

Primární server je případně možné zahrnout ve skupině dostupnosti AlwaysOn (AAG) nebo skupině dostupnosti databáze (DAG).

Obě metody vyžadují hluboké znalosti aplikace a práva správce. Primární server neustále spotřebovává výpočetní prostředky a prostor v úložišti rychlého obnovení po havárii. Vyžaduje z vaší strany údržbu: monitorování replikace, instalaci aktualizací softwaru, zálohování. Výhodou je minimální cíl bodu obnovení (RPO) a cíl času obnovení (RTO) s minimálním zatížením produkčního prostředí (ve srovnání se zálohováním celých serverů do cloudu).

Omezení

Obnovení po havárii není podporováno:

- pro virtuální počítače a kontejnery Virtuozzo,
- pro počítače Mac,
- pro počítače se systémem Linux, které mají logické svazky (LVM) nebo svazky naformátované se systémem souborů XFS nebo disky bez tabulky diskových oddílů,
- pro počítače Windows, které mají dynamické disky,
- pokud jsou zálohy původního počítače šifrované.

Server pro obnovení má jedno síťové rozhraní. Pokud má původní počítač více síťových rozhraní, emuluje se pouze jedno.

Cloudové servery nejsou šifrované.

10.1 Softwarové požadavky

Podporované operační systémy

Ochrana pomocí serveru pro obnovení byla testována pro následující operační systémy:

- Centos 6.6, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Debian 9
- Ubuntu 16.04, 18.04
- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – všechny možnosti instalace (s výjimkou Nano Serveru)

Počítačové operační systémy Windows nejsou podporované kvůli podmínkám, které platí pro produkty Microsoftu.

Tento software může fungovat s dalšími verzemi operačního systému Windows a distribucemi Linux, ale je to bez záruky.

Podporované virtualizační platformy

Ochrana virtuálních počítačů pomocí serveru pro obnovení byla testována pro následující virtualizační platformy:

- VMware ESXi 5.1, 5.5, 6.0, 6.5
- Windows Server 2008 R2 s Hyper-V
- Windows Server 2012/2012 R2 s Hyper-V
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 s Hyper V – všechny možnosti instalace (s výjimkou Nano Serveru)

- Microsoft Hyper-V Server 2016
- Virtuální počítače založené na jádře (KVM)
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2
- Virtuální počítače Azure

Zařízení VPN bylo testováno pro následující virtualizační platformy:

- VMware ESXi 5.1, 5.5, 6.0, 6.5
- Windows Server 2008 R2 s Hyper-V
- Windows Server 2012/2012 R2 s Hyper-V
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 s Hyper V – všechny možnosti instalace (s výjimkou Nano Serveru)
- Microsoft Hyper-V Server 2016

Tento software může fungovat s virtualizačními platformami a verzemi, ale je to bez záruky.

10.2 Konfigurace připojení VPN

Před vytvořením serveru pro obnovení nebo primárního serveru je třeba nastavit připojení VPN ke cloudovému serveru pro obnovení. Připojení VPN využívá dva virtuální počítače:

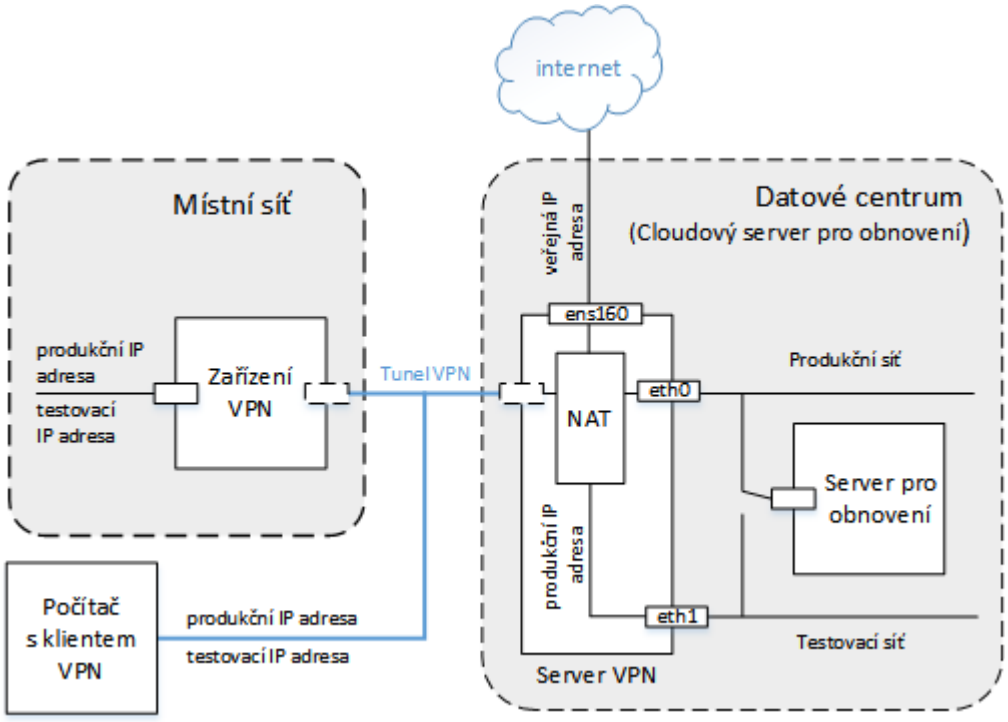
- zařízení VPN umístěné ve vaší firmě,
- server VPN umístěný na cloudovém serveru pro obnovení.

Zařízení VPN umožňuje připojení mezi cloudovým serverem pro obnovení a vaší místní sítí. Pokud je místní síť nedostupná, potřebujete mít možnost připojit se přímo k serveru VPN.

Následující diagram ukazuje metody připojení ke cloudovému serveru pro obnovení a překlad IP adres v režimech převzetí služeb při selhání a testování převzetí služeb při selhání.

- V režimu převzetí služeb při selhání (na obrázku) je server pro obnovení připojený k produkční síti a má přiřazenou produkční IP adresu.
- V režimu testování převzetí služeb při selhání je server pro obnovení připojený k izolované testovací síti a má také přiřazenou produkční IP adresu. Pro přístup k serveru přes VPN však musíte použít testovací IP adresu. Server VPN nahradí testovací IP adresu produkční IP adresou v rámci testovací sítě.

- Pokud má server pro obnovení veřejnou IP adresu, přeloží se i tato adresa na produkční IP adresu v režimech převzetí služeb při selhání i testování převzetí služeb při selhání.



10.2.1 Požadavky na zařízení VPN

Systémové požadavky

- 1 CPU
- 1 GB PAMĚTI RAM
- 8 GB místa na disku

Porty

- TCP 443 (odchozí) – pro připojení VPN
- TCP 80 (odchozí) – pro automatické aktualizace zařízení (str. 100)

Ujistěte se, že brány firewall a další součásti sítě umožňují připojení prostřednictvím těchto portů k jakékoli IP adrese.

10.2.2 Připojení pomocí zařízení VPN

Zařízení VPN rozšiřuje danou místní síť do cloudu přes zabezpečené tunelové připojení sítě VPN. Tento druh připojení se často nazývá S2S (site-to-site).

Nastavení připojení pomocí zařízení VPN

1. Klikněte na **Zařízení** > **Cloudový server pro obnovení**.
2. Na uvítací stránce klikněte na možnost **Spustit**.

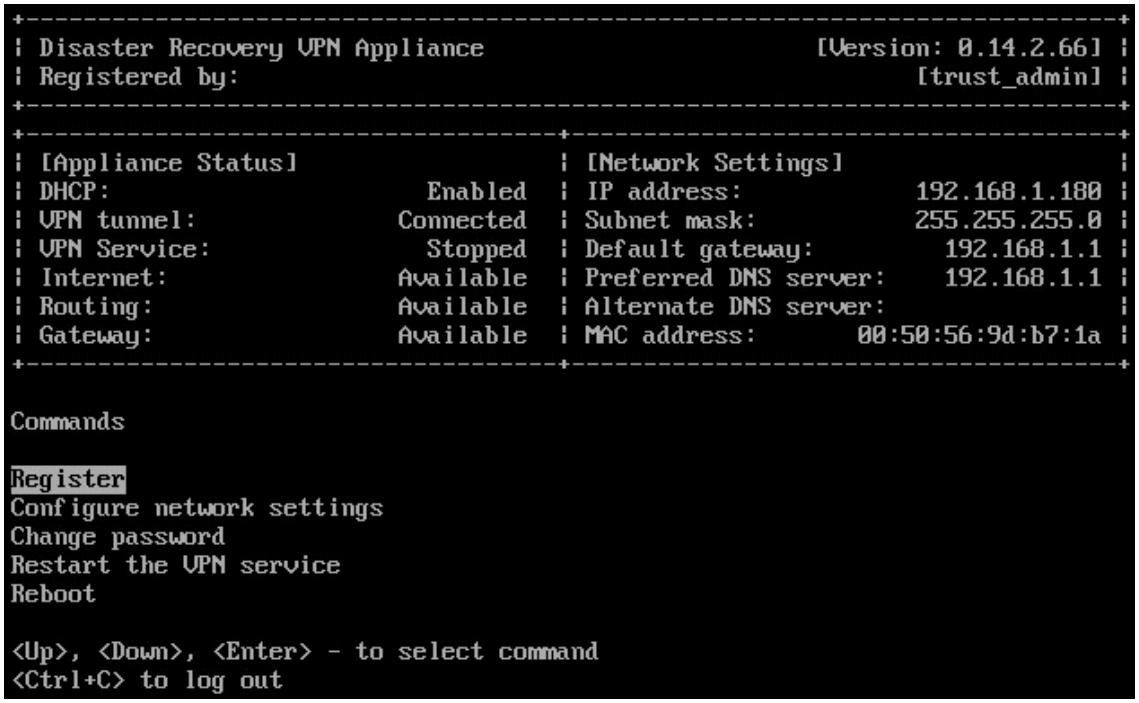
   Systém začne zasazovat server VPN do cloudu, což zabere nějaký čas. Mezitím můžete pokračovat dalším krokem.

Poznámka *Server VPN se poskytuje bezplatně. Pokud nebude v cloudu přítomen po dobu sedmi dnů žádný primární server ani server pro obnovení, není využita funkce obnovení po havárii a server bude vymazán.*

3. Podle toho, jako virtualizační platformu používáte, stáhněte si zařízení VPN pro VMware vSphere nebo Microsoft Hyper-V.
4. Nasaďte toto zařízení a připojte ho k produkční síti.

   V systému vSphere zajistěte, aby byl povolen **Promiskuitní režim** s nastavenou možností **Přijmout** pro všechny virtuální přepínače, které připojují zařízení VPN k produkční síti. K tomuto nastavení se v klientovi vSphere Client dostanete tak, že vyberete hostitele > **Shrnutí** > **Síť** > zvolíte přepínač > **Upravit nastavení...** > **Zabezpečení**.

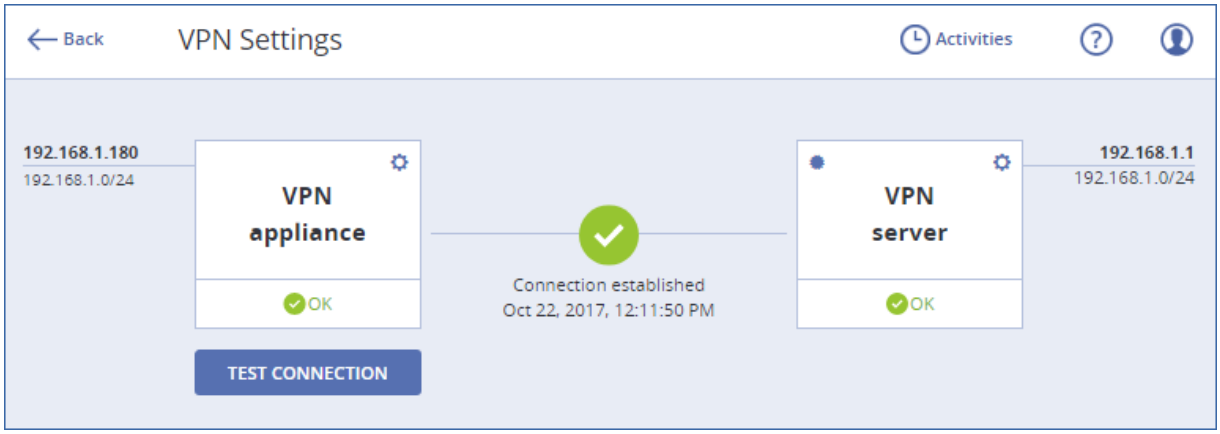
   V produktu Hyper-V vytvořte virtuální počítač Generation 1 s 1 024 MB paměti. V daném počítači také doporučujeme povolit dynamickou paměť. Po vytvoření počítače přejděte do **Nastavení** > **Hardware** > **Síťový adaptér** > **Pokročilé funkce** a zaškrtněte políčko**Povolit maskování adresy MAC**.
5. Zapněte zařízení.
6. Otevřete konzolu zařízení a přihlaste se uživatelského jména a hesla admin/admin.



7. [Volitelné] Změňte heslo.
8. [Volitelné] Změňte nastavení sítě. Je vhodné přiřadit zařízení statickou IP adresu.
9. Zaregistrujte zařízení do služby zálohování pomocí pověření správce společnosti.

   Tato pověření se použijí pouze jednou k získání certifikátu. Adresa URL datového centra je předdefinovaná.

Zařízení se připojí k serveru VPN. Po dokončení konfigurace se v zařízení zobrazí stav **OK**.



Jak testovat připojení VPN

1. Klikněte na **Zařízení** > **Cloudový server pro obnovení**.
2. Klikněte na **Nastavení VPN**.
3. Zkontrolujte, zda platí, že je zařízení VPN a VPN server ve stavu **OK**.
4. Klikněte na možnost **Testovat**.

   Zařízení VPN zkontroluje připojení k serveru VPN. Zobrazí se seznam prováděných testů a jejich výsledky.

10.2.3 Operace se zařízením VPN

V konzole zálohování (**Zařízení** > **Cloudový server pro obnovení** > **Nastavení VPN**) můžete:

- připojit nebo odpojit dané zařízení,
- zrušit registraci zařízení.

K těmto nastavením získáte přístup kliknutím na ikonu ozubeného kola na obrázku zařízení VPN.

V konzole zařízení můžete provést následující:

- změnit heslo k zařízení,
- zobrazit a změnit nastavení sítě,
- provést registraci nebo změnit registrační účet (opakováním registrace),
- restartovat službu VPN,
- restartovat zařízení,
- provést příkaz ping na síťovou adresu při odstraňování problémů.

Aktualizace zařízení VPN

Zařízení VPN jednou denně automaticky kontroluje aktualizace. Je-li zjištěna nová verze, provede se aktualizace automaticky bez restartování nebo zastavení služby VPN.

10.2.4 Připojení point-to-site (P2S)

Zařízení VPN umožňuje připojení mezi cloudovým serverem pro obnovení a vaší místní sítí. Pokud je místní síť nedostupná, potřebujete mít možnost připojit se přímo ke cloudovému serveru pro obnovení. Tento druh připojení se často nazývá P2S (point-to-site) a liší se od připojení S2S (site-to-site).

Jak nastavit uživatelské jméno a heslo pro připojení P2S

1. V konzole zálohování (**Zařízení** > **Cloudový server pro obnovení** > **Nastavení VPN**) klikněte na obrázku serveru VPN na ikonu ozubeného kola.
2. Klikněte na možnost **Změnit pověření**.
3. Vytvořte a zadejte uživatelské jméno.
4. Vytvořte a zadejte heslo.
5. Potvrďte heslo.
6. Klikněte na tlačítko **OK**.

Jak vytvořit připojení P2S

1. Nainstalujte klienta OpenVPN do počítače, který se má připojit ke cloudovému serveru pro obnovení.

   Podporované verze klienta OpenVPN: 2.4.0 a novější.
2. V konzole zálohování klikněte na **Zařízení** > **Cloudový server pro obnovení** > **Nastavení VPN**.
3. Klikněte na ikonu ozubeného kola v levém horním rohu serveru VPN.
4. Klikněte na možnost **Stáhnout konfiguraci pro OpenVPN**.
5. Naimportujte konfiguraci do OpenVPN.
6. Po vzniku připojení zadejte uživatelské jméno a heslo, které jste vytvořili podle popisu výše.

10.2.5 Parametry připojení point-to-site (P2S)

V konzole zálohování (**Zařízení** > **Cloudový server pro obnovení** > **Nastavení VPN**) klikněte na obrázku serveru VPN na ikonu ozubeného kola. Software zobrazí uživatelské jméno nastavené pro připojení P2S a následující položky nabídky.

Stáhnout konfiguraci pro OpenVPN

Tím se stáhne konfigurační soubor klienta OpenVPN. Tento soubor je nutný k vytvoření připojení P2S ke cloudovému serveru pro obnovení (str. 100).

Změnit pověření

Uživatelské jméno a heslo používané k připojení P2S můžete změnit.

Je to nutné v následujících případech:

- během počáteční konfigurace připojení P2S (str. 100),
- při plánované změně hesla podle zásad zabezpečení nastavených ve vaší organizaci,
- je-li nutné omezit přístup ke cloudovému serveru pro obnovení některým uživatelům (například bývalým zaměstnancům).

Po změně pověření zajistěte, aby byli uživatelé informováni o nutnosti používat jiná pověření.

Opětovné vygenerování konfiguračního souboru

Konfigurační soubor klienta OpenVPN můžete znovu vygenerovat.

Je to nutné v následujících případech:

- Jestliže brzy vyprší platnost certifikátu klienta VPN. Datum vypršení platnosti zobrazíte kliknutím na ikonu (i) na obrázku serveru VPN.
- Máte-li podezření, že došlo k ohrožení konfiguračního souboru.

Jakmile dojde k aktualizaci konfiguračního souboru, není již možné se připojit pomocí starého konfiguračního souboru. Zajistěte distribuci nového souboru uživatelům, kteří mají povoleno používat připojení P2S.

10.3 Práce se serverem pro obnovení

10.3.1 Vytvoření serveru pro obnovení

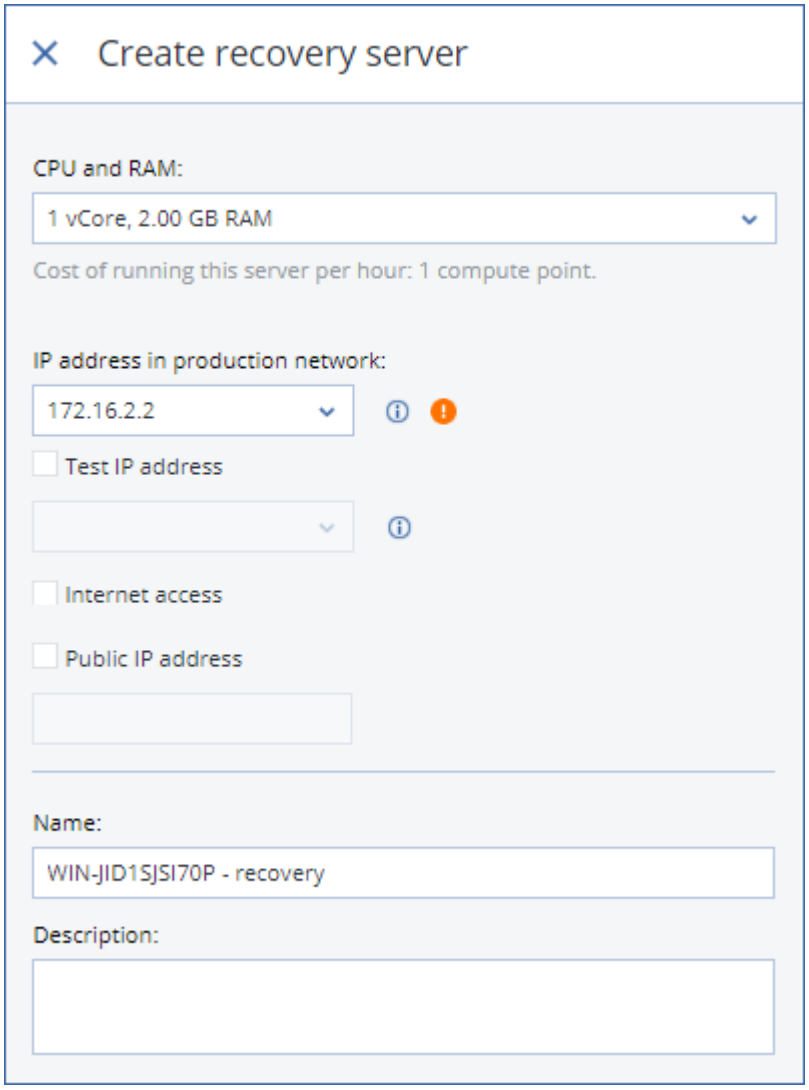
Předpoklady

- V počítači, který chcete ochránit, musí být zavedený plán zálohování.
  - Zálohovat můžete celý počítač nebo pouze disky požadované ke spuštění a poskytování potřebných služeb.
  - Jako cíl je nutné zvolit cloudové úložiště.
  - Musí být vypnuto šifrování záloh.
  - Doporučujeme, abyste před vytvořením serveru pro obnovení alespoň jednou spustili plán zálohování, kterým zajistíte úspěšné vytvoření cloudových záloh.
- Je třeba nastavit připojení VPN ke cloudovému serveru pro obnovení.

Jak vytvořit server pro obnovení

1. Vyberte počítač, který chcete ochránit.

2. Klikněte na možnost **Obnovení po havárii** a potom na **Vytvořit server pro obnovení**.



3. Vyberte počet virtuálních jader a velikost paměti RAM.

   Věnujte pozornost výpočetním bodům u každé možnosti. Počet výpočetních bodů odráží náklady na hodinu provozu serveru pro obnovení.

4. Zadejte IP adresu, kterou bude server mít v produkční síti. Jako výchozí se nastaví IP adresa původního počítače.

   Poznámka *Jestliže používáte server DHCP, přidejte tuto IP adresu do seznamu pro vyloučení serverů, abyste se vyhnuli konfliktům IP adres.*

5. [Volitelné] Zaškrtněte políčko **Testovat IP adresu** a potom ji zadejte.

   Tím získáte možnost se připojit k serveru pro obnovení pomocí RDP nebo SSH během testu převzetí služeb při selhání. V režimu testu převzetí služeb při selhání nahradí server VPN testovací IP adresu produkční IP adresou pomocí protokolu NAT.

   Pokud toto políčko nezaškrtnete, bude během testu převzetí služeb při selhání server přístupný pouze pomocí konzoly.

   Poznámka *Jestliže používáte server DHCP, přidejte tuto IP adresu do seznamu pro vyloučení serverů, abyste se vyhnuli konfliktům IP adres.*

   Je možné vybrat jednu z následujících navržených IP adres nebo zadat jinou.

6. [Volitelné] Zaškrtněte políčko **Přístup k internetu**.

Povolíte tím přístup serveru pro obnovení k internetu v průběhu převzetí služeb při selhání nebo testu převzetí služeb při selhání.

7. [Volitelné] Zaškrtněte políčko **Veřejná IP adresa**.

   Použitím veřejné IP adresy bude server pro obnovení dostupný z internetu v průběhu převzetí služeb při selhání nebo testu převzetí služeb při selhání. Pokud toto políčko nezaškrtnete, bude server k dispozici pouze v produkční síti.

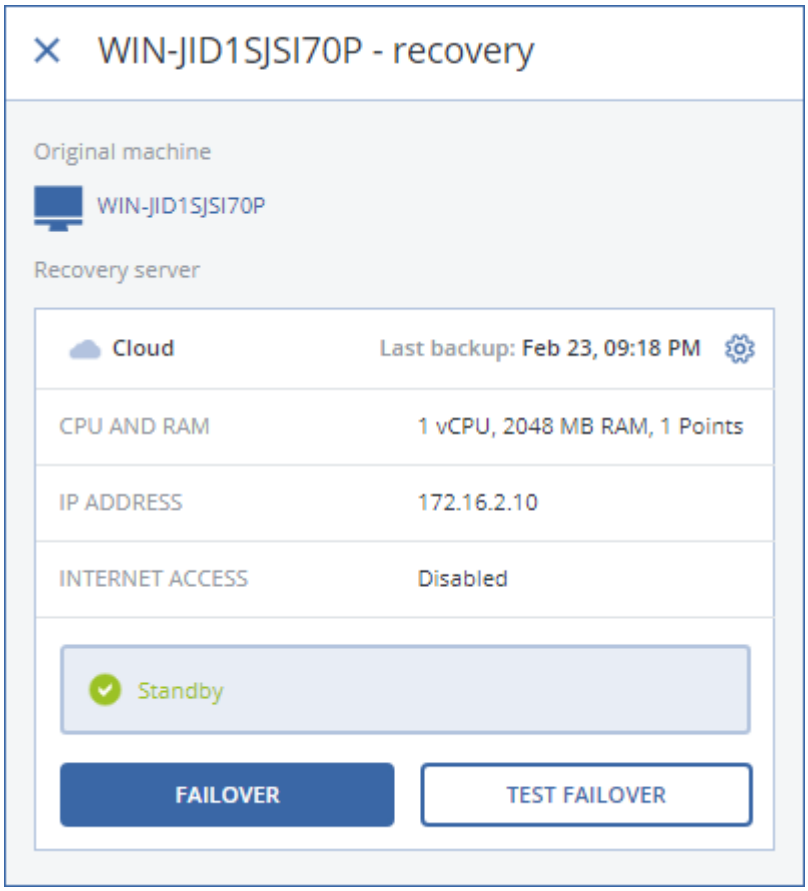
   Veřejná IP adresa se zobrazí po dokončení konfigurace. Pro příchozí spojení s veřejnými IP adresami jsou otevřené následující porty:

   TCP: 80, 443, 8088, 8443

   UDP: 1194

   Pokud potřebujete otevřít další porty, kontaktujte tým podpory.
8. [Volitelné] Změňte název serveru pro obnovení.
9. [Volitelné] Zadejte popis serveru pro obnovení.
10. Klikněte na tlačítko **Hotovo**.

Server pro obnovení se objeví v části **Cloudový server pro obnovení** konzoly pro zálohování. K jeho nastavení se také dostanete vybráním původního počítače a kliknutím na možnost **Obnovení po havárii**.



10.3.2 Jak funguje převzetí služeb při selhání

Operace převzetí služeb při selhání využívá funkci spuštění virtuálního počítače ze zálohy (str. 164).

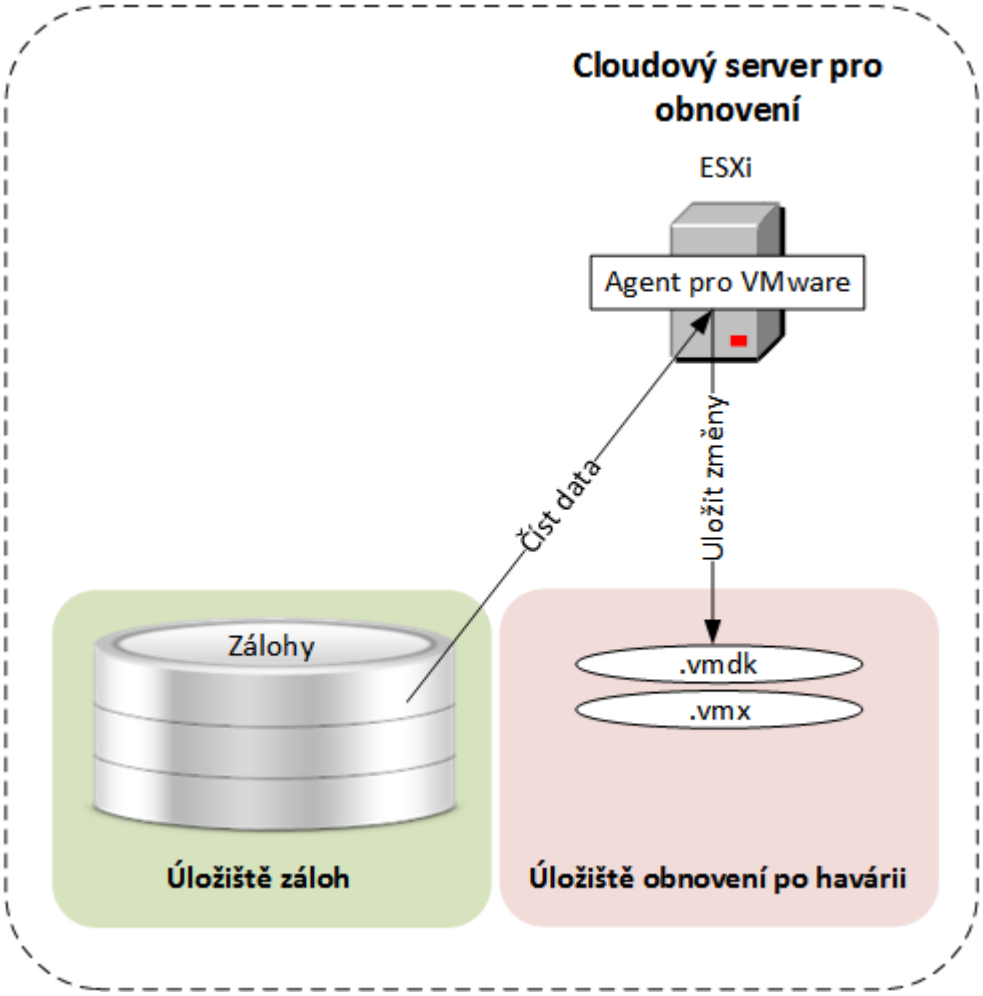
Spuštění serveru pro obnovení znamená, že se z některé zálohy původního počítače spustí virtuální počítač s předdefinovanými parametry.

Při **testovacím převzetí služeb při selhání** není virtuální počítač úplně hotový. Agent čte obsah virtuálních disků přímo ze zálohy a při tom náhodně přistupuje k různým částem zálohy. Server tedy může pracovat pomaleji, ale zabírá v datovém úložišti (úložiště obnovení po havárii) málo místa.

Při **skutečném převzetí služeb při selhání** je virtuální počítač dokončen co nejrychleji kvůli co nejlepšímu výkonu. Jakmile se server pro obnovení spustí, změní se jeho stav na **Dokončení**. Během tohoto procesu se virtuální disky serveru přenesou ze zálohy do úložiště pro obnovení po havárii. Obnovení virtuálního počítače vlastně probíhá za jeho běhu. Kvůli tomuto procesu může server pracovat pomaleji. Po skončení se výkon serveru vrátí na normální úroveň. Stav serveru se změní na **Převzetí služeb při selhání**.

Pokud obsahuje server pro obnovení agenta pro zálohování, dojde k zastavení služby daného agenta, aby nedošlo k nechtěným aktivitám, jako je například spuštění zálohování nebo vytváření zpráv o zastaralých stavech do služby zálohování.

Následující diagram ukazuje spuštění serveru pro obnovení včetně spotřeby úložiště.



10.3.3 Testování převzetí služeb při selhání

Testování převzetí služeb při selhání znamená spuštění serveru pro obnovení v testovací síti VLAN, která je oddělená od produkční sítě. Za účelem ověření vzájemné interakce můžete otestovat několik serverů pro obnovení najednou. V testovací síti komunikují servery pomocí svých produkčních IP adres, ale nemohou iniciovat připojení TCP nebo UDP k počítačům v místní síti.

I když je testování převzetí služeb při selhání volitelné, doporučujeme ho zařadit jako pravidelný proces, který se opakuje přiměřeně nákladům a bezpečnosti. Osvědčeným postupem je vytvořit runbook – sadu instrukcí popisujících způsob spuštění produkčního prostředí v cloudu.

