

# Acronis

acronis.cz

# Acronis Cyber Protect

## Home Office



# Obsah

<b>1 Úvod</b>	<b>10</b>
1.1 Co je Acronis Cyber Protect Home Office?	10
1.2 Zálohy vytvořené v aplikaci Acronis True Image (2020 či 2021) a Acronis Cyber Protect Home Office	10
1.2.1 Pojmenování souboru zálohy	11
1.2.2 Schémata zálohování	11
1.2.3 Vyčištění záloh formátu TIBX	11
1.2.4 Ruční čištění místních záloh má následující schéma:	11
1.2.5 Které zálohy zachovávají formát TIB	11
1.3 Systémové požadavky a podporovaná média	12
1.3.1 Minimální systémové požadavky	12
1.3.2 Podporované operační systémy	12
1.3.3 Podporované systémy souborů	13
1.3.4 Podporované typy připojení k internetu	14
1.3.5 Podporovaná úložná média	14
1.4 Instalace a odebrání aplikace Acronis Cyber Protect Home Office	15
1.5 Aktivuje se Acronis Cyber Protect Home Office	16
1.5.1 Aktivuje se Acronis Cyber Protect Home Office	16
1.5.2 Problém Příliš mnoho aktivací	17
1.5.3 Ruční správa licencí předplatného	18
1.6 Informace ke zkušební verzi	18
1.6.1 Obecná omezení	18
1.6.2 Synchronizace	18
1.6.3 Acronis Cloud	18
1.6.4 Zakoupení plné verze	19
1.7 Upgrade aplikace Acronis Cyber Protect Home Office	19
1.7.1 Integrovaný obchod	20
1.8 Technická podpora	20
1.8.1 Program údržby a podpory	20
<b>2 Začínáme</b>	<b>21</b>
2.1 Jazyk uživatelského rozhraní	21
2.2 Ochrana systému	21
2.2.1 Zálohuje se počítač	21
2.2.2 Jak vytvořit spouštěcí médium Acronis	23
2.3 Zálohování všech dat v počítači	24

2.4 Vytvoření sady Acronis Survival Kit .....	25
2.5 Zálohování souborů .....	27
2.6 Klonování pevného disku .....	28
2.6.1 Proč tuto funkci potřebuji? .....	28
2.6.2 Před spuštěním .....	29
2.6.3 Klonování disku .....	29
2.7 Obnovení počítače .....	30
2.8 Účet Acronis .....	32
2.9 Začínáme s úložištěm Acronis Cloud .....	33
2.9.1 Vzdálené úložiště .....	33
2.9.2 Webová aplikace .....	34
2.9.3 Jak zajišťujeme bezpečnost vašich dat .....	34
2.9.4 Informace o předplatném .....	34
<b>3 Základní pojmy .....</b>	<b>36</b>
3.1 Rozdíl mezi zálohami souborů a obrazy disků nebo diskových oddílů .....	37
3.1.1 Co obsahuje záloha disku nebo diskového oddílu? .....	38
3.1.2 Co je vyloučeno ze záloh disku? .....	38
3.2 Plné, přírůstkové a rozdílové zálohy .....	39
3.2.1 Plná metoda .....	39
3.2.2 Přírůstková metoda .....	40
3.2.3 Rozdílová metoda .....	40
3.2.4 Sledování změněných bloků (CBT) .....	42
3.3 Výběr místa k ukládání záloh .....	42
3.3.1 Příprava nového disku k zálohování .....	43
3.3.2 Připojení FTP .....	44
3.3.3 Nastavení ověření .....	44
3.4 Nonstop zálohování Acronis .....	45
3.4.1 Omezení služby nonstop zálohování .....	45
3.4.2 Jak to funguje .....	45
3.4.3 Pravidla zachování .....	46
3.4.4 Datové úložiště Nonstop zálohování Acronis .....	46
3.4.5 Nonstop zálohování – nejčastěji kladené otázky .....	47
3.5 Pojmenování souboru zálohy .....	48
3.5.1 Konvence pojmenování pro soubory zálohy vytvořené v aplikaci Acronis True Image (2020 či 2021) a Acronis Cyber Protect Home Office .....	48
3.5.2 Konvence pojmenování pro soubory zálohy vytvořené před aplikací Acronis True Image 2020 .....	49

3.6	Integrace s Windows .....	50
3.6.1	Nabídka Start systému Windows .....	50
3.6.2	Tlačítko Acronis Cyber Protect Home Office na panelu úloh .....	50
3.6.3	Centrum oznámení .....	50
3.6.4	Příkazy místní nabídky .....	50
3.6.5	Obnova na úrovni souborů v Průzkumníku souborů .....	51
3.7	Průvodci .....	51
3.8	Nejčastější dotazy týkající se zálohování, obnovy a klonování .....	52
<b>4</b>	<b>Zálohování dat .....</b>	<b>54</b>
4.1	Zálohování diskových oddílů a disků .....	54
4.2	Zálohování souborů a složek .....	55
4.3	Zálohování mobilních zařízení .....	57
4.3.1	Acronis Mobile .....	58
4.3.2	Místní cíl pro mobilní zálohy .....	59
4.4	Zálohování dat aplikace Office 365 .....	59
4.4.1	Proč zálohovat data aplikace Office 365? .....	59
4.4.2	Zálohování dat aplikace Office 365 .....	59
4.5	Možnosti zálohování .....	60
4.5.1	Plánování .....	61
4.5.2	Schémata zálohování .....	64
4.5.3	Upozornění na operace zálohování .....	71
4.5.4	Vyloučení položek ze zálohy .....	72
4.5.5	Režim tvorby diskového obrazu .....	74
4.5.6	Ochrana zálohy .....	74
4.5.7	Ochrana pomocí online zálohování .....	76
4.5.8	Příkazy Před/Po pro zálohování .....	76
4.5.9	Rozdělování záloh .....	77
4.5.10	Možnosti ověření zálohy .....	78
4.5.11	Rezervní kopie zálohy .....	78
4.5.12	Možnosti vyměnitelného média .....	79
4.5.13	Zpracování chyb .....	80
4.5.14	Nastavení zabezpečení zálohy na úrovni souborů .....	82
4.5.15	Vypnutí počítače .....	82
4.5.16	Rychlost průběhu zálohování .....	83
4.5.17	Výběr datového centra pro zálohu .....	85
4.5.18	Nastavení napájení notebooku .....	85
4.5.19	Sítě Wi-Fi pro zálohování do úložiště Acronis Cloud .....	86

4.6 Operace se zálohami .....	86
4.6.1 Nabídka Operace zálohování .....	86
4.6.2 Činnost zálohování a statistika .....	88
4.6.3 Třídění záloh v seznamu .....	90
4.6.4 Replikace záloh do úložiště Acronis Cloud .....	90
4.6.5 Ověřování záloh .....	91
4.6.6 Zálohování do různých umístění .....	92
4.6.7 Přidání existující zálohy do seznamu .....	92
4.6.8 Ověřená záloha .....	93
4.6.9 Čištění záloh, verzí záloh a replik .....	97
4.6.10 Uvolnění místa v Acronis Cloud .....	99
4.6.11 Odebrání dat zAcronis Cloud .....	100
<b>5 Obnovení dat .....</b>	<b>103</b>
5.1 Obnovení disků a diskových oddílů .....	103
5.1.1 Obnovení systému po havárii .....	103
5.1.2 Obnovení disků a diskových oddílů .....	116
5.1.3 Obnova dynamických/GPT disků a svazků .....	129
5.1.4 Uspořádání pořadí spouštění v systému BIOS a UEFI BIOS .....	133
5.1.5 Obnova disků z úložiště Cloud .....	134
5.2 Obnova souborů a složek .....	139
5.3 Hledání obsahu zálohy .....	141
5.4 Obnova dat aplikace Office 365 .....	142
5.4.1 Jaké položky lze obnovit? .....	142
5.4.2 Obnova dat aplikace Office 365 .....	143
5.5 Možnosti obnovy .....	143
5.5.1 Režim obnovy disku .....	144
5.5.2 Příkazy Před/Po pro obnovu .....	144
5.5.3 Možnosti ověřování .....	145
5.5.4 Restartování počítače .....	145
5.5.5 Možnosti obnovy souborů .....	145
5.5.6 Možnosti přepsání souborů .....	145
5.5.7 Rychlost průběhu obnovování .....	146
5.5.8 Upozornění na operace obnovení .....	147
<b>6 Archivace dat .....</b>	<b>149</b>
6.1 Co je archivace dat? .....	149
6.2 Co je vyloučeno z archivů? .....	150
6.3 Archivace v cloudu vs. online zálohování .....	150

6.4 Archivace dat .....	151
6.4.1 Možnosti archivace dat .....	152
6.5 Přístup k archivovaným souborům .....	153
<b>7 Sdílení dat .....</b>	<b>154</b>
<b>8 Ochrana rodinných dat .....</b>	<b>155</b>
8.1 Co je ochrana rodinných dat? .....	155
8.2 Přidání nového zařízení do aplikace Online kontrolní panel .....	155
8.3 Vzdálené zálohování dat .....	156
8.4 Obnova dat pomocí aplikace Online kontrolní panel .....	157
8.5 E-mailová oznámení .....	158
<b>9 Ochrana .....</b>	<b>159</b>
9.1 Kontrolní panel ochrany .....	159
9.2 Active protection .....	160
9.2.1 Ochrana proti ransomwaru .....	160
9.2.2 Ochrana v reálném čase .....	161
9.2.3 Webové filtrování .....	162
9.2.4 Konfigurace služby Active Protection .....	162
9.3 Antivirové kontroly .....	164
9.3.1 Konfigurace antivirových kontrol .....	165
9.4 Vyhodnocení bezpečnostních rizik .....	166
9.5 Správa zjištěných problémů .....	167
9.6 Správa souborů v karanténě .....	167
9.7 Konfigurace výjimek z ochrany .....	168
9.8 Ochrana pro aplikace Zoom, Cisco Webex a Microsoft Teams .....	168
9.9 Stahování aktualizací ochrany .....	169
<b>10 Synchronizace dat .....</b>	<b>170</b>
10.1 Funkce synchronizace .....	170
10.2 Co lze a nelze synchronizovat .....	170
10.2.1 Typy úložišť .....	170
10.2.2 Typy dat .....	170
10.3 Ikony synchronizace .....	171
10.3.1 Oznamovací oblast .....	171
10.3.2 Průzkumník souborů .....	171
10.4 Vytvoření synchronizace .....	172
10.5 Nastavte ukládání verzí v online úložišti. ....	173
10.5.1 Návrat k předchozí verzi souboru .....	173
10.6 Jak obnovit smazaný soubor .....	173

10.7 Odstranění synchronizace .....	174
<b>11 Klonování a migrace disku .....</b>	<b>175</b>
11.1 Nástroj pro klonování disku .....	175
11.1.1 Průvodce klonováním disku .....	175
11.1.2 Ruční rozdělení na diskové oddíly .....	177
11.1.3 Vyloučení položek z klonování .....	178
11.1.4 Způsob migrace .....	180
11.2 Migrace systému z pevného disku na disk SSD .....	186
11.2.1 Velikost SSD .....	186
11.2.2 Kterou metodu migrace použít .....	186
11.2.3 Co dělat v případě, že aplikace Acronis Cyber Protect Home Office nerozezná váš disk SSD .....	187
11.2.4 Migrace na disk SSD pomocí metody zálohy a obnovení .....	188
<b>12 Nástroje .....</b>	<b>190</b>
12.1 Tvůrce médií Acronis .....	190
12.1.1 Jak vytvořit spouštěcí médium Acronis .....	192
12.1.2 Parametry spuštění spouštěcího média Acronis .....	193
12.1.3 Přidání ovladačů do stávající bitové kopie WIM .....	195
12.1.4 Vytvoření souboru ISO ze souboru WIM .....	196
12.2 Kontrola, že spouštěcí médium lze v případě potřeby použít .....	197
12.2.1 Jak testovat spouštěcí média .....	197
12.2.2 Jak testovat obnovu a zkontrolovat ovladače a síťový adaptér .....	198
12.2.3 Výběr grafického režimu při spuštění ze spouštěcího média .....	201
12.3 Acronis Startup Recovery Manager .....	203
12.3.1 Další informace .....	204
12.4 Try&Decide .....	205
12.4.1 Kdy je režim Try&Decide užitečný .....	205
12.4.2 Jak režim Try&Decide funguje po restartování počítače .....	206
12.4.3 Omezení při používání režimu Try&Decide .....	206
12.4.4 Používání funkce Try&Decide .....	207
12.4.5 Možnosti a upozornění režimu Try&Decide .....	208
12.4.6 Try&Decide: typické případy použití .....	209
12.5 Acronis Secure Zone .....	210
12.5.1 Acronis Vyčištění zóny Secure Zone .....	211
12.5.2 Vytváření a řízení Acronis Secure Zone .....	211
12.5.3 Umístění zóny Acronis Secure Zone .....	212
12.5.4 Velikost Acronis Secure Zone .....	213



12.5.5	Ochrana zóny Acronis Secure Zone .....	214
12.5.6	Odstraňuje se Acronis .....	215
12.6	Přidání nového pevného disku .....	215
12.6.1	Výběr pevného disku .....	215
12.6.2	Výběr metody inicializace .....	216
12.6.3	Tvorba diskových oddílů .....	217
12.7	Nástroje zajišťující bezpečnost a soukromí .....	220
12.7.1	Acronis DriveCleanser .....	220
12.7.2	Vyčištění systému .....	225
12.7.3	Metody trvalého odstranění dat z pevného disku .....	233
12.8	Připojení diskového obrazu .....	234
12.8.1	Jak připojit diskový obraz .....	235
12.9	Odpojení diskového obrazu .....	236
12.10	Práce se soubory VHD(X) .....	236
12.10.1	Jak používat soubory VHD(X) .....	236
12.10.2	Omezení a další informace .....	236
12.10.3	Převod zálohy Acronis .....	237
12.11	Import a export nastavení zálohování .....	237
12.12	Acronis Universal Restore .....	238
12.12.1	Jaký problém se tím vyřeší? .....	239
12.12.2	Jak jej mám použít? .....	239
12.12.3	Vytváření média Acronis Universal Boot .....	239
12.12.4	Použití technologie univerzální obnovy Acronis .....	242
<b>13</b>	<b>Odstraňování problémů .....</b>	<b>244</b>
13.1	Řešení nejčastějších potíží .....	244
13.2	Systémová zpráva Acronis .....	244
13.3	Inteligentní hlášení chyb Acronis .....	246
13.3.1	Když jste připojeni k internetu .....	246
13.3.2	Když nejste připojeni k internetu .....	246
13.4	Odeslání zpětné vazby společnosti Acronis .....	247
13.5	Jak získat výpisy stavu systému .....	249
13.6	Program zkušeností uživatelů Acronis .....	249
<b>Slovníček</b>	.....	<b>251</b>
<b>Rejstřík</b>	.....	<b>256</b>



# Prohlášení o autorských právech

© Acronis International GmbH, 2003-2021. Všechna práva vyhrazena.

Všechny zmíněné ochranné známky a autorská práva jsou vlastnictvím svých příslušných vlastníků.

Distribuce podstatným způsobem změněných verzí tohoto dokumentu je bez výslovného dovození vlastníka autorských práv zakázána.

Distribuce tohoto díla nebo odvozených děl ve formě jakékoliv standardní (papírové) knihy pro obchodní účely je zakázáno, pokud není předem získáno povolení od vlastníka autorských práv.

DOKUMENTACE JE POSKYTOVÁNA „TAK, JAK JE“ A VEŠKERÉ VÝSLOVNÉ NEBO PŘEDPOKLÁDANÉ PODMÍNKY, VYJÁDŘENÍ A ZÁRUKY VČETNĚ VŠECH IMPLICITNÍCH ZÁRUK PRODEJNOSTI, VHODNOSTI PRO KONKRÉTNÍ ÚČEL NEBO NENARUŠENÍ CIZÍCH PRÁV, JSOU VYLOUČENY S VÝJIMKOU ROZSAHU, V NĚMŽ JSOU TAKOVÁTO ODMÍTNUTÍ ZÁRUK POVAŽOVÁNA ZA PRÁVNĚ NEÚČINNÁ.

Se softwarem a/nebo službami může být dodáván kód třetích stran. Licenční podmínky těchto produktů od jiných dodavatelů jsou popsány v souboru license.txt v kořenovém adresáři instalace. Nejnovější seznam kódů třetích stran a příslušné licenční podmínky těchto produktů používaných se softwarem nebo službami naleznete na adrese <https://kb.acronis.com/content/7696>.

## Technologie patentované společností Acronis

Technologie použité v tomto produktu jsou zahrnuty pod nejméně jeden z následujících patentů USA a jsou jimi chráněny: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234 a další patentové žádosti čekající na vyřízení.

# 1 Úvod

## 1.1 Co je Acronis Cyber Protect Home Office?

Acronis Cyber Protect Home Office je kompletní řešení kybernetické ochrany dat zajišťující bezpečnost všech vašich informací. S její pomocí můžete zálohovat dokumenty, fotografie, e-maily a vybrané diskové oddíly, dokonce i celý disk, včetně operačního systému, aplikací, nastavení a veškerých dat. Jednou z jeho hlavních výhod je ochrana dat a bezpečnostní funkce.

Zálohy umožňují obnovení systému počítače v případě nehody, například ztráty dat, nechtěného odstranění důležitých souborů a složek nebo úplného zničení pevného disku.

Online zálohování umožňuje ukládat nejdůležitější soubory a disky do úložiště Acronis Cloud. Vaše data budou chráněna i v případě, že počítač někdo ztratí, ukradne nebo zničí. Tato data lze v případě potřeby obnovit na nové zařízení.

### Klíčové funkce:

- Zálohování disku do místního úložiště a Acronis Cloud
- Zálohování souborů do místního úložiště a Acronis Cloud
- Antivirová ochrana a ochrana proti malwaru
- Spouštěcí médium Acronis
- Klonování pevného disku
- Archivace dat
- Ochrana rodinných dat
- Synchronizace souborů
- Nástroje zajišťující bezpečnost a soukromí

---

### Poznámka

Zálohy do úložiště Acronis Cloud nelze vytvářet pomocí programu Acronis Startup Recovery Manager a spouštěcích médií Acronis.

---

Naučte se chránit svůj počítač pomocí dvou jednoduchých kroků: „[Ochrana systému](#)“.

## 1.2 Zálohy vytvořené v aplikaci Acronis True Image (2020 či 2021) a Acronis Cyber Protect Home Office

Aplikace Acronis True Image z roku 2020 představila nový formát zálohy – TIBX, který je ještě spolehlivější a pohodlnější. Formát TIBX se používá k zálohám disku vytvořených na interních discích, externích discích, síťovém úložišti.

## 1.2.1 Pojmenování souboru zálohy

Název souboru .tibx obsahuje pouze název zálohy a přírůstkový čítač. Neobsahuje žádné další informace, jako je třeba metoda zálohování, číslo řetězce zálohy, číslo verze zálohy nebo číslo svazku, které byly využívány u formátu TIB.

Název zálohy může vypadat takto:

1. my\_data.tibx
2. my\_data\_0001.tibx:
3. my\_data\_0002.tibx:
4. my\_data\_0003.tibx:

## 1.2.2 Schémata zálohování

Zálohování ve formátu TIBX podporuje všechna schémata zálohování. Na rozdíl od formátu TIB, který ukládá každou verzi zálohy jako samostatný soubor, formát TIBX ukládá plnou a rozdílovou verzi zálohy jako samostatné soubory, zatímco přírůstkové verze zálohy jsou automaticky sloučeny do jejich základních záloh (plných nebo rozdílových).

## 1.2.3 Vyčištění záloh formátu TIBX

Pokud si přejete vyčistit verze záloh, které již nepotřebujete, použijte automatické a ruční metody čištění.

V případě, že jsou automatická nebo ruční čištění nakonfigurována, mohou některé malé pomocné soubory zůstat po vyčištění v úložišti. Systém Windows může zobrazit tyto soubory jako větší, než ve skutečnosti jsou. Jejich skutečnou velikost najdete ve vlastnostech souborů systému Windows.

---

### **Poznámka**

Neodstraňujte, prosím, žádné soubory ručně!

---

## 1.2.4 Ruční čištění místních záloh má následující schéma:

- Plné zálohy lze odstranit pouze se závislými verzemi.
- Rozdílové verze zálohy lze odstranit nezávisle na jakékoli jiné verzi zálohy.
- Přírůstkové zálohy:
  - Pokud se jedná o poslední řetězec zálohy, lze libovolnou přírůstkovou zálohu odstranit, aby se uvolnilo úložné místo.
  - Pokud se nejedná o poslední řetězec zálohy, lze libovolnou přírůstkovou zálohu odstranit pouze se všemi ostatními přírůstkovými verzemi stejného řetězce.

## 1.2.5 Které zálohy zachovávají formát TIB

Následující zálohy nadále používají formát TIB:

- Zálohy na úrovni souborů
- Nonstop zálohy
- Ověřené zálohy
- Zálohy využívající CD/DVD/Blu-ray, FTP nebo Acronis Secure Zone jako své cílové umístění

Detailní porovnání pojmenování archivu .tibx s archivem .tib naleznete v části [Pojmenování souboru zálohy](#).

Další informace o vyčištění naleznete v části [Čištění záloh, verzí záloh a replik](#).

## 1.3 Systémové požadavky a podporovaná média

### 1.3.1 Minimální systémové požadavky

Acronis Cyber Protect Home Office vyžaduje následující hardware.

- Procesor Intel CORE 2 Duo (2GHz) nebo ekvivalentní.  
Procesor musí podporovat instrukce SSE.
- 2 GB RAM
- 7 GB volného místa na systémovém pevném disku
- Vypalovací mechanika CD-RW/DVD-RW nebo USB disk pro tvorbu spouštěcích médií
  - Požadované volné místo se systémem Linux je 660 MB.
  - Požadované volné místo se systémem Windows je 700 MB.
- Rozlišení obrazovky je 1024 × 768
- Myš nebo jiné polohovací zařízení (doporučeno).

---

#### **Upozornění!**

Při instalaci ve virtuálním počítači není úspěch zálohování a obnovy zaručen.

---

#### Další požadavky

- K aktivaci produktu, stahování aktualizací ochrany a pro všechny funkce, které používají úložiště Acronis Cloud. Pokud váš počítač není připojen k internetu, je možné produkt aktivovat pomocí jiného počítače připojeného k internetu. Další informace naleznete v tématu [Aktivace aplikace Acronis Cyber Protect Home Office](#).
- K spuštění aplikace Acronis Cyber Protect Home Office jsou vyžadována oprávnění správce.

### 1.3.2 Podporované operační systémy

Aplikace Acronis Cyber Protect Home Office byla testována v následujících operačních systémech.

- Windows 11
- Windows 10

- Windows 8.1
- Windows 8
- Windows 7 SP1 (všechny verze)
- Windows Home Server 2011

---

**Poznámka**

- Beta sestavení nejsou podporována. Viz <https://kb.acronis.com/content/60589>.
- Windows Embedded, edice IoT, Windows 10 LTSC, Windows 10 LTSC a Windows 10 v režimu S nejsou podporovány.
- Pokud chcete Acronis Cyber Protect Home Office používat na operačním systému Windows 7, Windows 8 a Windows 8.1, budete potřebovat následující bezpečnostní aktualizace od společnosti Microsoft: KB4474419 a KB4490628. Viz <https://kb.acronis.com/content/69302>.

---

Aplikace Acronis Cyber Protect Home Office umožňuje také tvorbu spouštěcích disků CD-R/DVD-R nebo USB, pomocí nichž lze zálohovat a obnovit disk nebo diskový oddíl v počítači s libovolným operačním systémem pro PC s procesory Intel nebo AMD včetně operačního systému Linux®. Apple Macintosh založený na procesoru Intel není podporován.

Je možné, že tento software bude fungovat i na jiných verzích operačního systému Windows, ale není to garantováno.

---

**Upozornění!**

Úspěšné obnovení je zaručeno pouze u podporovaných operačních systémů. Jiné operační systémy lze zálohovat po jednotlivých sektorech, po obnovení je však nemusí být možné zavést.

---

### 1.3.3 Podporované systémy souborů

- NTFS
- Ext2/Ext3/Ext4
- ReiserFS(3) \*
- Linux SWAP \*
- HFS+\*\*/HFSX\*\*
- FAT16/32/exFAT \*\*

\* Systémy souborů jsou podporovány pouze pro operace zálohování/obnovy disku nebo oddílu.

\*\*Obnovení disku, obnovení diskového oddílu a operace klonování jsou podporovány bez nutnosti provedení změny velikosti.

Jestliže není systém souborů podporován nebo je poškozen, může aplikace Acronis Cyber Protect Home Office zkopírovat data sektor po sektor.

## 1.3.4 Podporované typy připojení k internetu

V tabulce níže naleznete typy připojení k internetu podporované funkcemi produktu.

	Typ připojení k internetu				
	Konzole Acronis v systému Windows		Spouštěcí médium Acronis		
	Jakékoli připojení vytvořené v systému Windows	Proxy server	Ethernetový kabel	Wi-Fi	Proxy server
Zálohování na úrovni disku a souborů do úložiště Acronis Cloud	+	-	-	-	-
Obnova disků z úložiště Acronis Cloud	+	-	+	+	-
Obnova souborů z úložiště Acronis Cloud	+	-	-	-	-
Synchronizace dat	+	-	-	-	-
Aktivace produktu	+	- *	-	-	-
Aktualizace produktu	+	- **	-	-	-

\* - Produkt můžete aktivovat pomocí aktivačního kódu. Podrobnosti naleznete v části **Aktivace z jiného počítače** v kapitole [Aktivace aplikace Acronis Cyber Protect Home Office](#).

\*\* - Chcete-li aktualizovat produkt, stáhněte si novější verzi z webové stránky Acronis a nainstalujte ji přes aktuální produkt.

## 1.3.5 Podporovaná úložná média

- Jednotky pevných disků (HDD)
- Jednotky polovodičových disků SSD (Solid State Drive)
- Síťová paměťová zařízení
- Servery FTP

### Poznámka

Server FTP musí umožňovat přenos souborů v pasivním režimu. Acronis Cyber Protect Home Office při zálohování přímo na server FTP se záloha rozdělí na soubory o velikosti 2 GB.

- CD-R/RW, DVD-R/RW, DVD+R (včetně dvouvrstvých DVD+R), DVD+RW, DVD-RAM, BD-R, BD-RE

- Paměťová zařízení s rozhraním USB 1.1/2.0/3.0, USB-C, eSATA, FireWire (IEEE-1394), rozhraní SCSI a kartou PC Card

### Omezení pro operace s dynamickými disky

- Tvorba zóny Acronis Secure Zone na dynamických discích není podporována.
- Obnovení dynamického svazku jako dynamického svazku s ruční změnou velikosti není podporováno.
- Režim Try&Decide® nelze použít k ochraně dynamických disků.
- Operace „Klonování disku“ není u dynamických disků podporována.

Pro správnou funkci by měla být brána firewall zdrojového počítače nastavena tak, aby byly porty 20 a 21 otevřené pro protokoly TCP a UDP. Služba **Směrování a vzdálený přístup** ve Windows by měla být vypnuta.

## 1.4 Instalace a odebrání aplikace Acronis Cyber Protect Home Office

### ***Jak nainstalovat aplikaci Acronis Cyber Protect Home Office***

1. Stáhněte si instalační soubor aplikace Acronis Cyber Protect Home Office z webových stránek společnosti Acronis na adrese <http://go.acronis.com/home-office>.
2. Spusťte instalační soubor.  
Před spuštěním instalace aplikace Acronis Cyber Protect Home Office zkontroluje, zda je na webových stránkách dostupná novější verze. Pokud ano, nabídne se k instalaci novější verze.
3. Klikněte na tlačítko **Instalovat**.  
Aplikace Acronis Cyber Protect Home Office bude nainstalována na systémový diskový oddíl (obvykle C:).
4. Po dokončení instalace klikněte na tlačítko **Spustit aplikaci**.
5. Přečtěte si a potvrďte podmínky licenční smlouvy aplikace Acronis Cyber Protect Home Office a Bonjour.  
Software Bonjour se nainstaluje do vašeho počítače a bude nabízet rozšířenou podporu zařízení NAS. Software můžete nainstalovat kdykoli.  
Můžete rovněž souhlasit s účastí v [Programu zkušeností uživatelů Acronis](#). Toto nastavení můžete kdykoli změnit.
6. V okně **Aktivace** můžete provést jednu z následujících akcí:
  - Chcete-li aktivovat aplikaci Acronis Cyber Protect Home Office, zadejte sériové číslo a klikněte na tlačítko **Aktivovat**. Produkt se aktivuje.
  - Chcete-li se přihlásit do svého účtu Acronis, klikněte na tlačítko **Přihlásit se**. Další informace naleznete v části Účet [Acronis](#).
  - Chcete-li spustit zkušební verzi, klikněte na tlačítko **Spustit zkušební verzi**.

### ***Obnovení po chybě aplikace Acronis Cyber Protect Home Office***



Pokud aplikace Acronis Cyber Protect Home Office přestane fungovat nebo způsobuje chyby, mohou být některé soubory poškozeny. Chcete-li tento problém vyřešit, je nutné nejprve aplikaci opravit. To lze provést spuštěním instalačního programu aplikace Acronis Cyber Protect Home Office. Ten nalezne v počítači aplikaci Acronis Cyber Protect Home Office a zeptá se, zda ji chcete opravit nebo odebrat.

### **Odebrání Acronis Cyber Protect Home Office**

- Používáte-li systém Windows 11, klikněte na tlačítko **Start > Nastavení > Systém > Aplikace a funkce > Acronis Cyber Protect Home Office > Odinstalovat**.
- Používáte-li systém Windows 10, klikněte na tlačítko **Start > Nastavení > Systém > Aplikace > Acronis Cyber Protect Home Office > Odinstalovat**.
- Používáte-li systém Windows 8, klikněte na ikonu **Nastavení** a vyberte možnost **Ovládací panely > Odinstalovat program > Acronis Cyber Protect Home Office > Odinstalovat**.
- Používáte-li systém Windows 7, klikněte na tlačítko **Start > Ovládací panely > Odinstalovat program > Acronis Cyber Protect Home Office > Odinstalovat**.

Poté postupujte podle pokynů na obrazovce. Po dokončení úlohy budete možná muset počítač restartovat.

---

### **Poznámka**

Pokud jste používali aplikaci "Acronis Secure Zone" (str. 210) nebo "Nonstop zálohování Acronis" (str. 45), vyberte v okně, které se zobrazí, co se má udělat se zónou nebo s úložišti nonstop zálohování.

---

## **1.5 Aktivuje se Acronis Cyber Protect Home Office**

Aplikaci Acronis Cyber Protect Home Office je třeba aktivovat přes internet. Bez aktivace funguje produkt bez omezení po dobu 30 dní. Pokud jej v tomto časovém období neaktivujete, všechny funkce aplikace kromě obnovy budou nedostupné.

### **1.5.1 Aktivuje se Acronis Cyber Protect Home Office**

Aplikaci Acronis Cyber Protect Home Office lze aktivovat buď v tomto, nebo jiném počítači, pokud váš počítač není připojen k internetu.

#### **Aktivace v počítači připojeném k internetu**

Je-li počítač připojen k internetu, dojde k aktivaci produktu automaticky.

Pokud počítač, do kterého instalujete aplikaci Acronis Cyber Protect Home Office, nemá připojení k internetu nebo pokud se aplikace nemůže připojit k aktivačnímu serveru Acronis, klikněte na bočním panelu na tlačítko **Účet** a zvolte jednu z následujících akcí:

- **Zkusit znovu** – tuto možnost zvolte, pokud se chcete znovu zkusit připojit k aktivačnímu serveru Acronis.

- **Aktivovat offline**– aplikaci lze aktivovat ručně z jiného počítače, který je připojen k internetu (viz níže).

### **Aktivace z jiného počítače**

Pokud váš počítač není připojen k internetu, aplikaci Acronis Cyber Protect Home Office je možné aktivovat pomocí jiného počítače připojeného k internetu.

#### ***Jak produkt aktivovat z jiného počítače***

1. Nainstalujte do počítače aplikaci Acronis Cyber Protect Home Office a spusťte ji.
2. Na postranním panelu klikněte na tlačítko **Účet** a potom na tlačítko **Aktivovat offline**.
3. V okně Aktivace Acronis Cyber Protect Home Office proveďte tyto tři jednoduché kroky:
  - a. Uložte instalační kód do souboru kliknutím na tlačítko **Uložit do souboru** a jako umístění souboru vyberte vyměnitelné médium (například USB flash disk). Také je možné tento kód opsat na kousek papíru.
  - b. V jiném počítači, který je připojen k internetu, přejděte na stránku <https://www.acronis.eu/activation/>. Podle pokynů na obrazovce získajte aktivační kód pomocí instalačního kódu. Uložte získaný aktivační kód do souboru na vyměnitelném médiu nebo si jej запиšte na papír.
  - c. V počítači klikněte na tlačítko **Nahrát ze souboru** a zadejte cestu k souboru s aktivačním kódem, nebo jej jednoduše opište do textového pole z papíru.
4. Klikněte na tlačítko **Aktivovat**.

Dále se povídejte na video s pokyny v angličtině na adrese <https://goo.gl/DHd1h5>.

## **1.5.2 Problém Příliš mnoho aktivací**

Možné důvody problému „Příliš mnoho aktivací“:

- **Překročili jste maximální počet počítačů s nainstalovanou aplikací Acronis Cyber Protect Home Office.**

Máte například jednu licenci nebo jedno sériové číslo pro jeden počítač a nainstalujete aplikaci Acronis Cyber Protect Home Office na druhý počítač.

#### **Řešení:**

- Zadejte nové sériové číslo. Pokud žádné nemáte, můžete jej zakoupit v integrovaném obchodě Acronis nebo na webových stránkách společnosti Acronis.
- Přesuňte licenci do nového počítače z počítače, ve kterém byl již produkt aktivován. Pokud chcete tuto akci provést, vyberte počítač, ze kterého chcete licenci přenést. Upozorňujeme, že program Acronis Cyber Protect Home Office bude v tomto počítači deaktivován.

- **Přeinštalovat systém Windows nebo změnit hardware počítače.**

Můžete například upgradovat základní desku nebo procesor počítače. Aktivace byla ztracena, protože program Acronis Cyber Protect Home Office vidí váš počítač jako nový.

#### **Řešení:**

Pokud chcete program Acronis Cyber Protect Home Office ve svém počítači aktivovat znovu, vyberte ze seznamu stejný počítač podle starého názvu.

### 1.5.3 Ruční správa licencí předplatného

Používáte-li předplacenou verzi aplikace Acronis Cyber Protect Home Office, můžete licence spravovat ručně na webových stránkách Acronis. Lze provést následující:

- Přesunout licence mezi počítači
- Přenést licence mezi účty
- Odebrat licenci z počítače
- Vyřešit problémy s aktivací produktu včetně problému Příliš mnoho aktivací
- Koupit nové licence

#### ***Jak spravovat licence***

1. Přejděte na adresu <https://account.acronis.com/> a přihlaste se pomocí svého účtu Acronis.
2. V části **Produkty** vyhledejte aplikaci Acronis Cyber Protect Home Office a klikněte na položku **Spravovat**.

## 1.6 Informace ke zkušební verzi

### 1.6.1 Obecná omezení

Zkušební verze aplikace Acronis Cyber Protect Home Office bude fungovat pouze během zkušebního třicetidenního období. Má následující omezení:

- [Klonování disku](#) je vypnuto.
- Při načítání ze spouštěcího média Acronis je jedinou dostupnou operací obnovení.

### 1.6.2 Synchronizace

Synchronizace dat je dostupná bez omezení, ale po vypršení zkušební doby:

- Váš počítač bude vyloučen ze všech synchronizací. Po aktivaci plné verze aplikace Acronis Cyber Protect Home Office se budete moci do synchronizací znovu zapojit.
- Všechny verze synchronizovaných souborů budou trvale odstraněny z úložiště [Acronis Cloud](#).