Jak spustit test převzetí služeb při selhání

1. Vyberte původní počítač nebo server pro obnovení, který chcete otestovat.
2. Klikněte na možnost **Obnovení po havárii**.

   Otevře se popis serveru pro obnovení.
3. Klikněte na možnost **Test převzetí služeb při selhání**.
4. Vyberte bod obnovy a klikněte na **Test převzetí služeb při selhání**.

   Po spuštění se stav serveru pro obnovení změní na **Testování převzetí služeb při selhání**.
5. Otestujte server pro obnovení pomocí jakékoli z následujících metod:
   - V konzole pro zálohování klikněte na **Zařízení** > **Cloudový server pro obnovení**, vyberte server pro obnovení a potom klikněte na možnost **Konzola** na pravém panelu.
   - Připojte se k serveru pro obnovení pomocí RDP nebo SSH a otestujte IP adresu, kterou jste zadali při vytváření tohoto serveru. Vyzkoušejte připojení uvnitř i vně produkční sítě (jak je popsáno v části Připojení point-to-site (str. 100)).
   - V rámci serveru pro obnovení spusťte skript.

     Skript může kontrolovat přihlašovací obrazovku, spouštění aplikací, připojení k internetu a schopnost jiných počítačů připojit se k serveru pro obnovení.
   - Pokud má server pro obnovení přístup k internetu a veřejné IP adrese, je vhodné použít aplikaci TeamViewer.
6. Po dokončení testu klikněte na možnost **Zastavit testování** v konzole zálohování.

   Server pro obnovení se zastaví. Veškeré změny provedené na serveru pro obnovení v průběhu testu budou ztraceny.

10.3.4 Provedení převzetí služeb při selhání

Převzetí služeb při selhání je proces přesunutí zátěže z vaší firmy do cloudu a také stav, kdy zůstává zátěž v cloudu.

Po zahájení převzetí služeb při selhání se v produkční síti spustí server pro obnovení. Z původního počítače budou odejmuty všechny plány zálohování. Automaticky se vytvoří nový plán zálohování a použije se na server pro obnovení.

Jak provést převzetí služeb při selhání

1. Ujistěte se, že není původní počítač dostupný v síti.
2. V konzole zálohování vyberte původní počítač nebo server pro obnovení, který tomuto počítači odpovídá.
3. Klikněte na možnost **Obnovení po havárii**.

   Otevře se popis serveru pro obnovení.
4. Klikněte na možnost **Převzetí služeb při selhání**.
5. Vyberte bod obnovy a klikněte na **Převzetí služeb při selhání**.

   Po spuštění serveru pro obnovení se jeho stav změní na **Dokončení** a po určité době na **Převzetí služeb při selhání**. Je důležité vědět, že server je v obou stavech dostupný, i když indikátor průběhu signalizuje činnost. Podrobnosti najdete v oddílu Jak funguje převzetí služeb při selhání (str. 104).

6. Zobrazením konzoly serveru pro obnovení se přesvědčte, zda je spuštěný. Klikněte na **Zařízení** > **Cloudový server pro obnovení**, vyberte server pro obnovení a potom klikněte na možnost **Konzola** na pravém panelu.
7. Ujistěte se, zda je možné k serveru pro obnovení přistupovat pomocí produkční IP adresy zadané při vytváření tohoto serveru.

Jakmile je server pro obnovení hotový, vytvoří se automaticky nový plán zálohování, který se také použije. Tento plán zálohování vychází z plánu zálohování použitého při vytváření serveru pro obnovení, ale má některá omezení. V tomto plánu můžete změnit pouze rozvrh a pravidla zachování. Další informace naleznete na stránce Zálohování cloudových serverů (str. 109).

Jediným způsobem, jak se dostat ze stavu převzetí služeb při selhání je navrácení služeb po obnovení.

10.3.5 Provedení navrácení služeb po obnovení

Navrácení služeb po obnovení je proces přesunutí zátěže z cloudu zpět do vaší firmy.

Během tohoto procesu je přesouvaný server nedostupný. Doba trvání údržby se přibližně rovná době trvání zálohování a následného obnovení serveru.

Jak provést navrácení služeb po obnovení

1. Vyberte server pro obnovení, který je ve stavu **převzetí služeb při selhání**.
2. Klikněte na možnost **Obnovení po havárii**.

   Otevře se popis serveru pro obnovení.
3. Klikněte na možnost **Připravit navrácení služeb po obnovení**.

   Server pro obnovení se zastaví a zazálohuje se do cloudového úložiště. Počkejte na dokončení zálohování.

   V dané chvíli budou k dispozici dvě akce: **Zrušit navrácení služeb po obnovení** a **Provést navrácení služeb po obnovení**. Kliknutím na možnost **Zrušit navrácení služeb po obnovení** se spustí server pro obnovení a bude pokračovat převzetí služeb při selhání.
4. Obnovte server z této zálohy do hardwaru nebo do virtuálního počítače ve vaší firmě.
   - Při použití spouštěcího média postupujte způsobem popsaným v tématu Obnova disků pomocí spouštěcího média (str. 80). Ujistěte se, že jste se přihlásili do cloudu s účtem, pro který je zaregistrován server, a že jste vybrali nejnovější zálohu.
   - Pokud je cílový počítač online nebo se jedná o virtuální počítač, můžete použít konzolu pro zálohování. Na kartě **Zálohy** vyberte cloudové úložiště. V okně **Počítač k procházení** vyberte cílový fyzický počítač nebo počítač, ve kterém je spuštěn agent, pokud je cílem virtuální počítač. Vybraný počítač musí být zaregistrován pro stejný účet, pro který je zaregistrován server. Vyhledejte nejnovější zálohu serveru, klikněte na možnost **Obnovit celý počítač** a potom nastavte další parametry obnovení. Podrobné pokyny naleznete v části Obnovení počítače (str. 76).

   Zkontrolujte, zda bylo obnovení dokončeno a obnovený počítač správně pracuje.
5. V konzole zálohování se vraťte k serveru pro obnovení a potom klikněte na možnost **Provést navrácení služeb po obnovení**.

   Server pro obnovení a body obnovy se připraví na další převzetí služeb při selhání. Nové body obnovy můžete vytvořit pomocí plánu zálohování na novém místním serveru.

10.4 Práce s primárním serverem

10.4.1 Vytvoření primárního serveru

Předpoklady

- Je třeba nastavit připojení VPN ke cloudovému serveru pro obnovení.

Jak vytvořit primární server

1. Klikněte na **Zařízení** > **Cloud**.
2. Klikněte na možnost **Nový**.
3. Vyberte šablonu nového virtuálního počítače.
4. Vyberte počet virtuálních jader a velikost paměti RAM.

   Věnujte pozornost výpočetním bodům u každé možnosti. Počet výpočetních bodů odráží náklady na hodinu provozu primárního serveru.
5. Zadejte IP adresu, kterou bude server mít v produkční síti. Jako výchozí se nastaví první volná IP adresa v produkční síti.

   Poznámka *Jestliže používáte server DHCP, přidejte tuto IP adresu do seznamu pro vyloučení serverů, abyste se vyhnuli konfliktům IP adres.*
6. [Volitelné] Zaškrtněte políčko **Přístup k internetu**.

   Povolíte tím přístup primárního serveru k internetu.
7. [Volitelné] Zaškrtněte políčko **Veřejná IP adresa**.

   Použitím veřejné IP adresy bude primární server dostupný z internetu. Pokud toto políčko nezaškrtnete, bude server k dispozici pouze v produkční síti.

   Veřejná IP adresa se zobrazí po dokončení konfigurace. Pro příchozí spojení s veřejnými IP adresami jsou otevřené následující porty:

   TCP: 80, 443, 8088, 8443

   UDP: 1194

   Pokud potřebujete otevřít další porty, kontaktujte tým podpory.
8. [Volitelné] Změňte velikost virtuálního disku. Pokud potřebujete více než jeden pevný disk, klikněte na tlačítko **Přidat disk** a potom zadejte velikost nového disku.
9. Vytvořte a zadejte název primárního serveru.
10. [Volitelné] Zadejte popis primárního serveru.
11. Klikněte na tlačítko **Hotovo**.

Primární server bude zpřístupněn v produkční síti. Tento server můžete spravovat pomocí příslušné konzoly, vzdálené plochy (RDP), služby SSH nebo aplikace TeamViewer.

10.4.2 Operace s primárním serverem

Primární server se objeví v části **Cloudový server pro obnovení** konzoly pro zálohování.

Server spustíte nebo zastavíte kliknutím na možnosti **Spustit** nebo **Zastavit** na pravém panelu.

Chcete-li upravit nastavení primárního serveru, zastavte ho, klikněte na **Informace** a potom na **Upravit**.

Chcete-li na primárním serveru použít plán zálohování, klikněte na možnost **Zálohovat**. Zobrazí se předdefinovaný plán zálohování, ve kterém můžete změnit pouze plán a pravidla zachování. Další informace naleznete na stránce Zálohování cloudových serverů (str. 109).

10.5 Zálohování cloudových serverů

Primární servery a servery pro obnovení zálohuje Agent pro VMware, který je nainstalovaný na cloudovém serveru pro obnovení. V první verzi má toto zálohování částečně omezenou funkčnost ve srovnání se zálohováním pomocí místních agentů. Tato omezení jsou dočasná a budou odstraněna v příštích verzích.

- Jediné možné umístění zálohy je v cloudovém úložišti.
- Plán zálohování nelze použít na více serverů. Každý server musí mít svůj vlastní plán zálohování, i když všechny plány zálohování mají stejné nastavení.
- Pro server lze použít pouze jeden plán zálohování.
- Zálohování s podporou aplikací není podporováno.
- Šifrování není k dispozici.
- Možnosti zálohování nejsou k dispozici.

Pokud odstraníte primární server, budou odstraněny také jeho zálohy.

Server pro obnovení se zálohuje pouze ve stavu převzetí služeb při selhání. Jeho zálohy pokračují v posloupnosti zálohování původního serveru. Když probíhá navrácení služeb po obnovení, může původní server pokračovat v posloupnosti zálohování. Zálohy serveru pro obnovení je tak možné odstranit pouze ručně nebo na základě použití pravidel zachování. Při odstranění serveru pro obnovení zůstávají jeho zálohy vždy zachovány.

10.6 Používání runbooků

Runbook je sada pokynů, které popisují způsob spuštění produkčního prostředí v cloudu. Runbooky můžete vytvářet v konzole pro zálohování. Pokud chcete získat přístup ke kartě **Runbooky**, vyberte **Obnovení po havárii** > **Runbooky**.

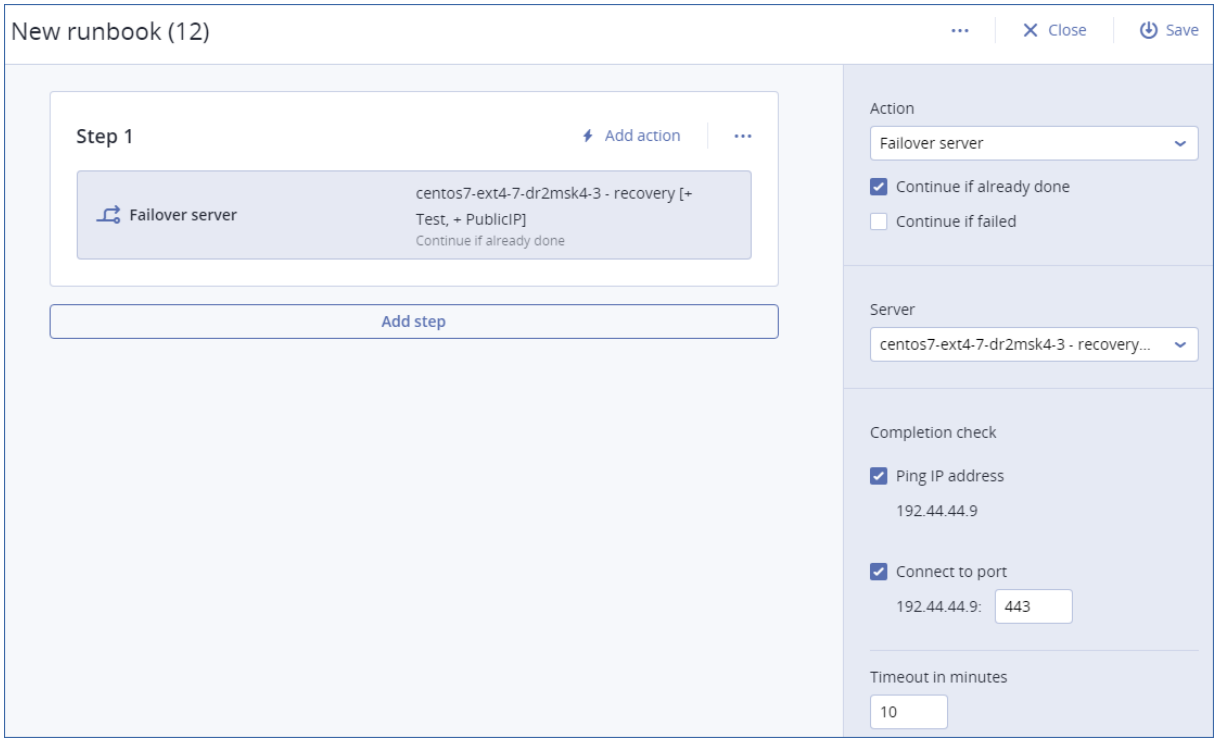
Proč používat sady runbook?

Co umožňují runbooky:

- Automaticky převzít služby při selhání jednoho nebo více serverů.
- Automaticky zkontrolovat výsledek převzetí služeb při selhání příkazem ping na IP adresu serveru a kontrolovat připojení k zadanému portu.
- Nastavit pořadí operací na serverech, na kterých běží distribuované aplikace.
- Zahrnout do pracovního postupu ruční operace.
- Ověřit integritu řešení pro obnovení po havárii spuštěním runbooků v testovacím režimu.

10.6.1 Vytvoření runbooku

Pokud chcete začít vytvářet runbook, klikněte na **Vytvořit runbook** > **Přidat krok** > **Přidat akci**. Akce a kroky můžete přesouvat přetažením. Nezapomeňte dát runbooku jedinečný název. Při vytváření dlouhého runbooku občas klikněte na **Uložit**. Až budete hotovi, klikněte na **Zavřít**.



Kroky a akce

Runbook se skládá z kroků, které se spouštějí postupně. Krok se skládá z akcí, které se spouštějí současně. Z čeho se může skládat akce:

- Z operace prováděné s cloudovým serverem (**server převzetí služeb při selhání**, **spuštění serveru**, **zastavení serveru**, **server navrácení služeb po obnovení**). Pokud chcete tuto operaci definovat, musíte zvolit operaci, cloudový server a parametry operace.
- Ruční operaci je potřeba slovně popsat. Po dokončení operace musí uživatel kliknout na tlačítko potvrzení, aby mohl runbook pokračovat.
- Spuštění dalšího runbooku Pokud chcete tuto operaci definovat, potřebujete zvolit runbook.

  Runbook může obsahovat jen jedno spuštění daného runbooku. Pokud například přidáte akci „spustit runbook A“, můžete přidat akci „spustit runbook B“, ale nemůžete přidat další akci „spustit runbook A“.

Poznámka: *V této verzi produktu musí uživatel provést navrácení služeb po obnovení ručně. Pokud je to nutné, zobrazí runbook výzvu.*

Parametry akce

Všechny operace s cloudovými servery mají následující parametry:

- **Pokračovat, pokud byla akce dokončena** (ve výchozím nastavení zapnuté)

  Tento parametr definuje chování runbooku po dokončení požadované operace (například bylo provedeno převzetí služeb při selhání nebo spuštění serveru). Pokud je nastavení zapnuté, runbook vydá upozornění a bude pokračovat. Pokud je nastavení vypnuté, operace i runbook selžou.

- **Pokračovat, pokud se akce nezdařila** (ve výchozím nastavení vypnuté)

  Tento parametr definuje chování runbooku, pokud požadovaná operace selže. Pokud je nastavení zapnuté, runbook vydá upozornění a bude pokračovat. Pokud je nastavení vypnuté, operace i runbook selžou.

Kontrola dokončení

K akcím **Server převzetí služeb při selhání** a **Spustit server** můžete přidat kontroly dokončení, abyste ověřili, že server je k dispozici a nabízí potřebné služby. Pokud některá z kontrol selže, považuje se za neúspěšnou i akce.

- **Otestovat IP adresu příkazem ping**

  Software odesílá příkaz ping na produkční IP adresu cloudového serveru, dokud server neodpoví nebo nevyprší časový limit – podle toho, co nastane dříve.
- **Připojit k portu** (výchozí port je 443)

  Software se pokouší připojit ke cloudovému serveru pomocí produkční IP adresy a zadaného portu, dokud se nenaváže spojení nebo nevyprší časový limit – podle toho, co nastane dříve. Tímto způsobem můžete zkontrolovat, jestli běží aplikace, která naslouchá na určeném portu.

Výchozí časový limit je 10 minut. Pokud chcete, můžete ho změnit.

10.6.2 Operace s runbooky

Pokud chcete získat přístup k seznamu operací, přejděte myší na runbook a klikněte na ikonu se třemi tečkami. Pokud runbook neběží, jsou dostupné následující operace:

- **Spustit**
- **Upravit**
- **Klonovat**
- **Odstranit**

Spuštění runbooku

Po každém kliknutí na **Spustit** se zobrazí výzva k zadání spouštěcích parametrů. Tyto parametry platí pro všechny operace převzetí služeb při selhání a navrácení služeb po obnovení, které jsou v runbooku. Runbooky zadané v operacích **Spustit runbook** tyto parametry dědí z hlavního runbooku.

- **Režim převzetí služeb při selhání a navrácení služeb po obnovení**

  Zvolte, jestli chcete spustit zkušební převzetí služeb při selhání (výchozí) nebo skutečné převzetí služeb při selhání (produkční prostředí). Režim navrácení služeb po obnovení bude odpovídat zvolenému režimu převzetí služeb při selhání.
- **Bod obnovy převzetí služeb při selhání**

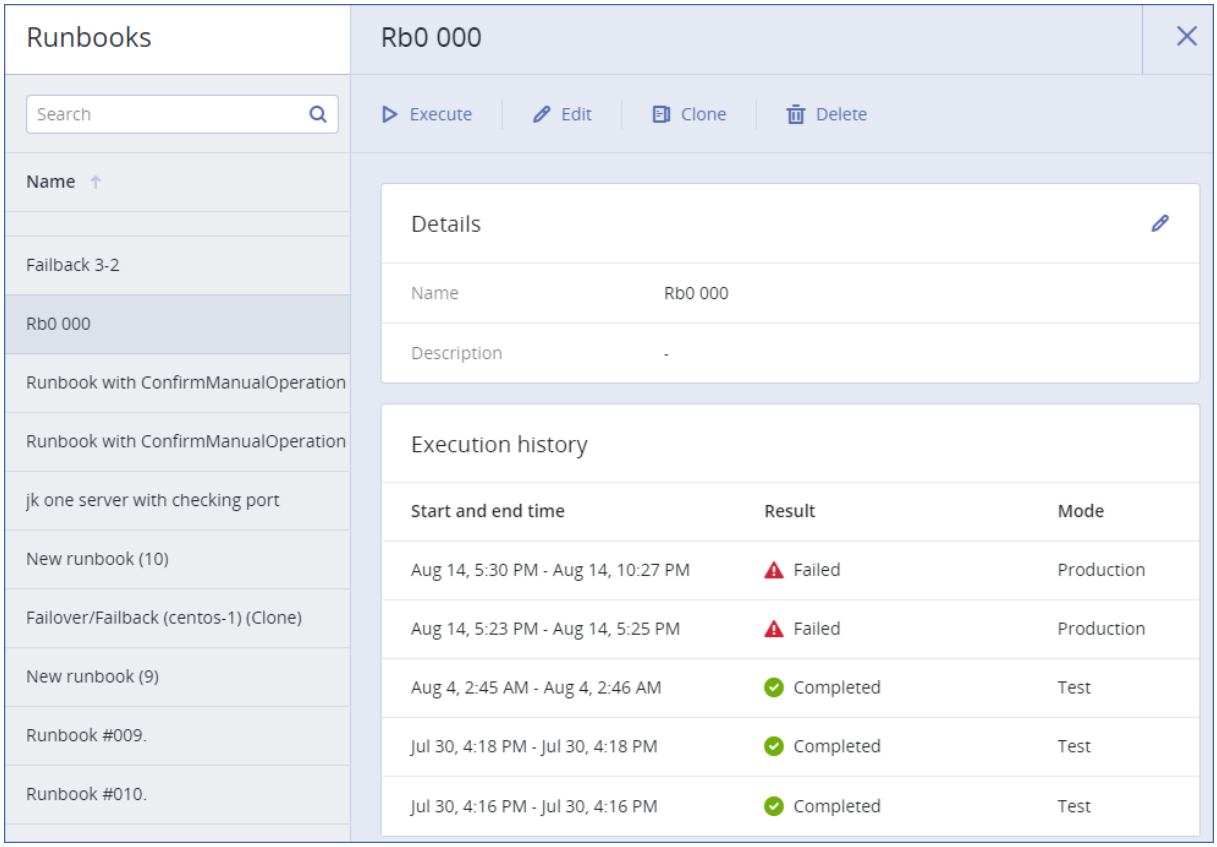
  Zvolte poslední bod obnovy (výchozí) nebo vyberte některý bod v minulosti. Pokud se rozhodnete pro bod v minulosti, vyberou se pro každý server nejbližší předchozí body obnovy před zadaným datem a časem.

Zastavení prováděného runbooku

U spuštěného runbooku můžete v seznamu operací vybrat příkaz **Zastavit**. Software dokončí všechny zahájené akce s výjimkou těch, které vyžadují zásah uživatele.

Zobrazení historie spouštění

Když vyberete runbook na kartě **Sady runbook**, zobrazí software podrobné informace o runbooku a historii spouštění. Pokud chcete zobrazit protokol spuštění, klikněte na řádek, který odpovídá určitému spuštění.



11 Operace se zálohami

11.1 Karta Zálohy

Karta **Zálohy** umožňuje získat přístup ke všem zálohám, včetně záloh počítačů ve stavu offline a počítačů, které již nejsou dále registrovány ve službě zálohování.

Zálohy uložené ve sdílených umístěních (například ve sdílených složkách SMB nebo NFS) jsou viditelné všem uživatelům, kteří mají pro dané umístění oprávnění ke čtení.

V případě cloudového úložiště mají uživatelé přístup pouze ke svým zálohám. Správce může zobrazit zálohy jménem jakéhokoli účtu, který patří dané jednotce nebo společnosti a jejím podřízeným skupinám. Tento účet se nepřímo vybere v okně **Počítač k procházení**. Karta **Zálohy** zobrazuje zálohy všech počítačů registrovaných pod stejným účtem, pod kterým je registrován počítač.

Zálohy vytvořené *cloudovým* agentem pro Office 365 a zálohy dat G Suite se nezobrazí v umístění **cloudového úložiště**, ale v samostatném oddílu s názvem **Zálohy cloudových aplikací**.

Umístění zálohy použitá v plánech zálohování se automaticky přidají do karty **Zálohy**. Chcete-li přidat vlastní složku (například vyměnitelné zařízení USB) do seznamu umístění záloh, klikněte na tlačítko **Procházet** a určete cestu ke složce.

Pokud jste k přidání nebo odebrání některých záloh použili správce souborů, klikněte na ikonu ozubeného kola vedle názvu umístění a pak klikněte na **Aktualizovat**.

Umístění zálohy (kromě cloudového úložiště) zmizí z karty **Zálohy**, pokud byly ze zálohovací služby odstraněny všechny počítače, které byly do příslušného umístění někdy zálohovány. Tak je zajištěno, že za zálohy uložené v tomto úložišti nemusíte platit. Jakmile dojde k zálohování do tohoto umístění, umístění se znovu přidá spolu se všemi zálohami, které jsou v něm uloženy.

Postup výběru body obnovy pomocí karty Zálohy

1. Na kartě **Zálohy** vyberte umístění, kde jsou uloženy zálohy.

   Software zobrazí všechny zálohy, u kterých má váš účet oprávnění je zobrazit v daném umístění. Zálohy jsou seskupeny do skupin. Názvy skupin se tvoří podle následující šablony:

   `<název počítače> – <název plánu zálohování>`
2. Vyberte skupinu, ze které chcete obnovit data.
3. [Volitelné] Klikněte na tlačítko **Změnit** vedle položky **Počítač k procházení** a poté vyberte jiný počítač. Některé zálohy smí procházet pouze určití agenti. Například pokud chcete procházet zálohy databází aplikace Microsoft SQL Server, je nutné vybrat počítač, na kterém běží Agent pro SQL.

   Důležité *Mějte na vědomí, že* ***Počítač k procházení*** *je výchozí umístění zálohy fyzického počítače, ze které se provede obnova. Po výběru bodu obnovy a kliknutí na možnost* ***Obnovit*** *zkontrolujte nastavení u položky* ***Cílový počítač****, abyste se ujistili, že chcete provést obnovu na tento konkrétní počítač. Chcete-li změnit umístění obnovy, vyberte jiný počítač pomocí možnost* ***Počítač k procházení****.*
4. Klikněte na možnost **Zobrazit zálohy**.
5. Vyberte bod obnovy.

11.2 Připojování svazků ze zálohy

Když připojíte svazek ze zálohy na úrovni disku, budete k němu moct přistupovat, jako by se jednalo o fyzický disk. Svazky jsou připojovány v režimu jen pro čtení.

Požadavky

- Tato funkce je dostupná jen ve Windows v Průzkumníku souborů.
- Na počítači, na kterém chcete svazek připojit, musí být nainstalovaný Agent pro Windows.
- Zálohovaný systém souborů musí být podporován tou verzí Windows, kterou váš počítač používá.
- Záloha musí být uložená v místní složce, v síťovém umístění (SMB/CIFS) nebo v oddílu Secure Zone.

Jak připojit svazek ze zálohy

1. V Průzkumníku souborů přejděte do umístění se zálohou.
2. Dvakrát klikněte na soubor zálohy. Názvy souborů se tvoří podle následující šablony:

   `<název počítače> – <GUID plánu zálohování>`.
3. Pokud je záloha zašifrovaná, zadejte šifrovací heslo. Jinak tento krok přeskočte.

   Průzkumník souborů zobrazí body obnovy.
4. Dvakrát klikněte na požadovaný bod obnovy.

   Průzkumník souborů zobrazí zálohované svazky.

   Tip *Když na svazek dvakrát kliknete, můžete procházet jeho obsah. Soubory a složky ze zálohy se dají kopírovat do jakékoli složky ve vašem systému souborů.*

5. Klikněte pravým tlačítkem na svazek, který chcete připojit, a poté klikněte na **Připojit v režimu jen pro čtení**.
6. Pokud je záloha uložená v síťovém umístění, zadejte pověření k přístupu. Jinak tento krok přeskočte.

   Software připojí vybraný svazek. Svazku bude přiděleno první nepoužité písmeno.

Jak odpojit svazek

1. V Průzkumníku souborů přejděte na **Počítač** (respektive **Tento počítač** v systému Windows 8.1 a starším).
2. Klikněte pravým tlačítkem na připojený svazek.
3. Klikněte na **Odpojit**.

   Software odpojí vybraný svazek.

11.3 Odstranění záloh

Postup odstranění záloh počítače, který je ve stavu online a je přítomný v konzole pro zálohování

1. Na kartě **Všechna zařízení** vyberte počítač, jehož zálohy chcete odstranit.
2. Klikněte na možnost **Obnova**.
3. Vyberte umístění, ze kterého chcete odstranit úlohy.
4. Proveďte jeden z následujících úkonů:
   - Chcete-li odstranit jednu zálohu, vyberte zálohu, kterou chcete odstranit, a poté klikněte na znak X.
   - Všechny zálohy ve vybraném umístění odstraníte kliknutím na **Odstranit vše**.
5. Potvrďte své rozhodnutí.

Jak odstranit zálohy libovolného počítače

1. Na kartě **Zálohy** vyberte umístění, ze kterého chcete odstranit zálohy.

   Software zobrazí všechny zálohy, u kterých má váš účet oprávnění je zobrazit v daném umístění. Zálohy jsou seskupeny do skupin. Názvy skupin se tvoří podle následující šablony:

   `<název počítače> – <název plánu zálohování>`
2. Vyberte skupinu.
3. Proveďte jeden z následujících úkonů:
   - Chcete-li odstranit jednu zálohu, klikněte na možnost **Zobrazit zálohy**, vyberte zálohu, kterou chcete odstranit, a poté klikněte na znak X.
   - Kliknutím na tlačítko **Odstranit** odstraníte vybranou skupinu.
4. Potvrďte své rozhodnutí.

Odstranění záloh přímo z cloudového úložiště

1. Přihlaste se do cloudového úložiště způsobem popsaným v části Stahování souborů z cloudového úložiště (str. 84).
2. Klikněte na název počítače, jehož zálohy chcete odstranit.

   Software zobrazí jednu nebo více skupin záloh.
3. Klikněte na ikonu ozubeného kola u skupiny záloh, kterou chcete odstranit.
4. Klikněte na **Odebrat**.
5. Potvrďte operaci.

Co dělat, pokud jste odstranili místní zálohy pomocí správce souborů

Doporučujeme, abyste zálohy odstraňovali pomocí konzoly pro zálohování, kdykoli je to možné. Pokud jste místní zálohy odstranili pomocí správce souborů, postupujte následovně:

1. Na kartě **Zálohy** klikněte na ikonu ozubeného kola vedle názvu umístění.
2. Klikněte na **Aktualizovat**.

Tímto způsobem informujete zálohovací službu o tom, že se snížilo využití místního úložiště.

12 Operace s plány zálohování

Informace o vytvoření plánu zálohování najdete v tématu o zálohování (str. 33).

Jak upravit plán zálohování

1. Pokud chcete upravit plán zálohování pro všechny počítače, pro které se používá, vyberte jeden z nich. Jinak vyberte konkrétní počítače, u kterých chcete plán zálohování upravit.
2. Klikněte na možnost **Zálohovat**.
3. Vyberte plán zálohování, který chcete upravit.
4. Klikněte na ikonu ozubeného kola vedle názvu plánu zálohování a potom na možnost **Upravit**.
5. Chcete-li upravit parametry plánu, klikněte na odpovídající část panelu plánu zálohování.
6. Klikněte na **Uložit změny**.
7. Pokud chcete plán zálohování změnit u všech počítačů, kde se používá, klikněte na možnost **Použít změny na tento plán zálohování**. Jinak klikněte na možnost **Vytvořit nový plán zálohování pouze pro zvolená zařízení**.

Jak zrušit plán zálohování u počítačů

1. Vyberte počítače, u kterých chcete plán zálohování zrušit.
2. Klikněte na možnost **Zálohovat**.
3. Pokud počítače používají několik plánů zálohování, vyberte ten, který chcete zrušit.
4. Klikněte na ikonu ozubeného kola vedle názvu plánu zálohování a potom klikněte na **Odejmout**.

Jak odstranit plán zálohování

1. Vyberte libovolný počítač, pro který platí plán zálohování, který chcete odstranit.
2. Klikněte na možnost **Zálohovat**.
3. Pokud počítač používá několik plánů zálohování, vyberte ten, který chcete odstranit.
4. Klikněte na ikonu ozubeného kola vedle názvu plánu zálohování a potom klikněte na **Odstranit**.
   Plán zálohování se zruší ze všech počítačů a zcela se odstraní z webového rozhraní.