### 1.6.3 Acronis Cloud

Během zkušebního období budete mít k dispozici 1 000 GB úložného prostoru v cloudu. Tento prostor můžete využít k ukládání online záloh, archivů a verzí synchronizovaných souborů. Po skončení zkušebního období bude úložiště Acronis Cloud fungovat ještě dalších 30 dní v režimu obnovy. Po skončení tohoto období nebudete moci službu Acronis Cloud používat a všechna data budou z cloudu odstraněna.

## 1.6.4 Zakoupení plné verze

Plnou verzi lze zakoupit na webových stránkách Acronis nebo pomocí funkce nákupu integrované v aplikaci. Podrobnosti naleznete v části [Upgrade aplikace Acronis Cyber Protect Home Office](#).

## 1.7 Upgrade aplikace Acronis Cyber Protect Home Office

Až bude na webových stránkách Acronis dostupná aktualizace pro aplikaci Acronis Cyber Protect Home Office, budete si ji moci stáhnout. Pokud máte aplikaci Acronis True Image (2017 či novější), nová verze ji zaktualizuje, takže není nutné odebírat starou verzi a znovu instalovat software. Pokud je vaše aktuální verze starší, doporučujeme nejprve odstranit aktuální verzi.

Vaše zálohy vytvořené pomocí předchozí verze aplikace Acronis Cyber Protect Home Office jsou zcela kompatibilní s novější verzí produktu. Po upgradu se všechny vaše zálohy automaticky přidají do seznamu zálohování.

Zálohy vytvořené v novějších verzích aplikace nemusí být kompatibilní s předchozími verzemi aplikace. Při přechodu na předchozí verzi aplikace Acronis Cyber Protect Home Office je nutné znovu vytvořit zálohy pomocí starší verze. Doporučujeme při každé aktualizaci programu Acronis Cyber Protect Home Office znovu vytvořit nové spouštěcí médium.

### **Zakoupení plné verze aplikace Acronis Cyber Protect Home Office**

1. Spustit Acronis Cyber Protect Home Office
2. Na postranním panelu klikněte na tlačítko **Účet** a potom na tlačítko **Koupit plnou verzi**. Otevře se integrovaný obchod.
3. Vyberte licenci, kterou chcete zakoupit, a klikněte na tlačítko **Koupit**.
4. Zadejte své platební údaje.

### **Aktualizace Acronis Cyber Protect Home Office**

1. Spustit Acronis Cyber Protect Home Office
2. Na bočním panelu klikněte na možnost **Účet**.  
Je-li k dispozici nová verze, zobrazí se u aktuálního čísla sestavení příslušná zpráva.
3. Klikněte na možnost **Stáhnout a nainstalovat**.

---

#### **Poznámka**

Než spustíte stahování, ujistěte se, že proces stahování nebude blokovat brána firewall.

---

4. Až se nová verze stáhne, klikněte na tlačítko **Instalovat nyní**.

Chcete-li aktualizace vyhledávat automaticky, přejděte na kartu **Nastavení** a zaškrtněte políčko **Při spuštění automaticky kontrolovat aktualizace**.

## 1.7.1 Integrovaný obchod

Acronis Cyber Protect Home Office nabízí funkci obchodu v rámci aplikace. Pomocí tohoto obchodu můžete:

- Koupit plnou verzi aplikace Acronis Cyber Protect Home Office.
- Koupit předplatné aplikace Acronis Cyber Protect Home Office.
- Koupit další úložný prostor v úložišti Acronis Cloud.

Chcete-li získat přístup k obchodu v rámci aplikace, přejděte na kartu **Účet** a pak klikněte na možnost **Obchod Acronis**. Zobrazí se obchod v rámci aplikace a všechny dostupné možnosti nákupu.

## 1.8 Technická podpora

### 1.8.1 Program údržby a podpory

Potřebujete-li pomoci s aplikací Acronis Cyber Protect Home Office, využijte stránku <https://www.acronis.eu/support/>.

## 2 Začínáme

### 2.1 Jazyk uživatelského rozhraní

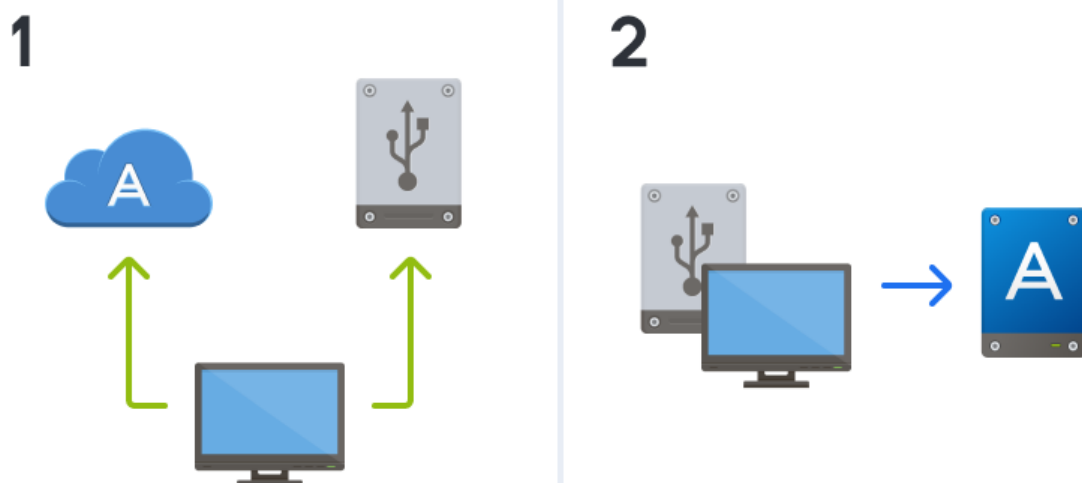
Než začnete, vyberte upřednostňovaný jazyk uživatelského rozhraní aplikace Acronis Cyber Protect Home Office. Implicitně je jazyk nastaven podle jazyka systému Windows.

#### **Chcete-li změnit jazyk uživatelského rozhraní**

1. Spustit Acronis Cyber Protect Home Office
2. V části **Nastavení** vyberte ze seznamu upřednostňovaný jazyk.

### 2.2 Ochrana systému

1. [Zálohujte počítač.](#)
2. [Vytvořte spouštěcí médium Acronis.](#)



- Doporučujeme také spouštěcí médium vyzkoušet podle postupu popsáno v části [Kontrola, že spouštěcí médium lze v případě potřeby použít](#).

#### 2.2.1 Zálohuje se počítač

##### **Kdy je třeba provést zálohu počítače?**

Vytvořte novou verzi zálohy po každé významné změně ve vašem systému.

Mezi takové změny patří například:

- Zakoupili jste nový počítač.
- Do svého počítače jste znovu nainstalovali systém Windows.

- Nakonfigurovali jste všechna systémová nastavení (např. čas, datum, jazyk) a nainstalovali do nového počítače všechny nezbytné programy.
- Důležitá aktualizace systému.

---

### **Poznámka**

Doporučujeme před zálohováním zkontrolovat disk na přítomnost virů, abyste měli jistotu, že zálohujete disk ve zdravém stavu. Pro tento účel prosím použijte antivirový software. Vezměte prosím v úvahu, že tato operace obvykle trvá delší dobu.

---

### ***Jak mohu vytvořit zálohu počítače?***

Máte k dispozici dvě možnosti ochrany systému:

- **Celá záloha počítače (doporučeno)**

Aplikace Acronis Cyber Protect Home Office zálohuje všechny interní pevné disky v režimu disku. Záloha obsahuje operační systém, nainstalované programy, nastavení systému a všechna osobní data včetně fotografií, hudby a dokumentů. Podrobnosti naleznete v části [Zálohování všech dat v počítači](#).

- **Zálohování systémového disku**

Můžete si zvolit zálohování systémového oddílu nebo celého systémového disku. Další informace naleznete v části [Zálohování disků a diskových oddílů](#).

Nedoporučujeme používat nonstop zálohování jako primární způsob ochrany systému, protože hlavním účelem této technologie je ochrana často měněných souborů. Pro zajištění bezpečnosti systému použijte jakýkoli jiný plán. Podrobnosti nabízí "Příklady vlastních schémat" (str. 69). Další informace týkající se nonstop zálohování naleznete v části Použití nonstop zálohování "Nonstop zálohování Acronis" (str. 45).

### ***Chcete-li zálohovat počítač***

1. Spustit Acronis Cyber Protect Home Office
2. Na bočním panelu klikněte na možnost **Záloha**.  
Je-li to vaše první záloha, zobrazí se obrazovka konfigurace zálohy. Máte-li v seznamu záloh již nějaké zálohy, klikněte na položku **Přidat zálohu**.
3. Klikněte na ikonu **Zdroj zálohování** a pak vyberte položku **Celý počítač**.  
Pokud chcete zálohovat pouze systémový disk, pak klikněte na položku **Disky a diskové oddíly** a poté vyberte systémový oddíl (obvykle C:) a diskový oddíl vyhrazený systému (pokud nějaký je).
4. Klikněte na ikonu **Cílové umístění zálohy** a pak vyberte cílové umístění pro zálohu (viz následující doporučení).
5. Klikněte na tlačítko **Zálohovat nyní**.

Poté se v seznamu záloh zobrazí pole nové zálohy. Budete-li chtít v budoucnu vytvořit novou verzi zálohy, zaškrtněte v seznamu pole zálohy a klikněte na položku **Zálohovat nyní**.

### ***Kam mám uložit své zálohy disku?***



- **Dobré** – Běžný pevný disk.
- **Lepší** – **Zóna Acronis Secure Zone**. Jde o speciální bezpečný diskový oddíl na vašem místním pevném disku pro ukládání záloh.
- **Nejlepší** – Úložiště **Acronis Cloud** nebo externí pevný disk.

Další informace naleznete v části [Výběr místa k ukládání záloh](#).

### ***Kolik verzí zálohy potřebuji?***

Ve většině případů potřebujete 2–3 **verze zálohy** veškerého obsahu počítače nebo systémového disku, maximálně 4–6 (viz část „Kdy je třeba provést zálohu systémového disku?“). Pomocí automatických pravidel mazání můžete řídit počet verzí záloh. Další informace naleznete v části [Vlastní schémata](#).

Pamatujte, že první verze zálohy (plná verze zálohy) je nejdůležitější. Je také největší, protože obsahuje všechna data uložená na disku. Další verze zálohy (přírůstkové a rozdílové verze záloh) mohou být uspořádány podle jiných schémat. Tyto verze obsahují jen změny dat. Proto jsou závislé na plné verzi zálohy, a proto je plná verze zálohy tak důležitá.

Ve výchozím nastavení se záloha disku vytváří jako přírůstková. Takové schéma je ve většině případů optimální.

---

### **Poznámka**

Pro zkušené uživatele: Dobrým postupem je vytvořit 2–3 plné verze zálohy a uložit je na jiná úložná zařízení. Tato metoda je mnohem spolehlivější.

---

## 2.2.2 Jak vytvořit spouštěcí médium Acronis

Spouštěcí médium Acronis je disk CD, DVD nebo USB flash disk či jiné vyměnitelné médium, ze kterého můžete spustit aplikaci Acronis Cyber Protect Home Office, pokud nelze spustit systém Windows. Spouštěcí médium můžete vytvořit pomocí nástroje Tvůrce médií Acronis.

### ***Jak vytvořit spouštěcí médium Acronis***

1. Vložte disk CD/DVD nebo zapojte USB jednotku (USB flash disk nebo externí disk HDD/SSD).
2. Spustit Acronis Cyber Protect Home Office
3. Na postranním panelu klikněte na tlačítko **Nástroje** a potom klikněte na možnost **Tvůrce záchranných médií**.
4. U prvního kroku vyberte položku **Jednoduchý**.
5. Vyberte zařízení, které chcete použít k vytvoření spouštěcího média.
6. Klikněte na tlačítko **Pokračovat**.

### ***Použijte spouštěcí médium Acronis.***

Spouštěcí médium Acronis použijte pro obnovu počítače, pokud nelze spustit systém Windows.

1. Připojte k počítači spouštěcí médium (vlozte disk CD/DVD nebo zapojte USB disk).
2. Nastavte pořadí spouštění v systému BIOS tak, aby se systém spustil ze spouštěcího média Acronis.  
Podrobnosti naleznete v části [Uspořádání pořadí spouštění v systému BIOS](#).
3. Spusťte svůj počítač ze spouštěcího média a vyberte možnost **Acronis Cyber Protect Home Office**.  
Po načtení aplikace Acronis Cyber Protect Home Office ji můžete použít pro obnovu vašeho počítače.

Další informace naleznete v části Program pro tvorbu médií [Acronis](#).

## 2.3 Zálohování všech dat v počítači

### **Co je zálohování celého počítače?**

Zálohování celého počítače představuje nejsnazší způsob jak zálohovat úplný obsah vašeho počítače. Pokud si nejste jisti, která data potřebujete chránit, doporučujeme vybrat tuto možnost. Chcete-li zálohovat pouze systémový oddíl, podrobnosti naleznete v části [Zálohování disků a diskových oddílů](#).

Pokud vyberete typ zálohování Celý počítač, aplikace Acronis Cyber Protect Home Office zálohuje všechny interní pevné disky v režimu disku. Záloha obsahuje operační systém, nainstalované programy, nastavení systému a všechna osobní data včetně fotografií, hudby a dokumentů.

Obnovení ze zálohy celého počítače je také zjednodušeno. Stačí vybrat datum, od kterého chcete data obnovit. Acronis Cyber Protect Home Office obnoví všechna data ze zálohy do původního umístění. Upozorňujeme, že k obnovení nemůžete vybrat konkrétní disky nebo oddíly ani nemůžete měnit výchozí cílové umístění. Pokud se potřebujete vyhnout těmto omezením, doporučujeme zálohovat data běžnou metodou zálohování na úrovni disků. Další informace naleznete v části [Zálohování disků a diskových oddílů](#).

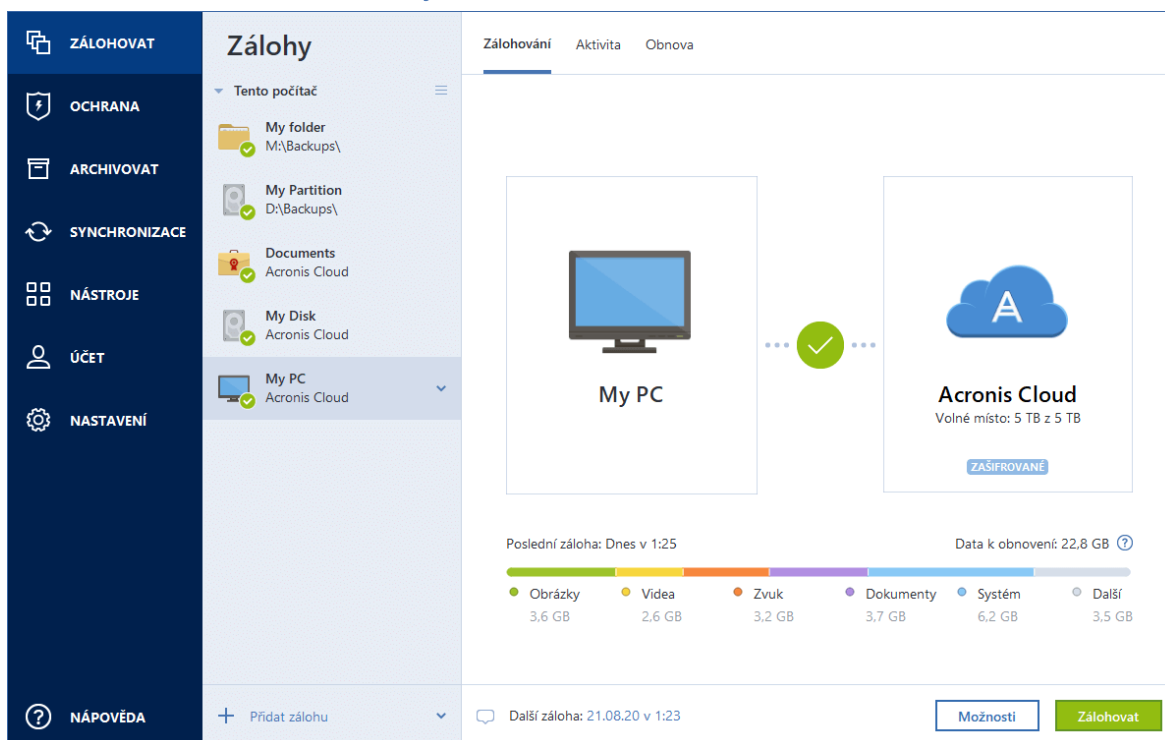
Můžete také obnovit konkrétní soubory a složky ze zálohy celého počítače. Další informace naleznete v části [Zálohování souborů a složek](#).

Pokud záloha celého počítače obsahuje dynamické disky, obnovte data v režimu oddílů. To znamená, že můžete vybrat oddíly k obnovení a změnit cílové umístění obnovení. Další informace naleznete v části [Obnova dynamických/GPT disků a svazků](#).

### **Vytvoření zálohy celého počítače**

1. Spustit Acronis Cyber Protect Home Office
2. Na bočním panelu klikněte na možnost **Záloha**.
3. Klikněte na znaménko plus ve spodní části seznamu zálohování.
4. Klikněte na ikonu **Zdroj zálohování** a pak vyberte položku **Celý počítač**.
5. Klikněte na ikonu **Cílové umístění zálohy** a pak vyberte cílové umístění pro zálohu.

Doporučujeme zálohovat počítač do úložiště Acronis Cloud nebo na místní nebo síťové úložiště. Další informace naleznete v části [Výběr místa k ukládání záloh](#).



- [volitelný krok] Kliknutím na možnost **Možnosti** můžete nastavit možnosti zálohy. Další informace naleznete v části [Možnosti zálohování](#).
- Klikněte na tlačítko **Zálohovat nyní**.

### Poznámka

Pokud zálohujete data do služby Acronis Cloud, dokončení prvního zálohování může trvat poměrně dlouho. Další zálohování již budou mnohem rychlejší, protože se budou přes internet přenášet pouze změny souborů.

Dále se povídejte na video s pokyny v angličtině na adrese <https://goo.gl/KjW5sM>.

## 2.4 Vytvoření sady Acronis Survival Kit

Chcete-li obnovit počítač v případě selhání, potřebujete dvě klíčové součásti – zálohu systémového disku a spouštěcí médium Acronis. Tyto dvě součásti jsou nejčastěji oddělené, systémová záloha je například uložena na externím disku nebo v úložišti Acronis Cloud a spouštěcí médium je malý USB flash disk. Sada Acronis Survival Kit kombinuje obě tyto součásti, a vy tak můžete mít jediné zařízení, které obsahuje vše potřebné k obnovení počítače v případě selhání. Jedná se o externí pevný disk, který obsahuje soubory spouštěcího média Acronis a zálohu systémového diskového oddílu, celého počítače nebo jakoukoli zálohu disku. Navíc záloha vašich dat může být použita jako běžná záloha: Může obsahovat jakákoli data, která musíte zabezpečit, můžete nastavit [Plánování](#) a aktualizovat ji jako běžnou zálohu. Externí pevný disk navíc není výlučně zablokován sadou Acronis Survival Kit, jeho spouštěcí média zabírají pouze 2 GB místa na disku a zbývající místo může být sdíleno se

systémovým diskovým oddílem nebo celou zálohou počítače, která je součástí sady Acronis Survival Kit, a s dalšími daty včetně dalších záloh, vašich osobních dat, fotografií atd. Na externím pevném disku nechte však pouze sadu Acronis Survival Kit.

Bez ohledu na to, kolik záloh je na externím pevném disku uloženo, je k obnovení počítače nutná pouze sada Acronis Survival Kit. Její součást spouštěcího média funguje s jakýmkoli systémovým oddílem nebo celou zálohou počítače, pokud jsou obě tyto položky vytvořeny pro stejný počítač nebo počítače se stejnou konfigurací.

Pro sadu Acronis Survival Kit můžete jako zařízení použít:

- **externí pevný disk**

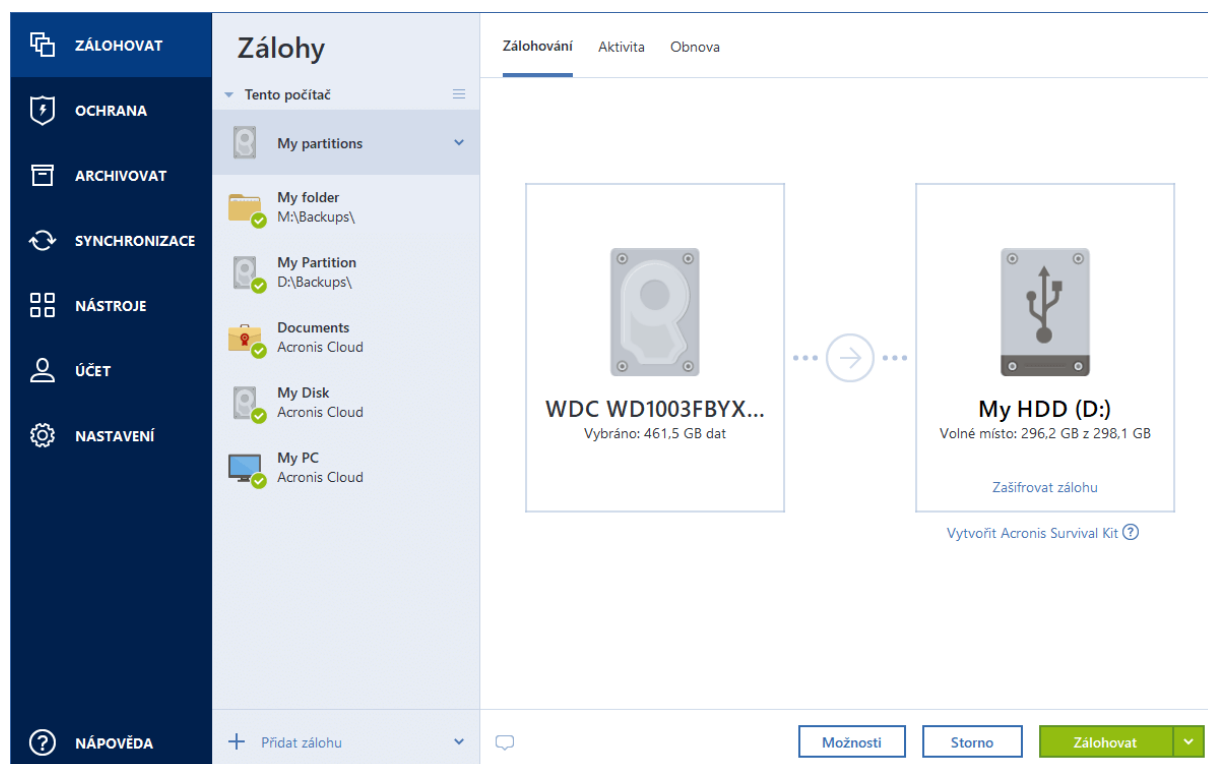
Měl by být větší než 32 GB a mít systém souborů NTFS, FAT32 či exFAT. Pokud má disk jiný souborový systém, aplikace Acronis Cyber Protect Home Office navrhne jeho zformátování.

- **USB flash disk**

Měl by to být flash disk MBR o minimální velikosti 32 GB. Pokud používáte flash disk GPT, Acronis Cyber Protect Home Office navrhne zformátování disku na MBR. Poznámka: Flash disky jsou podporovány pouze v systémech Windows 10 (sestavení 1703 a novější) a Windows 11.

### ***Jak vytvořit sadu Acronis Survival Kit***

Pokud konfigurujete zálohu systémového diskového oddílu, celého počítače nebo libovolného disku a jako cíl vyberete externí pevný disk, aplikace Acronis Cyber Protect Home Office navrhne vytvoření sady Acronis Survival Kit.



1. Klikněte na možnost **Zálohovat nyní** nebo **Vytvořit sadu Acronis Survival Kit**.
2. V otevřeném okně klikněte na příkaz **Vytvořit**.

Aplikace Acronis Cyber Protect Home Office vytvoří na vybraném disku malý oddíl a zapíše do něj spouštěcí soubory. Za účelem jeho vytvoření se změní velikost stávajících svazků. Pokud disk není typu GPT a má jiný souborový systém než NTFS, FAT32 nebo exFAT, aplikace Acronis Cyber Protect Home Office navrhne jeho zformátování. Upozorňujeme, že se při formátování disku odstraní veškerá data, která jsou na něm uložena.

3. Po úspěšném zapsání spouštěcích souborů se z disku stane spouštěcí médium Acronis, které lze použít k obnovení počítače. K dokončení vytvoření sady Acronis Survival Kit je nutné uložit zálohu systémového diskového oddílu, celého počítače nebo libovolného disku na tento disk. Chcete-li to provést, klikněte na tlačítko **Zálohovat**. Pokud tento krok přeskočíte, nezapomeňte si vytvořit zálohu na tomto disku později. Další informace naleznete v části [Zálohování disků a diskových oddílů](#).

Jakmile bude sada Acronis Survival Kit připravena, můžete ji použít k obnovení počítače. Další informace naleznete v části [Obnovení systému na stejný disk](#).

Při každé konfiguraci zálohy na externím zařízení, které obsahuje sadu Survival Kit, aplikace Acronis Cyber Protect Home Office zkontroluje její verzi. Pokud je k dispozici aktuální verze sady Survival Kit, aplikace Acronis Cyber Protect Home Office navrhne aktualizaci sady Survival Kit ve vašem externím zařízení.

## 2.5 Zálohování souborů

Chcete-li chránit soubory, jako jsou dokumenty, fotografie, hudební soubory a video soubory, není nutné zálohovat celý diskový oddíl obsahující tyto soubory. Můžete zálohovat konkrétní soubory a složky a ukládat je do následujících typů úložiště:

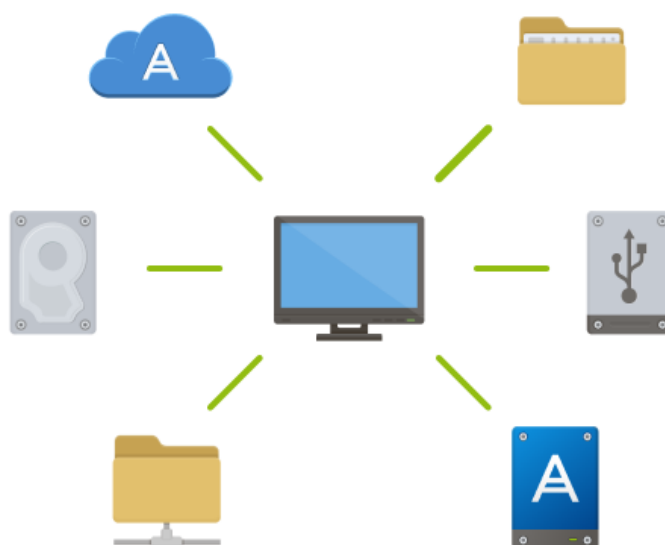
- **Místní nebo síťové úložiště**

Tato možnost je rychlá a jednoduchá. Použijte ji pro ochranu souborů, které se mění jen výjimečně.

- **Acronis Cloud**

Tato možnost je spolehlivá. Použijte ji pro ochranu důležitých souborů a souborů, které chcete sdílet v různých zařízeních nebo s dalšími osobami.

Chcete-li používat úložiště služby Acronis Cloud je nutné mít účet Acronis a předplacenou službu Acronis Cloud. Další informace naleznete v části "Informace o předplatném" (str. 34).



### **Zálohování souborů a složek**

1. Spustit Acronis Cyber Protect Home Office
2. Na bočním panelu klikněte na možnost **Záloha**.
3. Klikněte na ikonu **Zdroj zálohy** a poté vyberte možnost **Soubory a složky**.
4. V zobrazeném okně zaškrtněte políčka vedle souborů a složek, které chcete zálohovat, a klikněte na tlačítko **OK**.
5. Klikněte na ikonu **Cíl zálohy** a poté vyberte cíl zálohování.
  - **Acronis Cloud** – přihlaste se ke svému účtu a klikněte na tlačítko **OK**.
  - **Váš externí disk**– Máte-li k počítači připojený externí disk, můžete ho vybrat ze seznamu.
  - **NAS**– Ze seznamu nalezených zařízení NAS vyberte požadované zařízení NAS. Pokud máte pouze jedno zařízení NAS, aplikace Acronis Cyber Protect Home Office jej navrhne použít jako výchozí cílové umístění zálohování.
  - **Procházet**– Vyberte cílové umístění ze stromu složek.
6. Klikněte na tlačítko **Zálohovat nyní**.

Další informace naleznete v části [Zálohování souborů a složek](#).

Dále se povídejte na video s pokyny v angličtině na adrese <https://goo.gl/i4j1AN>.

## 2.6 Klonování pevného disku

### 2.6.1 Proč tuto funkci potřebuji?

Zjistíte-li, že volné místo na pevném disku není pro vaše data dostatečné, můžete chtít zakoupit nový, větší pevný disk a přenést všechna vaše data na nový disk. Obvyklé operace kopírování nezajistí, že nový pevný disk bude identický se starým diskem. Otevřete-li například Průzkumník

souborů a zkopírujete všechny soubory a složky na nový pevný disk, systém Windows se z nového pevného disku nespustí. Nástroj klonování disků umožňuje duplikovat všechna data a vytvořit na novém pevném disku spustitelný oddíl systému Windows.



## 2.6.2 Před spuštěním

Doporučujeme nainstalovat cílový (nový) disk tam, kde jej chcete používat, a zdrojový disk do jiného umístění, například do externího USB úložiště. To je důležité především u přenosných počítačů.

---

### Poznámka

Doporučujeme, aby původní i nový pevný disk pracovaly ve stejném režimu řadiče (například IDE nebo AHCI). Jinak se počítač z nového pevného disku nemusí spustit.

---

## 2.6.3 Klonování disku

1. V bočním panelu klikněte na možnost **Nástroje** a pak na možnost **Klonovat disk**.
2. V kroku **Režim klonování** doporučujeme vybrat režim **automatického** přenosu. V takovém případě bude velikost oddílů změněna, aby odpovídala novému pevnému disku. Režim **Ruční** poskytuje více možností. Další informace o ručním režimu naleznete v [průvodci nástroje Klonování disku](#).

---

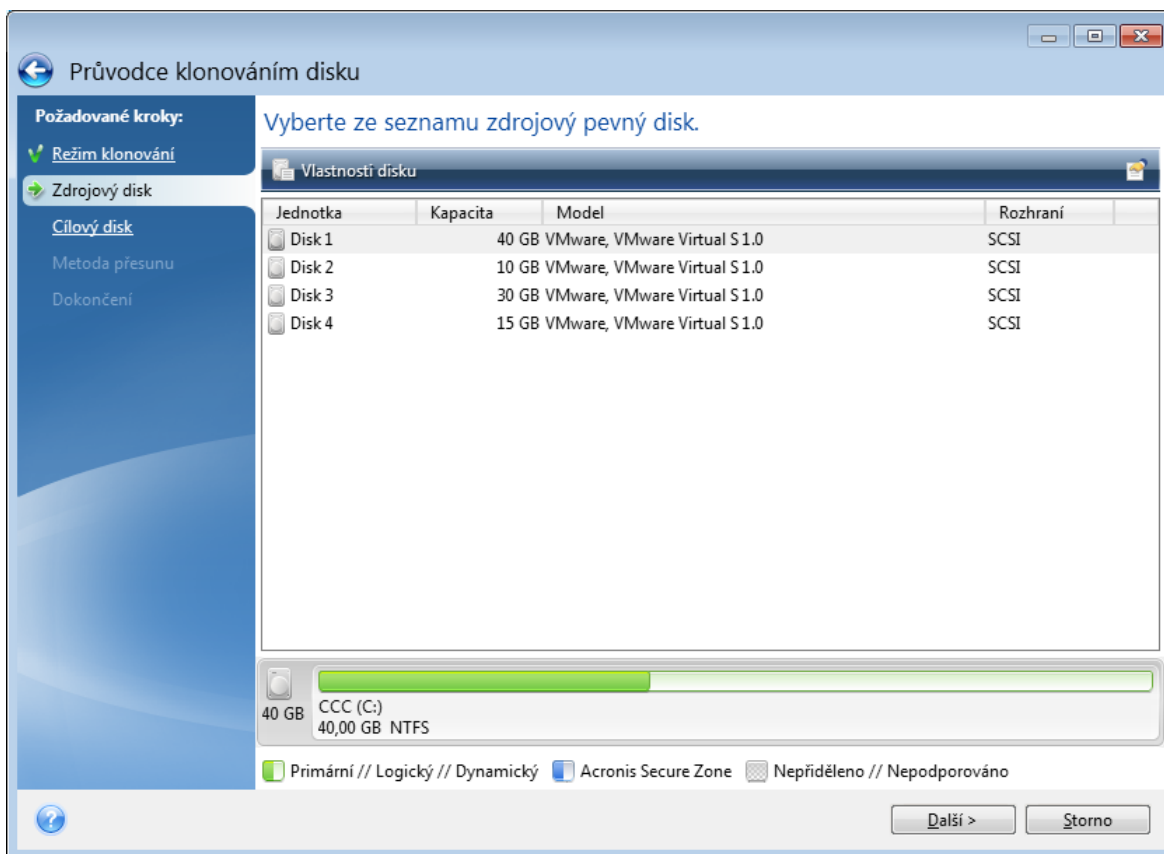
### Poznámka

Pokud aplikace najde dva disky, z nichž jeden je rozdělený na diskové oddíly a druhý ne, automaticky rozpozná jako zdrojový disk ten disk, který je rozdělen na diskové oddíly, a nerozdělený disk jako cílový disk. V takovém případě budou další kroky přeskočeny a zobrazí se obrazovka souhrnu klonování.

---

3. V kroku **Zdrojový disk** vyberte disk, který chcete klonovat.





4. V kroku **Cílový disk** vyberte cílový disk pro klonovaná data.

#### Poznámka

Pokud některý z disků neobsahuje žádný diskový oddíl, aplikace jej automaticky rozpozná jako cílový a tento krok přeskočí.

5. V kroku **Dokončit** ověřte, zda nakonfigurovaná nastavení odpovídají vašim potřebám a pak klikněte na tlačítko **Pokračovat**.

Ve výchozím nastavení aplikace Acronis Cyber Protect Home Office po dokončení procesu klonování vypne počítač. To umožní změnu nadřazených/podřazených přepínačů a odstranění jednoho z disků.

Dále se povídejte na video s pokyny v angličtině na adrese <https://goo.gl/bjWRLl>.

## 2.7 Obnovení počítače

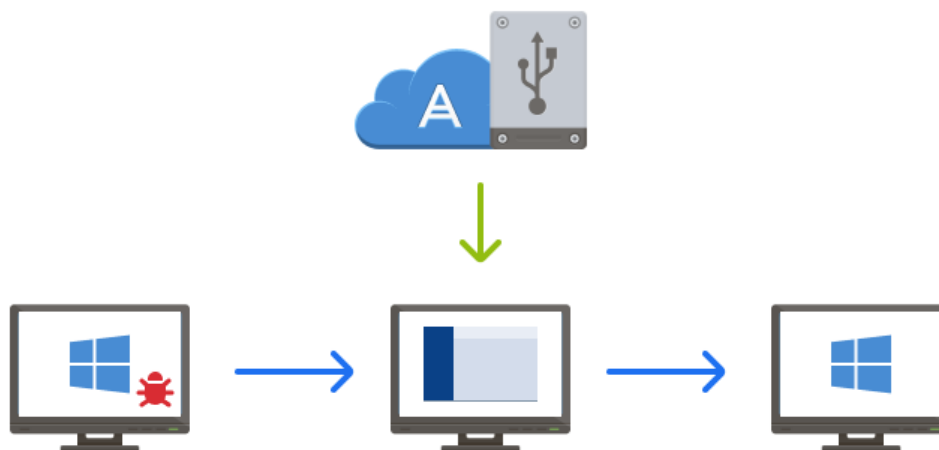
Mějte na paměti, že obnovení systémového disku je důležitá operace. Než začnete, doporučujeme vám pročíst si podrobné popisy v následujících tématech nápovědy:

- [Určování příčin havárie](#)
- [Příprava na obnovení](#)
- [Obnovení systému na stejný disk](#)

Uvažujme nyní o dvou různých případech:

1. Systém Windows nepracuje správně, ale aplikaci Acronis Cyber Protect Home Office můžete spustit.
2. Nelze spustit systém Windows (například spustíte počítač a na obrazovce se zobrazí něco neobvyklého).