13 Ochrana mobilních zařízení

K zálohování a obnovování dat z mobilních zařízení použijte zálohovací aplikaci.

Podporovaná mobilní zařízení

- Smartphony a tablety se systémem Android 4.1 nebo novějším.
- iPhony, iPady a iPody s iOS 8 nebo novějším.

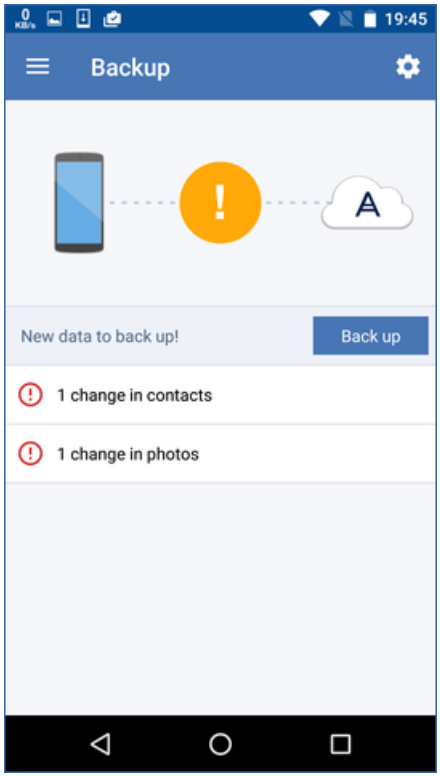
Co můžete zálohovat

- Kontakty

- Fotografie
- Videa
- Kalendáře
- Textové zprávy (jen na zařízeních s Androidem)
- Připomínky (jen na zařízeních se systémem iOS)

Co byste měli vědět

- Data se dají zálohovat jen do cloudového úložiště.
- Při každém otevření aplikace se vám zobrazí přehled změn, ke kterým v datech došlo, a vy budete moct ručně spustit zálohování.



- Funkce **Souvislá záloha** je ve výchozím nastavení zapnutá. V tomto režimu zálohovací aplikace každých šest hodin ověřuje, zda došlo ke změnám dat, a případně automaticky spustí zálohování. Souvislé zálohování můžete vypnout nebo ho v nastaveních aplikace změnit na **Jen během nabíjení**.
- K zálohovaným datům se dostanete z každého mobilního zařízení, které máte zaregistrované pod svým účtem. Díky tomu můžete snadno přenést data ze starého mobilního zařízení do nového. Kontakty a fotky ze zařízení se systémem Android nelze obnovit do systému iOS a naopak. Fotky, videa a kontakty si můžete stáhnout i do počítače, a to pomocí konzoly pro zálohování.
- K datům zálohovaným z mobilních zařízení registrovaných prostřednictvím vašeho účtu lze získat přístup pouze z tohoto účtu. Tato data nemůže zobrazit ani obnovit nikdo kromě vás.
- V zálohovací aplikaci lze obnovit jen data z nejnovější zálohy. Potřebujete-li obnovit data ze starších záloh, použijte k tomu konzolu pro zálohování na tabletu nebo na počítači.
- Pravidla zachování se nevztahují na zálohy mobilních zařízení.
- Máte-li během zálohování v zařízení vloženou SD kartu, budou se zálohovat i data uložená na této kartě. Data budou obnovena na libovolnou SD kartu, která je během obnovení vložena v zařízení, případně do interního úložiště, pokud není žádná SD karta dostupná.

- Bez ohledu na to, zda byla původní data uložená v interním úložišti zařízení, nebo na SIM kartě, budou obnovená data umístěna v interním úložišti.

Pokyny krok za krokem

Stažení zálohovací aplikace

1. V mobilním zařízení otevřete prohlížeč a zadejte adresu URL konzoly pro zálohování.
2. Přihlaste se pomocí svého účtu.
3. Klikněte na **Všechna zařízení** > **Přidat**.
4. V části **Mobilní zařízení** vyberte typ zařízení.

   Podle typu zařízení budete přesměrováni do obchodu App Store nebo Google Play.
5. [Pouze zařízení se systémem iOS] Klikněte na tlačítko **Získat**.
6. Chcete-li nainstalovat zálohovací aplikaci, klikněte na **Instalovat**.

Spuštění zálohování na zařízení se systémem iOS

1. Otevřete zálohovací aplikaci.
2. Přihlaste se pomocí svého účtu.
3. Vyberte kategorie dat, které chcete zálohovat. Ve výchozím nastavení jsou vybrané všechny kategorie.
4. Klepněte na tlačítko **Zálohovat nyní**.
5. Povolte aplikaci přístup k osobním datům. Jestliže k některým kategoriím dat zakážete přístup, nebudou příslušná data zálohována.

Zálohování bude zahájeno.

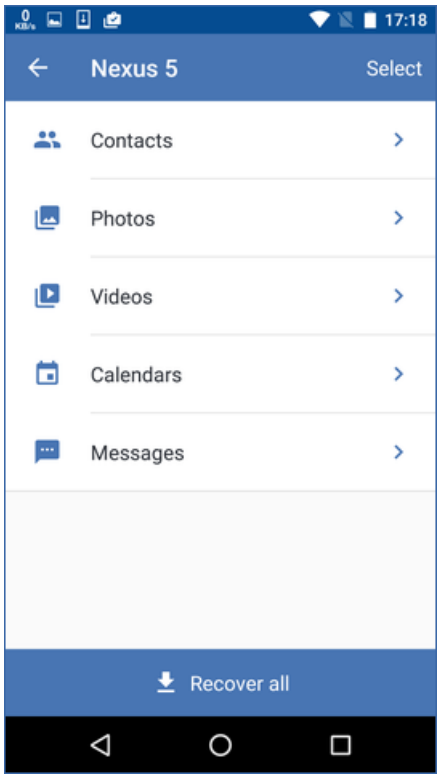
Spuštění zálohování na zařízení se systémem Android

1. Otevřete zálohovací aplikaci.
2. Přihlaste se svým účtem.
3. [Systém Android 6.0 a novější] Povolte aplikaci přístup k osobním datům. Jestliže k některým kategoriím dat zakážete přístup, nebudou příslušná data zálohována.
4. [Volitelné] Vyberte kategorie dat, které nechcete zálohovat. To provedete tak, že klepnete na ikonu ozubeného kola, klepnete na posuvníky u kategorií dat, které chcete vyloučit ze zálohování, a poté klepnete na šipku zpět.
5. Klepněte na tlačítko **Zálohovat**.

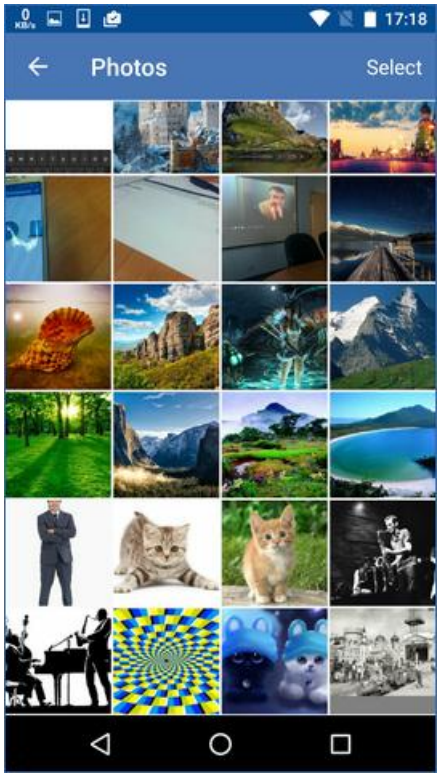
Obnovení dat do mobilního zařízení

1. Otevřete zálohovací aplikaci.
2. Potáhněte prstem doprava a poté klepněte na možnost **Přístup a obnovení**.
3. Klepněte na název zařízení.
4. Proveďte jeden z následujících úkonů:
   - Chcete-li obnovit všechna zálohovaná data, klepněte na tlačítko **Obnovit vše**. Žádné další akce již nejsou třeba.
   - Chcete-li obnovit jednu nebo více kategorií dat, klepněte na možnost **Vybrat** a potom zaškrtněte políčka u požadovaných kategorií. Klepněte na tlačítko **Obnovit**. Žádné další akce již nejsou třeba.

- Chcete-li obnovit jednu nebo více datových položek náležících do stejné kategorie dat, klepněte na požadovanou kategorii. Postupujte podle následujících kroků.



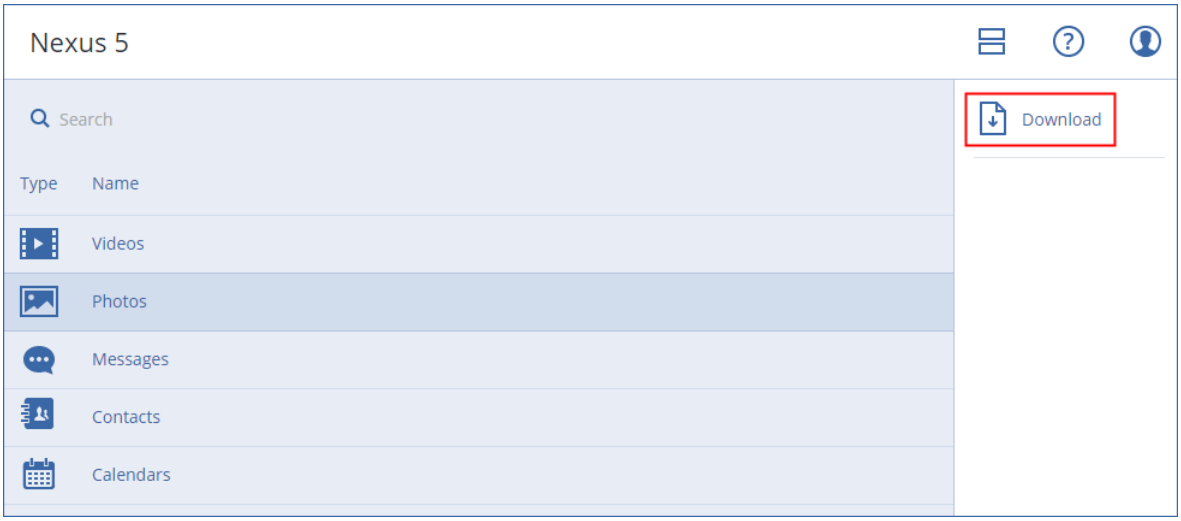
5. Proveďte jeden z následujících úkonů:
   - Jestliže chcete obnovit jedinou datovou položku, klepněte na ni.
   - Chcete-li obnovit více datových položek, klepněte na možnost **Vybrat** a potom zaškrtněte políčka u požadovaných datových položek.



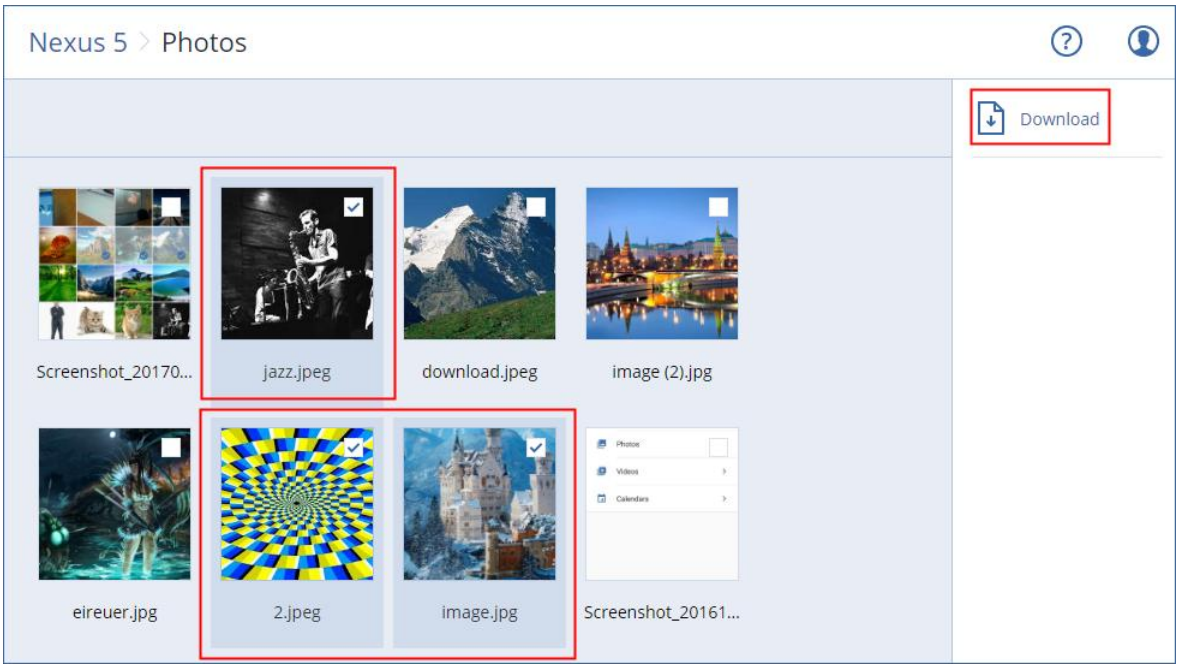
6. Klepněte na tlačítko **Obnovit**.

Přístup k datům pomocí konzoly pro zálohování

1. Na počítači otevřete prohlížeč a zadejte adresu URL konzoly pro zálohování.
2. Přihlaste se svým účtem.
3. V části **Všechna zařízení** vyberte název svého mobilního zařízení a klikněte na **Obnova**.
4. Vyberte bod obnovy.
5. Proveďte jeden z následujících úkonů:
   - Chcete-li stáhnout všechny fotografie, videa nebo kontakty, vyberte odpovídající kategorii dat. Klikněte na tlačítko **Stáhnout**.



   - Chcete-li stáhnout jednotlivé fotografie, videa nebo kontakty, klikněte na název odpovídající kategorie dat a potom zaškrtněte políčka u požadovaných datových položek. Klikněte na tlačítko **Stáhnout**.



   - Chcete-li zobrazit náhled textové zprávy, fotografie nebo kontaktu, klikněte na název odpovídající kategorie dat a potom klikněte na požadovanou datovou položku.

Další informace najdete v tématu http://www.acronis.com/redirector/products/atimobile/docs/?lang=cs. Tato nápověda je k dispozici i v zálohovací aplikaci (v nabídce aplikace klepněte na **Nastavení** > **Nápověda**).

14 Ochrana aplikací

Ochrana aplikací Microsoft SQL Server a Microsoft Exchange Server

Tyto aplikace lze chránit dvěma způsoby:

- **Zálohování databáze**

  Toto je zálohování databází a přidružených metadat na úrovni souborů. Databáze je možné obnovit do aktivní aplikace nebo jako soubory.

- **Zálohování s podporou aplikací**

  Toto je zálohování na úrovni disků, které také shromažďuje metadata aplikací. Tato metadata umožňují prohledávání a obnovu dat aplikací bez obnovení celého disku nebo svazku. Disk nebo svazek lze také obnovit jako celek. To znamená, že pro účely obnovy po havárii a ochrany dat lze použít jedno řešení s jediným plánem zálohy.

Ochrana služby Microsoft SharePoint

Farma Microsoft SharePoint se skládá ze serverů front-end, na kterých běží služby SharePoint, z databázových serverů, na kterých běží Microsoft SQL Server, a (volitelně) z aplikačních serverů, které přebírají některé služby SharePoint od serverů front-end. Některé front-end a aplikační servery mohou být shodné.

Jak chránit celou farmu SharePoint:

- Zálohujte všechny databázové servery pomocí zálohy s podporou aplikací.
- Zálohujte všechny jedinečné front-end a aplikační servery pomocí obvyklé zálohy na úrovni disku.

Zálohy všech serverů je třeba provádět podle stejného plánu.

Chcete-li chránit pouze obsah, můžete obsahové databáze zálohovat samostatně.

Ochrana řadiče domény

Počítač, na kterém běží doménové služby Active Directory, je možné zálohovat pomocí zálohy s podporou aplikací. Pokud doména obsahuje více řadičů a obnovíte jeden z nich, provede se neautoritativní obnova a po obnovení nedojde k vrácení čísla USN zpět.

Obnova aplikací

V následující tabulce jsou shrnuty dostupné možnosti obnovy aplikací.

	Ze zálohy databáze	Ze zálohy s podporou aplikací	Ze zálohy disku
Microsoft SQL Server	Databáze na aktivní instanci serveru SQL Server (str. 124) Databáze jako soubory (str. 124)	Celý počítač (str. 76) Databáze na aktivní instanci serveru SQL Server (str. 124) Databáze jako soubory (str. 124)	Celý počítač (str. 76)
Aplikace Microsoft Exchange Server	Databáze na aktivní server Exchange (str. 127) Databáze jako soubory (str. 127) Granulární obnova na aktivní server Exchange (str. 128)	Celý počítač (str. 76) Databáze na aktivní server Exchange (str. 127) Databáze jako soubory (str. 127) Granulární obnova na aktivní server Exchange (str. 128)	Celý počítač (str. 76)

Databázové servery Microsoft SharePoint	Databáze na aktivní instanci serveru SQL Server (str. 124) Databáze jako soubory (str. 124) Granulární obnova pomocí služby SharePoint Explorer	Celý počítač (str. 76) Databáze na aktivní instanci serveru SQL Server (str. 124) Databáze jako soubory (str. 124) Granulární obnova pomocí služby SharePoint Explorer	Celý počítač (str. 76)
Front-end webové servery Microsoft SharePoint	-	-	Celý počítač (str. 76)
Doménové služby Active Directory	-	Celý počítač (str. 76)	-

14.1 Předpoklady

Před konfigurací zálohy aplikací zkontrolujte, zda jsou splněny níže uvedené požadavky.

Stav zapisovačů VSS zkontrolujete pomocí příkazu **`vssadmin list writers`**.

Společné požadavky

U serveru Microsoft SQL Server zkontrolujte, zda:

- Je spuštěna alespoň jedna instance serveru Microsoft SQL Server.
- Zapisovač SQL pro VSS je zapnutý.

U serveru Microsoft Exchange Server zkontrolujte, zda:

- Je spuštěna služba úložiště informací aplikace Microsoft Exchange.
- Je nainstalováno prostředí Windows PowerShell. U verze Exchange 2010 nebo novější musí být verze Windows PowerShell alespoň 2.0.
- Je nainstalováno rozhraní Microsoft .NET Framework.

  U verze Exchange 2007 musí být verze rozhraní Microsoft .NET Framework alespoň 2.0.

  U verze Exchange 2010 nebo novější musí být verze rozhraní Microsoft .NET Framework alespoň 3.5.
- Zapisovač Exchange pro VSS je zapnutý.

U řadiče domény zkontrolujte, zda:

- Je zapnutý zapisovač Active Directory pro VSS.

Při tvorbě plánu zálohování zkontrolujte, zda:

- U fyzických počítačů je zapnuta možnost zálohování Služba Stínová kopie svazku (VSS) (str. 72).
- U virtuálních počítačů je zapnuta možnost zálohování Služba Stínová kopie svazku (VSS) pro virtuální počítače (str. 73).

Další požadavky pro zálohy s podporou aplikací

Při tvorbě plánu zálohování zkontrolujte, že je vybrána možnost **Celý počítač**.

Pokud aplikace běží na virtuálních počítačích, které zálohuje Agent pro VMware, zkontrolujte, že:

- Zálohované virtuální počítače splňují požadavky pro uvádění do stavu nečinnosti v souladu s aplikacemi uvedené v následujícím článku znalostní databáze VMware:

https://pubs.vmware.com/vsphere-6-5/index.jsp?topic=%2Fcom.vmware.vddk.pg.doc%2FvddkBkupVadp.9.6.html

- Nástroje VMware Tools jsou nainstalovány a aktualizovány v příslušných počítačích.
- Řízení uživatelských účtů (UAC) je v počítačích vypnuto. Pokud UAC vypnout nechcete, je nutné při zapnutí zálohování aplikací zadat pověření vestavěného účtu správce domény (DOMAIN\Administrator).

14.2 Zálohování databáze

Před zálohováním databází zkontrolujte, že jsou splněny požadavky uvedené v části Předpoklady (str. 121).

Vyberte databáze podle níže uvedených pokynů a zadejte další nastavení plánu zálohování podle potřeby (str. 34).

14.2.1 Výběr databází SQL

Záloha databáze SQL obsahuje databázové (.mdf, .ndf) a protokolové soubory (.ldf) a další související soubory. Soubory se zálohují pomocí služby SQL Writer. Služba musí být spuštěna ve chvíli, kdy služba stínové kopie svazku (VSS) požádá o zálohování nebo obnovu.

Soubory transakčních protokolů SQL se po každém úspěšném zálohování zkrátí. Zkrácení protokolů SQL je možné zakázat v možnostech plánu zálohování (str. 65).

Jak vybrat databáze SQL

1. Klikněte na možnost **Microsoft SQL**.

   Zobrazí se počítače s nainstalovaným Agentem pro SQL.
2. Vyhledejte data, která chcete zálohovat.

   Kliknutím dvakrát na počítač zobrazte instance serveru SQL, které obsahuje. Kliknutím dvakrát na instanci zobrazte databáze, které obsahuje.
3. Vyberte data, která chcete zálohovat. Můžete vybrat celé instance nebo jednotlivé databáze.
   - Pokud vyberete celé instance serveru SQL, budou zálohovány všechny stávající databáze a všechny databáze, které budou k vybraným instancím v budoucnu přidány.
   - Pokud vyberete přímo databáze, budou se zálohovat jenom tyto.
4. Klikněte na možnost **Zálohovat**. Pokud se zobrazí výzva, zadejte pověření k přístupu k serveru SQL. Účet musí být členem skupiny **Backup Operators** nebo **Administrators** na počítači a členem role **sysadmin** v každé instanci, kterou chcete zálohovat.

14.2.2 Výběr dat serveru Exchange

Následující tabulka shrnuje data serveru Microsoft Exchange, která lze vybrat pro zálohování, a minimální uživatelská oprávnění, která jsou k zálohování potřeba.

Verze Exchange	Datové položky	Uživatelská oprávnění
2007	Skupiny úložišť	Členství ve skupině role **Správci organizace Exchange**
2010/2013/2016	Databáze	Členství ve skupině role **Správa serveru**

Plná záloha obsahuje veškerá data vybraného serveru Exchange.

Přírůstková záloha obsahuje změněné bloky databázových souborů, soubory s kontrolními body a malé množství souborů protokolů, které jsou novější než odpovídající kontrolní bod databáze. Protože změny databázových souborů jsou zahrnuty do zálohy, není nutné zálohovat všechny záznamy transakčních protokolů od poslední zálohy. Po obnově je nutné přehrát pouze protokol, který je novější než kontrolní bod. Tímto se proces obnovy zrychluje a je zajištěno úspěšné zálohování databáze i se zapnutým cyklickým protokolováním.

Soubory transakčních protokolů se po každém úspěšném zálohování zkrátí.

Jak vybrat data serveru Exchange

1. Klikněte na možnost **Microsoft Exchange**.

   Zobrazí se počítače s nainstalovaným Agentem pro Exchange.
2. Vyhledejte data, která chcete zálohovat.

   Kliknutím dvakrát na počítač zobrazte databáze (skupiny úložišť), které obsahuje.
3. Vyberte data, která chcete zálohovat. Pokud se zobrazí výzva, zadejte pověření k přístupu k datům.
4. Klikněte na možnost **Zálohovat**.

14.3 Zálohování s podporou aplikací

Zálohování na úrovni disku s podporou aplikací je dostupné pro fyzické počítače a virtuální počítače ESXi.

Při zálohování počítače, kde je spuštěn Microsoft SQL Server, Microsoft Exchange Server nebo doménové služby Active Directory, zapněte možnost **Záloha aplikací** pro dodatečnou ochranu dat těchto aplikací.

Proč používat zálohy s podporou aplikací?

Pokud použijete zálohu s podporou aplikací, zajistíte, že:

1. Aplikace se budou zálohovat v konzistentním stavu a budou dostupné okamžitě po obnově počítače.
2. Můžete obnovovat databáze SQL a Exchange, poštovní schránky a položky schránek bez obnovení celého počítače.
3. Soubory transakčních protokolů SQL se po každém úspěšném zálohování zkrátí. Zkrácení protokolů SQL je možné zakázat v možnostech plánu zálohování (str. 65). Soubory transakčních protokolů Exchange se zkracují pouze ve virtuálních počítačích. Pokud chcete zkracovat transakční protokoly Exchange ve fyzických počítačích, můžete použít možnost plné zálohy VSS (str. 72).
4. Pokud doména obsahuje více řadičů a obnovíte jeden z nich, provede se neautoritativní obnova a po obnovení nedojde k vrácení čísla USN zpět.

Co je třeba k tvorbě zálohy s podporou aplikací?

Na fyzickém počítači musí být kromě Agenta pro Windows nainstalován Agent pro SQL a/nebo Agent pro Exchange.

Na virtuálních počítačích není instalace agenta nutná; předpokládá se, že počítač zálohuje Agent pro VMware (ve Windows).

Agent pro VMware (virtuální zařízení) může vytvářet zálohy s podporou aplikací, ale nemůže z nich obnovovat data aplikace. K obnovení dat aplikace ze záloh vytvořených těmito agenty potřebujte Agenta pro VMware (Windows), Agenta pro SQL nebo Agenta pro Exchange na počítači, který má přístup k umístění, kde jsou zálohy uložené. Při konfiguraci obnovení dat aplikací vyberte bod obnovy na kartě **Zálohy** a potom vyberte tento počítač v okně **Počítač k procházení**.

Ostatní požadavky jsou uvedeny v částech Předpoklady (str. 121) a Požadovaná uživatelská oprávnění (str. 124).

14.3.1 Požadovaná uživatelská oprávnění

Záloha s podporou aplikace obsahuje metadata aplikací s podporou služby VSS, která se nacházejí na disku. Pokud chce agent přistoupit k těmto metadatům, potřebuje k tomu účet s příslušnými oprávněními, která jsou uvedena níže. Při povolování zálohy aplikace budete vyzváni k určení tohoto účtu.

- U serveru SQL:

  Účet musí být členem skupiny **Backup Operators** nebo **Administrators** na počítači a členem role **sysadmin** v každé instanci, kterou chcete zálohovat.
- U serveru Exchange:

  Exchange 2007: Účet musí být členem skupiny **Správci Organizace Exchange**.

  Exchange 2010 a novější: Účet musí být členem skupiny **Správa organizace**.
- U služby Active Directory:

  Účet musí být správce domény.

14.4 Obnovení databází SQL

Tato část popisuje obnovu ze záloh databází i záloh podporujících aplikace.

Databáze SQL je možné obnovit do instance serveru SQL Server, pokud je v počítači, kde je instance spuštěna, nainstalován Agent pro SQL. Bude nutné zadat pověření pro účet, který je členem skupiny **Backup Operators** nebo **Administrators** v počítači a členem role **sysadmin** v cílové instanci.

Databáze můžete také obnovit jako soubory. To může být užitečné v případě, že potřebujete extrahovat data pro dolování dat, audit nebo další zpracování nástroji od externích dodavatelů. Soubory databáze SQL můžete připojit k instanci serveru SQL Server; postup je popsán v tématu Připojení databází SQL serveru (str. 126).

Pokud používáte jenom Agenta pro VMware (Windows), je obnovení databází do souborů jedinou dostupnou metodou obnovení. Obnovení databází pomocí Agenta pro VMware (virtuální zařízení) není možné.

Systémové databáze se v podstatě obnovují stejným způsobem jako uživatelské databáze. Zvláštnosti obnovy systémových databází jsou popsány v tématu Obnovení systémových databází (str. 126).

Jak obnovit databáze SQL

1. Při obnově ze zálohy databáze klikněte na možnost **Microsoft SQL**. Jinak tento krok přeskočte.
2. Vyberte počítač, který původně obsahoval data, která chcete obnovit.
3. Klikněte na možnost **Obnova**.

4. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Proveďte jeden z následujících úkonů:

   - Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte počítač ve stavu online, na kterém je nainstalován agent pro SQL, a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Zálohy (str. 112).

   Počítač vybraný při výše uvedených úkonech se stane cílovým počítačem pro obnovu databází SQL.
5. Proveďte jeden z následujících úkonů:
   - Při obnově ze zálohy databáze klikněte na možnosti **Obnovit databáze SQL**.
   - Při obnově ze zálohy s podporou aplikací klikněte na možnosti **Obnovit** > **Databáze SQL**.
6. Vyberte data, která chcete obnovit. Kliknutím dvakrát na instanci zobrazte databáze, které obsahuje.
7. Pokud chcete obnovit databáze jako soubory, klikněte na možnost **Obnovit jako soubory**, vyberte místní nebo síťovou složku, do které se soubory uloží, a klikněte na možnost **Obnovit**. Jinak tento krok přeskočte.
8. Klikněte na příkaz **Obnovit**.
9. Ve výchozím nastavení se databáze obnoví do původních. Pokud původní databáze neexistuje, bude vytvořena. Můžete vybrat jinou instanci serveru SQL Server (spuštěnou na stejném počítači), kam se databáze obnoví.

   Jak obnovit databázi jako jinou do stejné instance:

   a. Klikněte na název databáze.
   b. V části **Obnovit do** vyberte možnost **Nová databáze**.
   c. Zadejte název nové databáze.
   d. Zadejte cestu k nové databázi a k protokolu. Zadaná složka nesmí obsahovat původní soubory databáze a protokolu.
10. [Volitelné] Chcete-li změnit stav databáze po obnově, klikněte na její název a vyberte jednu z následujících možností:
    - **Připraveno k použití (RESTORE WITH RECOVERY)** (výchozí)

      Po dokončení obnovy bude databáze připravena k použití. Uživatelé k ní budou mít plný přístup. Software vrátí všechny neprovedené transakce obnovené databáze, které jsou uloženy v souboru transakčního protokolu. Z nativních záloh Microsoft SQL nebude možné obnovit další soubory transakčních protokolů.
    - **Nefunkční (RESTORE WITH NORECOVERY)**

      Po dokončení obnovy nebude databáze funkční. Uživatelé k ní nebudou mít přístup. Software zachová všechny neprovedené transakce obnovené databáze. Bude možné obnovit další soubory transakčních protokolů z nativních záloh Microsoft SQL a získat tak potřebný bod obnovení.
    - **Pouze ke čtení (RESTORE WITH STANDBY)**

      Po dokončení obnovy budou mít uživatelé k databázi přístup pouze ke čtení. Software vrátí všechny neprovedené transakce. Tyto akce však uloží do dočasného souboru, aby bylo možné dopady obnovení vrátit zpět.

      Pomocí této hodnoty se primárně detekuje bod v čase, kdy nastala chyba serveru SQL.
11. Klikněte na možnost **Spustit obnovu**.

Postup obnovy se zobrazuje na kartě **Aktivity**.

14.4.1 Obnova systémových databází

Všechny systémové databáze jedné instance se obnoví najednou. Při obnově systémových databází software automaticky restartuje cílovou instanci v jednouživatelském režimu. Po dokončení obnovy software restartuje instanci a obnoví ostatní databáze (pokud nějaké jsou).

Další důležité informace týkající se obnovy systémových databází:

- Systémové databáze je možné obnovit pouze na instanci stejné verze jako původní instance.
- Systémové databáze se vždy obnoví ve stavu "připraveno k použití".

Obnova hlavní databáze

Systémové databáze zahrnují i **hlavní** databázi. **Hlavní** databáze zaznamenává informace o všech databázích instance. Proto **hlavní** databáze (master) v záloze obsahuje informace o databázích, které existovaly v instanci v době zálohy. Po obnovení **hlavní** databáze bude možná nutné provést následující kroky:

- Databáze, které se zobrazily v instanci po provedení databáze, nejsou instancí viditelné. Chcete-li tyto databáze obnovit, připojte je k instanci ručně pomocí sady SQL Server Management Studio.
- Databáze, které byly odstraněny po provedení zálohy, se v instanci zobrazují jako offline. Odstraňte tyto databáze pomocí sady SQL Server Management Studio.

14.4.2 Připojení databází serveru SQL

V tomto tématu je popsán postup připojení databáze v serveru SQL pomocí aplikace SQL Server Management Studio. V libovolném okamžiku může být připojena pouze jedna databáze.

Připojení databáze vyžaduje libovolné z následujících oprávnění: **CREATE DATABASE** (tvorba databáze), **CREATE ANY DATABASE** (tvorba libovolné databáze) nebo **ALTER ANY DATABASE** (změna libovolné databáze). Tato oprávnění jsou obvykle udělována roli **sysadmin** v instanci.

Jak připojit databázi

1. Spusťte aplikaci Microsoft SQL Server Management Studio.
2. Připojte se k požadované instanci serveru SQL a rozbalte ji.
3. Klikněte pravým tlačítkem na možnost **Databases** (Databáze) a klikněte na možnost **Attach** (Připojit).
4. Klikněte na tlačítko **Add** (Přidat).
5. V dialogovém okně **Locate Database Files** (Vyhledat soubory databáze) najděte a vyberte soubor MDF databáze.
6. V části **Database Details** (Podrobnosti databáze) zkontrolujte, zda byly nalezeny ostatní soubory databáze (NDF a LDF).

   Podrobnosti. Soubory databáze serveru SQL nemusí být nalezeny automaticky, pokud:

   - Nejsou ve výchozím umístění nebo nejsou ve stejné složce jako primární soubor databáze (MDF). Řešení: Zadejte cestu k požadovaným souborům ručně do sloupce **Current File Path** (Aktuální cesta souboru).
   - Obnovili jste neúplnou sadu souborů tvořících databázi. Řešení: Obnovte chybějící soubory databáze serveru SQL ze zálohy.
7. Jakmile budou všechny soubory nalezeny, klikněte na tlačítko **OK**.

14.5 Obnova databází Exchange

Tato část popisuje obnovu ze záloh databází i záloh podporujících aplikace.

Data serveru Exchange můžete obnovit na aktivní server Exchange. Může jít o původní server Exchange nebo server se stejnou verzí spuštěný na počítači se stejným plně kvalifikovaným názvem domény (FQDN). V cílovém počítači musí být nainstalován Agent pro Exchange.

Následující tabulka shrnuje data serveru Exchange, která lze vybrat pro obnovu, a minimální uživatelská oprávnění, která jsou k obnově potřeba.

Verze Exchange	Datové položky	Uživatelská oprávnění
2007	Skupiny úložišť	Členství ve skupině role **Správci organizace Exchange**.
2010/2013/2016	Databáze	Členství ve skupině role **Správa serveru**

Databáze (skupiny úložišť) můžete také obnovit jako soubory. Databázové soubory spolu s transakčními protokoly se extrahují ze zálohy do zadané složky. To může být užitečné, pokud potřebujete rozbalit data a zkontrolovat je či dále zpracovat pomocí nástrojů od externích dodavatelů nebo pokud se obnova z nějakého důvodu nezdaří a vy chcete databázi připojit ručně (str. 128).

Pokud používáte jenom Agenta pro VMware (Windows), je obnovení databází do souborů jedinou dostupnou metodou obnovení. Obnovení databází pomocí Agenta pro VMware (virtuální zařízení) není možné.

Jak obnovit data Exchange

Databáze i skupiny úložišť budeme v rámci této procedury označovat jako „databáze“.

1. Při obnově ze zálohy databáze klikněte na možnost **Microsoft Exchange**. Jinak tento krok přeskočte.
2. Vyberte počítač, který původně obsahoval data, která chcete obnovit.
3. Klikněte na možnost **Obnova**.
4. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Použijte jiné způsoby obnovy:

   - Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte počítač ve stavu online, na kterém je nainstalován agent pro Exchange, a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Zálohy (str. 112).

   Počítač vybraný při výše uvedených úkonech se stane cílovým počítačem pro obnovu dat Exchange.
5. Klikněte na možnost **Obnovit** > **Databáze Exchange**.
6. Vyberte data, která chcete obnovit.
7. Pokud chcete obnovit databáze jako soubory, klikněte na možnost **Obnovit jako soubory**, vyberte místní nebo síťovou složku, do které se soubory uloží, a klikněte na možnost **Obnovit**. Jinak tento krok přeskočte.
8. Klikněte na příkaz **Obnovit**. Pokud se zobrazí výzva, zadejte pověření k přístupu k serveru Exchange.
9. Ve výchozím nastavení se databáze obnoví do původních. Pokud původní databáze neexistuje, bude vytvořena.

   Jak obnovit databázi jako jinou:

a. Klikněte na název databáze.
b. V části **Obnovit do** vyberte možnost **Nová databáze**.
c. Zadejte název nové databáze.
d. Zadejte cestu k nové databázi a k protokolu. Zadaná složka nesmí obsahovat původní soubory databáze a protokolu.

10. Klikněte na možnost **Spustit obnovu**.

Postup obnovy se zobrazuje na kartě **Aktivity**.

14.5.1 Připojení databází aplikace Exchange Server

Po obnovení souborů databází je možné databáze aktivovat jejich připojením. Připojení se provádí pomocí Konzoly pro správu serveru Exchange, Správce systému Exchange nebo prostředí Exchange Management Shell.

Obnovené databáze budou ve stavu nesprávného vypnutí. Databázi, která je ve stavu nesprávného vypnutí, je možné připojit systémem, pokud je obnovena do svého původního umístění (tzn. informace o původní databázi se nacházejí ve službě Active Directory). Při obnově databáze do alternativního umístění (například nová databáze nebo databáze obnovy) není možné databázi připojit, dokud ji nedostanete do stavu správného vypnutí pomocí příkazu **`Eseutil /r <Enn>`**. **`<Enn>`** určuje předponu protokolového souboru pro databázi (nebo skupinu úložišť obsahující databázi), do které je třeba aplikovat protokolové soubory transakcí.

Účet, který použijete k připojení databáze, musí mít přidělenu roli Exchange Server Administrator a musí být členem místní skupiny Administrators cílového serveru.

Podrobnosti o připojování databází naleznete v následujících článcích:

- Pro Exchange 2010 nebo novější: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

14.6 Obnovení poštovních schránek a položek schránek aplikace Exchange

Tato část popisuje postup pro obnovu poštovních schránek a položek schránek Exchange z databázových záloh a ze záloh s podporou aplikací.

Přehled

Granulární obnovu lze provést jen v systému Microsoft Exchange Server 2010 Service Pack 1 (SP1) nebo novějším. Zdrojová záloha může obsahovat databáze z jakékoli podporované verze Exchange.

Granulární obnovu může provádět Agent pro Exchange nebo Agent pro VMware (ve Windows). Cílový server Exchange a počítač, na kterém je agent spuštěný, musí patřit do stejné stromové struktury Active Directory.

Je možné obnovit následující položky:

- Poštovní schránky (kromě archivačních poštovních schránek)
- Veřejné složky
- Položky veřejné složky
- E-mailové složky
- E-mailové zprávy

- Události kalendáře
- Úlohy
- Kontakty
- Položky žurnálu
- Poznámky

Položky můžete najít pomocí vyhledávání.

Když obnovíte poštovní schránku do už existující schránky, přepíší se existující položky se shodnými identifikátory.

Při obnově položek poštovních schránek se nic nepřepisuje. Položky poštovní schránky se vždy obnovují do složky **Obnovené položky** v cílové schránce.

Požadavky na uživatelské účty

K poštovní schránce obnovené ze zálohy musí být přidružený uživatelský účet ve službě Active Directory.

Poštovní schránky uživatelů a jejich obsah lze obnovit pouze v případě, že jejich přidružené uživatelské účty jsou *povolené*. Sdílené poštovní schránky, schránky místností a schránky vybavení se dají obnovit pouze v případě, že jsou jejich přidružené uživatelské účty *zakázané*.

Poštovní schránka, která nesplňuje výše uvedené podmínky, bude během obnovy vynechána.

Jestliže byly některé schránky vynechány, obnova bude úspěšná s upozorněními. Pokud budou vynechány všechny schránky, obnova bude neúspěšná.

14.6.1 Obnova schránek

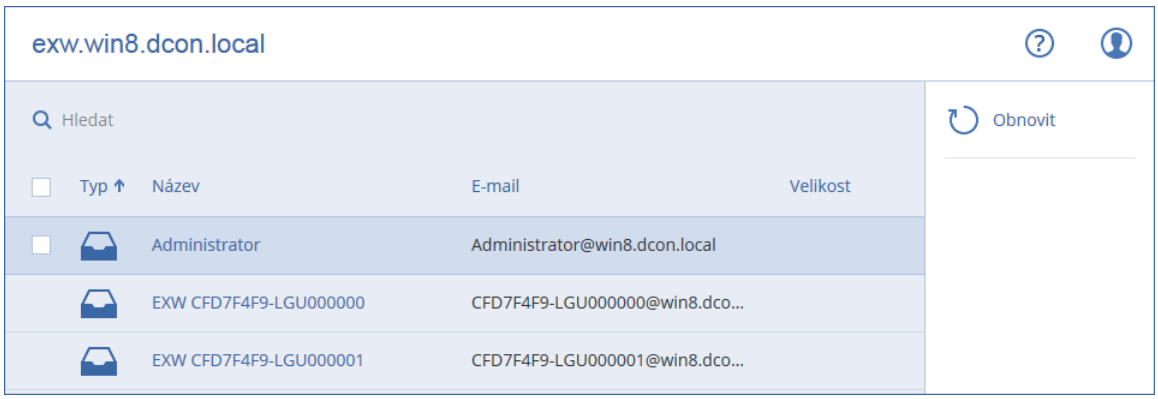
1. Při obnově ze zálohy databáze klikněte na možnost **Microsoft Exchange**. Jinak tento krok přeskočte.
2. Vyberte počítač, který původně obsahoval data, která chcete obnovit.
3. Klikněte na možnost **Obnova**.
4. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Použijte jiné způsoby obnovy:

   - Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte počítač ve stavu online, na kterém je nainstalován agent pro Exchange, nebo agent pro VMware a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Zálohy (str. 112).

   Místo původního počítače, který je offline, teď obnovu provede počítač, který jste v některém z předchozích kroků zvolili pro procházení.
5. Klikněte na možnost **Obnovit**>**Schránky Exchange**.
6. Vyberte schránky, které chcete obnovit.

Můžete je vyhledávat podle názvu. Zástupné znaky nejsou podporovány.



7. Klikněte na příkaz **Obnovit**.
8. Kliknutím na **Cílový počítač se systémem Microsoft Exchange Server** vyberete nebo změníte cílový počítač. Tento krok umožňuje obnovu na počítač, kde není spuštěn Agent pro Exchange.

   Zadejte plně kvalifikovaný název domény (FQDN) počítače, kde je zapnutá role pro **klientský přístup** serveru Microsoft Exchange Server. Počítač musí patřit ke stejnému stromu Active Directory jako počítač, který provádí obnovu.

   Pokud budete vyzváni, zadejte pověření účtu, který se bude používat pro přístup k počítači. Požadavky na tento účet jsou uvedené v části Požadovaná uživatelská oprávnění (str. 131).
9. [Volitelné] Kliknutím na možnost **Databáze pro nové vytvoření všech chybějících poštovních schránek** změňte automaticky vybranou databázi.
10. Klikněte na možnost **Spustit obnovu**.
11. Potvrďte své rozhodnutí.

Postup obnovy se zobrazuje na kartě **Aktivity**.

14.6.2 Obnovení položek poštovní schránky

1. Při obnově ze zálohy databáze klikněte na možnost **Microsoft Exchange**. Jinak tento krok přeskočte.
2. Vyberte počítač, který původně obsahoval data, která chcete obnovit.
3. Klikněte na možnost **Obnova**.
4. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Použijte jiné způsoby obnovy:

   - Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte počítač ve stavu online, na kterém je nainstalován agent pro Exchange, nebo agent pro VMware a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Zálohy (str. 112).

   Místo původního počítače, který je offline, teď obnovu provede počítač, který jste v některém z předchozích kroků zvolili pro procházení.
5. Klikněte na možnost **Obnovit**>**Schránky Exchange**.
6. Klikněte na poštovní schránku, která původně obsahovala položky, jež chcete obnovit.
7. Vyberte položky, které chcete obnovit.

   Dostupné jsou následující možnosti vyhledávání. Zástupné znaky nejsou podporovány.

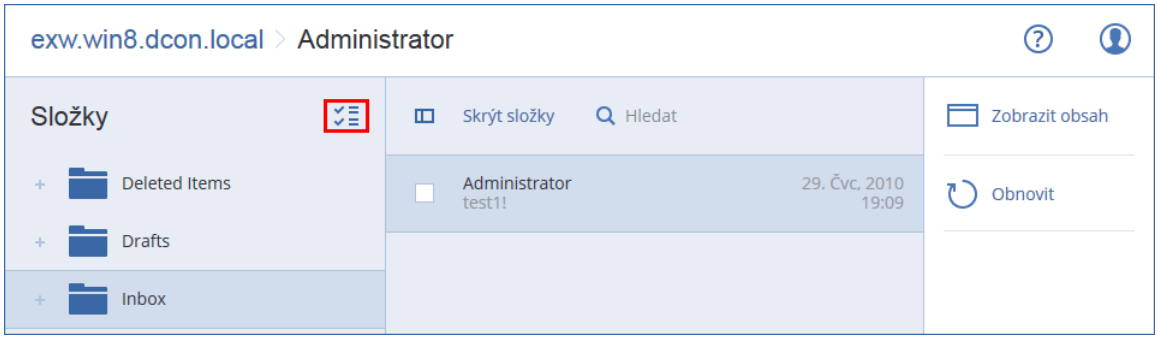
   - U e-mailových zpráv: vyhledávání podle předmětu, odesílatele, příjemce a data.
   - U událostí: vyhledávání podle názvu a data.

- U úkolů: vyhledávání podle předmětu a data.
- U kontaktů: vyhledávání podle jména, e-mailové adresy a telefonního čísla.

Když je vybraná e-mailová zpráva, můžete kliknout na možnost **Zobrazit obsah** a zobrazit její obsah včetně příloh.

Tip *Kliknutím na název přiloženého souboru jej stáhnete.*

Chcete-li vybírat složky, klikněte na ikonu obnovy složek.



8. Klikněte na příkaz **Obnovit**.
9. Kliknutím na **Cílový počítač se systémem Microsoft Exchange Server** vyberete nebo změníte cílový počítač. Tento krok umožňuje obnovu na počítač, kde není spuštěn Agent pro Exchange.

   Zadejte plně kvalifikovaný název domény (FQDN) počítače, kde je zapnutá role pro **klientský přístup** serveru Microsoft Exchange Server. Počítač musí patřit ke stejnému stromu Active Directory jako počítač, který provádí obnovu.

   Pokud budete vyzváni, zadejte pověření účtu, který se bude používat pro přístup k počítači. Požadavky na tento účet jsou uvedené v části Požadovaná uživatelská oprávnění (str. 131).
10. V části **Cílová poštovní schránka** si můžete prohlédnout, zadat nebo změnit cílovou schránku.

    Ve výchozím nastavení je vybrána původní poštovní schránka. Pokud tato poštovní schránka neexistuje nebo je vybrán jiný než původní cílový počítač, je nutné cílovou schránku zadat.
11. Klikněte na možnost **Spustit obnovu**.
12. Potvrďte své rozhodnutí.

Postup obnovy se zobrazuje na kartě **Aktivity**.

14.6.3 Požadovaná uživatelská oprávnění

Pokud chce Agent pro Exchange přistupovat k poštovním schránkám, potřebuje k tomu účet s příslušnými oprávněními. Při konfiguraci různých operací s poštovními schránkami budete vyzváni k určení tohoto účtu.

Členství daného účtu ve skupině role **Správa organizace** umožňuje přístup k libovolné poštovní schránce, včetně těch, které budou vytvořeny v budoucnosti.

Minimální požadovaná uživatelská oprávnění jsou následující:

- Účet musí být členem skupiny role **Správa příjemců**.
- Účet musí mít povolenou roli správy **ApplicationImpersonation** pro všechny uživatele a skupiny uživatelů, k jejichž poštovním schránkám má agent mít přístup.

  Informace o konfiguraci role správy **ApplicationImpersonation** najdete v následujícím článku znalostní databáze Microsoft Knowledge Base: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

15 Ochrana dat v Office 365

Proč zálohovat data Office 365?

Přestože je Microsoft Office 365 sada cloudových služeb, pravidelné zálohy nabízejí další vrstvu ochrany proti chybám uživatelů nebo úmyslnému poškození. Zálohy vám navíc umožní obnovit odstraněné položky i poté, co vyprší období uchovávání ve službě Office 365. Můžete také uchovávat místní kopii poštovních schránek Exchange Online, pokud to vyžadují závazné předpisy.

Agent pro Office 365

V závislosti požadované funkčnosti můžete nainstalovat Agenta pro Office 365 místně, použít agenta instalovaného v cloudu, nebo oboje. V následující tabulce jsou shrnuty funkce místního a cloudového agenta.

	Místní agent pro Office 365	**Cloudový agent pro Office 365**
Zálohovatelné datové položky	**Exchange Online**: poštovní schránky uživatelů a sdílené poštovní schránky	▪ **Exchange Online**: poštovní schránky uživatelů a skupin a sdílené poštovní schránky ▪ **OneDrive**: uživatelské soubory a složky ▪ **SharePoint Online**: klasické kolekce webů, skupinové (týmové) weby, komunikační weby, jednotlivé položky dat
Zálohování archivních poštovních schránek (**místní archiv**)	Ne	Ano
Plán zálohování	Definovaný uživatelem (str. 43)	Nelze změnit. Každý plán zálohování je spouštěn denně ve stejnou denní dobu.*
Umístění záloh	Cloudové úložiště, místní složka, síťová složka	Pouze cloudové úložiště
Automatická ochrana nových uživatelů, skupin a webů Office 365	Ne	Ano, pokud použijete plán zálohování u skupin **Všichni uživatelé**, **Všechny skupiny** a **Všechny weby**.
Ochrana více organizací Office 365	Ne	Ano
Částečná obnova	Ano	Ano
Obnovení do jiného uživatele v organizaci	Ano	Ano
Obnovení do jiné organizace	Ne	Ano
Obnovení do místního serveru Microsoft Exchange	Ne	Ne

	Místní agent pro Office 365	Cloudový agent pro Office 365
Maximální počet položek, které lze zálohovat bez snížení výkonu	Při zálohování do cloudového úložiště: 5 000 poštovních schránek na jednu společnost Při zálohování do jiných cílových umístění: 2 000 poštovních schránek na jeden plán zálohování (bez omezení počtu schránek na společnost)	5 000 chráněných položek na jednu společnost (poštovní schránky, úložiště OneDrive nebo weby)

* Vzhledem k tomu, že cloudový agent slouží více zákazníkům, určuje sám počáteční čas každého plánu zálohování, aby zajistil rovnoměrné zatížení během dne a stejnou kvalitu služeb pro všechny zákazníky.

Omezení

Při obnovení nemůžete automaticky vytvářet uživatele, skupiny ani weby. Pokud chcete obnovit třeba odstraněný web služby SharePoint Online, nejprve vytvořte ručně nový web a potom ho vyberte jako cílový web při obnovení.

Požadovaná uživatelská oprávnění

V zálohovací službě

Každý agent pro Office 365, ať už místní nebo cloudový, musí být zaregistrovaný pod zákaznickým účtem správce.

V Microsoft Office 365

Váš účet musí mít ve službě Microsoft Office 365 přiřazenu roli globálního správce.

- Místní agent se do služby Office 365 přihlásí tímto účtem. Aby agent mohl přistupovat k obsahu všech poštovních schránek, bude účtu přiřazena role správy **ApplicationImpersonation**. Pokud změníte heslo pro tento účet, aktualizujte heslo v konzole pro zálohování, jak je popsáno v tématu Změna pověření k přístupu pro Office 365 (str. 135).
- Cloudový agent se nepřihlašuje k Office 365. Agent získá potřebné oprávnění přímo z Microsoft Office 365. Udělení těchto oprávnění stačí potvrdit jenom jednou, když jste přihlášení jako globální správce. Agent neukládá přihlašovací údaje k účtu ani je nepoužívá k zálohování a obnovení. Změna hesla pro tento účet v Office 365 nemá vliv na fungování agenta.

15.1 Použít místně nainstalovaného agenta pro Office 365.

15.1.1 Přidání organizace Microsoft Office 365

Přidání organizace Microsoft Office 365

1. Přihlaste se ke konzole pro zálohování jako správce společnosti.
2. Klikněte na ikonu účtu v pravém horním rohu stránky a potom klikněte na **Stažené soubory** > **Agent pro Office 365**.
3. Stáhněte si agenta a nainstalujte ho v počítači se systémem Windows, který je připojen k internetu.
4. Do dokončení instalace klikněte na možnost **Zařízení** > **Microsoft Office 365** a zadejte pověření globálního správce služby Office 365.

Důležité: *Organizace (skupina společnosti) smí mít jen jednoho místně nainstalovaného agenta pro Office 365.*

Výsledkem bude, že se položky dat vaší organizace zobrazí v zálohovací konzole na stránce **Microsoft Office 365**.

15.1.2 Ochrana poštovních schránek Exchange Online

Jaké položky lze zálohovat?

Můžete zálohovat poštovní schránky uživatelů a sdílené poštovní schránky. Nemůžete zálohovat skupinové ani archivní poštovní schránky (**místní archiv**).

Jaké položky lze obnovit?

Ze zálohy poštovní schránky lze obnovit následující položky:

- Poštovní schránky
- E-mailové složky
- E-mailové zprávy
- Události kalendáře
- Úlohy
- Kontakty
- Položky žurnálu
- Poznámky

Položky můžete najít pomocí vyhledávání.

Když obnovíte poštovní schránku do už existující schránky, přepíší se existující položky se shodnými identifikátory.

Při obnově položek poštovních schránek se nic nepřepisuje. Místo toho je v cílové složce znovu vytvořena úplná cesta k položce poštovní schránky.

15.1.2.1 Výběr poštovních schránek

Vyberte poštovní schránky podle níže uvedených pokynů a zadejte další nastavení plánu zálohování podle potřeby (str. 34).

Výběr poštovních schránek

1. Klikněte na **Microsoft Office 365**.
2. Pokud se zobrazí výzva, přihlaste se do služby Microsoft Office 365 jako globální správce.
3. Vyberte poštovní schránky, které chcete zálohovat.
4. Klikněte na možnost **Zálohovat**.

15.1.2.2 Obnovení poštovních schránek a jejich položek

Obnova schránek

1. Klikněte na **Microsoft Office 365**.
2. Klikněte na poštovní schránku, kterou chcete obnovit, a potom klikněte na možnost **Obnova**.
   Můžete je vyhledávat podle názvu. Zástupné znaky nejsou podporovány.

Jestliže byla poštovní schránka odstraněna, vyberte ji na kartě Zálohy (str. 112), a poté klikněte na možnost **Zobrazit zálohy**.

3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.
4. Klikněte na **Obnovit** > **Poštovní schránka**.
5. V části **Cílová poštovní schránka** si můžete prohlédnout, zadat nebo změnit cílovou schránku.

   Ve výchozím nastavení je vybrána původní poštovní schránka. Pokud tato poštovní schránka neexistuje, je nutné zadat cílovou schránku.
6. Klikněte na možnost **Spustit obnovu**.

Obnovení položek poštovní schránky

1. Klikněte na **Microsoft Office 365**.
2. Klikněte na poštovní schránku, která původně obsahovala položky, jež chcete obnovit, a potom klikněte na možnost **Obnova**.

   Můžete je vyhledávat podle názvu. Zástupné znaky nejsou podporovány.

   Jestliže byla poštovní schránka odstraněna, vyberte ji na kartě Zálohy (str. 112), a poté klikněte na možnost **Zobrazit zálohy**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.
4. Klikněte na **Obnovit** > **E-mailové zprávy**.
5. Vyberte položky, které chcete obnovit.

   Dostupné jsou následující možnosti vyhledávání. Zástupné znaky nejsou podporovány.

   - U e-mailových zpráv: vyhledávání podle předmětu, odesílatele, příjemce a data.
   - U událostí: vyhledávání podle názvu a data.
   - U úkolů: vyhledávání podle předmětu a data.
   - U kontaktů: vyhledávání podle jména, e-mailové adresy a telefonního čísla.

   Když je vybraná e-mailová zpráva, můžete kliknout na možnost **Zobrazit obsah** a zobrazit její obsah včetně příloh.

   Tip *Kliknutím na název přiloženého souboru jej stáhnete.*

   Když je vybraná e-mailová zpráva, můžete kliknout na možnost **Odeslat jako e-mail** a odeslat zprávu na e-mailovou adresu. Zpráva bude odeslána z e-mailové adresy vašeho účtu správce.

   Chcete-li vybírat složky, klikněte na ikonu obnovy složek. 
6. Klikněte na příkaz **Obnovit**.
7. V části **Cílová poštovní schránka** si můžete prohlédnout, zadat nebo změnit cílovou schránku.

   Ve výchozím nastavení je vybrána původní poštovní schránka. Pokud tato poštovní schránka neexistuje, je nutné zadat cílovou schránku.
8. Klikněte na možnost **Spustit obnovu**.
9. Potvrďte své rozhodnutí.

Položky poštovní schránky se vždy obnovují do složky **Obnovené položky** v cílové schránce.

15.1.2.3 Změna pověření k přístupu pro Office 365

Pověření k přístupu pro Office 365 můžete změnit bez přeinstalování agenta.

Změna pověření k přístupu pro Office 365

1. Klikněte na **Zařízení** > **Microsoft Office 365**.

2. Klikněte na **Zadejte přihlašovací údaje**.
3. Zadejte pověření globálního správce služby Office 365 a potom klikněte na **OK**.

   Agent se do služby Office 365 přihlásí pomocí tohoto účtu. Aby agent mohl přistupovat k obsahu všech poštovních schránek, bude účtu přiřazena role správy **ApplicationImpersonation**.

15.2 Použít cloudového agenta pro Office 365.

15.2.1 Přidání organizace Microsoft Office 365

Přidání organizace Microsoft Office 365

1. Přihlaste se ke konzole pro zálohování jako správce společnosti.
2. Klikněte na **Zařízení** > **Přidat** > **Microsoft Office 365 pro firmy**.
3. Vyberte datové centrum Microsoftu, které organizace používá.

   Software vás přesměruje na přihlašovací stránku služby Microsoft Office 365.
4. Přihlaste se přihlašovacími údaji globálního správce Office 365.

   Microsoft Office 365 zobrazí seznam oprávnění potřebných k zálohování a obnovení dat organizace.
5. Potvrďte, že tato oprávnění službě pro zálohování udělujete.

Výsledkem bude, že se položky dat vaší organizace zobrazí v zálohovací konzole na stránce **Microsoft Office 365**.

Tipy pro další použití

- Cloudový agent synchronizuje data s Office 365 každých 24 hodin od okamžiku, kdy byla organizace přidána do zálohovací služby. Pokud přidáte nebo odeberete uživatele, skupinu nebo web, nezobrazí se změna v konzole pro zálohování ihned. Pokud chcete cloudového agenta synchronizovat s Office 365 ihned ručně, vyberte na stránce **Microsoft Office 365** organizaci a klikněte na **Aktualizovat**.
- Pokud jste plán zálohování použili u skupin **Všichni uživatelé**, **Všechny skupiny** nebo **Všechny weby**, budou nově přidané položky zahrnuty do zálohy až po synchronizaci.
- Zásady Microsoftu uvádějí, že když z grafického uživatelského rozhraní Office 365 odeberete uživatele, skupinu nebo web, budou ještě několik dní dostupné prostřednictvím API. Po tuto dobu je odebraná položka v konzole pro zálohování neaktivní (zašedlá) a není zálohována. Jakmile odebraná položka přestane být dostupná v rozhraní API, zmizí i z konzoly pro zálohování. Příslušné zálohy (pokud existují) jsou dostupné na kartě **Zálohy** > **Zálohy cloudových aplikací**.

15.2.2 Ochrana poštovních schránek Exchange Online

Jaké položky lze zálohovat?

Můžete zálohovat poštovní schránky uživatelů, sdílené poštovní schránky a skupinové poštovní schránky. Můžete také zálohovat archivní poštovní schránky (**místní archiv**) vybraných poštovních schránek.

Jaké položky lze obnovit?

Ze zálohy poštovní schránky lze obnovit následující položky:

- Poštovní schránky
- E-mailové složky
- E-mailové zprávy

- Události kalendáře
- Úlohy
- Kontakty
- Položky žurnálu
- Poznámky

Položky můžete najít pomocí vyhledávání.

Při obnovování poštovních schránek a položek poštovních schránek můžete vybrat, jestli chcete položky v cílovém umístění přepsat.

15.2.2.1 Výběr poštovních schránek

Vyberte poštovní schránky podle níže uvedených pokynů a zadejte další nastavení plánu zálohování podle potřeby (str. 34).

Výběr poštovních schránek Exchange Online

1. Klikněte na **Microsoft Office 365**.
2. Pokud jste do zálohovací služby přidali více organizací Office 365, vyberte organizaci, jejíž data uživatelů chcete zálohovat. Jinak tento krok přeskočte.
3. Proveďte jeden z následujících úkonů:
   - Pokud chcete zálohovat poštovní schránky všech uživatelů a všechny sdílené poštovní schránky (včetně poštovních schránek, které budou vytvořeny v budoucnosti), rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé** a klikněte na **Skupina zálohování**.
   - Pokud chcete zálohovat poštovní schránky jednotlivých uživatelů nebo jednotlivé sdílené poštovní schránky, rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jejichž poštovní schránky chcete zálohovat, a klikněte na **Zálohovat**.
   - Pokud chcete zálohovat všechny skupinové poštovní schránky (včetně skupinových poštovních schránek, které budou vytvořeny v budoucnosti), rozbalte uzel **Skupiny**, vyberte **Všechny skupiny** a klikněte na **Skupina zálohování**.
   - Pokud chcete zálohovat jednotlivé skupinové poštovní schránky, rozbalte uzel **Skupiny**, vyberte **Všechny skupiny**, vyberte skupiny, jejichž poštovní schránky chcete zálohovat, a klikněte na **Zálohovat**.
4. Na panelu plánu zálohování:
   - Ověřte, že v části **Co se má zálohovat** je vybraná položka **Poštovní schránky**.
   - Pokud nechcete zálohovat archivní poštovní schránky, vypněte přepínač **Archivační poštovní schránka**.

15.2.2.2 Obnovení poštovních schránek a jejich položek

Obnova schránek

1. Klikněte na **Microsoft Office 365**.
2. Pokud jste do služby zálohování přidali více organizací Office 365, vyberte organizaci, jejíž zálohovaná data chcete obnovit. Jinak tento krok přeskočte.
3. Proveďte jeden z následujících úkonů:
   - Pokud chcete obnovit poštovní schránku uživatele, rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jehož poštovní schránku chcete obnovit, a klikněte na **Obnova**.

- Pokud chcete obnovit sdílenou poštovní schránku, rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte sdílenou poštovní schránku, kterou chcete obnovit, a klikněte na **Obnova**.
- Pokud chcete obnovit skupinovou poštovní schránku, rozbalte uzel **Skupiny**, vyberte **Všechny skupiny**, vyberte skupinu, jejíž poštovní schránku chcete obnovit, a klikněte na **Obnova**.
- Pokud došlo k odstranění uživatele, skupiny nebo sdílené poštovní schránky, vyberte příslušnou položku v oddílu **Zálohy cloudových aplikací** na kartě Zálohy (str. 112) a klikněte na **Zobrazit zálohy**.