**Případ 1: Jak obnovit počítač, když systém Windows nepracuje správně?**



1. Spustit Acronis Cyber Protect Home Office
2. Na bočním panelu klikněte na možnost **Záloha**.
3. Na seznamu záloh vyberte zálohu obsahující váš systémový disk. Zálohu lze vyhledat v místním nebo síťovém úložišti či v úložišti Acronis Cloud.
4. V pravém panelu klikněte na tlačítko **Obnova**.
5. V závislosti na typu zálohy klikněte na tlačítko **Obnovit počítač** nebo **Obnovit disky**.
6. V zobrazeném okně vyberte verzi zálohy (stav dat z konkrétního data a času).
7. Vyberte systémový diskový oddíl a diskový oddíl vyhrazený systému (pokud nějaký je), které mají být obnoveny.
8. Klikněte na možnost **Obnovit**.

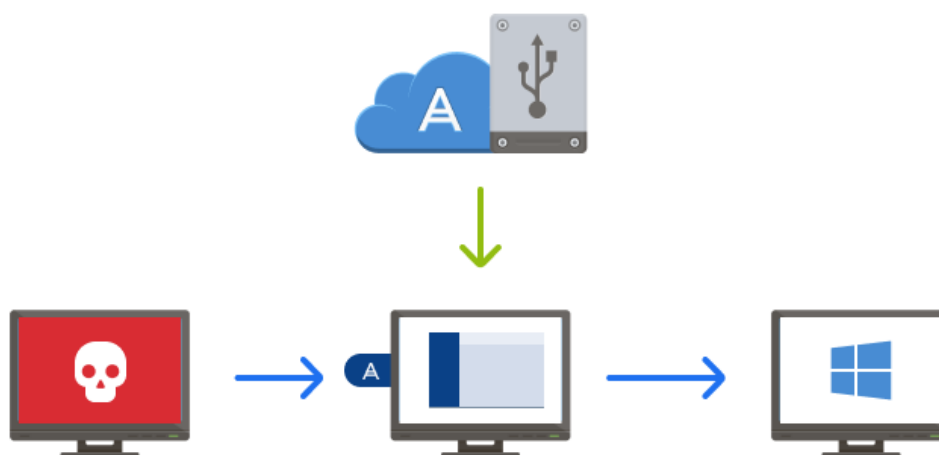
---

**Poznámka**

Pro dokončení operace musí aplikace Acronis Cyber Protect Home Office restartovat systém.

---

**Případ 2: Jak obnovit počítač, když systém Windows nelze spustit?**



1. Připojte k počítači spouštěcí médium aplikace Acronis a spusťte zvláštní samostatnou verzi aplikace Acronis Cyber Protect Home Office.  
Podrobnosti naleznete v části [Krok 2: Tvorba spouštěcího média Acronis a Uspořádání pořadí spouštění v systému BIOS](#).
2. Na uvítací obrazovce vyberte možnost **Moje disky** pod položkou **Obnovit**.
3. Vyberte zálohu systémového disku, který se má obnovit. Klikněte pravým tlačítkem myši a vyberte příkaz **Zálohovat**.  
Pokud se záloha nezobrazí, klikněte na tlačítko **Procházet** a zadejte cestu k záloze ručně. Ve stejném okně se můžete připojit k úložišti Acronis Cloud a vybrat online zálohování. Další informace naleznete v části [Obnova systému z úložiště Acronis Cloud](#).
4. V kroku **Metoda obnovy** vyberte možnost **Obnovit celé disky a oddíly**.
5. Vyberte systémový diskový oddíl (obvykle C) v okně **Co bude obnoveno**. Nezapomeňte, že můžete diskový oddíl označit vlaječkami Pri, Act. Dále vyberte diskový oddíl vyhrazený systému (pokud nějaký je).
6. Můžete nechat všechna nastavení oddílů beze změn a kliknout na možnost **Dokončit**.
7. Zkontrolujte přehled operací a klikněte na možnost **Pokračovat**.
8. Po dokončení operace ukončete samostatnou verzi aplikace Acronis Cyber Protect Home Office, odeberte spouštěcí médium (pokud nějaké je) a spusťte systém z obnoveného systémového diskového oddílu. Zkontrolujte, zda jste obnovili systém Windows do potřebného stavu, a obnovte původní pořadí spouštění.

## 2.8 Účet Acronis

Účet Acronis potřebujete, pokud:

- Registrujete produkt Acronis.
- Zálohujete do úložiště Acronis Cloud.
- Synchronizujete data.
- Archivujete data.

### ***Jak vytvořit účet Acronis***

1. Na postranním panelu klikněte na tlačítko **Účet** a potom na tlačítko **Přihlásit nebo vytvořit účet**.
2. Klikněte na tlačítko **Vytvořit účet**.
3. Vyplňte registrační formulář. Poskytněte požadované informace, přijměte všeobecné podmínky a volitelně se přihlaste k příležitostnému odběru novinek a propagačních nabídek.

---

#### **Poznámka**

Chcete-li zajistit bezpečnost dat, zvolte pro online zálohy dostatečně silné heslo, zajistěte, aby se nedostalo do nepovolaných rukou, a občas je změňte.

---

4. Klikněte na tlačítko **Vytvořit účet**.
5. Na vámi zadanou adresu bude odeslána e-mailová zpráva. Tuto zprávu otevřete a potvrďte své přání vytvořit účet.

### ***Přihlášení pomocí účtu Acronis***

1. Na postranním panelu klikněte na tlačítko **Účet** a potom na tlačítko **Přihlásit nebo vytvořit účet**.
2. Zadejte registrační e-mailovou adresu a pak klikněte na tlačítko **Přihlásit**.

### ***Chcete-li se odhlásit z účtu Acronis:***

1. Na bočním panelu klikněte na možnost **Účet**.
2. Klikněte na e-mailovou adresu a pak vyberte možnost **Odhlásit**.

## 2.9 Začínáme s úložištěm Acronis Cloud

---

### **Poznámka**

Aplikace Acronis Cloud nemusí být ve vaší oblasti dostupná. Další informace naleznete na adrese: <https://kb.acronis.com/content/4541>

---

### 2.9.1 Vzdálené úložiště

Na jedné straně je služba Acronis Cloud bezpečné vzdálené úložiště, ve kterém můžete ukládat:

- Zálohy souborů a složek
- Zálohy diskových oddílů a disků

- Verze synchronizovaných souborů a složek

Protože jsou soubory uloženy ve vzdáleném úložišti, jsou chráněny i v případě, že počítač někdo ukradne nebo vám shoří dům. V případě havárie nebo poškození dat můžete obnovit soubory a dokonce i celý obsah počítače.

S pomocí jednoho účtu můžete ukládat data z několika počítačů a všech mobilních zařízení s operačním systémem iOS nebo Android.

Abyste mohli začít používat službu Acronis Cloud, je třeba si tuto službu předplatit. Další informace naleznete v části [Informace o předplatném](#).

## 2.9.2 Webová aplikace

Na druhé straně je služba Acronis Cloud webová aplikace, která umožňuje obnovu a správu dat uložených ve službě Acronis Cloud. S touto aplikací můžete pracovat na jakémkoli počítači připojeném k internetu.

Chcete-li otevřít aplikaci, přejděte na web <https://www.acronis.com/my/online-backup/webrestore/> a pak se přihlaste do svého účtu Acronis.

## 2.9.3 Jak zajišťujeme bezpečnost vašich dat

Když používáte službu Acronis Cloud jako úložiště, chcete si být jisti, že se vaše osobní data nedostanou do nesprávných rukou. Můžete se obávat obzvláště o bezpečnost vašich mobilních zařízení, protože všechna vaše data jsou přenášena přes internet.

Můžeme vás ujistit, že vaše data zůstanou v bezpečí. V první řadě používáme k přenosu všech dat přes internet a sítě LAN šifrované protokoly (SSL, TLS). Chcete-li získat přístup k datům, přihlaste se k vašemu účtu pomocí e-mailové adresy a hesla pro daný účet. Za druhé můžete pro zálohování svých dat použít pouze chráněné sítě Wi-Fi. V tomto případě jsou vaše data při přenosu do úložiště Acronis Cloud zcela zabezpečena. V položce Nastavení vyberte zabezpečenou možnost [Sítě Wi-Fi pro zálohování](#).

## 2.9.4 Informace o předplatném

Funkce aplikace Acronis Cyber Protect Home Office, které využívají úložiště Acronis Cloud (například online zálohování, archivace v cloudu nebo synchronizace cloudu), vyžadují předplatné úložiště Acronis Cloud. Chcete-li se přihlásit k odběru, spusťte aplikaci Acronis Cyber Protect Home Office, přejděte na kartu **Účet** a pak vyberte, zda chcete spustit zkušební předplatné nebo jej zakoupit.

---

### Poznámka

Upozorňujeme, že na úložiště Acronis Cloud se vztahují naše zásady spravedlivého využívání. Další podrobnosti naleznete na adrese <https://kb.acronis.com/ati/fairusage>.

---

### Zkušební verze

Když aktivujete zkušební verzi produktu, vašemu účtu je automaticky přiřazeno úložiště o velikosti 1 000 GB a bezplatné předplatné služby Acronis Cloud na zkušební dobu Acronis Cyber Protect Home Office. Další informace naleznete v části [Informace o zkušební verzi](#).

### ***Plná verze***

Plné předplatné služby Acronis Cloud lze zakoupit v části **Účet** vaší verze aplikace Acronis Cyber Protect Home Office nebo na webových stránkách společnosti Acronis. Podrobnosti naleznete v části [Upgrade aplikace Acronis Cyber Protect Home Office](#).

## 3 Základní pojmy

Toto téma obsahuje obecné informace o základních koncepcích, které mohou pomoci pochopit, jak aplikace funguje.

### **Zálohování a obnova**

**Při zálohování** jsou vytvořeny kopie dat, aby je bylo možné použít k **obnovení** původních dat po jejich ztrátě.

Zálohy jsou vhodné především ke dvěma účelům:

- K obnovení operačního systému, pokud je poškozený nebo nelze spustit (nazývá se zotavení po havárii). Další informace o ochraně počítače před poruchou naleznete v tématu [Ochrana systému](#).
- K obnovení konkrétních souborů a složek, které byly nechtěně odstraněny nebo poškozeny.

Aplikace Acronis Cyber Protect Home Office umožňuje používat obě varianty pomocí tvorby diskových obrazů (nebo diskových oddílů) a záloh na úrovni souborů.

Metody obnovení:

- **Úplné obnovení** lze provést do původního nebo nového umístění. V případě výběru původního umístění budou data v daném umístění zcela přepsána daty ze zálohy. V případě nového umístění se data pouze zkopírují ze zálohy do nového umístění.
- **Přírůstkové obnovení** se provádí pouze do původního umístění a pouze ze zálohy v cloudu. Před zahájením obnovení se soubory v původním umístění porovnávají se soubory v záloze podle atributů souboru, například velikosti souboru a data poslední úpravy. Soubory, které se neshodují, jsou označeny k obnovení. Zbývající soubory budou během obnovení přeskočeny. Tímto způsobem obnoví aplikace Acronis Cyber Protect Home Office, na rozdíl od úplného obnovení, pouze změněné soubory. Tato metoda významně zkracuje dobu obnovení a šetří přenosy přes internet při obnovení z úložiště Acronis Cloud.

### **Verze záloh**

Verze záloh jsou soubory vytvořené během operací zálohování. Počet vytvořených verzí se rovná počtu spuštění zálohy. Verze tedy představuje bod v čase, do kterého lze systém nebo data obnovit.

Verze záloh představují plné, přírůstkové a rozdílové zálohy – viz téma [Plné, přírůstkové a rozdílové zálohy](#).

Verze záloh jsou podobné verzím souborů. Koncepce verzí souborů je známá uživatelům systému Windows, kteří používají funkci „Předchozí verze souborů“. Tato funkce umožňuje obnovit soubor z určitého data a času. Verze zálohy umožňuje obnovit data podobným způsobem.

### **Klonování disku**

Tato operace kopíruje veškerý obsah jednoho pevného disku na jiný. To může být užitečné například, když budete chtít naklonovat operační systém, aplikace a data na nový disk s větší kapacitou. To lze provést dvěma způsoby:

- Použijte nástroj Klonování disku.
- Zálohujte původní pevný disk a pak zálohu obnovte na nový.

### **Formát souboru zálohy**

Aplikace Acronis Cyber Protect Home Office obvykle ukládá data zálohy v proprietárním komprimovaném formátu TIB. Data ze záloh v souborech TIB lze obnovit pouze pomocí produktů Acronis Cyber Protect Home Office v systému Windows nebo v prostředí obnovy.

Nonstop zálohování Acronis používá zvláštní skryté úložiště dat i metadat. Zálohovaná data jsou komprimována a rozdělena na soubory o velikosti přibližně 1 GB. Tyto soubory jsou rovněž v proprietárním formátu a data z nich mohou být obnovena pouze pomocí aplikace Acronis Cyber Protect Home Office.

### **Ověření zálohy**

Funkce ověření zálohy umožňuje zjistit, zda je možné data obnovit. Aplikace přidává k zálohovaným blokům dat hodnoty kontrolních součtů. Během ověření zálohy aplikace Acronis Cyber Protect Home Office otevře soubor zálohy, vypočítá znovu hodnoty kontrolních součtů a porovná je s uloženými hodnotami. Pokud se všechny porovnávané hodnoty shodují, soubor zálohy není poškozen.

### **Plánování**

Aby byly zálohy opravdu užitečné, je třeba udržovat je co nejvíce aktuální. Naplánujte automatické pravidelné zálohování.

### **Odstranění záloh**

Když chcete odstranit zálohy a verze záloh, které již nepotřebujete, použijte k tomu nástroje aplikace Acronis Cyber Protect Home Office. Další informace naleznete v části [Odstraňování záloh a verzí záloh](#).

Aplikace Acronis Cyber Protect Home Office ukládá informace o zálohách v databázi metadat. Odstraněním nepotřebných souborů záloh v Průzkumníku souborů se tedy neodstraní informace o těchto zálohách z databáze. To způsobí chybu, když se aplikace pokusí provádět operace s neexistujícími zálohami.

## **3.1 Rozdíl mezi zálohami souborů a obrazy disků nebo diskových oddílů**

Při zálohování souborů a složek jsou komprimovány a uloženy pouze soubory a strom složek.

Zálohy disků nebo oddílů se liší od záloh souborů a složek. Aplikace Acronis Cyber Protect Home Office uloží přesný snímek disku nebo oddílu. Tento proces se nazývá vytvoření diskového obrazu nebo vytvoření diskové zálohy a výsledná záloha se často nazývá obraz disku / diskového oddílu nebo záloha disku / diskového oddílu.



### 3.1.1 Co obsahuje záloha disku nebo diskového oddílu?

Záloha disku / diskového oddílu obsahuje všechna data uložená na disku či v oddílu:

1. Nultou stopu pevného disku se záznamem MBR (platí pouze pro zálohy disků MBR).
2. Jeden nebo více diskových oddílů včetně:
  - a. Spouštěcího kódu,
  - b. metadat systému souborů včetně servisních souborů, alokační tabulky souborů (FAT) a spouštěcího záznamu diskového oddílu,
  - c. dat systému souborů, včetně operačního systému (systémové soubory, registry, ovladače), uživatelských dat a softwarových aplikací,
3. oddílu rezervovaného systémem (je-li přítomen),
4. systémového oddílu EFI (je-li přítomen) (platí pouze pro zálohy disků GPT).

### 3.1.2 Co je vyloučeno ze záloh disku?

V zájmu zmenšení velikosti obrazu a zrychlení jeho tvorby ukládá aplikace Acronis Cyber Protect Home Office ve výchozím nastavení pouze sektory pevného disku, které obsahují data.

Následující soubory aplikace Acronis Cyber Protect Home Office ze zálohy disku vyloučí:

- pagefile.sys
- hiberfil.sys (tedy soubor, který uchovává obsah paměti RAM při přechodu počítače do režimu spánku)

Výchozí způsob můžete změnit zapnutím režimu sektor po sektoru. V takovém případě zkopíruje aplikace Acronis Cyber Protect Home Office všechny sektory pevného disku, a nikoli pouze ty, které obsahují data.

Při zálohování systémového diskového oddílu nebo disku do úložiště Acronis Cloud navíc aplikace Acronis Cyber Protect Home Office vyloučí následující data:

- Složky Temp, obvyklé umístění:
  - C:\Windows\Temp\
  - C:\Users\\AppData\Local\Temp
- Složku System Volume Information (obvyklé umístění C:\System Volume Information\)
- Koš
- Dočasná data webového prohlížeče:
  - Dočasné soubory internetu
  - Soubory cookie
  - Historii
  - Mezipaměť

- Soubory TIB a TIBX
- Soubory TMP
- Soubory ~

## 3.2 Plné, přírůstkové a rozdílové zálohy

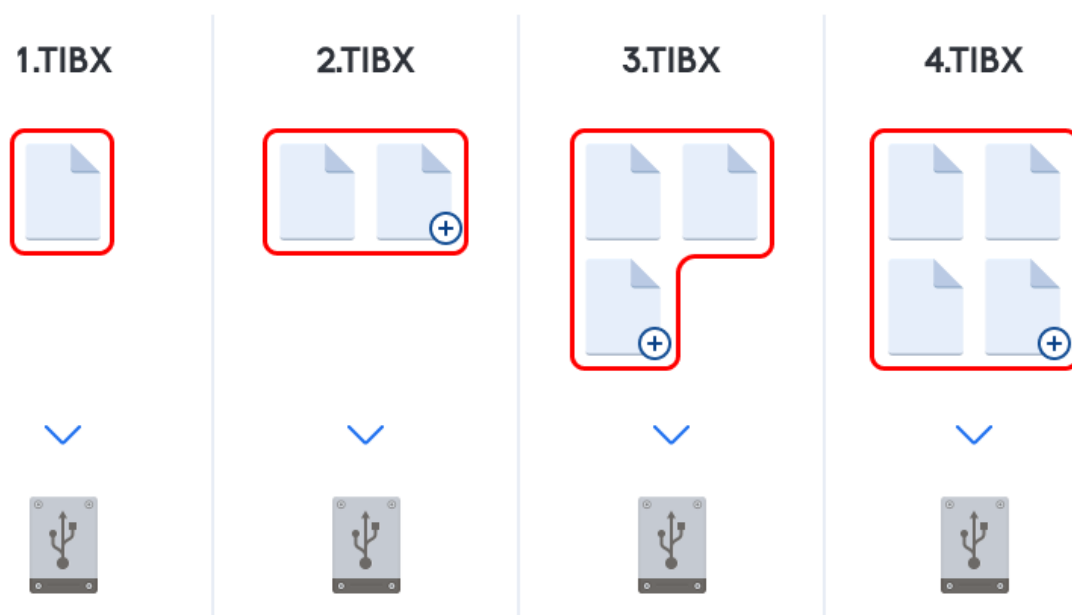
Aplikace Acronis Cyber Protect Home Office nabízí tři metody zálohování: plné, přírůstkové a rozdílové.