Uživatele i skupiny můžete hledat podle jména. Zástupné znaky nejsou podporovány.

4. Vyberte bod obnovy.

Tip: *Pokud chcete zobrazit jenom body obnovy, které obsahují poštovní schránky, vyberte v nabídce* ***Filtrovat podle obsahu*** *možnost* ***Poštovní schránky****.*

5. Klikněte na **Obnovit** > **Celá poštovní schránka**.
6. Pokud jste do zálohovací služby přidali více organizací Office 365, klikněte na položku **Organizace Office 365**, která umožňuje zobrazit, změnit nebo zadat cílovou organizaci.

   Automaticky je vybraná původní organizace. Pokud tato organizace není ve službě zálohování zaregistrovaná, musíte zadat cílovou organizaci.
7. V nabídce **Obnovit do poštovní schránky** můžete zobrazit, změnit nebo zadat cílovou poštovní schránku.

   Ve výchozím nastavení je vybrána původní poštovní schránka. Pokud tato poštovní schránka neexistuje nebo není vybraná původní organizace, musíte zadat cílovou poštovní schránku.
8. Klikněte na možnost **Spustit obnovu**.
9. Vyberte jednu z možností přepisu:
   - **Přepsat existující položky**
   - **Nepřepisovat existující položky**
10. Potvrďte volbu kliknutím na **Pokračovat**.

Obnovení položek poštovní schránky

1. Klikněte na **Microsoft Office 365**.
2. Pokud jste do služby zálohování přidali více organizací Office 365, vyberte organizaci, jejíž zálohovaná data chcete obnovit. Jinak tento krok přeskočte.
3. Proveďte jeden z následujících úkonů:
   - Pokud chcete obnovit položky z poštovní schránky uživatele, rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jehož poštovní schránka původně obsahovala položky, které chcete obnovit, a klikněte na **Obnova**.
   - Pokud chcete obnovit položky ze sdílené poštovní schránky, rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte sdílenou poštovní schránku, která původně obsahovala položky, jež chcete obnovit, a klikněte na **Obnova**.
   - Pokud chcete obnovit položky ze skupinové poštovní schránky, rozbalte uzel **Skupiny**, vyberte **Všechny skupiny**, vyberte skupinu, jejíž poštovní schránka původně obsahovala položky, které chcete obnovit, a klikněte na **Obnova**.
   - Pokud došlo k odstranění uživatele, skupiny nebo sdílené poštovní schránky, vyberte příslušnou položku v oddílu **Zálohy cloudových aplikací** na kartě Zálohy (str. 112) a klikněte na **Zobrazit zálohy**.

   Uživatele i skupiny můžete hledat podle jména. Zástupné znaky nejsou podporovány.
4. Vyberte bod obnovy.

Tip: *Pokud chcete zobrazit jenom body obnovy, které obsahují poštovní schránky, vyberte v nabídce* ***Filtrovat podle obsahu*** *možnost* ***Poštovní schránky****.*

5. Klikněte na **Obnovit** > **E-mailové zprávy**.
6. Přejděte k požadované složce nebo vyhledejte seznam požadovaných položek.

   Dostupné jsou následující možnosti vyhledávání. Zástupné znaky nejsou podporovány.

   - U e-mailových zpráv: vyhledávání podle předmětu, odesílatele, příjemce a data.
   - U událostí: vyhledávání podle názvu a data.
   - U úkolů: vyhledávání podle předmětu a data.
   - U kontaktů: vyhledávání podle jména, e-mailové adresy a telefonního čísla.
7. Vyberte položky, které chcete obnovit. Chcete-li vybírat složky, klikněte na ikonu obnovy složek:

   Můžete také použít některou z následujících možností:

   - Pokud je vybraná položka, kliknutím na **Zobrazit obsah** zobrazíte obsah včetně příloh. Když kliknete na název připojeného souboru, soubor se stáhne.
   - Pokud je vybraná e-mailová zpráva nebo kalendářová položka, kliknutím na **Odeslat jako e-mail** odešlete položku na zadané e-mailové adresy. Můžete vybrat odesílatele a napsat text, který se přidá k přeposílané položce.
   - Pokud záloha nebyla zašifrovaná, použili jste vyhledávání a vybrali jste ve výsledcích hledání jen jednu položku, klikněte na **Zobrazit verze** a vyberte verzi položky, kterou chcete obnovit. Můžete vybrat kteroukoli zálohovanou verzi, která je starší nebo novější než vybraný bod obnovy.
8. Klikněte na příkaz **Obnovit**.
9. Pokud bylo do služby zálohování přidáno více organizací Office 365, klikněte na položku **Organizace Office 365**, která umožňuje zobrazit, změnit nebo zadat cílovou organizaci.

   Automaticky je vybraná původní organizace. Pokud tato organizace není ve službě zálohování zaregistrovaná, musíte zadat cílovou organizaci.
10. V nabídce **Obnovit do poštovní schránky** můžete zobrazit, změnit nebo zadat cílovou poštovní schránku.

    Ve výchozím nastavení je vybrána původní poštovní schránka. Pokud tato poštovní schránka neexistuje nebo není vybraná původní organizace, musíte zadat cílovou poštovní schránku.
11. [Pouze při obnově do poštovní schránky uživatele nebo sdílené poštovní schránky] V poli **Cesta** si můžete prohlédnout cílovou složku cílové poštovní schránky nebo ji zde můžete změnit. Ve výchozím nastavení se vybere složka **Obnovené položky**.

    Položky ve skupinových poštovních schránkách se vždy obnovují do složky **Doručená pošta**.
12. Klikněte na možnost **Spustit obnovu**.
13. Vyberte jednu z možností přepisu:

    - **Přepsat existující položky**
    - **Nepřepisovat existující položky**
14. Potvrďte volbu kliknutím na **Pokračovat**.

15.2.3 Ochrana souborů na OneDrivu

Jaké položky lze zálohovat?

Můžete zálohovat celý OneDrive nebo jednotlivé soubory a složky.

Se soubory se zálohuje i oprávnění k jejich sdílení. Rozšířené úrovně oprávnění (pro **návrh**, **úplné** oprávnění, oprávnění **přispět**) se nezálohují.

Jaké položky lze obnovit?

Můžete obnovit celý OneDrive nebo libovolný zálohovaný soubor nebo složku.

Položky můžete najít pomocí vyhledávání.

Můžete vybrat, jestli chcete obnovit i oprávnění ke sdílení nebo chcete, aby soubory převzaly oprávnění ze složky, do které se obnovují.

Odkazy na soubory a složky určené ke sdílení se neobnoví.

15.2.3.1 Výběr souborů na OneDrivu

Vyberte soubory (viz následující popis) a podle potřeby (str. 34) zadejte další nastavení plánu zálohování.

Výběr souborů na OneDrivu

1. Klikněte na **Microsoft Office 365**.
2. Pokud jste do zálohovací služby přidali více organizací Office 365, vyberte organizaci, jejíž data uživatelů chcete zálohovat. Jinak tento krok přeskočte.
3. Proveďte jeden z následujících úkonů:
   - Pokud chcete zálohovat soubory všech uživatelů (včetně uživatelů, kteří budou vytvořeni v budoucnosti), rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé** a klikněte na **Skupina zálohování**.
   - Pokud chcete zálohovat soubory jednotlivých uživatelů, rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jejichž soubory chcete zálohovat, a klikněte na **Zálohovat**.
4. Na panelu plánu zálohování:
   - Ověřte, že v části **Co se má zálohovat** je vybraná položka **OneDrive**.
   - V části **Položky k zálohování** proveďte jednu z následujících akcí:
     - Nechte výchozí nastavení **[Vše]** (všechny soubory).
     - Zadejte názvy souborů a složek nebo cesty k souborům a složkám, které se mají zálohovat.

       Můžete používat zástupné znaky (*, ** a ?). Další informace o zadávání cest a používání zástupných znaků naleznete v části Filtry souborů (str. 63).
     - Vyberte zálohované soubory a složky tím, že k nim přejdete.

       Odkaz **Procházet** je k dispozici jen při vytváření plánu zálohování jednoho uživatele.
   - [Volitelné] V části **Položky k zálohování** klikněte na **Zobrazit vyloučení** a zadejte soubory a složky, které chcete při zálohování přeskočit.

     Vyloučené soubory přepíší vybrané soubory. To znamená, že pokud zadáte stejný soubor do obou polí, při zálohování se přeskočí.

15.2.3.2 Obnovení OneDrivu a souborů na OneDrivu

Obnovení celého OneDrivu

1. Klikněte na **Microsoft Office 365**.

2. Pokud jste do služby zálohování přidali více organizací Office 365, vyberte organizaci, jejíž zálohovaná data chcete obnovit. Jinak tento krok přeskočte.
3. Rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jehož OneDrive chcete obnovit, a klikněte na **Obnova**.

   Pokud byl uživatel odstraněn, vyberte ho v části **Zálohy cloudových aplikací** na kartě Zálohy (str. 112) a potom klikněte na možnost **Zobrazit zálohy**.

   Uživatele můžete hledat podle jména. Zástupné znaky nejsou podporovány.
4. Vyberte bod obnovy.

   ***Tip**: Pokud chcete zobrazit jenom body obnovení, které obsahují soubory OneDrive, vyberte v nabídce **Filtrovat podle obsahu** možnost **OneDrive**.*
5. Klikněte na **Obnovit** > **Celý OneDrive**.
6. Pokud bylo do služby zálohování přidáno více organizací Office 365, klikněte na položku **Organizace Office 365**, která umožňuje zobrazit, změnit nebo zadat cílovou organizaci.

   Automaticky je vybraná původní organizace. Pokud tato organizace není ve službě zálohování zaregistrovaná, musíte zadat cílovou organizaci.
7. V části **Obnovit na jednotku** můžete zobrazit, změnit nebo zadat cílového uživatele.

   Automaticky je vybraný původní uživatel. Pokud tento uživatel neexistuje nebo je vybraná jiná než původní organizace, musíte zadat cílového uživatele.
8. Vyberte, jestli chcete u souborů obnovit i oprávnění ke sdílení.
9. Klikněte na možnost **Spustit obnovu**.
10. Vyberte jednu z možností přepisu:
    - **Přepsat existující soubory**
    - **Přepsat existující soubor, pokud je starší**
    - **Nepřepisovat existující soubory**
11. Potvrďte volbu kliknutím na **Pokračovat**.

Obnovení souborů na OneDrivu

1. Klikněte na **Microsoft Office 365**.
2. Pokud jste do služby zálohování přidali více organizací Office 365, vyberte organizaci, jejíž zálohovaná data chcete obnovit. Jinak tento krok přeskočte.
3. Rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jehož soubory na OneDrivu chcete obnovit, a klikněte na **Obnova**.

   Pokud byl uživatel odstraněn, vyberte ho v části **Zálohy cloudových aplikací** na kartě Zálohy (str. 112) a potom klikněte na možnost **Zobrazit zálohy**.

   Uživatele můžete hledat podle jména. Zástupné znaky nejsou podporovány.
4. Vyberte bod obnovy.

   ***Tip**: Pokud chcete zobrazit jenom body obnovení, které obsahují soubory OneDrive, vyberte v nabídce **Filtrovat podle obsahu** možnost **OneDrive**.*
5. Klikněte na **Obnovit** > **Soubory/složky**.
6. Přejděte do požadované složky nebo pomocí vyhledávání získejte seznam požadovaných souborů a složek.

   Je možné použít více zástupných znaků (* a ?). Více informací o používání zástupných znaků naleznete v části Filtry souborů (str. 63).

   Vyhledávání není dostupné, pokud je záloha zašifrovaná.

7. Vyberte soubory, které chcete obnovit.

   Pokud není záloha zašifrovaná a vyberete jen jeden soubor, klikněte na **Zobrazit verze** a vyberte verzi souboru, kterou chcete obnovit. Můžete vybrat kteroukoli zálohovanou verzi, která je starší nebo novější než vybraný bod obnovy.
8. Pokud chcete stáhnout soubor, vyberte ho, klikněte na **Stáhnout**, vyberte místo pro uložení souboru a potom klikněte na **Uložit**. Jinak tento krok přeskočte.
9. Klikněte na příkaz **Obnovit**.
10. Pokud bylo do služby zálohování přidáno více organizací Office 365, klikněte na položku **Organizace Office 365**, která umožňuje zobrazit, změnit nebo zadat cílovou organizaci.

    Automaticky je vybraná původní organizace. Pokud tato organizace není ve službě zálohování zaregistrovaná, musíte zadat cílovou organizaci.
11. V části **Obnovit na jednotku** můžete zobrazit, změnit nebo zadat cílového uživatele.

    Automaticky je vybraný původní uživatel. Pokud tento uživatel neexistuje nebo je vybraná jiná než původní organizace, musíte zadat cílového uživatele.
12. V poli **Cesta** si můžete prohlédnout cílovou složku na OneDrivu cílového uživatele nebo ji zde můžete změnit. Automaticky je vybrané původní umístění.
13. Vyberte, jestli chcete u souborů obnovit i oprávnění ke sdílení.
14. Klikněte na možnost **Spustit obnovu**.
15. Vyberte jednu z možností pro přepis souborů:
    - **Přepsat existující soubory**
    - **Přepsat existující soubor, pokud je starší**
    - **Nepřepisovat existující soubory**
16. Potvrďte volbu kliknutím na **Pokračovat**.

15.2.4 Ochrana webů SharePointu Online

Jaké položky lze zálohovat?

Zálohovat můžete klasické kolekce webů SharePoint, skupinové (týmové) weby a komunikační weby. Můžete také zálohovat jednotlivé podřízené weby, seznamy nebo knihovny.

Následující položky budou při zálohování *přeskočeny*:

- Nastavení webu, která se týkají jeho **vzhledu a chování** (s výjimkou **názvu, popisu a loga**).
- Komentáře ke stránkám webu a nastavení komentářů ke stránkám (**zapnuté** nebo **vypnuté** komentáře).
- Nastavení webu, která se týkají **funkcí webu**.
- Stránky webových částí a webové části vložené do stránek wikiwebu (kvůli omezením rozhraní API SharePointu Online).
- Soubory OneNotu (kvůli omezením rozhraní API SharePointu Online).
- Typy sloupců s externími daty a spravovanými metadaty.
- Výchozí kolekce webu „domain-my.sharepoint.com“. V této kolekci se nacházejí všechny soubory OneDrivu uživatelů v organizaci.
- Obsah koše.

Omezení

- Názvy a popisy webů, podřízených webů, seznamů a sloupců jsou během zálohování zkráceny, pokud velikost názvu nebo popisu přesahuje 10 000 bajtů.

Jaké položky lze obnovit?

Ze zálohy webu lze obnovit následující položky:

- Celý Web
- Podřízené weby
- Seznamy
- Položky seznamu
- Knihovny dokumentů
- Dokumenty
- Přílohy položek seznamu
- Webové stránky a stránky wikiwebu

Položky můžete najít pomocí vyhledávání.

Položky můžete obnovit na původní web nebo na nepůvodní web. Cesta k obnovené položce je stejná jako na původním webu. Pokud tato cesta neexistuje, vytvoří se.

Můžete si vybrat, jestli chcete obnovit i oprávnění ke sdílení nebo chcete, aby obnovené položky převzaly oprávnění z nadřazeného objektu.

Následující položky nelze obnovit:

- Podřízené weby založené na šabloně **úložiště procesů aplikace Visio** (Visio Process Repository).
- Seznamy následujících typů: **seznam průzkumů**, **seznam úloh**, **knihovna obrázků**, **odkazy**, **kalendář**, **diskusní vývěska**, **externí tabulka** a **importovaná tabulka**.
- Seznamy s povolenými různými typy obsahu.

15.2.4.1 Výběr dat SharePointu Online

Vyberte data (viz následující popis) a podle potřeby (str. 34) zadejte další nastavení plánu zálohování.

Výběr dat SharePointu Online

1. Klikněte na **Microsoft Office 365**.
2. Pokud jste do zálohovací služby přidali více organizací Office 365, vyberte organizaci, jejíž data uživatelů chcete zálohovat. Jinak tento krok přeskočte.
3. Proveďte jeden z následujících úkonů:
   - Pokud chcete v organizaci zálohovat všechny klasické weby SharePointu (včetně webů, které budou vytvořeny v budoucnosti), rozbalte uzel **Kolekce webů**, vyberte **Všechny kolekce webů** a klikněte na **Skupina zálohování**.
   - Pokud chcete zálohovat jednotlivé klasické weby, rozbalte uzel **Kolekce webů**, vyberte **Všechny kolekce webů**, vyberte weby, které chcete zálohovat, a klikněte na **Zálohovat**.
   - Pokud chcete zálohovat všechny skupinové weby (včetně webů, které budou vytvořeny v budoucnosti), rozbalte uzel **Skupiny**, vyberte **Všechny skupiny** a klikněte na **Skupina zálohování**.
   - Pokud chcete zálohovat jednotlivé skupinové weby, rozbalte uzel **Skupiny**, vyberte **Všechny skupiny**, vyberte skupiny, jejíž weby chcete zálohovat, a klikněte na **Zálohovat**.
4. Na panelu plánu zálohování:
   - Ověřte, že v části **Co se má zálohovat** je vybraná možnost **Weby SharePointu**.
   - V části **Položky k zálohování** proveďte jednu z následujících akcí:
     - Nechte výchozí nastavení **[Vše]** (všechny položky vybraných webů).

- Zadejte podřízené weby, seznamy a knihovny, které chcete zálohovat. Uděláte to tak, že přidáte jejich názvy nebo cesty.

  Pokud chcete zálohovat podřízený web nebo seznam či knihovnu webu nejvyšší úrovně, zadejte zobrazovaný název v tomto tvaru: `/zobrazovany nazev/**`.

  Pokud chcete zálohovat seznam nebo knihovnu podřízeného webu, zadejte zobrazovaný název v tomto tvaru: `/zobrazovany nazev podrizeneho webu/zobrazovany nazev seznamu/**`

  Zobrazované názvy podřízených webů a knihoven se zobrazí na stránce **Obsah webu** webu nebo podřízeného webu SharePointu.
- Vyberte zálohované podřízené weby tím, že k nim přejdete.

  Odkaz **Procházet** je k dispozici jen při vytváření plánu zálohování jednoho webu.

- [Volitelné] V nabídce **Položky k zálohování** klikněte na **Zobrazit vyloučení** a zadejte podřízené weby, seznamy a knihovny, které chcete ze zálohování vynechat.

  Vyloučené položky přepíší vybrané položky. To znamená, že pokud zadáte stejný podřízený web do obou polí, při zálohování se vynechá.

15.2.4.2 Obnovení dat SharePointu Online

1. Klikněte na **Microsoft Office 365**.
2. Pokud jste do služby zálohování přidali více organizací Office 365, vyberte organizaci, jejíž zálohovaná data chcete obnovit. Jinak tento krok přeskočte.
3. Proveďte jeden z následujících úkonů:
   - Pokud chcete obnovit data ze skupinového webu, rozbalte uzel **Skupiny**, vyberte **Všechny skupiny**, vyberte skupinu, jejíž web původně obsahoval položky, které chcete obnovit, a klikněte na **Obnova**.
   - Pokud chcete obnovit data z klasického webu, rozbalte uzel **Kolekce webů**, vyberte **Všechny weby**, vyberte web, který původně obsahoval obnovované položky, a klikněte na **Obnova**.
   - Pokud byl web odstraněn, vyberte ho v oddílu **Zálohy cloudových aplikací** na kartě Zálohy (str. 112) a klikněte na **Zobrazit zálohy**.

   Skupiny a weby můžete hledat podle jména. Zástupné znaky nejsou podporovány.
4. Vyberte bod obnovy.

   Tip: *Pokud chcete zobrazit jenom body obnovy, které obsahují weby SharePointu, vyberte v nabídce* ***Filtrovat podle obsahu*** *možnost* ***Weby SharePointu****.*
5. Klikněte na **Obnovit soubory SharePointu**.
6. Přejděte k požadované složce nebo vyhledejte seznam požadovaných položek dat.

   Je možné použít více zástupných znaků (* a ?). Více informací o používání zástupných znaků naleznete v části Filtry souborů (str. 63).

   Vyhledávání není dostupné, pokud je záloha zašifrovaná.
7. Vyberte položky, které chcete obnovit.

   Pokud záloha není zašifrovaná, použili jste vyhledávání a ve výsledcích hledání vyberete jen jednu položku, můžete kliknout na **Zobrazit verze** a vybrat verzi položky, kterou chcete obnovit. Můžete vybrat kteroukoli zálohovanou verzi, která je starší nebo novější než vybraný bod obnovy.
8. Pokud chcete stáhnout položku, vyberte ji, klikněte na **Stáhnout**, vyberte místo pro uložení položky a potom klikněte na **Uložit**. Jinak tento krok přeskočte.
9. Klikněte na příkaz **Obnovit**.

10. Pokud bylo do služby zálohování přidáno více organizací Office 365, klikněte na položku **Organizace Office 365**, která umožňuje zobrazit, změnit nebo zadat cílovou organizaci.

    Automaticky je vybraná původní organizace. Pokud tato organizace není ve službě zálohování zaregistrovaná, musíte zadat cílovou organizaci.
11. V části **Obnovit na web** můžete zobrazit, změnit nebo zadat cílový web.

    Automaticky je vybraný původní web. Pokud tento web neexistuje nebo je vybraná jiná než původní organizace, musíte zadat cílový web.
12. Vyberte, jestli chcete u obnovovaných položek obnovit i oprávnění ke sdílení.
13. Klikněte na možnost **Spustit obnovu**.
14. Vyberte jednu z možností přepisu:
    - **Přepsat existující soubory**
    - **Přepsat existující soubor, pokud je starší**
    - **Nepřepisovat existující soubory**
15. Potvrďte volbu kliknutím na **Pokračovat**.

15.2.5 Upgrade cloudového agenta

Tato část popisuje postup pro upgrade na aktuální verzi řešení zálohování pro Microsoft Office 365. Tato verze podporuje zálohování služeb OneDrive a SharePoint Online a poskytuje vylepšený výkon zálohování a obnovení.

Dostupnost upgradu závisí na připravenosti datového centra a nastavení provedených vaším poskytovatelem služeb. Pokud je upgrade k dispozici, konzola pro zálohování zobrazí upozornění v horní části karty **Microsoft Office 365 (v1)**.

Proces upgradu

Během upgradu jsou uživatelé Office 365 ve vaší organizaci přidáni do nového řešení zálohování. Plány zálohování jsou migrovány a použity pro příslušné uživatele.

Dříve vytvořené zálohy jsou zkopírovány z jednoho umístění v cloudu do jiného. Zkopírované zálohy se na kartě **Zálohy** zobrazí v samostatném oddílu s názvem **Zálohy cloudových aplikací**, zatímco původní zálohy zůstanou v umístění **Cloudové úložiště**. Po dokončení procesu upgradu jsou původní zálohy z umístění **Cloudové úložiště** odstraněny.

Upgrade může trvat několik hodin nebo i dní podle počtu uživatelů v organizaci, počtu záloh a rychlosti přístupu k Office 365. Během upgradu je možné provádět obnovení z dříve vytvořených záloh. Zálohy a plány zálohování vytvořené v průběhu upgradu ale budou ztraceny.

Pokud se upgrade nezdaří, což je nepravděpodobné, zůstane řešení zálohování plně funkční a upgrade můžete restartovat od bodu selhání.

Zahájení procesu upgradu

1. Klikněte na **Microsoft Office 365 (v1)**.
2. Klikněte na **Upgradovat** v oznámení zobrazeném v horní části obrazovky.
3. Potvrďte, že chcete spustit proces upgradu.
4. Vyberte datové centrum Microsoftu, které organizace používá.

   Software vás přesměruje na přihlašovací stránku služby Microsoft Office 365.
5. Přihlaste se přihlašovacími údaji globálního správce Office 365.

Microsoft Office 365 zobrazí seznam oprávnění potřebných k zálohování a obnovení dat organizace.

6. Potvrďte, že tato oprávnění službě pro zálohování udělujete.

   Budete přesměrováni do konzole pro zálohování a bude zahájen proces upgradu. Průběh upgradu se zobrazí na panelu **Microsoft Office 365** > **Aktivity**.

16 Ochrana dat v G Suite

Co znamená ochrana služby G Suite?

- Zálohování a obnovení uživatelských dat G Suite (poštovní schránky Gmail, Kalendáře, Kontakty, Disky Google) a Týmových disků G Suite mezi cloudy.
- Granulární obnova e-mailů, souborů, kontaktů a dalších položek.
- Podpora pro několik organizací G Suite a obnovení napříč organizacemi.
- Volitelná notarizace zálohovaných souborů s využitím databáze blockchainu Ethereum. Je-li tato volba zapnutá, umožňuje potvrdit, že soubor je autentický a nebyl od zálohy změněn.
- Volitelné fulltextové vyhledávání. Pokud je povolené, můžete prohledávat e-maily podle jejich obsahu.
- Bez snížení výkonu lze ochránit až 5 000 položek (poštovní schránky, Disky Google a Týmové disky) na jednu společnost.

Požadovaná uživatelská oprávnění

Abyste mohli přidat organizaci G Suite do služby zálohování, musíte být přihlášeni jako supersprávce.

Heslo supersprávce není nikde uloženo a nepoužívá se k provádění operací zálohování ani obnovení. Změna tohoto hesla ve službě G Suite nemá vliv na fungování služby zálohování.

Dojde-li k odstranění supersprávce, který přidal organizaci G Suite, nebo je mu přiřazena role s nižším oprávněním, zálohování se nezdaří a zobrazí se chyba odepření přístupu. V tom případě opakujte postup Přidání organizace G Suite (str. 146) a zadejte platná pověření supersprávce. Pokud se chcete vyhnout podobné situaci, doporučujeme vytvořit speciálního uživatele supersprávce pro potřeby zálohování a obnovování.

Ve službě zálohování musíte být správcem společnosti. Správci jednotek a uživatelé nemohou zálohovat ani obnovit službu G Suite.

O plánu zálohování

Vzhledem k tomu, že cloudový agent slouží více zákazníkům, určuje sám počáteční čas každého plánu zálohování, aby zajistil rovnoměrné zatížení během dne a stejnou kvalitu služeb pro všechny zákazníky.

Každý plán zálohování je spouštěn denně ve stejnou denní dobu.

Omezení

Hledání v šifrovaných zálohách není podporováno.

16.1 Přidání organizace G Suite

Postup přidání organizace G Suite

1. Přihlaste se ke konzole pro zálohování jako správce společnosti.

2. Klikněte na **Zařízení** > **Přidat** > **G Suite**.
3. Postupujte podle pokynů zobrazených v softwaru:
   a. Klikněte na **Spustit Marketplace**.
   b. Přihlaste se s pověřením supersprávce.
   c. Klikněte na možnost **Doménová instalace**.
   d. Potvrďte instalaci pro celou doménu.
      Služba G Suite zobrazí seznam oprávnění potřebných k zálohování a obnovení dat organizace.
   e. Potvrďte, že tato oprávnění službě pro zálohování udělujete.
   f. Dokončete průvodce instalací.
   g. Klikněte na **Spustit**.

Budete přesměrováni zpět do konzoly pro zálohování. Položky dat vaší organizace se zobrazí v konzole pro zálohování na stránce **G Suite**.

Tipy pro další použití

- Cloudový agent synchronizuje data se službou G Suite každých 24 hodin od okamžiku, kdy byla organizace přidána do služby zálohování. Pokud přidáte nebo odeberete uživatele nebo Týmový disk, nezobrazí se změna v konzole pro zálohování ihned. Pokud chcete cloudového agenta synchronizovat se službou G Suite ihned ručně, vyberte na stránce **G Suite** organizaci a klikněte na **Aktualizovat**.
- Pokud jste plán zálohování použili u skupin **Všichni uživatelé** nebo **Všechny Týmové disky**, budou nově přidané položky zahrnuty do zálohy až po synchronizaci.
- Zásady Google uvádějí, že když z grafického uživatelského rozhraní G Suite odeberete uživatele nebo Týmový disk, budou ještě několik dní dostupné prostřednictvím API. Po tuto dobu je odebraná položka v konzole pro zálohování neaktivní (zašedlá) a není zálohována. Jakmile odebraná položka přestane být dostupná v rozhraní API, zmizí i z konzoly pro zálohování. Příslušné zálohy (pokud existují) jsou dostupné na kartě **Zálohy** > **Zálohy cloudových aplikací**.

16.2 Ochrana dat v Gmailu

Jaké položky lze zálohovat?

Můžete zálohovat poštovní schránky uživatelů Gmailu. Záloha poštovní schránky zahrnuje také data Kalendáře a Kontaktů. Volitelně můžete také zálohovat sdílené kalendáře.

Následující položky budou při zálohování *přeskočeny*:

- Kalendáře **Narozeniny**, **Připomenutí**, **Úkoly**
- Složky připojené k událostem kalendáře
- Složka **Directory** v Kontaktech

Následující položky kalendáře jsou *přeskočeny* z důvodu omezení rozhraní API Kalendáře Google:

- Bloky pro schůzky
- Pole konference události
- Nastavení kalendáře **Upozornění na celodenní události**
- Nastavení kalendáře **Automaticky přijmout pozvánky** (v kalendářích pro místnosti nebo sdílené prostory)

Následující položky kontaktů jsou *přeskočeny* z důvodu omezení rozhraní Google People API:

- Složka **Další kontakty**

- Externí profily kontaktu (**profil Directory**, **profil Google**)
- Pole kontaktu **Zařadit jako**

Jaké položky lze obnovit?

Ze zálohy poštovní schránky lze obnovit následující položky:

- Poštovní schránky
- Složky e-mailu (podle názvosloví Google jde o štítky; **Štítky** se v zálohovacím softwaru zobrazují jako složky z důvodu konzistence s dalšími uváděnými daty)
- E-mailové zprávy
- Události kalendáře
- Kontakty

Položky v záloze můžete najít pomocí vyhledávání, pokud není záloha zašifrovaná. Hledání v šifrovaných zálohách není podporováno.

Při obnovování poštovních schránek a položek poštovních schránek můžete vybrat, jestli chcete položky v cílovém umístění přepsat.

Omezení

- Fotky kontaktů nelze obnovit.
- Položka kalendáře **Nejsem v práci** se obnovuje jako běžná událost kalendáře z důvodu omezení rozhraní API Kalendáře Google.

16.2.1 Výběr poštovních schránek

Vyberte poštovní schránky podle níže uvedených pokynů a zadejte další nastavení plánu zálohování podle potřeby (str. 34).

Postup výběru poštovních schránek Gmail

1. Klikněte na **G Suite**.
2. Pokud jste do služby zálohování přidali více organizací G Suite, vyberte organizaci, jejíž data uživatelů chcete zálohovat. Jinak tento krok přeskočte.
3. Proveďte jeden z následujících úkonů:
   - Pokud chcete zálohovat poštovní schránky všech uživatelů (včetně poštovních schránek, které budou vytvořeny v budoucnosti), rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé** a klikněte na **Skupina zálohování**.
   - Pokud chcete zálohovat poštovní schránky jednotlivých uživatelů, rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jejichž poštovní schránky chcete zálohovat, a klikněte na **Zálohovat**.
4. Na panelu plánu zálohování:
   - Ověřte, že v části **Co se má zálohovat** je vybraná položka **Gmail**.
   - Chcete-li zálohovat kalendáře nasdílené s vybranými uživateli, aktivujte přepínač **Zahrnout sdílené kalendáře**.
   - Rozhodněte se, zda budete potřebovat fulltextové vyhledávání (str. 149) v zálohovaných e-mailových zprávách. Tuto možnost nastavíte kliknutím na ikonu ozubeného kola > **Možnosti zálohování** > **Fulltextové vyhledávání**.

16.2.1.1 Fulltextové vyhledávání

Tato možnost definuje, zda cloudový agent indexuje obsah e-mailových zpráv.

Výchozí nastavení: **Povoleno**.

Je-li tato možnost povolená, bude se obsah zpráv indexovat a můžete prohledávat jejich obsah. Jinak je možné prohledávat pouze předmět, odesílatele, příjemce a datum.

Poznámka *Hledání v šifrovaných zálohách není podporováno.*

Proces indexování nemá vliv na výkon zálohování, protože jej provádí jiná softwarová součást. Indexování první (plné) zálohy může nějakou dobu trvat. Proto se může obsah ve výsledcích hledání zobrazovat po dokončení zálohování se zpožděním.

Index zabírá 10–30 procent prostoru úložiště zabraného zálohami poštovních schránek. Přesnou hodnotu zjistíte kliknutím na **Zálohy** > **Zálohy cloudových aplikací** a zobrazením sloupce **Velikost indexu**. Chcete-li tento úložný prostor ušetřit, je vhodné zakázat fulltextové vyhledávání. Po dokončení příštího zálohování se hodnota ve sloupci **Velikost indexu** sníží na několik megabajtů. Toto minimální množství metadat je potřeba k vyhledávání podle předmětu, odesílatele, příjemce a data.

Pokud znovu obnovíte fulltextové vyhledávání, naindexuje software všechny zálohy dříve vytvořené v rámci plánu zálohování. Bude to chvíli trvat.

16.2.2 Obnovení poštovních schránek a jejich položek

16.2.2.1 Obnova schránek

1. Klikněte na **G Suite**.
2. Pokud jste do služby zálohování přidali více organizací G Suite, vyberte organizaci, jejíž zálohovaná data chcete obnovit. Jinak tento krok přeskočte.
3. Rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jehož poštovní schránku chcete obnovit, a klikněte na **Obnova**.

   Pokud byl uživatel odstraněn, vyberte ho v části **Zálohy cloudových aplikací** na kartě Zálohy (str. 112) a potom klikněte na možnost **Zobrazit zálohy**.

   Uživatele i skupiny můžete hledat podle jména. Zástupné znaky nejsou podporovány.
4. Vyberte bod obnovy.

   Tip: *Pokud chcete zobrazit jenom body obnovy, které obsahují poštovní schránky, vyberte v nabídce* ***Filtrovat podle obsahu*** *možnost* ***Gmail****.*
5. Klikněte na **Obnovit** > **Celá poštovní schránka**.
6. Pokud bylo do služby zálohování přidáno více organizací G Suite, klikněte na položku **Organizace G Suite**, která umožňuje zobrazit, změnit nebo zadat cílovou organizaci.

   Automaticky je vybraná původní organizace. Pokud tato organizace není ve službě zálohování zaregistrovaná, musíte zadat cílovou organizaci.
7. V nabídce **Obnovit do poštovní schránky** můžete zobrazit, změnit nebo zadat cílovou poštovní schránku.

   Ve výchozím nastavení je vybrána původní poštovní schránka. Pokud tato poštovní schránka neexistuje nebo není vybraná původní organizace, musíte zadat cílovou poštovní schránku.
8. Klikněte na možnost **Spustit obnovu**.
9. Vyberte jednu z možností přepisu:

- **Přepsat existující položky**
- **Nepřepisovat existující položky**

10. Potvrďte volbu kliknutím na **Pokračovat**.

16.2.2.2 Obnovení položek poštovní schránky

1. Klikněte na **G Suite**.
2. Pokud jste do služby zálohování přidali více organizací G Suite, vyberte organizaci, jejíž zálohovaná data chcete obnovit. Jinak tento krok přeskočte.
3. Rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jehož poštovní schránka původně obsahovala položky, které chcete obnovit, a klikněte na **Obnova**.

   Pokud byl uživatel odstraněn, vyberte ho v části **Zálohy cloudových aplikací** na kartě Zálohy (str. 112) a potom klikněte na možnost **Zobrazit zálohy**.

   Uživatele i skupiny můžete hledat podle jména. Zástupné znaky nejsou podporovány.
4. Vyberte bod obnovy.

   Tip: *Pokud chcete zobrazit jenom body obnovy, které obsahují poštovní schránky, vyberte v nabídce* ***Filtrovat podle obsahu*** *možnost* ***Gmail****.*
5. Klikněte na **Obnovit** > **E-mailové zprávy**.
6. Přejděte do požadované složky. Pokud není záloha zašifrovaná, můžete seznam požadovaných položek získat hledáním.

   Dostupné jsou následující možnosti vyhledávání. Zástupné znaky nejsou podporovány.
   - U e-mailových zpráv: vyhledávání podle předmětu, odesílatele, příjemce, data, názvu přílohy a obsahu zprávy. U posledních dvou možností dostanete výsledky, pouze pokud byla při zálohování povolena možnost **Fulltextové vyhledávání**. Jako další parametr je možné zadat jazyk fragmentu prohledávané zprávy.
   - U událostí: vyhledávání podle názvu a data.
   - U kontaktů: vyhledávání podle jména, e-mailové adresy a telefonního čísla.
7. Vyberte položky, které chcete obnovit. Chcete-li vybírat složky, klikněte na ikonu obnovy složek: 

   Můžete také použít některou z následujících možností:
   - Pokud je vybraná položka, kliknutím na **Zobrazit obsah** zobrazíte obsah včetně příloh. Když kliknete na název připojeného souboru, soubor se stáhne.
   - Pokud záloha nebyla zašifrovaná, použili jste vyhledávání a vybrali jste ve výsledcích hledání jen jednu položku, klikněte na **Zobrazit verze** a vyberte verzi položky, kterou chcete obnovit. Můžete vybrat kteroukoli zálohovanou verzi, která je starší nebo novější než vybraný bod obnovy.
8. Klikněte na příkaz **Obnovit**.
9. Pokud bylo do služby zálohování přidáno více organizací G Suite, klikněte na položku **Organizace G Suite**, která umožňuje zobrazit, změnit nebo zadat cílovou organizaci.

   Automaticky je vybraná původní organizace. Pokud tato organizace není ve službě zálohování zaregistrovaná, musíte zadat cílovou organizaci.
10. V nabídce **Obnovit do poštovní schránky** můžete zobrazit, změnit nebo zadat cílovou poštovní schránku.

    Ve výchozím nastavení je vybrána původní poštovní schránka. Pokud tato poštovní schránka neexistuje nebo není vybraná původní organizace, musíte zadat cílovou poštovní schránku.

11. V poli **Cesta** si můžete prohlédnout cílovou složku v poštovní schránce cílového uživatele nebo ji zde můžete změnit. Ve výchozím nastavení je vybraná původní složka.
12. Klikněte na možnost **Spustit obnovu**.
13. Vyberte jednu z možností přepisu:
    - **Přepsat existující položky**
    - **Nepřepisovat existující položky**
14. Potvrďte volbu kliknutím na **Pokračovat**.

16.3 Ochrana souborů Disku Google

Jaké položky lze zálohovat?

Můžete zálohovat celý Disk Google nebo jednotlivé soubory a složky. Volitelně můžete také zálohovat soubory, které jsou sdílené s uživatelem Disku Google.

Se soubory se zálohuje i oprávnění k jejich sdílení.

Následující položky budou při zálohování *přeskočeny*:

- Sdílený soubor, pokud má uživatel přístup k přidávání komentářů nebo prohlížení souboru a vlastník souboru zakázal pro tyto úrovně přístupu možnost soubor stáhnout, vytisknout nebo zkopírovat.
- Složka **Počítače** (vytvořená klientem pro zálohu a synchronizaci).

Omezení

- Z formátů souborů Google se zálohují pouze Dokumenty Google, Tabulky Google, Prezentace Google a Nákresy Google.

Jaké položky lze obnovit?

Můžete obnovit celý Disk Google nebo libovolný zálohovaný soubor nebo složku.

Položky v záloze můžete najít pomocí vyhledávání, pokud není záloha zašifrovaná. Hledání v šifrovaných zálohách není podporováno.

Můžete vybrat, jestli chcete obnovit i oprávnění ke sdílení nebo chcete, aby soubory převzaly oprávnění ze složky, do které se obnovují.

Omezení

- Nelze obnovit komentáře v souborech.
- Odkazy na soubory a složky určené ke sdílení se neobnoví.
- V průběhu obnovování nelze u sdílených souborů změnit atribut pouze ke čtení v **Nastavení vlastníka** (**Zakázat editorům možnost měnit přístup a přidávat nové uživatele** a **Zakázat možnost stahovat, tisknout a kopírovat uživatelům s úrovní přístupu pro komentáře a prohlížení**).
- Je-li pro tuto složku povolená možnost **Zakázat editorům možnost měnit přístup a přidávat nové uživatele**, nelze během obnovování změnit vlastnictví sdílené složky. Toto nastavení zabraňuje rozhraní API Disku Google v zobrazení oprávnění pro složky. Vlastnictví souborů ve složce se obnoví správně.

16.3.1 Výběr souborů Disku Google

Vyberte soubory (viz následující popis) a podle potřeby (str. 34) zadejte další nastavení plánu zálohování.

Postup výběru souborů Disku Google

1. Klikněte na **G Suite**.
2. Pokud jste do služby zálohování přidali více organizací G Suite, vyberte organizaci, jejíž data uživatelů chcete zálohovat. Jinak tento krok přeskočte.
3. Proveďte jeden z následujících úkonů:
   - Pokud chcete zálohovat soubory všech uživatelů (včetně uživatelů, kteří budou vytvořeni v budoucnosti), rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé** a klikněte na **Skupina zálohování**.
   - Pokud chcete zálohovat soubory jednotlivých uživatelů, rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jejichž soubory chcete zálohovat, a klikněte na **Zálohovat**.
4. Na panelu plánu zálohování:
   - Ověřte, že v části **Co se má zálohovat** je vybraná položka **Disk Google**.
   - V části **Položky k zálohování** proveďte jednu z následujících akcí:
     - Nechte výchozí nastavení **[Vše]** (všechny soubory).
     - Zadejte názvy souborů a složek nebo cesty k souborům a složkám, které se mají zálohovat.

       Můžete používat zástupné znaky (*, ** a ?). Další informace o zadávání cest a používání zástupných znaků naleznete v části Filtry souborů (str. 63).
     - Vyberte zálohované soubory a složky tím, že k nim přejdete.

       Odkaz **Procházet** je k dispozici jen při vytváření plánu zálohování jednoho uživatele.
   - [Volitelné] V části **Položky k zálohování** klikněte na **Zobrazit vyloučení** a zadejte soubory a složky, které chcete při zálohování přeskočit.

     Vyloučené soubory přepíší vybrané soubory. To znamená, že pokud zadáte stejný soubor do obou polí, při zálohování se přeskočí.
   - Chcete-li zálohovat soubory nasdílené s vybranými uživateli, aktivujte přepínač **Zahrnout sdílené soubory**.
   - Pokud chcete povolit notarizaci všech souborů zvolených pro zálohování, aktivujte přepínač **Notarizace**. Další informace o notarizaci naleznete v části Notarizace (str. 157).

16.3.2 Obnova Disku Google a souborů Disku Google

16.3.2.1 Obnovení celého Disku Google

1. Klikněte na **G Suite**.
2. Pokud jste do služby zálohování přidali více organizací G Suite, vyberte organizaci, jejíž zálohovaná data chcete obnovit. Jinak tento krok přeskočte.
3. Rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jehož Disk Google chcete obnovit, a klikněte na **Obnova**.

   Pokud byl uživatel odstraněn, vyberte ho v části **Zálohy cloudových aplikací** na kartě Zálohy (str. 112) a potom klikněte na možnost **Zobrazit zálohy**.

   Uživatele můžete hledat podle jména. Zástupné znaky nejsou podporovány.

4. Vyberte bod obnovy.

   ***Tip**: Pokud chcete zobrazit jenom body obnovení, které obsahují soubory Disku Google, vyberte v nabídce **Filtrovat podle obsahu** možnost **Disk Google**.*

5. Klikněte na **Obnovit** > **Celý Disk**.
6. Pokud bylo do služby zálohování přidáno více organizací G Suite, klikněte na položku **Organizace G Suite**, která umožňuje zobrazit, změnit nebo zadat cílovou organizaci.

   Automaticky je vybraná původní organizace. Pokud tato organizace není ve službě zálohování zaregistrovaná, musíte zadat cílovou organizaci.
7. V části **Obnovit na jednotku** můžete zobrazit, změnit nebo zadat cílového uživatele nebo cílové Týmové disky.

   Automaticky je vybraný původní uživatel. Pokud tento uživatel neexistuje nebo je vybraná jiná než původní organizace, musíte zadat cílového uživatele nebo cílové Týmové disky.

   Pokud záloha obsahuje sdílené soubory, obnoví se do kořenové složky cílového disku.
8. Vyberte, jestli chcete u souborů obnovit i oprávnění ke sdílení.
9. Klikněte na možnost **Spustit obnovu**.
10. Vyberte jednu z možností přepisu:
    - **Přepsat existující soubory**
    - **Přepsat existující soubor, pokud je starší**
    - **Nepřepisovat existující soubory**
11. Potvrďte volbu kliknutím na **Pokračovat**.

16.3.2.2 Obnova souborů Disku Google

1. Klikněte na **G Suite**.
2. Pokud jste do služby zálohování přidali více organizací G Suite, vyberte organizaci, jejíž zálohovaná data chcete obnovit. Jinak tento krok přeskočte.
3. Rozbalte uzel **Uživatelé**, vyberte **Všichni uživatelé**, vyberte uživatele, jehož soubory Disku Google chcete obnovit, a klikněte na **Obnova**.

   Pokud byl uživatel odstraněn, vyberte ho v části **Zálohy cloudových aplikací** na kartě Zálohy (str. 112) a potom klikněte na možnost **Zobrazit zálohy**.

   Uživatele můžete hledat podle jména. Zástupné znaky nejsou podporovány.
4. Vyberte bod obnovy.

   ***Tip**: Pokud chcete zobrazit jenom body obnovení, které obsahují soubory Disku Google, vyberte v nabídce **Filtrovat podle obsahu** možnost **Disk Google**.*

5. Klikněte na **Obnovit** > **Soubory/složky**.
6. Přejděte do požadované složky nebo pomocí vyhledávání získejte seznam požadovaných souborů a složek.

   Je možné použít více zástupných znaků (* a ?). Více informací o používání zástupných znaků naleznete v části Filtry souborů (str. 63).

   Vyhledávání není dostupné, pokud je záloha zašifrovaná.
7. Vyberte soubory, které chcete obnovit.

   Pokud není záloha zašifrovaná a vyberete jen jeden soubor, klikněte na **Zobrazit verze** a vyberte verzi souboru, kterou chcete obnovit. Můžete vybrat kteroukoli zálohovanou verzi, která je starší nebo novější než vybraný bod obnovy.

8. Pokud chcete stáhnout soubor, vyberte ho, klikněte na **Stáhnout**, vyberte místo pro uložení souboru a potom klikněte na **Uložit**. Jinak tento krok přeskočte.
9. Klikněte na příkaz **Obnovit**.
10. Pokud bylo do služby zálohování přidáno více organizací G Suite, klikněte na položku **Organizace G Suite**, která umožňuje zobrazit, změnit nebo zadat cílovou organizaci.

    Automaticky je vybraná původní organizace. Pokud tato organizace není ve službě zálohování zaregistrovaná, musíte zadat cílovou organizaci.
11. V části **Obnovit na jednotku** můžete zobrazit, změnit nebo zadat cílového uživatele nebo cílové Týmové disky.

    Automaticky je vybraný původní uživatel. Pokud tento uživatel neexistuje nebo je vybraná jiná než původní organizace, musíte zadat cílového uživatele nebo cílové Týmové disky.
12. V poli **Cesta** si můžete prohlédnout nebo změnit cílovou složku na Disku Google cílového uživatele nebo na cílových Týmových discích. Automaticky je vybrané původní umístění.
13. Vyberte, jestli chcete u souborů obnovit i oprávnění ke sdílení.
14. Klikněte na možnost **Spustit obnovu**.
15. Vyberte jednu z možností pro přepis souborů:
    - **Přepsat existující soubory**
    - **Přepsat existující soubor, pokud je starší**
    - **Nepřepisovat existující soubory**
16. Potvrďte volbu kliknutím na **Pokračovat**.

16.4 Ochrana souborů Týmových disků

Jaké položky lze zálohovat?

Můžete zálohovat celé Týmové disky nebo jednotlivé soubory a složky.

Se soubory se zálohuje i oprávnění k jejich sdílení.

Omezení

- Z důvodu omezení rozhraní API Disku Google nelze zálohovat Týmové disky bez členů.
- Z formátů souborů Google se zálohují pouze Dokumenty Google, Tabulky Google, Prezentace Google a Nákresy Google.

Jaké položky lze obnovit?

Můžete obnovit celé Týmové disky nebo libovolný zálohovaný soubor nebo složku.

Položky v záloze můžete najít pomocí vyhledávání, pokud není záloha zašifrovaná. Hledání v šifrovaných zálohách není podporováno.

Můžete vybrat, jestli chcete obnovit i oprávnění ke sdílení nebo chcete, aby soubory převzaly oprávnění ze složky, do které se obnovují.

Následující položky nelze obnovit:

- Je-li v cílových Týmových discích zakázáno sdílení mimo organizaci, neobnoví se oprávnění ke sdílení u souboru, který byl nasdílen uživatelem mimo organizaci.
- Je-li v cílových Týmových discích zakázáno **sdílení s nečleny**, neobnoví se oprávnění ke sdílení u souboru nasdíleného uživatelem, který není členem cílových Týmových disků.

Omezení

- Nelze obnovit komentáře v souborech.
- Odkazy na soubory a složky určené ke sdílení se neobnoví.

16.4.1 Výběr souborů Týmových disků

Vyberte soubory (viz následující popis) a podle potřeby (str. 34) zadejte další nastavení plánu zálohování.

Postup výběru souborů Týmových disků

1. Klikněte na **G Suite**.
2. Pokud jste do služby zálohování přidali více organizací G Suite, vyberte organizaci, jejíž data uživatelů chcete zálohovat. Jinak tento krok přeskočte.
3. Proveďte jeden z následujících úkonů:
   - Pokud chcete zálohovat soubory všech Týmových disků (včetně Týmových disků, které budou vytvořeny v budoucnosti), rozbalte uzel **Týmové disky**, vyberte **Všechny Týmové disky** a klikněte na **Skupina zálohování**.
   - Pokud chcete zálohovat soubory jednotlivých Týmových disků, rozbalte uzel **Týmové disky**, vyberte **Všechny Týmové disky**, vyberte požadované Týmové disky k zálohování a potom klikněte na **Záloha**.
4. Na panelu plánu zálohování:
   - V části **Položky k zálohování** proveďte jednu z následujících akcí:
     - Nechte výchozí nastavení **[Vše]** (všechny soubory).
     - Zadejte názvy souborů a složek nebo cesty k souborům a složkám, které se mají zálohovat.

       Můžete používat zástupné znaky (*, ** a ?). Další informace o zadávání cest a používání zástupných znaků naleznete v části Filtry souborů (str. 63).
     - Vyberte zálohované soubory a složky tím, že k nim přejdete.

       Odkaz **Procházet** je k dispozici jen při vytváření plánu zálohování jedné instance Týmových disků.
   - [Volitelné] V části **Položky k zálohování** klikněte na **Zobrazit vyloučení** a zadejte soubory a složky, které chcete při zálohování přeskočit.

     Vyloučené soubory přepíší vybrané soubory. To znamená, že pokud zadáte stejný soubor do obou polí, při zálohování se přeskočí.
   - Pokud chcete povolit notarizaci všech souborů zvolených pro zálohování, aktivujte přepínač **Notarizace**. Další informace o notarizaci naleznete v části Notarizace (str. 157).

16.4.2 Obnova Týmových disků a souborů Týmových disků

16.4.2.1 Obnovení celých Týmových disků

1. Klikněte na **G Suite**.
2. Pokud jste do služby zálohování přidali více organizací G Suite, vyberte organizaci, jejíž zálohovaná data chcete obnovit. Jinak tento krok přeskočte.
3. Rozbalte uzel **Týmové disky**, vyberte **Všechny Týmové disky**, vyberte Týmové disky, které chcete obnovit, a klikněte na **Obnova**.

   Pokud byly Týmové disky odstraněny, vyberte je v oddílu **Zálohy cloudových aplikací** na kartě Zálohy (str. 112) a klikněte na **Zobrazit zálohy**.

Týmové disky můžete prohledávat podle jména. Zástupné znaky nejsou podporovány.

4. Vyberte bod obnovy.
5. Klikněte na **Obnovit** > **Celé Týmové disky**.
6. Pokud bylo do služby zálohování přidáno více organizací G Suite, klikněte na položku **Organizace G Suite**, která umožňuje zobrazit, změnit nebo zadat cílovou organizaci.

   Automaticky je vybraná původní organizace. Pokud tato organizace není ve službě zálohování zaregistrovaná, musíte zadat cílovou organizaci.
7. V části **Obnovit na jednotku** můžete zobrazit, změnit nebo zadat cílové Týmové disky nebo cílového uživatele. Zadáte-li uživatele, obnoví se data na jeho Disk Google.

   Jako výchozí jsou vybrány původní Týmové disky. Pokud tyto Týmové disky neexistují nebo je vybraná jiná než původní organizace, musíte zadat cílové Týmové disky nebo cílového uživatele.
8. Vyberte, jestli chcete u souborů obnovit i oprávnění ke sdílení.
9. Klikněte na možnost **Spustit obnovu**.
10. Vyberte jednu z možností přepisu:
    - **Přepsat existující soubory**
    - **Přepsat existující soubor, pokud je starší**
    - **Nepřepisovat existující soubory**
11. Potvrďte volbu kliknutím na **Pokračovat**.

16.4.2.2 Obnova souborů Týmových disků

1. Klikněte na **G Suite**.
2. Pokud jste do služby zálohování přidali více organizací G Suite, vyberte organizaci, jejíž zálohovaná data chcete obnovit. Jinak tento krok přeskočte.
3. Rozbalte uzel **Týmové disky**, vyberte **Všechny Týmové disky**, vyberte Týmové disky s původními soubory, které chcete obnovit, a klikněte na **Obnova**.

   Pokud byly Týmové disky odstraněny, vyberte je v oddílu **Zálohy cloudových aplikací** na kartě Zálohy (str. 112) a klikněte na **Zobrazit zálohy**.

   Týmové disky můžete prohledávat podle jména. Zástupné znaky nejsou podporovány.
4. Vyberte bod obnovy.
5. Klikněte na **Obnovit** > **Soubory/složky**.
6. Přejděte do požadované složky nebo pomocí vyhledávání získejte seznam požadovaných souborů a složek.

   Je možné použít více zástupných znaků (* a ?). Více informací o používání zástupných znaků naleznete v části Filtry souborů (str. 63).

   Vyhledávání není dostupné, pokud je záloha zašifrovaná.
7. Vyberte soubory, které chcete obnovit.

   Pokud není záloha zašifrovaná a vyberete jen jeden soubor, klikněte na **Zobrazit verze** a vyberte verzi souboru, kterou chcete obnovit. Můžete vybrat kteroukoli zálohovanou verzi, která je starší nebo novější než vybraný bod obnovy.
8. Pokud chcete stáhnout soubor, vyberte ho, klikněte na **Stáhnout**, vyberte místo pro uložení souboru a potom klikněte na **Uložit**. Jinak tento krok přeskočte.
9. Klikněte na příkaz **Obnovit**.
10. Pokud bylo do služby zálohování přidáno více organizací G Suite, klikněte na položku **Organizace G Suite**, která umožňuje zobrazit, změnit nebo zadat cílovou organizaci.

Automaticky je vybraná původní organizace. Pokud tato organizace není ve službě zálohování zaregistrovaná, musíte zadat cílovou organizaci.

11. V části **Obnovit na jednotku** můžete zobrazit, změnit nebo zadat cílové Týmové disky nebo cílového uživatele. Zadáte-li uživatele, obnoví se data na jeho Disk Google.

    Jako výchozí jsou vybrány původní Týmové disky. Pokud tyto Týmové disky neexistují nebo je vybraná jiná než původní organizace, musíte zadat cílové Týmové disky nebo cílového uživatele.
12. V poli **Cesta** si můžete prohlédnout nebo změnit cílovou složku na cílových Týmových discích nebo na Disku Google cílového uživatele. Automaticky je vybrané původní umístění.
13. Vyberte, jestli chcete u souborů obnovit i oprávnění ke sdílení.
14. Klikněte na možnost **Spustit obnovu**.
15. Vyberte jednu z možností pro přepis souborů:
    - **Přepsat existující soubory**
    - **Přepsat existující soubor, pokud je starší**
    - **Nepřepisovat existující soubory**
16. Potvrďte volbu kliknutím na **Pokračovat**.

16.5 Notarizace

Notarizace umožňuje potvrdit, že soubor je autentický a nebyl od zálohy změněn Notarizaci doporučujeme povolit při zálohování souborů právních dokumentů nebo dalších souborů, které vyžadují potvrzení pravosti.

Notarizace je k dispozici pouze pro zálohy souborů Disku Google a souborů Týmových disků G Suite.

Použití notarizace

Pokud chcete povolit notarizaci všech souborů zvolených pro zálohování, aktivujte přepínač **Notarizace** při vytváření plánu zálohování.

Při konfiguraci obnovení budou notarizované soubory označeny zvláštní ikonou a můžete ověřit pravost souborů.

Jak to funguje

Během zálohování agent vypočítá kódy hash zálohovaných souborů, vytvoří hashovací strom (založený na struktuře složek), uloží strom do zálohy a poté odešle kořenový hashovací strom notářské službě. Notářská služba uloží kořenový hashovací strom v databázi blockchain Ethereum, čímž se zajistí, že tato hodnota se nezmění.

Při ověřování pravosti souborů agent vypočítá hash souboru a porovná jej s kódem hash, který je uložen v hashovacím stromu uvnitř zálohy. Pokud se kódy hash neshodují, soubor není považován za autentický. V opačném případě je autenticita souboru zaručena hashovacím stromem.

Chcete-li ověřit, že samotný hashovací strom nebyl zfalšován, agent odešle kořenový hashovací strom notářské službě. Notářská služba jej porovná se stromem uloženým v databázi blockchain. Když se kódy hash shodují, je zaručena autenticita souboru. V opačném případě se zobrazí zpráva s upozorněním, že soubor není autentický.

16.5.1 Ověřování autenticity souboru pomocí služby Notary

Pokud byla během zálohování zapnutá notarizace, můžete ověřit autenticitu souboru.

Jak ověřit autenticitu souboru

1. Proveďte jeden z následujících úkonů:
   - Autentičnost souboru Disku Google ověříte vybráním souboru podle kroků 1–7 v části Obnova souborů Disku Google (str. 153).
   - Autentičnost souboru Týmových disků G Suite ověříte vybráním souboru podle kroků 1–7 v části Obnova souborů Týmových disků (str. 156).
2. Zkontrolujte, zda je vybraný soubor označený následující ikonou:  . To znamená, že soubor je notarizován.
3. Proveďte jeden z následujících úkonů:
   - Klikněte na možnost **Ověřit**.

     Software zkontroluje autenticitu souboru a zobrazí výsledek.
   - Klikněte na možnost **Získat certifikát**.

     V okně webového prohlížeče se zobrazí certifikát potvrzující notarizaci souboru. Okno také obsahuje pokyny, které vám umožní ověřit autenticitu souboru ručně.

17 Active Protection

Active protection chrání systém před ransomwarem a malwarem zaměřeným na těžbu kryptoměn. Ransomware šifruje soubory a za šifrovací klíč požaduje výkupné. Malware pro těžbu kryptoměn provádí matematické výpočty na pozadí, což má za následek snížení výpočetního výkonu a vyšší zatížení sítě.

Active protection je dostupná u počítačů se systémem Windows 7 nebo novějším a Windows Server 2008 R2 nebo novějším. Na počítači musí být nainstalovaný Agent pro Windows.

Active Protection je k dispozici u agentů od verze 12.0.4290. Chcete-li aktualizovat agenta, postupujte podle pokynů v článku Aktualizace agentů (str. 30).

Jak to funguje

Active protection sleduje procesy běžící na chráněném počítači. Když se proces třetích stran pokusí zašifrovat soubory nebo těžit kryptoměny, Active protection vygeneruje výstrahu a provede další akce (pokud jsou určeny v konfiguraci).

Kromě toho Active protection brání před neoprávněnými změnami vlastních procesů zálohovacího softwaru, záznamů v registru, spustitelných a konfiguračních souborů a záloh uložených v místních složkách.

K identifikaci škodlivých procesů používá Active protection behaviorální heuristiku. Srovnává řetězec akcí provedený procesem s řetězci událostí zaznamenanými v databázi vzorců škodlivého chování. Tento přístup umožňuje Active Protection rozpoznávat nový malware na základě jeho typického chování.

Nastavení Active Protection

Chcete-li omezit prostředky využívané heuristickou analýzou a vyloučit takzvané falešně pozitivní výsledky, kdy je důvěryhodný program považován za ransomware, můžete definovat následující nastavení:

- Důvěryhodné procesy, které nikdy nebudou považovány za ransomware. Procesy podepsané společností Microsoft jsou vždy důvěryhodné.

- Škodlivé procesy, které budou vždy považovány za ransomware. Tyto procesy nebudou moci být spuštěny, dokud je v počítači povolena Active protection.
- Složky, ve kterých nebudou změny souborů sledovány.

Zadejte úplnou cestu ke spustitelnému souboru procesu, počínaje písmenem jednotky. Příklad: **`C:\Windows\Temp\er76s7sdkh.exe`**.

K zadání složky můžete použít zástupné znaky * a ?: Znak hvězdičky (*) nahrazuje nula nebo více znaků. Znak otazníku (?) nahrazuje přesně jeden znak. Proměnné prostředí, jako %AppData%, nelze použít.

Plán Active Protection

Všechna nastavení Active Protection se nachází v plánu Active Protection. Tento plán je možné použít na více počítačích.

V jedné organizaci (skupině společnosti) je možné mít pouze jeden plán Active Protection. Plán mohou instalovat, upravit nebo odvolat pouze správci společnosti a správci vyšších úrovní.

Instalace plánu Active Protection

1. Vyberte počítače, na kterých chcete Active Protection nainstalovat.
2. Klikněte na možnost **Active protection**.
3. [Volitelné] Klikněte na tlačítko **Upravit**, abyste upravili následující nastavení:
   - U možnosti **Akce při detekování** vyberte akci, kterou software provede při zjištění aktivity typu ransomware, a potom klikněte na **Hotovo**. Je možné vybrat jednu z následujících možností:
     - **Pouze upozornit**

       Software o tomto procesu vygeneruje výstrahu.
     - **Zastavit proces** (výchozí)

       Software o tomto procesu vygeneruje výstrahu a zastaví ho.
     - **Vrátit pomocí mezipaměti**

       Software vygeneruje výstrahu, zastaví proces a vrátí změny souboru pomocí služby mezipaměti.
   - U možnosti **Škodlivé procesy** určete škodlivé procesy, které budou vždy považované za ransomware, a potom klikněte na **Hotovo**.
   - U možnosti **Důvěryhodné procesy** určete důvěryhodné procesy, které nikdy nebudou považované za ransomware, a potom klikněte na **Hotovo**. Procesy podepsané společností Microsoft jsou vždy důvěryhodné.
   - U možnosti **Výjimky složek** určete seznam složek, ve kterých nebudou sledovány změny souborů, a potom klikněte na **Hotovo**.
   - Vypněte přepínač **Vlastní ochrana**.