### 3.2.1 Plná metoda

Výsledek plné metody zálohování (označuje se také jako plná verze zálohy) obsahuje všechna data ve chvíli vytvoření zálohy.

**Příklad:** Každý den napíšete jednu stránku dokumentu a zálohujete ji pomocí úplné metody. Acronis Cyber Protect Home Office uloží celý dokument při každém spuštění zálohování.

1.tibx, 2.tibx, 3.tibx, 4.tibx – soubory plné verze zálohy.



#### Další informace

Plná verze zálohy vytváří výchozí zálohu pro další přírůstkové nebo rozdílové zálohy. Také ji lze použít jako samostatnou zálohu. Samostatná plná záloha může být optimální řešením v případě, že často vracíte systém do počátečního stavu nebo když nechcete spravovat více verzí zálohy.

**Obnova:** V příkladu výše je k obnovení celé práce ze souboru 4.tibx potřeba pouze jedna verze zálohy – 4.tib.

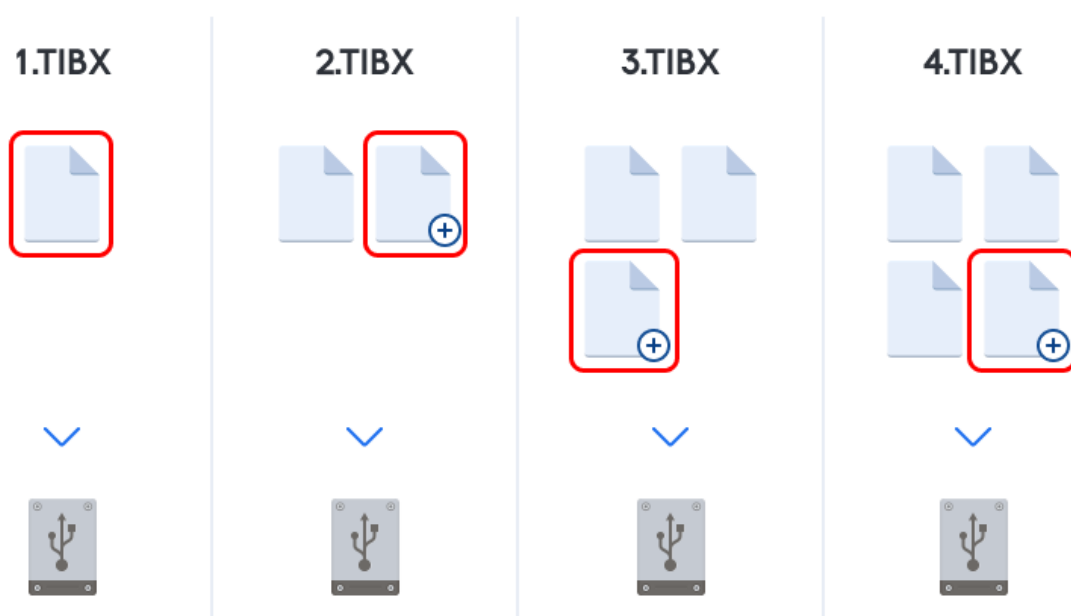
## 3.2.2 Přírůstková metoda

Výsledek přírůstkové metody zálohování (označuje se také jako přírůstková verze zálohy) obsahuje pouze ty soubory, které se od POSLEDNÍ ZÁLOHY změnily.

**Příklad:** Každý den napíšete jednu stránku dokumentu a zálohujete ji pomocí přírůstkové metody. Acronis Cyber Protect Home Office uloží novou stránku při každém spuštění zálohování.

**Poznámka:** První verze zálohy, kterou vytvoříte, vždy využívá plnou metodu.

- 1.tibx – soubor plné verze zálohy.
- 2.tibx, 3.tibx, 4.tibx – soubory přírůstkových verzí zálohy.



### Další informace

Přírůstková metoda je nejvhodnější v případě, že potřebujete často zálohovat a mít možnost vrátit se do určitého bodu v čase. Přírůstkové verze zálohy jsou obecně mnohem menší než plné nebo rozdílové verze. Naproti tomu přírůstkové verze vyžadují od aplikace více práce na zajištění obnovení.

**Obnova:** Na příkladu výše jsou k obnovení celé práce ze souboru 4.tibx potřeba všechny verze zálohy – 1.tibx, 2.tibx, 3.tibx a 4.tibx. Pokud se tedy přírůstková verze zálohy ztratí nebo poškodí, žádná další přírůstková záloha nebude použitelná.

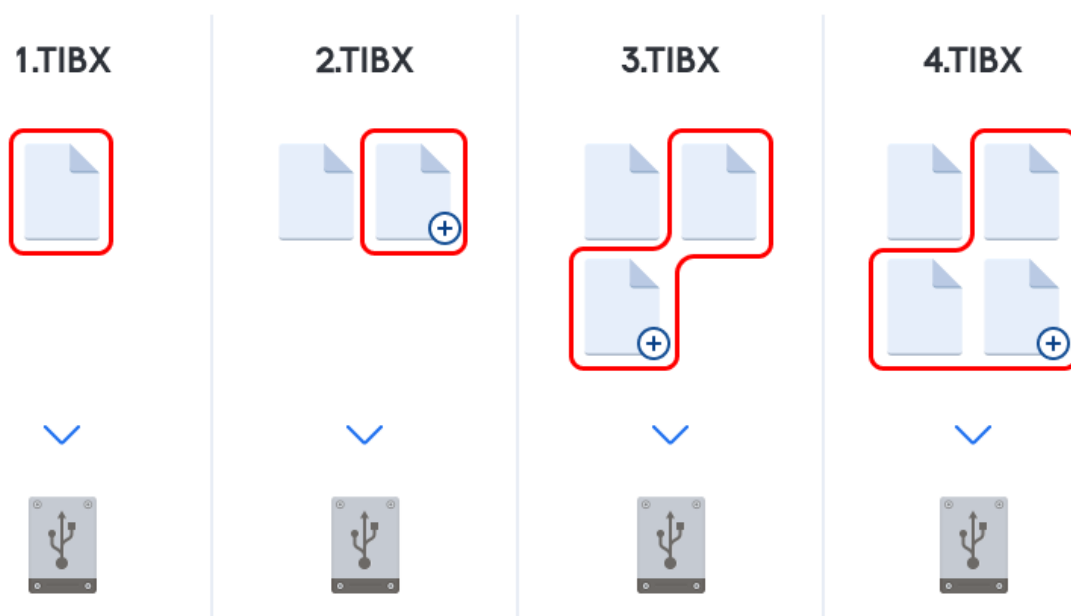
## 3.2.3 Rozdílová metoda

Výsledek rozdílové metody zálohování (označuje se také jako rozdílová verze zálohy) obsahuje pouze ty soubory, které se změnily od POSLEDNÍ PLNÉ ZÁLOHY.

**Příklad:** Každý den napíšete jednu stránku dokumentu a zálohujete ji pomocí rozdílové metody. Acronis Cyber Protect Home Office uloží celý dokument kromě první stránky uložené ve verzi plné zálohy.

**Poznámka:** První verze zálohy, kterou vytvoříte, vždy využívá plnou metodu.

- 1.tibx – soubor plné verze zálohy.
- 2.tibx, 3.tibx, 4.tibx – soubory rozdílových verzí zálohy.



### Další informace

Rozdílová metoda je mezikrokem mezi těmito dvěma přístupy. Trvá kratší dobu a zabírá méně místa než „Plná“, ale více než „Přírůstková“. K obnovení dat z rozdílové verze zálohy aplikace Acronis Cyber Protect Home Office potřebuje pouze rozdílovou verzi a poslední plnou verzi zálohy. Naproti tomu obnovení z rozdílové verze je jednodušší a spolehlivější než obnovení z přírůstkové verze.

**Obnova:** Na příkladu výše jsou k obnovení celé práce ze souboru 4.tibx potřeba dvě verze zálohy – 1.tibx a 4.tibx.

Chcete-li si přizpůsobit metodu zálohování, je obvykle třeba nakonfigurovat vlastní schéma zálohování. Další informace naleznete v tématu [Vlastní schémata](#).

---

### Poznámka

Přírůstková nebo rozdílová záloha vytvořená po defragmentaci disku může být podstatně větší než obvykle. Je to způsobeno tím, že defragmentační program změní umístění souborů na disku a tyto změny se odrazí v záloze. Proto je po defragmentaci disku doporučeno znovu vytvořit plnou zálohu.

---

### 3.2.4 Sledování změněných bloků (CBT)

Technologie CBT zrychluje zálohování, protože vytváří místní přírůstkové nebo rozdílové verze záloh na úrovni disku. Změny obsahu disku jsou neustále sledovány na úrovni bloků. Při spuštění zálohování lze změny okamžitě uložit do zálohy.

## 3.3 Výběr místa k ukládání záloh

Aplikace Acronis Cyber Protect Home Office podporuje mnoho úložných zařízení. Další informace naleznete v dokumentu "Podporovaná úložná média" (str. 14).

V následující tabulce jsou zobrazena možná cílová umístění pro vaše data.

	<b>Pevný disk*</b>	<b>SSD*</b>	<b>USB flash disk</b>	<b>Acronis Cloud</b>	<b>Souborový server, NAS nebo NDAS</b>	<b>Sdílená síťová složka</b>	<b>SMB</b>	<b>FTP</b>	<b>DVD</b>	<b>Paměťová karta</b>
Diskové oddíly MBR nebo celé disky (HDD, SSD)	+	+	+	+	+	+	+	+	+	+
GPT či dynamické svazky nebo disky	+	+	+	+	+	+	+	+	+	+
Soubory a složky	+	+	+	+	+	+	+	+	+	+

\*Interní nebo externí.

Přestože je nejjednodušší možností zálohovat na místní pevný disk, doporučujeme ukládat zálohy na jiném místě, neboť to zvyšuje bezpečnost vašich dat.

#### **Doporučená úložná média:**

##### **1. Acronis Cloud**

##### **2. Externí disk**

Jestliže plánujete používat externí pevný disk USB se stolním počítačem, doporučujeme disk připojit k zadnímu konektoru krátkým kabelem.

##### **3. Domácí souborový server, NAS nebo NDAS**

Zkontrolujte, zda aplikace Acronis Cyber Protect Home Office vybrané úložiště záloh nalezne. Toto je třeba zkontrolovat jak ve Windows, tak i při spouštění ze spouštěcího média.

K získání přístupu k úložišti NDAS budete v mnoha případech muset zadat ID zařízení NDAS (20 znaků) a klíč k zápisu (pět znaků). Klíč k zápisu umožní použít zařízení NDAS v režimu umožňujícím zápis (například k ukládání záloh). ID zařízení NDAS a klíč k zápisu jsou obvykle vytištěny na štítku zezadu zařízení NDAS nebo uvnitř krytu. Pokud štítek nenaleznete, bude třeba kontaktovat prodejce zařízení NDAS a požádat o tyto informace.

#### 4. **Sdílená síťová složka**

Viz také: [Nastavení ověřování](#)

#### 5. **Server FTP**

Viz také: [Připojení FTP](#)

#### 6. **Optické disky (CD, DVD, BD)**

Prázdné optické disky, například DVD-R a DVD+R, jsou velmi levné, takže představují nejlevnější řešení pro zálohování dat, jsou však nejpomalejší.

Kvůli potřebě výměny médií doporučujeme vyhnout se zálohování na DVD, pokud je jejich počet větší než tři. Pokud neexistuje alternativa k zálohování na DVD, doporučujeme zkopírovat všechna DVD do složky na pevném disku a provést obnovení z této složky.

### 3.3.1 Příprava nového disku k zálohování

Nový interní nebo externí pevný disk nemusí být rozpoznán aplikací Acronis Cyber Protect Home Office. V takovém případě využijte nástroje operačního systému ke změně stavu disku na **Online** a pak disk inicializujte.

#### ***Postup změny stavu disku na Online***

1. Otevřete položku **Správa disků**. To provedete otevřením položky **Ovládací panely** -> **Systém a zabezpečení** -> **Nástroj pro správu**, spuštěním položky **Správa počítače** a pak kliknutím na položku **Správa disku**.
2. Vyhledejte disk označený jako **Offline**. Pravým tlačítkem klikněte na disk a potom na položku **Online**.
3. Stav disku se změní na **Online**. Následně budete moci disk inicializovat.

#### ***Inicializace disku***

1. Otevřete položku **Správa disků**. To provedete otevřením položky **Ovládací panely** -> **Systém a zabezpečení** -> **Nástroj pro správu**, spuštěním položky **Správa počítače** a pak kliknutím na položku **Správa disku**.
2. Vyhledejte disk označený jako **Neinicializováno**. Pravým tlačítkem klikněte na disk a potom na položku **Inicializovat disk**.
3. Vyberte tabulku diskových oddílů disku – MBR nebo GPT a pak klikněte na tlačítko **OK**.
4. [volitelný krok] Chcete-li vytvořit svazek na disku, klikněte pravým tlačítkem na disk, klikněte na položku **Nový jednoduchý svazek** a pak postupujte podle kroků průvodce a nakonfigurujte nový svazek. Chcete-li vytvořit další svazek, tento postup opakujte.

## 3.3.2 Připojení FTP

Aplikace Acronis Cyber Protect Home Office umožňuje zálohy ukládat na servery FTP.

Chcete-li vytvořit nové připojení FTP, při výběru umístění zálohy klikněte na možnost **Připojení FTP** a do otevřeného okna zadejte:

- cestu k serveru FTP, například: *my.server.com*;
- Port
- Uživatelské jméno
- Heslo

Nastavení zkontrolujte kliknutím na tlačítko **Testovat připojení**. Počítač se pokusí připojit k vybranému serveru FTP. Jestliže se naváže zkušební připojení, kliknutím na tlačítko **Připojit** připojení FTP přidejte.

Vytvořené FTP připojení se zobrazí ve stromu složek. Vyberte připojení a procházením vyberte umístění zálohy, které chcete použít.

---

### Poznámka

Nezapomeňte, že pouhým otevřením kořenové složky serveru FTP se nedostanete do domovského adresáře.

---

### Poznámka

Při obnově dat přímo ze serveru FTP nesmí záloha obsahovat soubory větší než 2 GB.

---

### Poznámka

Kvůli tomuto omezení aplikace Acronis Cyber Protect Home Office rozdělí během přímého zálohování na server FTP zálohu do souborů o velikosti 2 GB. Pokud provádíte zálohu na pevný disk a chcete ji později přenést na server FTP, je možné zálohu rozdělit do jednotlivých souborů o velikosti 2 GB nastavením požadované velikosti souborů v možnostech zálohy.

---

### Poznámka

Server FTP musí mít zapnutý pasivní režim přenosu souborů.

---

### Poznámka

Pro správnou funkci by měla být brána firewall zdrojového počítače nastavena tak, aby byly porty 20 a 21 otevřené pro protokoly TCP a UDP. Služba **Směrování a vzdálený přístup** ve Windows by měla být vypnuta.

---

## 3.3.3 Nastavení ověření

Při připojování k počítači v síti je ve většině případů třeba zadat potřebná pověření pro přístup ke sdílenému síťovému úložišti. To je například možné v případě, že vyberete úložiště zálohování. Okno **Nastavení ověřování** se zobrazí automaticky, vyberete-li název počítače v síti.

Je-li to třeba, zadejte uživatelské jméno a heslo a poté klikněte na tlačítko **Testovat připojení**. Když test úspěšně proběhne, klikněte na tlačítko **Připojit**.

## Odstraňování problémů

Když vytvoříte síťovou sdílenou složku, kterou plánujete využívat jako záložní úložiště, ověřte, zda je splněna alespoň jedna z následujících podmínek:

- Účet Windows obsahuje heslo v počítači, kde se nachází sdílená složka.
- Heslem chráněné sdílení je v systému Windows vypnuto.

Toto nastavení najdete v části **Ovládací panely**—> **Sít a internet**—> **Centrum síťových připojení a sdílení**—> **Pokročilé nastavení sdílení**—> Vypnout sdílení chráněné heslem.

V opačném případě se nebudete moci připojit ke sdílené složce.

## 3.4 Nonstop zálohování Acronis

Nonstop zálohování Acronis umožňuje snadnou ochranu vašich disků a souborů. Umožňuje obnovovat celé disky, jednotlivé soubory a jejich různé verze.

Hlavním účelem nonstop zálohování Acronis je souvislá ochrana dat (souborů, složek, kontaktů atd.), ale můžete ji také použít k ochraně diskových oddílů. Pokud budete chránit celý diskový oddíl, budete jej moci obnovit jako celek pomocí postupu obnovení diskového obrazu.

Nedoporučujeme používat nepřetržité zálohování jako hlavní způsob ochrany systému. Pro zajištění bezpečnosti systému použijte jakýkoli jiný plán. Příklady a podrobnosti naleznete v části [Příklady vlastních schémat](#).

### 3.4.1 Omezení služby nonstop zálohování

- Vytvořit lze pouze jedno nonstop zálohování.
- Úložiště Acronis Cloud nelze použít jako cíl nonstop zálohy na úrovni disku.
- Knihovny Windows (dokumenty, hudba apod.) lze chránit pouze pomocí nepřetržitého zálohování na úrovni disku.
- Nemůžete chránit data uložená na externích pevných discích.
- Není možné současně používat nonstop zálohování a režim Try&Decide.