     Vlastní ochrana brání před neoprávněnými změnami softwarových vlastních procesů, záznamů v registru, spustitelných a konfiguračních souborů a záloh uložených v místních složkách. Tuto funkci doporučujeme nevypínat.
   - Změňte **Možnosti ochrany** (str. 160).
4. Pokud jste tato nastavení upravili, klikněte na tlačítko **Uložit změny**. Změny se projeví na všech počítačích, na kterých je Active protection zapnuta.
5. Klikněte na tlačítko **Použít**.

17.1 Možnosti ochrany

Zálohy

Tato možnost funguje, pokud je v plánu Active Protection zapnutá možnost **Vlastní ochrana**.

Tato možnost platí pro soubory s příponami .tibx, .tib, .tia, které jsou v místních složkách.

U této možnosti můžete vybrat, jaké procesy smí měnit soubory zálohy, i když tyto soubory mají vlastní ochranu. Je to praktické, například když jste použili skript, kterým soubory zálohy odstraníte nebo je přesunete jinam.

Výchozí nastavení: **Povoleno**.

Pokud je tato možnost povolena, mohou soubory záloh měnit jen procesy podepsané dodavatelem zálohovacího softwaru. Software tak může používat pravidla zachování a odstraňovat zálohy, jen když o to požádá uživatel ve webovém rozhraní. Jiné procesy zálohy měnit nemohou – bez ohledu na to, jestli jsou nebo nejsou podezřelé.

Pokud je tato možnost vypnutá, můžete ostatním procesům povolit upravovat zálohy. Zadejte úplnou cestu ke spustitelnému souboru procesu, počínaje písmenem jednotky.

Ochrana proti těžbě kryptoměn

Tato možnost definuje, zda Active protection detekuje potenciální malware pro těžbu kryptoměn.

Výchozí nastavení: **Zakázáno**.

Je-li detekována aktivita těžby kryptoměn, provede se zvolená **Akce při detekování** (s výjimkou vrácení souborů z vyrovnávací paměti, protože se nic nevrátí).

Malware pro těžbu kryptoměn degraduje výkon užitečných aplikací, zvyšuje účty za elektřinu, může způsobit selhání systému a dokonce poškodit hardware v důsledku zneužití. Doporučujeme, abyste malware pro těžbu kryptoměn přidali do seznamu **Škodlivé procesy**, aby nedošlo k jeho spuštění.

Mapované jednotky

Tato volba definuje, jestli Active Protection chrání síťové složky mapované jako místní jednotky.

Tato možnost platí pro složky sdílené prostřednictvím SMB i NFS.

Výchozí nastavení: **Povoleno**.

Pokud se soubor původně nacházel na mapované jednotce, nemůžete ho při extrakci z mezipaměti akcí **Vrátit pomocí mezipaměti** uložit na původní místo. Místo toho se uloží do složky, kterou určíte v nastavení této možnosti. Výchozí složka je **C:\ProgramData\Acronis\Restored Network Files**. Pokud tato složka neexistuje, bude vytvořena. Pokud ji chcete změnit, nezapomeňte zadat místní složku. Síťové složky včetně složek na mapovaných jednotkách nejsou podporovány.

18 Ochrana webových stránek a hostingových serverů

18.1 Ochrana webových stránek

V důsledku neoprávněného přístupu nebo malwarového útoku může dojít k poškození webové stránky. Zálohování webové stránky vám v případě jejího poškození umožní její snadné obnovení do funkčního stavu.

Co je třeba k zálohování webové stránky?

Webová stránka musí být přístupná prostřednictvím protokolu SFTP nebo SSH. Nemusíte instalovat agenta, stačí přidat webovou stránku způsobem popsaným v této části.

Jaké položky lze zálohovat?

Zálohovat můžete následující položky:

- **Soubory obsahu webové stránky**

  Všechny soubory přístupné pro účet, který určíte pro připojení SFTP nebo SSH.
- **Propojené databáze (pokud existují) hostované na serverech MySQL**

  Všechny databáze přístupné pro účet MySQL, který zadáte.

Pokud vaše webová stránka používá databáze, doporučujeme zálohovat soubory i databáze, abyste je mohli obnovit do konzistentního stavu.

Omezení

- Jako jediné úložiště záloh webových stránek je dostupné cloudové úložiště.
- Plány zálohování nelze použít na více webových stránek. Každá webová stránka musí mít svůj vlastní plán zálohování, i když všechny plány zálohování mají stejné nastavení.
- Pro webovou stránku lze použít pouze jeden plán zálohování.
- Možnosti zálohování nejsou k dispozici.

18.1.1 Zálohování webové stránky

Přidání webové stránky a konfigurace jejího zálohování

1. Klikněte na **Zařízení** > **Přidat**.
2. Klikněte na možnost **Webová stránka**.
3. Nakonfigurujte pro webovou stránku následující nastavení přístupu:
   - Do pole **Název webové stránky** zadejte název své webové stránky. Tento název se zobrazí v konzoli pro zálohování.
   - Do pole **Hostitel** zadejte název hostitele nebo IP adresu, která se použije pro přístup k webové stránce prostřednictvím protokolu SFTP nebo SSH. Příklad: `muj.server.com` nebo `10.250.100.100`.
   - Do pole **Port** zadejte číslo portu.
   - Do polí **Uživatelské jméno** a **Heslo** zadejte pověření účtu, který se bude používat pro přístup k webové stránce prostřednictvím protokolu SFTP nebo SSH.

     Důležité: *Zálohovány budou pouze soubory, které jsou přístupné zadanému účtu.*

Místo hesla můžete zadat svůj soukromý klíč SSH. Chcete-li tak učinit, zaškrtněte políčko **Místo hesla použít soukromý klíč SSH** a poté zadejte klíč.

4. Klikněte na tlačítko **Další**.
5. Pokud vaše webová stránka používá databáze MySQL, nakonfigurujte nastavení přístupu k databázím. V opačném případě klikněte na tlačítko **Přeskočit**.
   a. V části **Typ připojení** vyberte, jak chcete přistupovat k databázím z cloudu:
      - **Prostřednictvím SSH od hostitele** – Databáze budou přístupné prostřednictvím hostitele, kterého jste zadali v kroku 3.
      - **Přímé připojení** – Databáze budou přístupné přímo. Toto nastavení zvolte pouze tehdy, pokud jsou databáze přístupné z internetu.
   b. Do pole **Hostitel** zadejte název nebo IP adresu hostitele, ve kterém je spuštěn server MySQL.
   c. Do pole **Port** zadejte číslo portu pro připojení TCP/IP k serveru. Výchozí číslo portu je 3306.
   d. Do polí **Uživatelské jméno** a **Heslo** zadejte pověření účtu MySQL.

      Důležité: *Zálohovány budou pouze databáze, které jsou přístupné zadanému účtu.*

   e. Klikněte na tlačítko **Vytvořit**.
6. Software zobrazí šablonu nového plánu zálohování. V případě potřeby změňte nastavení a potom klikněte na možnost **Použít**.

Změna nastavení připojení

1. Klikněte na možnost **Zařízení** > **Webové stránky** a vyberte požadovanou webovou stránku.
2. Klikněte na možnost **Přehled**.
3. Klikněte na ikonu tužky vedle nastavení připojení k webové stránce nebo databázi.
4. Proveďte potřebné změny a potom klikněte na tlačítko **Uložit**.

Úprava plánu zálohování

1. Klikněte na možnost **Zařízení** > **Webové stránky** a vyberte požadovanou webovou stránku.
2. Klikněte na možnost **Zálohovat**.
3. Klikněte na ikonu ozubeného kola vedle názvu plánu zálohování a potom na možnost **Upravit**.
4. Proveďte potřebné změny a potom klikněte na tlačítko **Uložit změny**.

18.1.2 Obnovení webové stránky

Obnovení webové stránky

1. Klikněte na možnost **Zařízení** > **Webové stránky** a vyberte webovou stránku, kterou chcete obnovit.

   Webové stránky můžete vyhledávat podle názvu. Zástupné znaky nejsou podporovány.
2. Klikněte na možnost **Obnova**.
3. Vyberte bod obnovy.
4. Klikněte na možnost **Obnovit** a vyberte, co chcete obnovit: **Soubory/složky** nebo **Databáze SQL** (pokud existuje).

   Chcete-li zajistit, aby webová stránka byla obnovena do konzistentního stavu, doporučujeme obnovit soubory i databáze (v libovolném pořadí).
5. Proveďte jeden z následujících úkonů podle toho, co jste vybrali:

Obnovení souborů a složek webové stránky

1. Přejděte do požadované složky nebo pomocí vyhledávání získejte seznam požadovaných souborů a složek.

Je možné použít více zástupných znaků * a ?. Podrobnosti o používání zástupných znaků naleznete v tématu Filtry souborů (str. 63).

2. Vyberte soubory, které chcete obnovit.
3. Pokud chcete soubory uložit do souboru .zip, klikněte na **Stáhnout**, vyberte umístění, do kterého se mají data uložit, a klikněte na **Uložit**. Jinak tento krok přeskočte.
4. Klikněte na tlačítko **Obnovit** a poté akci potvrďte.

   Vybrané soubory a složky budou obnoveny do původního umístění.

Obnovení databází

1. Vyberte databáze, které chcete obnovit.
2. Pokud chcete databáze uložit do souboru .zip, klikněte na tlačítko **Stáhnout**, vyberte umístění, do kterého se mají data uložit, a klikněte na tlačítko **Uložit**. Jinak tento krok přeskočte.
3. Klikněte na tlačítko **Obnovit** a poté akci potvrďte.

   Vybrané databáze budou obnoveny do původního umístění.

18.2 Ochrana webhostingových serverů

Správci webhostingu, kteří používají platformy Plesk nebo cPanel, mohou integrovat tyto platformy do zálohovací služby.

Integrace umožní správci provádět následující akce:

- Zálohovat celý server Plesk nebo cPanel do cloudového úložiště pomocí zálohy na úrovni disku.
- Obnovit celý server, včetně všech webových stránek.
- Plesk: provádět granulární obnovu webových stránek, jednotlivých souborů, poštovních schránek nebo databází.
- cPanel: provádět granulární obnovu webových stránek, jednotlivých souborů, poštovních schránek, poštovních filtrů, pravidel pro přeposílání pošty, databází a účtů.
- Povolit samoobslužnou obnovu pro zákazníky používají platformy Plesk a cPanel.

Integrace se provádí pomocí rozšíření zálohovací služby. Pokud potřebujete rozšíření pro Plesk nebo cPanel, kontaktujte poskytovatele zálohovací služby.

Podpora verzí platforem Plesk a cPanel

- Plesk pro Linux 17.0 a novější
- Libovolná verze cPanel s PHP 5.6 a novější

Kvóty

Každý zálohovaný server Plesk nebo cPanel spotřebovává kvótu **Webhostingové servery**. Je-li tato kvóta vypnutá nebo je překročen limit kvóty, dojde k následujícímu:

- Pokud je server fyzický, použije se kvóta **Servery**. Je-li tato kvóta vypnutá nebo je překročen limit kvóty, zálohování se nezdaří.
- Pokud je server virtuální, použije se kvóta **Virtuální počítače**. Je-li tato kvóta vypnutá nebo je překročen limit kvóty, použije se kvóta **Servery**. Je-li tato kvóta vypnutá nebo je překročen limit kvóty, zálohování se nezdaří.

19 Speciální operace s virtuálními počítači

19.1 Spuštění virtuálního počítače ze zálohy (funkce okamžitého obnovení)

Ze zálohy na úrovni disku, která obsahuje operační systém, můžete spustit virtuální počítač. Tato operace se nazývá okamžité obnovení a umožňuje spuštění virtuálního serveru během několika sekund. Virtuální disky se emulují přímo ze zálohy a nespotřebovávají tedy místo v datovém úložišti. Prostor úložiště je nutný pouze pro záznam změn virtuálních disků.

Doporučujeme, aby takový dočasný virtuální počítač byl spuštěn maximálně tři dny. Potom jej můžete úplně odstranit nebo převést na běžný virtuální počítač (finalizovat) bez jakékoliv odstávky.

Dokud dočasný virtuální počítač existuje, nelze na zálohu, kterou používá, použít pravidla zachování. Zálohy původního počítače mohou běžet dál.

Příklady použití

- **Obnovení po havárii**

  Je možné okamžitě zprovoznit kopii havarovaného počítače.
- **Testování zálohy**

  Počítač můžete spustit ze zálohy a zkontrolovat, zda hostovaný OS a aplikace správně fungují.
- **Přístup k datům aplikací**

  Když je počítač spuštěn, můžete pomocí nativních nástrojů aplikace pro správu získat přístup k požadovaným datům a extrahovat je.

Předpoklady

- Ve službě zálohování musí být zaregistrován alespoň jeden Agent pro VMware nebo Agent pro Hyper-V.
- Záloha může být uložena v síťové nebo místní složce na počítači, kde je Agent pro VMware nebo Agent pro Hyper-V nainstalován. Pokud vyberete síťovou složku, musí být z tohoto počítače přístupná. Virtuální počítač lze spustit také ze zálohy uložené v cloudovém úložišti, tato operace je však pomalejší, protože vyžaduje velmi náročné čtení ze zálohy s náhodným přístupem.
- Záloha musí obsahovat celý počítač nebo všechny svazky, které jsou ke spuštění operačního systému potřeba.
- Je možné použít zálohy fyzických i virtuálních počítačů. Zálohy *kontejnerů* Virtuozzo nelze použít.
- Zálohy, které obsahují logické svazky systému Linux (LVM), musí být vytvořeny Agentem pro VMware nebo Agentem pro Hyper-V. Virtuální počítač musí být stejného typu jako původní počítač (ESXi nebo Hyper-V).

19.1.1 Spouštění počítače

1. Proveďte jeden z následujících úkonů:
   - Vyberte zálohovaný počítač, klikněte na možnost **Obnova** a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Zálohy (str. 112).
2. Klikněte na možnost **Spustit jako virtuální počítač**.

Software automaticky vybere hostitele a další požadované parametry.

3. [Volitelné] Klikněte na možnost **Cílový počítač** a poté změňte typ virtuálního počítače (ESXi nebo Hyper-V), hostitele nebo název virtuálního počítače.
4. [Volitelné] Klikněte na možnost **Datové úložiště** u ESXi nebo na možnost **Cesta** u Hyper-V a poté vyberte datové úložiště virtuálního počítače.

   Změny na virtuálních discích se za běhu počítače shromažďují. Zajistěte, že vybrané na datovém úložišti bude dostatek volného místa.
5. [Volitelné] Pomocí možnosti **Nastavení virtuálního počítače** změňte velikost paměti a síťová připojení virtuálního počítače.
6. [Volitelné] Vyberte stav napájení virtuálního počítače (**Zapnuto**/**Vypnuto**).
7. Klikněte na možnost **Spustit**.

Ve výsledku se počítač zobrazí ve webovém rozhraní s jednou z následujících ikon:  nebo 

. Tyto virtuální počítače není možné vybrat k zálohování.

19.1.2 Odstranění počítače

Nedoporučujeme odstraňovat dočasný virtuální počítač přímo ve vSphere/Hyper-V. Toto může vést k artefaktům ve webovém rozhraní. Taktéž záloha, ze které počítač běžel, by mohla na chvíli zůstat zamknutá (nemůže být odstraněna pravidly zachování).

Jak odstranit virtuální počítač, který běží ze zálohy

1. Na kartě **Všechna zařízení** vyberte počítač, který běží ze zálohy.
2. Klikněte na možnost **Odstranit**.

Počítač bude odebrán z webového rozhraní. Odebere se také z inventáře a datového úložiště vSphere nebo Hyper-V. Veškeré změny dat provedené za běhu počítače budou ztraceny.

19.1.3 Dokončení počítače

Pokud virtuální počítač běží ze zálohy, obsah virtuálních disků je získáván přímo z příslušné zálohy. Proto pokud je ztraceno spojení s umístěním zálohy nebo s agentem zálohy, počítač přestane být dostupný nebo dokonce dojde k jeho poškození.

U počítačů ESXi existuje možnost nastavit počítač jako trvalý, jinými slovy obnovit všechny jeho virtuální disky společně se změnami, které se provedly za běhu počítače, do datového úložiště, které uchovává tyto změny. Tento proces se nazývá dokončení.

Dokončení se provede bez výpadku. Virtuální počítač *nebude* během dokončení vypnut.

Jak dokončit počítač, který běží ze zálohy

1. Na kartě **Všechna zařízení** vyberte počítač, který běží ze zálohy.
2. Klikněte na možnost **Dokončit**.
3. [Volitelné] Určete nový název počítače.
4. [Volitelné] Změňte režim poskytování disku. Ve výchozím nastavení je nastaven režim **Tenký**.
5. Klikněte na možnost **Dokončit**.

Název počítače se okamžitě změní. Postup obnovy se zobrazuje na kartě **Aktivity**. Jakmile se obnova dokončí, ikona počítače se změní na ikonu běžného virtuálního počítače.

Co potřebujete vědět o dokončení

Dokončení vs. běžné obnovení

Proces dokončení je pomalejší než běžné obnovení, a to z následujících důvodů:

- Během dokončení agent provádí náhodný přístup k různým částem zálohy. Při obnovení celého počítače agent načítá data ze zálohy postupně.
- Pokud je během dokončení spuštěn virtuální počítač, agent načítá data ze zálohy častěji, aby udržoval oba procesy současně. Během běžného obnovení je virtuální počítač nečinný.

Dokončení počítačů spuštěných z cloudových záloh

Kvůli intenzivnímu přístupu k zálohovaným datům rychlost dokončení velmi závisí na šířce pásma připojení mezi umístěním zálohy a agentem. Dokončení bude pomalejší u záloh umístěných v cloudu ve srovnání s místními zálohami. Pokud je internetové připojení velmi pomalé nebo nestabilní, může dokončení počítače spuštěného z cloudové zálohy selhat. Doporučujeme spouštět virtuální počítače z místních záloh, pokud plánujete provést dokončení a máte na výběr.

19.2 Replikace virtuálních počítačů

Replikace je k dispozici pouze u virtuálních počítačů VMware ESXi.

Replikace je proces, při kterém se vytvoří přesná kopie (repliky) virtuálního počítače a replika se poté udržuje v synchronizaci s původním počítačem. Pokud replikujete důležitý virtuální počítač, budete mít vždy kopii tohoto počítače připravenou ke spuštění.

Replikaci je možné spustit ručně nebo ji naplánovat. První replikace je plná (kopie celého počítače). Všechny následující replikace jsou přírůstkové a provádějí se s možností Sledování změněných bloků (str. 170), pokud tato možnost není zakázána.

Replikace vs. zálohování

Na rozdíl od plánovaných záloh replika zachovává pouze nejnovější stav virtuálního počítače. Replika zabírá místo v datovém úložišti, zatímco záloha může být uchovávána v levnějším úložišti.

Spouštění repliky je však mnohem rychlejší, než obnova a spouštění virtuálního počítače ze zálohy. Zapnutá replika pracuje rychleji než virtuální počítač spuštěný ze zálohy a nenačítá agenta pro VMware.

Příklady použití

- **Replikace virtuálního počítače na vzdáleném serveru.**

  Replikace vám umožní odolávat částečným nebo úplným selháním datového centra pomocí klonování virtuálních počítačů z primárního serveru na sekundární server. Sekundární soubor se obvykle nachází na vzdáleném místě, u nějž je nepravděpodobné, že by byl ovlivněn faktory prostředí, infrastruktury a dalšími faktory, které mohly způsobit selhání primárního serveru.
- **Replikace virtuálního počítače v rámci jednoho serveru (z jednoho hostitele/datového úložiště do jiného).**

  Replikaci v rámci jednoho serveru je možné použít u scénářů vysoké dostupnosti a obnovy po havárii.

Jaké činnosti je možné provést s replikou

- **Testování repliky** (str. 168)

  Replika bude zapnuta k otestování. Pomocí aplikace vSphere Client nebo jiných nástrojů zkontrolujte, zda replika pracuje správně. Replikace je během procesu testování pozastavena.
- **Převzetí služeb při selhání replikou** (str. 169)

  Převzetí služeb při selhání je převod pracovního zatížení z původního virtuálního počítače na jeho repliku. Replikace je během procesu převzetí služeb při selhání pozastavena.
- **Zálohování repliky**

  Jak zálohování, tak replikace vyžadují přístup k virtuálním diskům a proto ovlivňují výkon hostitele, na kterém běží virtuální počítač. Pokud chcete mít repliku i zálohy virtuálního počítače, ale nechcete dále zvyšovat zátěž produkčního hostitele, replikujte počítač na jiného hostitele a nastavte zálohy repliky.

Omezení

Následující typy virtuálních počítačů není možné replikovat:

- Počítače odolné vůči chybám běžící na ESXi 5.5 a nižší.
- Počítače běžící se záloh.
- Repliky virtuálních počítačů

19.2.1 Tvorba plánu replikace

Plány replikace je nutné vytvářet pro každý počítač jednotlivě. Již existující plán není možné použít pro jiné počítače.

Jak vytvořit plán replikace

1. Vyberte virtuální počítač, který chcete replikovat.

2. Klikněte na možnost **Replikace**.

   Software zobrazí šablonu nového plánu replikace.
3. [Volitelné] Pokud chcete upravit název plánu replikace, klikněte na výchozí název.
4. Klikněte na možnost **Cílový počítač** a proveďte toto:
   a. Vyberte, zda chcete vytvořit novou repliku nebo použít existující repliku původního počítače.
   b. Vyberte hostitele ESXi a zadejte název nové repliky nebo vyberte existující.

      Výchozí název nové repliky je **[název původního počítače]_replica**.
   c. Klikněte na tlačítko **OK**.
5. [Pouze při replikaci na nový počítač] Klikněte na možnost **Datové úložiště** a vyberte datové úložiště pro virtuální počítač.
6. [Volitelné] Klikněte na možnost **Plán** a změňte plán replikace.

   Ve výchozím nastavení se replikace provádí denně (od pondělí do pátku). Čas spuštění replikace si můžete vybrat.

   Pokud chcete změnit frekvenci replikací, posuňte posuvník a zadejte plán.

   Můžete také provést toto:
   - Nastavte období, pro které plán platí. Zaškrtněte políčko **Spustit plán v časovém rozsahu** a zadejte období.
   - Vypněte použití plánu. V tomto případě je možné replikaci spustit ručně.
7. [Volitelné] Klikněte na ikonu ozubeného kola a upravte možnosti replikace (str. 170).
8. Klikněte na tlačítko **Použít**.
9. [Volitelné] Chcete-li plán spustit ručně, klikněte na panelu plánu na tlačítko **Spustit**.

Po spuštění plánu replikace se replika virtuálního počítače zobrazí v seznamu **Všechna zařízení** s touto ikonou: 

19.2.2 Testování repliky

Jak připravit repliku pro testování

1. Vyberte repliku, kterou chcete testovat.
2. Klikněte na možnost **Testovat repliku**.
3. Klikněte na možnost **Spustit testování**.
4. Vyberte, zda se má zapnutá replika připojit k síti. Ve výchozím nastavení nebude replika připojena k síti.
5. [Volitelné] Pokud chcete připojit repliku k síti, zaškrtněte políčko **Zastavit původní virtuální počítač**, aby se původní počítač před zapnutím repliky vypnul.
6. Klikněte na možnost **Spustit**.

Jak zastavit testování repliky

1. Vyberte repliku, jejíž testování probíhá.
2. Klikněte na možnost **Testovat repliku**.
3. Klikněte na možnost **Zastavit testování**.
4. Potvrďte své rozhodnutí.

19.2.3 Převzetí služeb při selhání replikou

Jak převzít služby počítače při selhání replikou

1. Vyberte repliku, která má služby převzít.
2. Klikněte na možnost **Akce repliky**.
3. Klikněte na možnost **Podpora převzetí služeb při selhání**.
4. Vyberte, zda se má zapnutá replika připojit k síti. Ve výchozím nastavení bude replika připojena ke stejné síti jako původní počítač.
5. [Volitelné] Pokud chcete repliku připojit k síti, zrušte zaškrtnutí políčka **Zastavit původní virtuální počítač**, aby původní počítač zůstal online.
6. Klikněte na možnost **Spustit**.

Když je replika ve stavu převzetí služeb, můžete si vybrat jednu z následujících akcí:

- **Zastavit převzetí služeb při selhání** (str. 169)

  Zastaví převzetí služeb, pokud bude původní počítač opraven. Replika se vypne. Replikace bude obnovena.
- **Trvalé převzetí služeb replikou** (str. 169)

  Tato okamžitá operace odstraní z virtuálního počítače označení repliky; replikace na něj tedy již nebude možná. Pokud chcete obnovit replikaci, upravte plán replikace a vyberte tento počítač jako zdroj.
- **Navrácení služeb po obnovení** (str. 169)

  Provede navrácení služeb po obnovení, pokud došlo k převzetí služeb počítačem, který není určen pro nepřetržitý provoz. Replika bude obnovena na původní nebo nový virtuální počítač. Až bude obnova na původní počítač dokončena, počítač se zapne a replikace se obnoví. Pokud vyberete obnovu na nový počítač, upravte plán replikace a vyberte tento počítač jako zdroj.

19.2.3.1 Zastavení převzetí služeb při selhání

Jak zastavit převzetí služeb při selhání

1. Vyberte repliku, která je ve stavu převzetí služeb při selhání.
2. Klikněte na možnost **Akce repliky**.
3. Klikněte na možnost **Zastavit převzetí služeb při selhání**.
4. Potvrďte své rozhodnutí.

19.2.3.2 Provedení trvalého převzetí služeb při selhání

Jak provést trvalé převzetí služeb při selhání

1. Vyberte repliku, která je ve stavu převzetí služeb při selhání.
2. Klikněte na možnost **Akce repliky**.
3. Klikněte na možnost **Trvalé převzetí služeb při selhání**.
4. [Volitelné] Změňte název virtuálního počítače.
5. [Volitelné] Zaškrtněte políčko **Zastavit původní virtuální počítač**.
6. Klikněte na možnost **Spustit**.

19.2.3.3 Navrácení služeb po obnovení

Jak provést navrácení služeb po obnovení z repliky

1. Vyberte repliku, která je ve stavu převzetí služeb při selhání.

2. Klikněte na možnost **Akce repliky**.
3. Klikněte na možnost **Navrácení služeb po obnovení z repliky**.
   Software automaticky vybere původní počítač jako cílový.
4. [Volitelné] Klikněte na možnost **Cílový počítač** a proveďte toto:
   a. Vyberte, zda se navrácení služeb provede na nový nebo existující počítač.
   b. Vyberte hostitele ESXi a zadejte název nového počítače nebo vyberte existující.
   c. Klikněte na tlačítko **OK**.
5. [Volitelné] Při navrácení služeb na nový počítač můžete udělat i toto:
   - Klikněte na možnost **Datové úložiště** a vyberte datové úložiště pro virtuální počítač.
   - Pomocí možnosti **Nastavení virtuálního počítače** změňte velikost paměti, počet procesorů a síťová připojení virtuálního počítače.
6. [Volitelné] Klikněte na možnost **Možnosti obnovy** a upravte možnosti navrácení služeb (str. 170).
7. Klikněte na možnost **Spustit obnovu**.
8. Potvrďte své rozhodnutí.

19.2.4 Možnosti replikace

Chcete-li upravit možnosti replikace, klikněte na ikonu ozubeného kola vedle názvu plánu replikace a poté klikněte na možnost **Možnosti replikace**.

Sledování změněných bloků (CBT)

Tato možnost je podobná jako možnost zálohování Sledování změněných bloků (CBT) (str. 61).

Poskytování disku

Tato možnost definuje nastavení poskytování disku u repliky.

Výchozí nastavení: **Tenké poskytování**.

Jsou k dispozici následující hodnoty: **Tenké poskytování**, **Tlusté poskytování**, **Ponechat původní nastavení**.

Zpracování chyb

Tato možnost je podobná možnosti zálohování Zpracování chyb (str. 62).

Příkazy před-po

Tato možnost je podobná možnosti zálohování Příkazy před-po (str. 68).

Služba VSS pro virtuální počítače

Tato možnost je podobná možnosti zálohování Služba VSS pro virtuální počítače (str. 73).

19.2.5 Možnosti navrácení služeb po obnovení

Možnosti navrácení služeb po obnovení změníte kliknutím na odkaz **Možnosti obnovy** při konfiguraci.

Zpracování chyb

Tato možnost je podobná jako možnost Zpracování chyb (str. 90) při obnově.

Výkon

Tato možnost je podobná jako možnost Výkon (str. 91) při obnově.

Příkazy před-po

Tato možnost je podobná jako možnost Příkazy před-po (str. 91) při obnově.

Správa napájení virtuálního počítače

Tato možnost je podobná jako možnost Správa napájení virtuálního počítače (str. 93) při obnově.

19.2.6 Naplnění počáteční repliky

Abyste urychlili replikaci do vzdáleného umístění a ušetřili šířku pásma sítě, můžete provést naplnění repliky.

Důležité *Aby bylo možné provést naplnění repliky, musí být na cílovém hostiteli ESXi spuštěný Agent pro VMware (Virtual Appliance).*

Postup naplnění počáteční repliky

1. Proveďte jeden z následujících úkonů:
   - Pokud lze původní virtuální počítač vypnout, vypněte ho a přejděte ke kroku 4.
   - Pokud původní virtuální počítač vypnout nejde, pokračujte dalším krokem.
2. Vytvoření plánu replikace (str. 167).

   Při vytváření plánu vyberte v části **Cílový počítač** možnost **Nová replika** a hostitele ESXi původního počítače.
3. Plán jednou spusťte.

   V původním hostiteli ESXi se vytvoří replika.
4. Vyexportujte soubory virtuálního počítače (nebo repliky) na externí pevný disk.
   a. Připojte externí pevný disk k počítači se spuštěným klientem vSphere.
   b. Připojte klienta vSphere k původnímu serveru vCenter nebo hostiteli ESXi.
   c. Vyberte nově vytvořenou repliku v inventáři.
   d. Klikněte na **Soubor** > **Exportovat** > **Exportovat šablonu OVF**.
   e. V poli **Adresář** zadejte složku na externím pevném disku.
   f. Klikněte na tlačítko **OK**.
5. Přeneste pevný disk do vzdáleného umístění.
6. Naimportujte repliku do cílového hostitele ESXi.
   a. Připojte externí pevný disk k počítači se spuštěným klientem vSphere.
   b. Připojte klienta vSphere k cílovému serveru vCenter nebo hostiteli ESXi.
   c. Klikněte na **Soubor** > **Nasadit šablonu OVF**.
   d. V poli **Nasadit ze souboru nebo URL** zadejte šablonu, kterou jste exportovali v kroku 4.
   e. Dokončete proces importu.
7. Upravte plán replikace vytvořený v kroku 2. V poli **Cílový počítač** vyberte možnost **Existující replika** a poté vyberte naimportovanou repliku.

Software bude poté pokračovat v aktualizaci repliky. Všechny replikace budou přírůstkové.

19.3 Správa prostředí pro virtualizaci

Prostředí vSphere, Hyper-V a Virtuozzo si můžete prohlédnout v nativním zobrazení. Po instalaci a registraci odpovídajícího klienta se karta **VMware**, **Hyper-V** nebo **Virtuozzo** zobrazí v části **Zařízení**.