### 3.4.2 Jak to funguje

Po spuštění nonstop zálohování Acronis se vytvoří počáteční plná záloha dat, která se mají chránit. Nonstop zálohování Acronis pak bude nepřetržitě sledovat chráněné soubory (včetně otevřených). Po zjištění úpravy dojde k zálohování změněných dat. Nejkratší interval mezi přírůstkovými operacemi zálohování činí pět minut. To vám umožní obnovit váš systém do konkrétního bodu v čase.



Nonstop zálohování Acronis kontroluje změny souborů na disku, nikoli v paměti. Pokud například pracujete v aplikaci Word a dlouho nepoužijete příkaz „Uložit“, vaše aktuální změny v dokumentu aplikace Word nebudou zálohovány.

Můžete si myslet, že při takové frekvenci zálohování bude úložiště brzy zaplněno. Toho se však nemusíte bát, protože aplikace Acronis Cyber Protect Home Office zálohuje pouze „rozdíly“. To znamená, že budou zálohovány jenom rozdíly mezi starými a novými verzemi, a ne celé změněné soubory. Pokud používáte například aplikaci Microsoft Outlook nebo Windows Mail, může být soubor PST velmi velký. Navíc se mění s každým přijatým nebo odeslaným e-mailem. Kdyby se při každé změně zálohoval celý soubor PST, bylo by to nepřijatelné plýtvání prostorem úložiště, proto Acronis Cyber Protect Home Office zálohuje kromě původního zálohovaného souboru jen jeho změny.

### 3.4.3 Pravidla zachování

#### Místní zálohy

Nonstop zálohování Acronis ukládá veškeré zálohy za posledních 24 hodin. Starší zálohy se slučují tak, aby mohla aplikace Nonstop zálohování uchovávat denní zálohy za posledních 30 dní a týdenní zálohy, dokud není využito veškeré místo úložiště aplikace Nonstop zálohování.

Slučování se provádí každý den mezi půlnocí a 01:00. První sloučení proběhne, když je nonstop zálohování spuštěné již 24 hodin. Nonstop zálohování tedy zapnete například 12. července v 10:00. V takovém případě proběhne první sloučení mezi 00:00 a 01:00 dne 14. července. Aplikace slučuje data každý den ve stejný čas. Když je počítač mezi 00:00 a 01:00 vypnutý, provede se sloučení po jeho zapnutí. Pokud nonstop zálohování na nějaký čas vypnete, slučování se bude po jeho novém zapnutí dále spouštět.

#### Zálohy v cloudu

Acronis Cyber Protect Home Office ponechá pouze následující verze zálohy:

- Všechny verze z poslední hodiny
- První verze z každé hodiny za posledních 24 hodin
- První verzi z každého dne za poslední týden
- První verzi z každého týdne za poslední měsíc
- První verzi každého měsíce

Všechny ostatní verze se automaticky smažou. Pravidla zachování jsou předem nastavena a nelze je změnit.

### 3.4.4 Datové úložiště Nonstop zálohování Acronis

Datové úložiště Nonstop zálohování Acronis může být vytvořeno pouze na místních pevných discích jednotkách (interních i externích) nebo na úložišti Acronis Cloud.

V mnoha případech bude nejlepší volbou pro datové úložiště nonstop zálohování použití externího pevného disku. Externí disk můžete použít s jakýmkoliv z následujících rozhraní: USB (včetně USB 3.0), eSATA, FireWire a SCSI.

Jako úložiště lze také použít NAS, avšak s jedním omezením – musí být přístupné prostřednictvím protokolu SMB. Nezáleží na tom, zda je úložiště NAS, které chcete použít, přiřazeno jako místní disk nebo ne. Pokud úložiště požaduje přihlášení, bude třeba zadat správné uživatelské jméno a heslo. Další informace naleznete v části [Nastavení ověřování](#). Aplikace Acronis Cyber Protect Home Office si pověření zapamatuje a následná připojení k úložišti již přihlášení vyžadovat nebudou.

Jestliže není k dispozici externí disk nebo NAS, nonstop zálohování může být provedeno na interní disk, včetně dynamického. Jako úložiště nonstop zálohování nemůžete použít oddíl, který má být chráněný. Pokud má váš počítač jeden pevný disk s jedním oddílem, ale chcete přesto používat Nonstop zálohování Acronis, můžete pro datové úložiště nonstop zálohování použít zónu Acronis Secure Zone.

Před vytvořením datového úložiště Nonstop zálohování Acronis aplikace Acronis Cyber Protect Home Office zkontroluje, zda je ve vybraném umístění dostatek volného místa. Vynásobí objem dat, která mají být chráněna, číslem 1,2 a porovná vypočítanou hodnotu s dostupným místem. Pokud volné místo v cíli splňuje minimální požadavky na místo, cíl lze použít k ukládání dat Nonstop zálohování.

### 3.4.5 Nonstop zálohování – nejčastěji kladené otázky

**Proč se nonstop zálohování Acronis samo od sebe zastaví?** – Jedná se o korektní chování nonstop zálohování Acronis. Když zatížení systému dosáhne kritické úrovně, nonstop zálohování Acronis obdrží varování při přetížení od systému Windows a zastaví se. To pomáhá systému Windows uvolnit zatížení způsobené dalšími aplikacemi. Přetížení může být způsobeno spuštěnými aplikacemi náročnými na prostředky (například provádění hloubkové kontroly systému antivirovým softwarem).

V takovém případě se nonstop zálohování automaticky zastaví a nelze jej znovu spustit. Po zastavení čeká nonstop zálohování Acronis jednu hodinu, aby systém mohl uvolnit zatížení, a poté se pokusí znovu spustit.

Počet automatických restartování nonstop zálohování Acronis je 6. To znamená, že po prvním automatickém opakovaném restartování se nonstop zálohování Acronis pokusí opět spustit ještě pětkrát v intervalech po jedné hodině.

Po šestém neúspěšném pokusu počká nonstop zálohování Acronis na další kalendářní den. Další den se počítadlo automatických opakovaných spuštění automaticky vynuluje. Pokud nezasáhnete, nonstop zálohování Acronis se pokusí za den znovu spustit šestkrát.

Počet pokusů o opakované spuštění lze vynulovat následujícími způsoby:

- Restartováním služby nonstop zálohování Acronis;
- restartováním počítače.

Restartováním služby nonstop zálohování Acronis pouze vynulujete počítadlo opakovaných spuštění. Pokud systém bude i nadále přetížen, nonstop zálohování Acronis se zastaví znovu. Informace o restartování služby nonstop zálohování Acronis, viz článek <https://kb.acronis.com/content/14708>.

Restartováním počítače se eliminuje zátěž a vynuluje počítadlo. Pokud bude systém znovu přetížen, nonstop zálohování Acronis se zastaví.

**Proč občas nonstop zálohování Acronis způsobuje vysokou zátěž procesoru?** – Jedná se o očekávané chování nonstop zálohování Acronis. Tato situace může nastat po opakovaném spuštění zastaveného nonstop zálohování Acronis, pokud bylo během zastavení upraveno větší množství dat.

Například pokud ručně zastavíte nonstop zálohování Acronis, kterým chráníte svůj systémový diskový oddíl, a poté nainstalujete novou aplikaci. Když poté nonstop zálohování Acronis zase spustíte, bude nějakou dobu zatěžovat procesor. Proces `afcdpsrv.exe` se však poté vrátí do normálního stavu.

To je způsobeno tím, že nonstop zálohování Acronis potřebuje zkontrolovat zálohovaná data oproti datům, která byla během zastavení změněna, aby se zajistila souvislá ochrana. Jestliže bylo upravených dat mnoho, proces může chvíli zatěžovat procesor. Po dokončení kontroly a zálohování veškerých upravených dat se nonstop zálohování Acronis vrátí do normálního stavu.

**Lze jako úložiště pro nonstop zálohování Acronis použít oddíl se systémem souborů FAT32 na místním pevném disku?** – Ano, jako úložiště lze použít diskový oddíl se systémem souborů FAT32 nebo NTFS.

**Lze nastavit úložiště nonstop zálohování Acronis ve sdíleném síťovém úložišti nebo NAS?** – Ano, nonstop zálohování Acronis podporuje síťová sdílení, mapované disky, NAS a další zařízení připojená přes síť s jedním omezením – musí používat protokoly SMB.

## 3.5 Pojmenování souboru zálohy

V závislosti na verzi, ve které byla záloha vytvořena, se liší její název.

### 3.5.1 Konvence pojmenování pro soubory zálohy vytvořené v aplikaci Acronis True Image (2020 či 2021) a Acronis Cyber Protect Home Office

Název souboru zálohy obsahuje pouze název zálohy a přírůstkový čítač. Neobsahuje žádné další informace, jako je třeba metoda zálohování, číslo řetězce zálohy, číslo verze zálohy nebo číslo svazku.

Název zálohy může vypadat takto:

1. `my_documents.tibx`
2. `my_documents_0001.tibx`

3. my\_documents\_0002.tibx
4. my\_documents\_0003.tibx

Plné a rozdílové zálohy se ukládají do samostatných souborů a přírůstkové zálohy se automaticky slučují do plných záloh.

Následující zálohy nadále používají formát TIB a související zásady vytváření názvů:

- Zálohy na úrovni souboru pro všechny cílové složky s výjimkou úložiště Acronis Cloud. Zálohy na úrovni souboru do úložiště Acronis Cloud jsou ve formátu TIBX.
- Nonstop zálohy
- Ověřené zálohy
- Zálohy využívající CD/DVD/Blu-ray, FTP nebo "Acronis Secure Zone" (str. 210) jako své cílové umístění

## 3.5.2 Konvence pojmenování pro soubory zálohy vytvořené před aplikací Acronis True Image 2020

Název souboru zálohy TIB má následující atributy:

- Název zálohy
- Metoda zálohování (full, inc, diff: plná, přírůstková, rozdílová)
- Číslo řetězce zálohy<sup>1</sup> (ve formě b#)
- Číslo verze zálohy<sup>2</sup> (ve formě s#)
- Číslo svazku (ve formě v#)

Pokud zálohu rozdělíte do několika souborů, dojde například ke změně tohoto příznaku. Další informace naleznete v části [Dělení zálohy](#).

Proto název zálohy může vypadat následovně:

1. my\_documents\_full\_b1\_s1\_v1.tib
2. my\_documents\_full\_b2\_s1\_v1.tib
3. my\_documents\_inc\_b2\_s2\_v1.tib
4. my\_documents\_inc\_b2\_s3\_v1.tib

Pokud vytváříte novou zálohu a ve složce se nachází soubor se stejným jménem, aplikace neodstraní starý soubor, ale přidá k novému souboru příponu „-číslo“, například my\_documents\_inc\_b2\_s2\_v1-2.tib.

---

<sup>1</sup>Posloupnost alespoň dvou verzí záloh, která se skládá z první plné verze zálohy a následné jedné nebo více přírůstkových nebo rozdílových verzí záloh. Řetězec verzí záloh pokračuje až do další plné verze zálohy (pokud nějaká je).

<sup>2</sup>Výsledek jedné operace zálohování. Ve skutečnosti se jedná o soubor nebo sadu souborů, které obsahují kopii zálohovaných dat z určité doby. Verze záloh souborů vytvořené aplikací Acronis Cyber Protect Home Office mají příponu TIBX. Soubory TIBX vzniklé sloučením verzí záloh se také označují jako verze záloh.

## 3.6 Integrace s Windows

Během instalace poskytuje aplikace Acronis Cyber Protect Home Office bližší integraci s operačním systémem Windows. Umožňuje tak maximální využití možností vašeho počítače.

Aplikace Acronis Cyber Protect Home Office nabízí následující součásti:

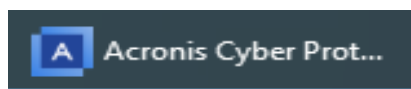
- Položky Acronis v nabídce **Start** systému Windows
- Tlačítko Acronis Cyber Protect Home Office na panelu úloh
- Příkazy místní nabídky

### 3.6.1 Nabídka Start systému Windows

V nabídce **Start** se zobrazují příkazy a nástroje služby Acronis. Zajišťují přístup k funkci Acronis Cyber Protect Home Office bez nutnosti spouštět aplikaci.

### 3.6.2 Tlačítko Acronis Cyber Protect Home Office na panelu úloh

Tlačítko Acronis Cyber Protect Home Office na panelu úloh systému Windows zobrazuje postup a výsledky operací aplikace Acronis Cyber Protect Home Office.



### 3.6.3 Centrum oznámení

Když je aplikace Acronis Cyber Protect Home Office otevřená, vidíte stav všech operací. Protože však některé operace, jako například záloha, mohou trvat déle, není aplikace Acronis Cyber Protect Home Office potřeba k zjištění výsledků.

Centrum oznámení obsahuje nejnovější upozornění na jednom místě a umožňuje prohlížení důležitých stavů bez otevření aplikace Acronis Cyber Protect Home Office ve chvíli, kdy je potřebujete. V centru oznámení Acronis se zobrazují tyto informace: Informace o výsledku zálohování a další důležitá oznámení z aplikace Acronis Cyber Protect Home Office. Centrum oznámení se minimalizuje a v panelu se skryje pod aplikaci Acronis Cyber Protect Home Office.

### 3.6.4 Příkazy místní nabídky

Chcete-li přejít na příkazy místní nabídky, otevřete Průzkumník souborů, klikněte pravým tlačítkem myši na vybrané položky, přejděte na aplikaci Acronis Cyber Protect Home Office a zvolte požadovaný příkaz.

- Chcete-li vytvořit novou zálohu na úrovni souborů, zvolte příkaz **Nová záloha souborů**.
- Chcete-li vytvořit novou zálohu na úrovni disku, zvolte příkaz **Nová záloha disku**.

- Chcete-li připojit zálohu na úrovni disku (soubor TIB), zvolte příkaz **Připojit**.
- Chcete-li ověřit zálohu (soubor TIB), zvolte příkaz **Ověřit**.

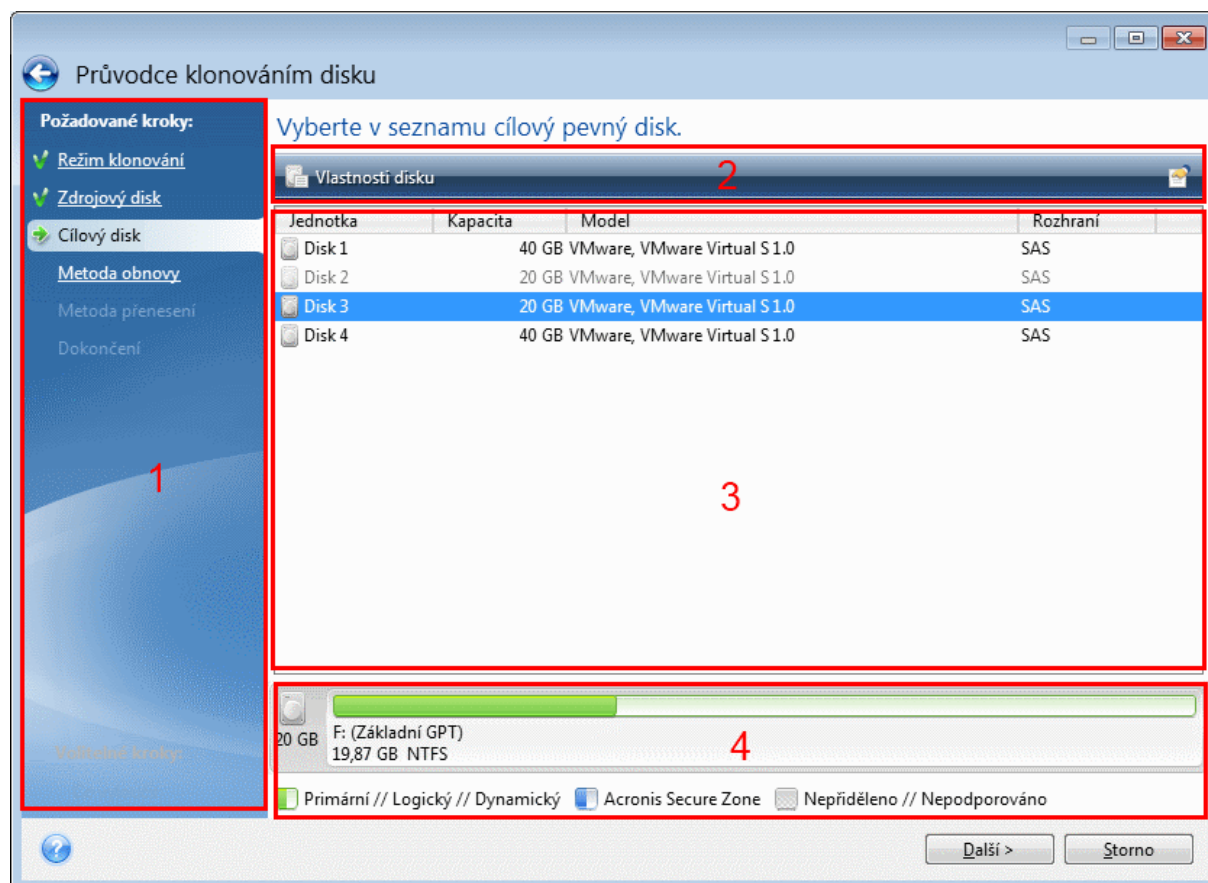
### 3.6.5 Obnova na úrovni souborů v Průzkumníku souborů

1. V Průzkumníku souborů dvakrát klikněte na soubor zálohy (soubor TIB), který obsahuje data k obnovení.
2. Zkopírujte nebo přetáhněte soubory a složky do libovolného umístění v počítači, jako by byly uloženy na běžném disku.

## 3.7 Průvodci

Při použití dostupných nástrojů aplikace Acronis Cyber Protect Home Office vás aplikace v mnoha případech provede operacemi pomocí průvodců.

Příklad je zobrazen na následujícím obrázku.







Okno průvodce se obvykle skládá z následujících částí:

1. Toto je seznam kroků potřebných k dokončení operace. Vedle dokončeného kroku se zobrazí zelené zatržítko. Zelená šipka ukazuje na aktuální krok. Po dokončení všech kroků se v aplikaci v kroku **Dokončit** zobrazí okno Souhrn. Zkontrolujte souhrn a kliknutím na tlačítko **Pokračovat** spusťte operaci.