Karta **VMware** umožňuje změnu přístupových pověření pro server vCenter nebo samostatného hostitele ESXi bez nutnosti opakované instalace klienta.

Jak změnit přístupová pověření serveru vCenter nebo hostitele ESXi

1. V části **Zařízení** klikněte na možnost **VMware**.
2. Klikněte na možnost **Hostitelské počítače a clustery**.
3. V seznamu **Hostitelské počítače a clustery** (vpravo od stromu **Hostitelské počítače a clustery**), vyberte server vCenter nebo samostatného hostitele ESXi, kterého jste určili při instalaci Agenta pro VMware.
4. Klikněte na možnost **Přehled**.
5. V části **Pověření** klikněte na uživatelské jméno.
6. Zadejte nová přístupová pověření a klikněte na tlačítko **OK**.

19.4 Migrace počítače

Migraci počítače je možné provést pomocí obnovy jeho zálohy na jiný počítač než původní.

Následující tabulka shrnuje dostupné možnosti migrace.

Typ zálohovaného počítače	Dostupná umístění obnovy				
	Fyzický počítač	Virtuální počítač ESXi	Virtuální počítač Hyper-V	Virtuální počítač Virtuozzo	Kontejner Virtuozzo
Fyzický počítač	+	+	+	-	-
Virtuální počítač VMware ESXi	+	+	+	-	-
Virtuální počítač Hyper-V	+	+	+	-	-
Virtuální počítač Virtuozzo	+	+	+	+	-
Kontejner Virtuozzo	-	-	-	-	+

Pokyny k provedení migrace naleznete v následujících tématech:

- Migrace z fyzického počítače na virtuální (P2V) - "Fyzikální počítač na virtuální" (str. 77)
- Migrace z virtuálního počítače na virtuální (V2V) - "Virtuální počítač" (str. 78)
- Migrace z virtuálního počítače na fyzický (V2P) - "Virtuální počítač" (str. 78) nebo "Obnova disků pomocí spouštěcího média" (str. 80)

Přestože je možné provést migraci V2P ve webovém rozhraní, doporučujeme ve specifických případech použití spouštěcího média. Někdy je užitečné použít médium u migrací na ESXi nebo Hyper-V.

Médium vám umožní provést následující úkony:

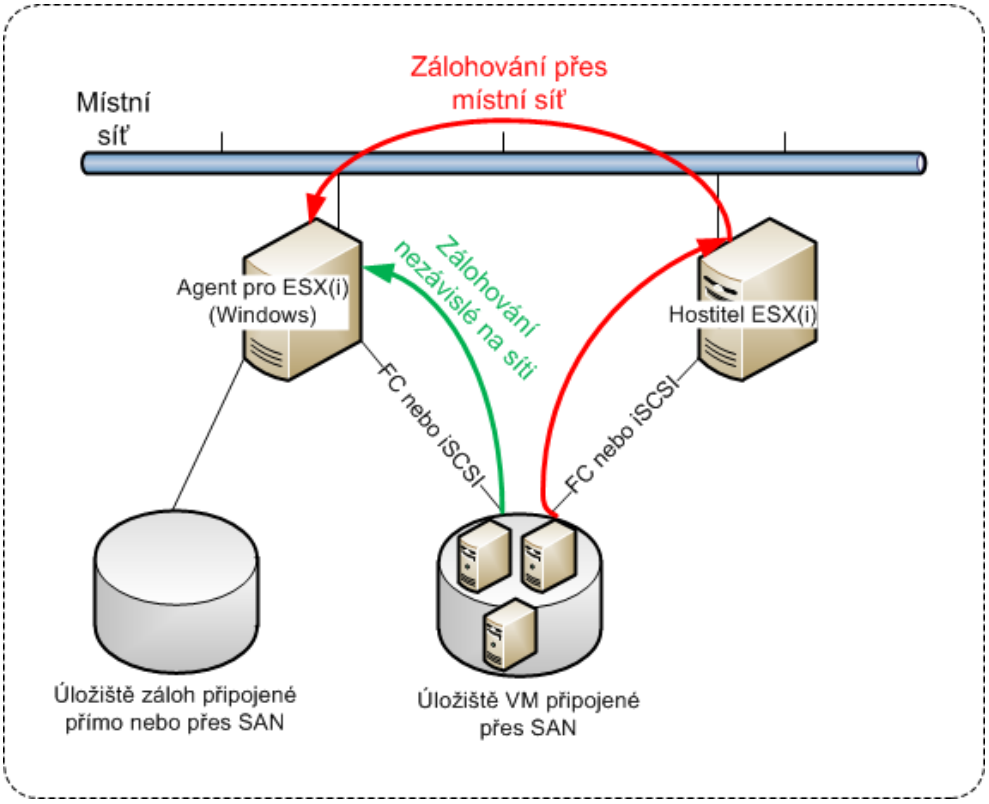
- Vybrat jednotlivé disky nebo svazky k obnově.

- Ručně mapovat disky ze zálohy na disky cílového počítače.
- Provést migraci P2V, migraci V2P nebo migraci V2V z Virtuozzo, počítače se systémem Linux obsahujícím logické svazky (LVM). Použít Agenta pro Linux k vytvoření zálohy a spouštěcího média pro obnovení.
- Zprostředkovat ovladače pro určitý hardware, který je důležitý pro spouštění systému.

19.5 Agent pro VMware – zálohování nezávislé na LAN

Pokud ESXi používá úložiště připojené pomocí sítě SAN, nainstalujte agenta do počítače připojeného ke stejné síti SAN. Agent bude zálohovat virtuální počítače přímo z úložiště a ne pomocí hostitele ESXi a LAN. Tato funkce se nazývá zálohování nezávislé na LAN.

Na následujícím obrázku je zálohování založené na LAN a zálohování bez LAN. Přístup na virtuální počítače bez LAN je dostupný, pokud máte síť SAN se standardem Fibre Channel nebo iSCSI. Chcete-li zcela odstranit přenos zálohovaných dat prostřednictvím LAN, uložte zálohy na místní disk počítače agenta nebo na úložiště připojené pomocí SAN.



Jak agentovi povolit přímý přístup k datovému úložišti

1. Nainstalujte Agenta pro VMware do počítače se systémem Windows, který má síťový přístup k serveru vCenter.
2. Připojte k počítači číslo logické jednotky (LUN), které hostí datové úložiště. Zvažte následující:
   - Použijte stejný protokol, (tj. iSCSI nebo FC), který je použitý pro připojení datového úložiště k ESXi.
   - LUN *nesmí* být inicializováno a ve **Správci disků** se musí zobrazit jako vypnutý (offline) disk. Pokud systém Windows inicializuje LUN, může se poškodit a stát se pro VMware vSphere nečitelným.

Agent tak pro přístup k virtuálním diskům použije transportní režim SAN, tj. přečte sektory LUN prostřednictvím protokolu iSCSI/FC bez rozpoznání systému souborů VMFS (na což systém Windows není upozorněn).

Omezení

- V systému vSphere 6.0 a novějším agent nemůže použít transportní režim SAN, pokud některé disky virtuálního počítače jsou umístěny na virtuálním svazku VMware (VVol) a jiné nikoli. Zálohování takových virtuálních počítačů se nezdaří.
- Šifrované virtuální počítače, zavedené ve verzi VMware vSphere 6.5, budou zálohovány prostřednictvím sítě LAN, a to i v případě, že pro agenta nakonfigurujete transportní režim SAN. Agent se vrátí do transportního režimu NBD, protože VMware nepodporuje transportní režim SAN k zálohování šifrovaných virtuálních disků.

Příklad

Používáte-li úložiště iSCSI SAN, nakonfigurujte spouštěč iSCSI na počítači se systémem Windows, na kterém je nainstalován Agent pro VMware.

Postup konfigurace zásad SAN

1. Přihlaste se jako správce, otevřete příkazový řádek, zadejte **`diskpart`** a poté stiskněte klávesu **Enter**.
2. Zadejte **`san`** a poté stiskněte klávesu **Enter**. Ověřte, že se zobrazí následující údaje: **SAN Policy : Offline All**.
3. Pokud je pro zásady SAN nastavena jiná hodnota:
   a. Zadejte příkaz **`san policy=offlineall`**.
   b. Stiskněte klávesu **Enter**.
   c. Chcete-li ověřit, zda bylo nastavení správně uloženo, proveďte znovu druhý krok.
   d. Restartujte počítač.

Postup konfigurace spouštěče iSCSI

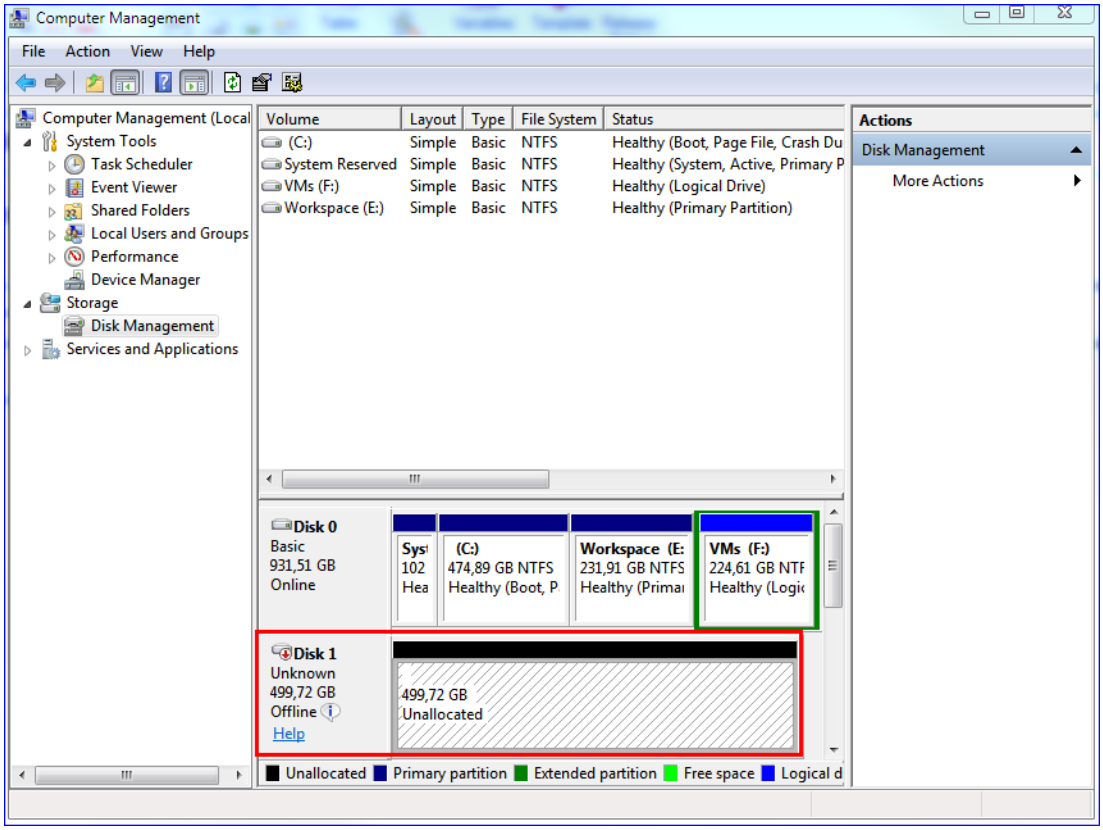
1. Přejděte na **Ovládací panely** > **Nástroje pro správu** > **Iniciátor iSCSI**.

   ***Tip**: Pokud applet **Nástroje pro správu** nevidíte, bude pravděpodobně potřeba použít jiné zobrazení **Ovládacích panelů** než **Domů** nebo **Kategorie**, případně použijte hledání.*

2. Pokud Iniciátor iSCSI společnosti Microsoft spouštíte poprvé, potvrďte, že chcete spustit Službu iniciátoru iSCSI společnosti Microsoft.
3. Na kartě **Cíle** zadejte plně kvalifikovaný název domény nebo IP adresu zařízení SAN a poté klikněte na tlačítko **Rychlé připojení**.
4. Vyberte LUN, které hostí datové úložiště, a klikněte na tlačítko **Připojit**.

   Není-li zobrazeno žádné LUN, přesvědčte se, zda nastavení zón na cíli iSCSI povolujte počítačům se spuštěnými agenty přístup k LUN. Příslušný počítač musí být na cíli přidán k povoleným spouštěčům iSCSI.
5. Klikněte na tlačítko **OK**.

Připravené zařízení SAN LUN by se mělo objevit v okně **Správa disků**, jak je zobrazeno na snímku obrazovky níže.



19.6 Agent pro VMware – potřebná oprávnění

Aby mohl Agent pro VMware provádět operace na všech hostitelích a clusterech spravovaných přes vCenter Server, potřebuje mít na vCenter Serveru příslušná oprávnění. Chcete-li agentovi povolit provádění operací jen na konkrétním hostiteli ESXi, přiřaďte mu stejná oprávnění na tomto hostiteli.

Účet s potřebnými oprávněními můžete určit během instalace nebo konfigurace Agenta pro VMware. Budete-li účet chtít později změnit, přečtěte si část Správa virtualizačních prostředí (str. 172).

		Operace			
Objekt	**Oprávnění**	**Zálohování virtuálního počítače**	**Obnovení do nového virtuálního počítače**	**Obnovení do existujícího virtuálního počítače**	**Spuštění VM ze zálohy**
Kryptografické operace (počínaje vSphere 6.5)	**Přidání disku**	+*			
	Přímý přístup	+*			
Datové úložiště	**Přidělit prostor**		+	+	+
	Procházet datové úložiště				+

		Operace			
Objekt	**Oprávnění**	**Zálohování virtuálního počítače**	**Obnovení do nového virtuálního počítače**	**Obnovení do existujícího virtuálního počítače**	**Spuštění VM ze zálohy**
	Konfigurovat datové úložiště	+	+	+	+
	Operace se soubory na nízké úrovni				+
Globální	**Licence**	+	+	+	+
	Zakázat metody	+	+	+	
	Povolit metody	+	+	+	
Konfigurace > hostitele	**Konfigurace oddílu úložiště**				+
Místní operace > hostitele	**Vytvořit virtuální počítač**				+
	Odstranit virtuální počítač				+
	Změnit konfiguraci virtuálního počítače				+
Síť	**Přiřadit síť**		+	+	+
Zdroj	**Přiřadit virtuální počítač k fondu zdrojů**		+	+	+
Konfigurace > virtuálního počítače	**Přidat existující disk**	+	+		+
	Přidat nový disk		+	+	+
	Přidat nebo odebrat zařízení		+		+
	Pokročilé	+	+	+	
	Změnit počet CPU		+		
	Sledován změn disku	+		+	
	Zapůjčení disku	+		+	
	Paměť		+		
	Odebrat disk	+	+	+	+
	Přejmenovat		+		
	Nastavit poznámku				+
	Nastavení		+	+	+
Hostované operace >virtuálního počítače	**Spuštění programu hostovaných operací**	+**			

		Operace			
Objekt	**Oprávnění**	**Zálohování virtuálního počítače**	**Obnovení do nového virtuálního počítače**	**Obnovení do existujícího virtuálního počítače**	**Spuštění VM ze zálohy**
	Dotazování hostovaných operací	+**			
	Změny hostovaných operací	+**			
Interakce > **virtuálního počítače**	**Získat kontrolní lístek pro hosty** (vSphere 4.1 a 5.0)				+
	Konfigurovat disky CD		+	+	
	Správa hostovaného operačního systému prostřednictvím rozhraní API VIX (vSphere 5.1 a novější)				+
	Vypnout			+	+
	Zapnout		+	+	+
Inventář > **virtuálního počítače**	**Vytvořit z existujícího**		+	+	+
	Vytvořit nový		+	+	+
	Registrovat				+
	Odebrat		+	+	+
	Zrušit registraci				+
Poskytování > **virtuálního počítače**	**Povolit přístup k disku**		+	+	+
	Povolit přístup k disku v režimu jen pro čtení	+		+	
	Povolit stažení virtuálního počítače	+	+	+	+
Stav > **virtuálního počítače**	**Vytvořit snímek**	+		+	+
	Odebrat snímek	+		+	+
Virtuální zařízení vApp	**Přidat virtuální počítač**				+

* Toto oprávnění je vyžadováno pouze pro zálohování šifrovaných počítačů.

** Toto oprávnění je vyžadováno pouze pro zálohování s podporou aplikací.

19.7 Virtuální počítače Windows Azure a Amazon EC2

Abyste mohli zálohovat virtuální počítače Windows Azure nebo Amazon EC2, nainstalujte si na ně agenta pro zálohování. Operace zálohování a obnovy jsou stejné jako u fyzického počítače. Když ale budete nastavovat limit počtu počítačů, bude tento počítač stále považován za virtuální.

Rozdíl od fyzického počítače spočívá v tom, že virtuální počítače Windows Azure a Amazon EC2 se nedají spustit ze spouštěcích médií. Potřebujete-li obnovit virtuální počítač Windows Azure nebo Amazon EC2, řiďte se následujícím postupem.

Obnovení počítače jako virtuálního počítače Windows Azure nebo Amazon EC2

1. Vytvořte nový virtuální počítač z obrazu nebo šablony uložené ve Windows Azure nebo Amazon EC2. Nový počítač musí mít stejnou konfiguraci disku jako počítač, který chcete obnovit.
2. Na nový počítač nainstalujte aplikaci Agent pro Windows nebo Agent pro Linux.
3. Obnovte zálohovaný počítač podle postupu popsaného v části Fyzický počítač (str. 76). Při konfiguraci obnovy vyberte jako cílový počítač právě tento nový počítač.

19.8 Omezení celkového počtu současně zálohovaných virtuálních počítačů

Možnost zálohování **Plánování** (str. 71) určuje, kolik virtuálních počítačů může agent zálohovat současně při provádění daného plánu zálohování.

Pokud se více plánů zálohování překrývá v čase, sčítají se čísla uvedená v jejich možnostech zálohování. Přestože je výsledné celkové číslo programově omezeno na 10, překrývající se plány mohou ovlivnit výkon zálohování a přetížit hostitele i úložiště virtuálního počítače.

Můžete proto dále omezit celkový počet virtuálních počítačů, které může agent pro VMware nebo agent pro Hyper-V současně zálohovat.

Omezení celkového počtu virtuálních počítačů, které může agent pro VMware (Windows) nebo agent pro Hyper-V zálohovat

1. V počítači, ve kterém je spuštěný agent, vytvořte nový textový dokument a otevřete jej v textovém editoru, jako je Poznámkový blok.
2. Zkopírujte a vložte do souboru následující řádky:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Nahraďte hodnotu `00000001` hexadecimální hodnotou omezení, které chcete nastavit. Například `00000001` je 1 a `0000000A` je 10.
4. Uložte soubor pod názvem **limit.reg**.
5. Spusťte soubor jako správce.
6. Potvrďte, že chcete upravit registr systému Windows.
7. Restartujte agenta následujícím postupem:
   a. V nabídce **Start** klikněte na příkaz **Spustit** a zadejte **cmd**.
   b. Klikněte na tlačítko **OK**.
   c. Spusťte následující příkazy:

```
net stop mms
net start mms
```

Pokud chcete omezit celkový počet virtuálních počítačů, které může Agent pro VMware (virtuální zařízení) zálohovat.

1. Pokud chcete spustit příkazové prostředí, stiskněte v uživatelském rozhraní virtuálního zařízení klávesy CTRL+SHIFT+F2.
2. Otevřete soubor **/etc/Acronis/MMS.config** v textovém editoru, jako je **vi**.
3. Vyhledejte následující oddíl:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Nahraďte hodnotu `10` desítkovou hodnotou omezení, které chcete nastavit.
5. Uložte soubor.
6. Spusťte příkaz **`reboot`**, kterým restartujete agenta.

20 Správa uživatelských účtů a organizačních jednotek

Správa uživatelských účtů a organizačních jednotek je k dispozici na portálu pro správu. Pokud chcete získat přístup k portálu pro správu, klikněte při přihlašování k zálohovací službě na **Portál pro správu** nebo klikněte  na ikonu v pravém horním rohu a pak klikněte na **Portál pro správu**. Na tento portál mají přístup pouze uživatelé s oprávněním správce.

Informace o správě uživatelských účtů a organizačních jednotek získáte v Příručce správce portálu pro správu. Dokument zpřístupníte kliknutím na ikonu otazníku na portálu pro správu.

Tento oddíl poskytuje další informace související se správou služby zálohování.

20.1 Kvóty

Kvóty vám umožňují omezit, jak uživatelé používají danou službu. Kvóty nastavíte tak, že vyberete uživatele na kartě **Uživatelé** a potom kliknete na ikonu tužky v oddílu **Kvóty**.

Pokud je kvóta překročena, odešle se upozornění na e-mailovou adresu uživatele. Pokud nenastavíte překročení kvóty, bude kvóta považována za měkkou. To znamená, že se neuplatní omezení na používání služby zálohování.

Je také možné určit překročení kvóty. Limit překročení umožňuje uživateli kvótu o zadanou hodnotu překročit. Po překročení této hodnoty jsou použita omezení pro využívání dané služby zálohování.

Poskytovatelé spravovaných služeb mohou také podobným způsobem určit kvóty svým zákaznickým společnostem.

20.1.1 Zálohování

Můžete zadat kvótu cloudového úložiště, kvótu pro místní zálohy a maximální počet počítačů, zařízení, nebo webových stránek, které může uživatel chránit. Jsou k dispozici následující kvóty.

Kvóty na zařízení

- **Pracovní stanice**
- **Servery**
- **Virtuální počítače**
- **Mobilní zařízení**
- **Webhostingové servery**
- **Webové stránky**

Počítač, zařízení nebo web se považují za chráněné, pokud používají aspoň jeden plán zálohování. Mobilní zařízení je chráněno po provedení první zálohy.

Pokud dojde k překročení u několika zařízení, nebude uživatel moci použít plán zálohování u více zařízení.

Kvóty na cloudové zdroje dat

- **Licence Office 365**

  Tuto kvótu použije poskytovatel služby na celou společnost. Společnost může chránit soubory v **poštovních schránkách**, **soubory na OneDrivu** nebo oboje. Správci společnosti si mohou tuto kvótu a její využití prohlédnout na portálu pro správu, ale nemohou ji nastavit uživateli.

- **Office 365 SharePoint Online**

  Tuto kvótu použije poskytovatel služby na celou společnost. Tato kvóta zapíná nebo vypíná možnost ochrany webů SharePoint Online. Pokud je tato kvóta povolena, může být chráněn jakýkoli počet webů SharePoint Online. Správci společnosti si nemohou tuto kvótu prohlédnout na portálu pro správu, ale mohou ve zprávě o využití zobrazit velikost úložiště obsazenou zálohami SharePoint Online.

- **Počet licencí G Suite**

  Tuto kvótu použije poskytovatel služby na celou společnost. Společnost může chránit soubory v poštovních schránkách **Gmail** (včetně kalendáře a kontaktů), soubory **OneDrive** nebo oboje. Správci společnosti si mohou tuto kvótu a její využití prohlédnout na portálu pro správu, ale nemohou ji nastavit uživateli.

- **Týmové disky G Suite**

  Tuto kvótu použije poskytovatel služby na celou společnost. Tato kvóta zapíná nebo vypíná možnost ochrany Týmových disků G Suite. Pokud je tato kvóta povolena, může být chráněn jakýkoli počet Týmových disků. Správci společnosti si nemohou tuto kvótu prohlédnout na portálu pro správu, ale mohou ve zprávě o využití zobrazit velikost úložiště obsazenou zálohami SharePoint Online.

Licence Office 365 se považuje za chráněnou, pokud poštovní schránka uživatele nebo jeho OneDrive používají aspoň jeden plán zálohování. Licence G Suite se považuje za chráněnou, pokud poštovní schránka uživatele nebo jeho Disk Google používají aspoň jeden plán zálohování.

Pokud dojde k překročení u několika licencí, nebude správce společnosti moci použít plán zálohování u více licencí.

Kvóta na úložiště

- **Místní záloha**

  Kvóty na **místní zálohy** omezují celkovou velikost místních záloh vytvořených pomocí cloudové infrastruktury. Pro tuto kvótu nelze nastavit limit překročení.

- **Cloudové zdroje**

Kvóta na **Cloudové zdroje** se skládá z kvóty na úložiště záloh a kvót na obnovení po havárii. Kvóta na úložiště záloh omezuje celkovou velikost záloh umístěných v cloudovém úložišti. Při překročení kvóty na úložiště záloh se nezdaří zálohování.

20.1.2 Obnovení po havárii

Tyto kvóty používá poskytovatel služeb v rámci celé společnosti. Správce společnosti může tyto kvóty a využití zobrazit v portálu pro správu, ale nemůže nastavit kvóty pro uživatele.

- **Úložiště obnovení po havárii**

  Toto úložiště používají primární servery a servery pro obnovení. V případě dosažení limitu této kvóty není možné vytvořit primární servery a servery pro obnovení nebo přidat/rozšířit disky existujících primárních serverů. V případě překročení limitu této kvóty není možné zahájit převzetí služeb při selhání ani jen spustit zastavený server. Spuštěné servery zůstanou v činnosti.

  V případě vypnutí kvóty se všechny servery odstraní. Karta **Cloudový server pro obnovení** zmizí z konzoly pro zálohování.

- **Výpočetní body**

  Tato kvóta omezuje prostředky procesoru a paměti RAM využívané primárními servery a servery pro obnovení v průběhu zúčtovacího období. V případě dosažení limitu této kvóty se všechny primární servery a servery pro obnovení vypnou. Tyto servery nebude možné používat až do začátku příštího zúčtovacího období. Výchozí zúčtovací období je jeden celý kalendářní měsíc.

  Pokud je kvóta vypnutá, nelze servery používat, a to bez ohledu na zúčtovací období.

- **Veřejné IP adresy**

  Tato kvóta omezuje počet veřejných IP adres, které lze přiřadit primárním serverům a serverům pro obnovení. V případě dosažení limitu této kvóty nebude možné povolit veřejné IP adresy pro další servery. Použití veřejné IP adresy můžete u serveru vypnout zrušením zaškrtnutí políčka **Veřejná IP adresa** v nastavení serveru. Potom můžete povolit použití veřejné IP adresy na jiném serveru, která většinou nebude stejná.

  Pokud je kvóta vypnutá, přestanou všechny servery používat veřejné IP adresy, a nebudou tak dostupné z internetu.

- **Cloudové servery**

  Tato kvóta omezuje celkový počet primárních serverů a serverů pro obnovení. V případě dosažení limitu této kvóty není možné vytvořit primární servery ani servery pro obnovení.

  Je-li kvóta vypnutá, budou servery viditelné v konzole pro zálohování, ale jediná dostupná operace bude **Odstranit**.

- **Přístup k internetu**

  Tato kvóta zapíná nebo vypíná přístup k internetu z primárních serverů a serverů pro obnovení.

  V případě vypnutí kvóty se primární servery a servery pro obnovení ihned odpojí od internetu. Přepínač **Přístup k internetu** ve vlastnostech serveru nebude vybraný a bude neaktivní.

20.2 Upozornění

Chcete-li změnit nastavení upozornění pro některého uživatele, vyberte daného uživatele na kartě **Uživatelé** a potom klikněte na ikonu tužky v oddílu **Nastavení**. K dispozici jsou následující nastavení upozornění:

- **Upozornění na překročení kvót** (ve výchozím nastavení zapnuté)

  Upozornění na překročené kvóty.

- **Naplánované zprávy o využití**

Zprávy o využití, které jsou popsané níže, se odesílají první den každého měsíce.

- **Upozornění na chyby**, **Upozornění** a **Upozornění na úspěšné dokončení** (ve výchozím nastavení vypnuté)

  Oznámení o výsledcích spuštění plánů zálohování a výsledcích operací obnovení po havárii u každého zařízení.

- **Denní shrnutí aktivních výstrah** (ve výchozím nastavení zapnuto)

  Toto shrnutí informuje o nezdařených zálohách, vynechaných zálohách a dalších potížích. Shrnutí je odesláno v 10:00 (čas datového centra). Pokud to této chvíle nenastaly žádné potíže, shrnutí se neodešle.

Všechna upozornění se odesílají na e-mailovou adresu uživatele.

20.3 Zprávy o využití

Zpráva o využití služby zálohování obsahuje následující data o společnosti nebo jednotce:

- Velikost záloh podle jednotky, uživatele a typu zařízení.
- Počet chráněných zařízení podle jednotky, uživatele a typu zařízení.
- Cena podle jednotky, uživatele a typu zařízení.
- Celková velikost záloh.
- Celkový počet chráněných zařízení.
- Celková cena.

21 Odstraňování problémů

Tato část popisuje, jak uložit protokol agenta do souboru .zip. Pokud zálohování selže z nejasného důvodu, tento soubor pomůže personálu technické podpory identifikovat problém.

Jak shromáždit protokoly

1. Vyberte počítač, ze kterého chcete shromáždit protokoly.
2. Klikněte na možnost **Aktivity**.
3. Klikněte na možnost **Shromáždit informace o systému**.
4. Určete umístění, kam se má soubor uložit, pokud k tomu budete webovým prohlížečem vyzváni.

22 Slovníček

J

Jednosouborový formát zálohy

Jedná se o nový formát zálohy, ve kterém se počáteční plná a následující přírůstkové zálohy uloží do jednoho souboru .tib nebo .tibx, namísto řetězce souborů. Tento formát využívá rychlosti přírůstkové metody zálohování a vyhýbá se tak své hlavní nevýhodě – obtížnému odstraňování neaktuálních záloh. Software označí bloky použité neaktuálními zálohami jako „volné“ a nové zálohy poté zapisuje do těchto bloků. Výsledkem je velmi rychlé vyčištění s minimální spotřebou zdrojů.

Jednosouborový formát zálohy není dostupný při zálohování do umístění, které é nepodporují čtení a zápis s náhodným přístupem.

P

Plná záloha

Je to samostatná záloha obsahující veškerá data vybraná k zálohování. Pokud chcete obnovit data z plné zálohy, není nutné mít přístup k jiným zálohám.

Přírůstková záloha

Je to záloha, která ukládá změny dat vzhledem k poslední záloze. Pokud chcete obnovit data z přírůstkové zálohy, potřebujete přístup k ostatním zálohám.

R

Rozdílová záloha

Rozdílová záloha ukládá změnu dat vzhledem k poslední plné záloze (str. 183). Pro obnovu dat z rozdílové zálohy potřebujete přístup k odpovídající plné záloze.

S

Sada záloh

Skupina záloh, na kterou je možné použít jednotlivá pravidla zachování.

U schématu zálohování **Vlastní** sady záloh odpovídají metodám zálohování (**Plná**, **Rozdílová** a **Přírůstková**).

Ve všech ostatních případech jsou sady záloh **Měsíčně**, **Denně**, **Týdně** a **Po hodině**.

- Měsíční záloha se vytvoří jako první po začátku měsíce.
- Týdenní záloha se vytvoří jako první v den, který vyberete pomocí možnosti **Týdenní zálohování** (klikněte na ikonu ozubeného kola a poté na možnost **Možnosti zálohování** > **Týdenní zálohování**).

  Pokud se týdenní záloha vytvoří jako první po začátku měsíce, je tato záloha považována za měsíční. V takovém případě bude týdenní záloha vytvořena ve vybraný den příštího týdne.

- Denní záloha je první záloha vytvořená po začátku dne, pokud tato záloha nespadá do definice měsíční nebo týdenní zálohy.
- Hodinová záloha je první záloha vytvořená po začátku hodiny, pokud tato záloha nespadá do definice měsíční, týdenní nebo denní zálohy.