2. Tato lišta nástrojů obsahuje tlačítka ke správě objektů vybraných v oblasti 3.

Například:

-  **Podrobnosti**– zobrazí se okno s podrobnými informacemi o vybrané záloze.
-  **Vlastnosti**– zobrazí se okno vlastností vybrané položky.
-  **Vytvořit nový diskový oddíl**– zobrazí se okno, ve kterém můžete nakonfigurovat nastavení nového diskového oddílu.
-  **Sloupce**– umožňuje zvolit, jaké sloupce tabulky se zobrazí a v jakém pořadí.

3. Jedná se o hlavní oblast, ve které vybíráte položky a měníte nastavení.

4. V této oblasti se zobrazují další informace o položce vybrané v části 3.

## 3.8 Nejčastější dotazy týkající se zálohování, obnovy a klonování

- **Mám systémový oddíl o velikosti 150 GB, ale je na něm zabráno pouze 80 GB. Co zahrne aplikace Acronis Cyber Protect Home Office do zálohy?** – Ve výchozím nastavení aplikace Acronis Cyber Protect Home Office kopíruje pouze sektory pevného disku, které obsahují data, takže v záloze bude zahrnuto pouze 80 GB dat. Je také možné zvolit režim sektor po sektoru. Tento režim zálohování je vyžadován pouze ve zvláštních případech. Další informace naleznete v části [Režim tvorby diskového obrazu](#). Při vytváření zálohy sektor po sektoru program kopíruje volné i využitě sektory pevného disku, což většinou vytvoří mnohem větší soubor zálohy.
- **Zahrnuje záloha systémového disku ovladače, dokumenty, obrázky atd.?**– Ano, taková záloha zahrnuje ovladače, stejně jako obsah složky Moje dokumenty a jejích podsložek v případě, že bylo zachováno výchozí umístění složky Moje dokumenty. Pokud máte ve vašem počítači pouze jeden pevný disk, taková záloha bude zahrnovat operační systém a veškeré aplikace a data.
- **Ve svém notebooku mám starý pevný disk, který je téměř plný. Zakoupil jsem si nový, větší pevný disk. Jakým způsobem je možné přenést systém Windows, programy a data na nový disk?** – V takovém případě je možné starý pevný disk naklonovat do nového nebo starý pevný disk zazálohovat a zálohu poté obnovit na nový pevný disk. Ideální metoda většinou závisí na rozložení oddílů starého pevného disku.
- **Chci migrovat starý systémový pevný disk na disk SSD. Lze to provést pomocí aplikace Acronis Cyber Protect Home Office?** – Ano, aplikace Acronis Cyber Protect Home Office tuto funkci poskytuje. Další informace naleznete v části [Migrace systému z pevného disku na disk SSD](#)
- **Jaký je nejlepší postup migrace systému na nový disk: klonování nebo záloha a obnovení?** – Metoda zálohování a obnovení je flexibilnější. V každém případě doporučujeme provést zálohu starého pevného disku i v případě, že se rozhodnete použít klonování. Tímto způsobem můžete zachránit data, pokud se během klonování původního pevného disku něco přihodí. Vyskytly se například případy, kdy uživatel vybral jako cíl nesprávný disk a smazal tak systémový disk. Je také možné z důvodu zvýšení bezpečnosti vytvořit nadbytečnou zálohu.

- **Co je lepší zálohovat: oddíl nebo celý disk?** – Ve většině případů je lepší zálohovat celý disk. Někdy je ovšem lepší zálohovat oddíl. Pokud má například váš notebook jeden pevný disk se dvěma oddíly: systémový oddíl (písmeno jednotky C) a datový oddíl (písmeno jednotky D). V systémovém oddílu máte uloženy pracovní dokumenty ve složce Moje dokumenty a jejich podsložkách. V datovém oddílu jsou uložena vaše videa, obrázky a hudební soubory. Takové soubory jsou již komprimovány a jejich záloha pomocí aplikace Acronis Cyber Protect Home Office znatelně nezmenší velikost souboru zálohy. Pokud je ovšem na vašem disku dostatek místa, doporučujeme vytvořit alespoň jednu zálohu celého disku.
- **Jak se používá klonování: v systému Windows nebo po spuštění ze spouštěcího média Acronis?** I v případě, že spustíte klonování v systému Windows, se počítač restartuje do prostředí Linuxu, stejně jako při jeho spuštění ze spouštěcího média Acronis. Proto je lepší klonovat po spuštění ze spouštěcího média Acronis. Například může dojít k tomu, že vaše jednotky pevných disků budou rozpoznány v systému Windows, ale už ne v systému Linux. V takovém případě operace klonování po restartu selže. Při spuštění počítače ze spouštěcího média můžete před spuštěním klonování zkontrolovat, že aplikace Acronis Cyber Protect Home Office rozpozná zdrojové i cílové disky.
- **Je možné klonovat nebo zálohovat a obnovit počítač se dvěma operačními systémy?** Ano, je to možné, pokud se jedná o operační systémy Windows. Pokud jsou vaše operační systémy nainstalovány v samostatných oddílech stejného fyzického pevného disku, klonování nebo obnovení většinou proběhne bez jakýchkoliv problémů. Pokud jsou systémy na jiných fyzických pevných discích, mohou se po obnovení vyskytnout problémy se spuštěním.
- **Podporuje aplikace Acronis Cyber Protect Home Office technologii RAID?** – Aplikace Acronis Cyber Protect Home Office podporuje hardwarová pole RAID všech běžných typů. Je k dispozici i podpora konfigurací softwarového pole RAID na dynamických discích. Acronis spouštěcí médium podporuje většinu oblíbených hardwarových řadičů RAID. Pokud standardní spouštěcí médium Acronis „nevidí“ pole RAID jako jediný svazek, na médiu chybí odpovídající ovladače. Můžete se pokusit vytvořit spouštěcí médium na základě prostředí WinPE. Toto médium může poskytnout nezbytné ovladače.



## 4 Zálohování dat

### 4.1 Zálohování diskových oddílů a disků

Na rozdíl od záloh souborů obsahují zálohy disků a diskových oddílů veškerá data uložená na disku nebo diskovém oddílu. Pomocí tohoto typu zálohy se obvykle vytváří přesná kopie systémového diskového oddílu nebo celého systémového disku. Tyto zálohy umožňují obnovu počítače, pokud systém Windows nepracuje správně nebo se nedokáže spustit.

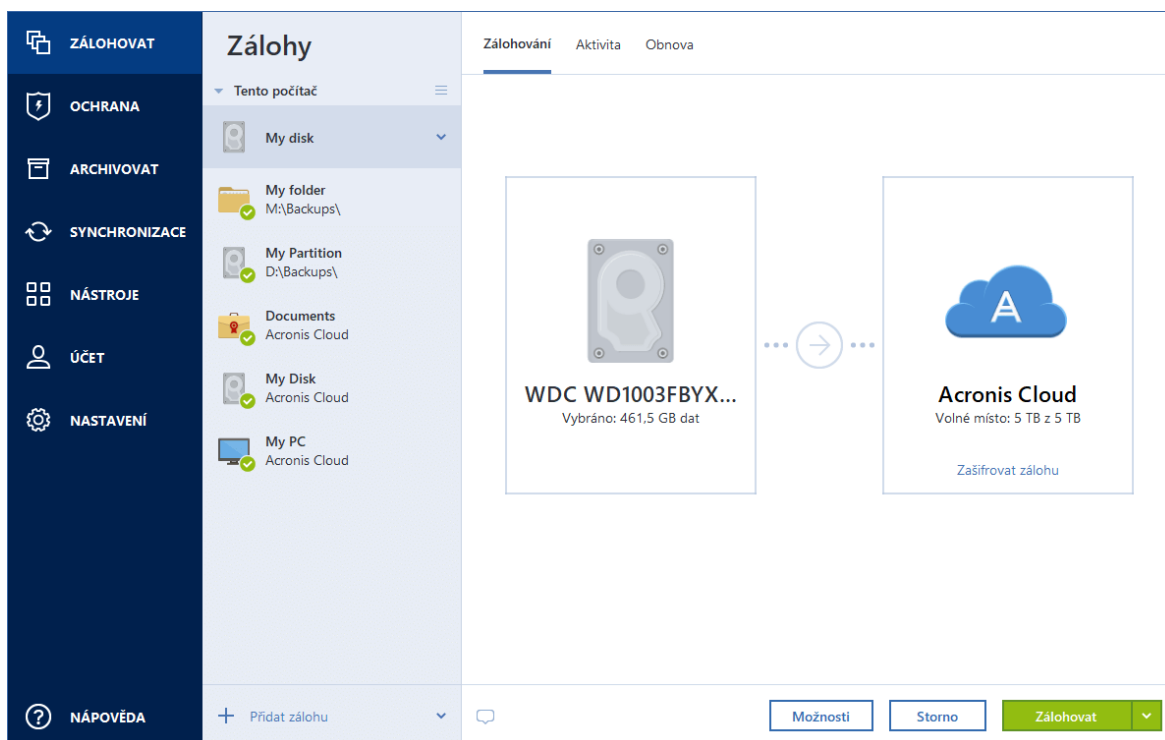
#### **Chcete-li zálohovat diskové oddíly nebo disky**

1. Spustit Acronis Cyber Protect Home Office
2. Na bočním panelu klikněte na možnost **Záloha**.
3. Klikněte na položku **Přidat zálohu**.
4. [Volitelné] Chcete-li přejmenovat zálohu, klikněte na šipku vedle názvu zálohy, klikněte na tlačítko **Přejmenovat** a pak zadejte nový název.
5. Klikněte na oblast **Zdroj zálohy** a poté vyberte možnost **Disky a diskové oddíly**.
6. V zobrazeném okně zaškrtněte políčka vedle diskových oddílů a disků, které chcete zálohovat, a klikněte na tlačítko **OK**.

Chcete-li zobrazit skryté diskové oddíly, klikněte na možnost **Úplný seznam diskových oddílů**.

#### **Poznámka**

Chcete-li zálohovat dynamické disky, můžete použít pouze režim diskového oddílu.



7. Klikněte na oblast **Cíl zálohy** a poté vyberte cíl zálohování:
  - **Acronis Cloud** – přihlaste se ke svému účtu a klikněte na tlačítko **OK**.  
Nemáte-li ještě účet Acronis, klikněte na tlačítko **Vytvořit účet**, zadejte e-mailovou adresu a heslo a poté klikněte na tlačítko **Vytvořit účet**. Další informace naleznete v části [Účet Acronis](#).
  - **Váš externí disk**– Máte-li k počítači připojený externí disk, můžete ho vybrat ze seznamu.
  - **NAS**– Ze seznamu nalezených zařízení NAS vyberte požadované zařízení NAS. Pokud máte pouze jedno zařízení NAS, aplikace Acronis Cyber Protect Home Office jej navrhne použít jako výchozí cílové umístění zálohování.
  - **Procházet**– Vyberte cílové umístění ze stromu složek.

---

#### **Poznámka**

Pokud je to možné, vyhněte se ukládání záloh systémového diskového oddílu na dynamických discích, protože systémový diskový oddíl se obnovuje v prostředí Linux. Systémy Linux a Windows s dynamickými disky pracují odlišně. To může v průběhu obnovy způsobit potíže.

---

8. [volitelný krok] Kliknutím na možnost **Možnosti** můžete nastavit možnosti zálohy. Další informace naleznete v části [Možnosti zálohování](#).
9. [volitelný krok] Klikněte na ikonu **Přidat komentář** a napište komentář na verzi zálohy. Komentáře k zálohám vám pomohou najít zálohu kdykoliv později při obnově dat.
10. Proveďte jednu z následujících akcí:
  - Chcete-li provést zálohu okamžitě, klikněte na tlačítko **Zálohovat nyní**.
  - Pokud chcete zálohování spustit později nebo podle plánu, klikněte na šipku vpravo od tlačítka **Zálohovat nyní** a poté na tlačítko **Později**.

---

#### **Poznámka**

Pokud zálohujete data do služby Acronis Cloud, dokončení prvního zálohování může trvat poměrně dlouho. Další zálohování již budou mnohem rychlejší, protože se budou přes internet přenášet pouze změny souborů.

---

---

#### **Poznámka**

Jakmile se online zálohování spustí, můžete aplikaci Acronis Cyber Protect Home Office zavřít. Zálohování bude pokračovat na pozadí. Pokud zálohování pozastavíte, vypněte počítač nebo ho odpojte od internetu a zálohování bude pokračovat po kliknutí na tlačítko Zálohovat nyní nebo po obnovení připojení k internetu. Přerušování zálohování nezpůsobí dvojité odeslání dat.

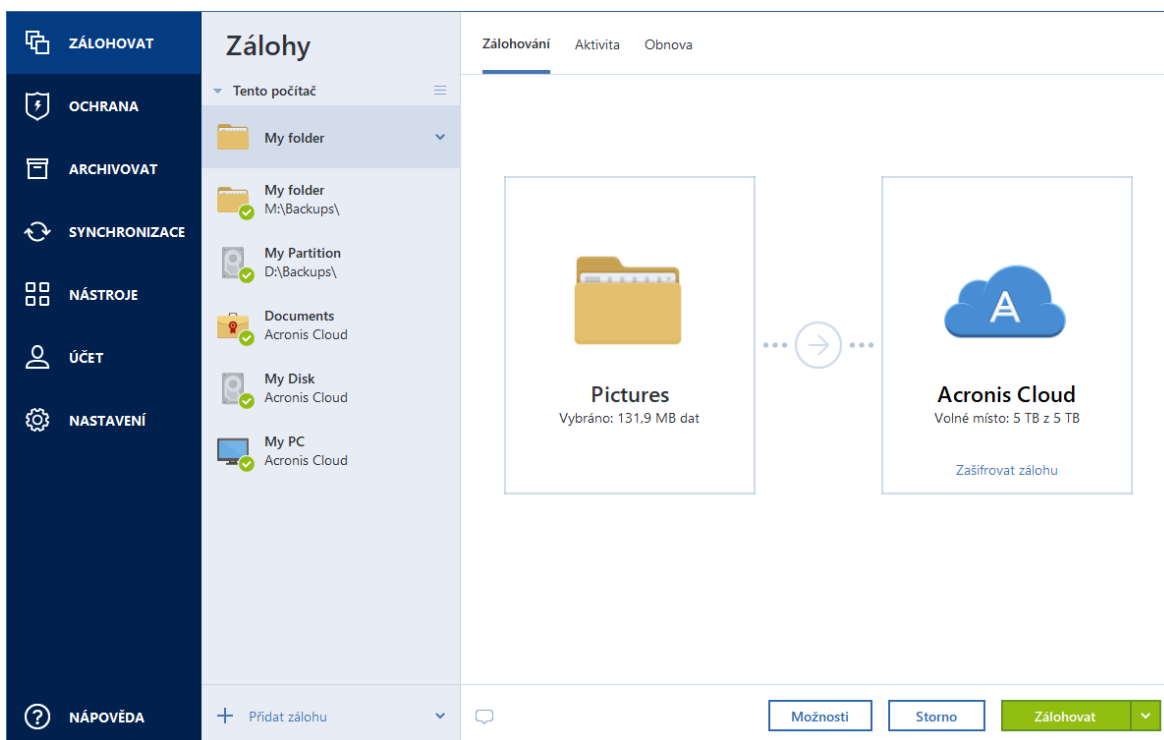
---

## 4.2 Zálohování souborů a složek

Chcete-li chránit soubory jako jsou dokumenty, fotografie, hudební soubory a videa, není nutné zálohovat celý diskový oddíl obsahující tyto soubory. Můžete zálohovat konkrétní soubory a složky.

### **Zálohování souborů a složek**

1. Spustit Acronis Cyber Protect Home Office
2. Na bočním panelu klikněte na možnost **Záloha**.
3. Klikněte na položku **Přidat zálohu**.
4. [Volitelné] Chcete-li přejmenovat zálohu, klikněte na šipku vedle názvu zálohy, klikněte na tlačítko **Přejmenovat** a pak zadejte nový název.
5. Klikněte na oblast **Zdroj zálohy** a poté vyberte možnost **Soubory a složky**.
6. V zobrazeném okně zaškrtněte políčka vedle souborů a složek, které chcete zálohovat, a klikněte na tlačítko **OK**.



7. Klikněte na oblast **Cíl zálohy** a poté vyberte cíl zálohování:
  - **Acronis Cloud** – přihlaste se ke svému účtu a klikněte na tlačítko **OK**.  
Nemáte-li ještě účet Acronis, klikněte na tlačítko **Vytvořit účet**, zadejte e-mailovou adresu a heslo a poté klikněte na tlačítko **Vytvořit účet**. Další informace naleznete v části [Účet Acronis](#).
  - **Váš externí disk**– Máte-li k počítači připojený externí disk, můžete ho vybrat ze seznamu.
  - **NAS**– Ze seznamu nalezených zařízení NAS vyberte požadované zařízení NAS. Pokud máte pouze jedno zařízení NAS, aplikace Acronis Cyber Protect Home Office jej navrhne použít jako výchozí cílové umístění zálohování.
  - **Procházet**– Vyberte cílové umístění ze stromu složek.
8. [volitelný krok] Kliknutím na možnost **Možnosti** můžete nastavit možnosti zálohy. Další informace naleznete v části [Možnosti zálohování](#).
9. [volitelný krok] Klikněte na ikonu **Přidat komentář** a napište komentář na verzi zálohy. Komentáře k zálohám vám pomohou najít zálohu kdykoliv později při obnově dat.
10. Proveďte jednu z následujících akcí:

- Chcete-li provést zálohu okamžitě, klikněte na tlačítko **Zálohovat nyní**.
- Pokud chcete zálohování spustit později nebo podle plánu, klikněte na šipku dolů napravo od tlačítka **Zálohovat nyní** a poté na tlačítko **Později**.

---

### Poznámka

Pokud zálohujete data do služby Acronis Cloud, dokončení prvního zálohování může trvat poměrně dlouho. Další zálohování již budou mnohem rychlejší, protože se budou přes internet přenášet pouze změny souborů.

---

Dále se povídejte na video s pokyny v angličtině na adrese <https://goo.gl/i4j1AN>.

## 4.3 Zálohování mobilních zařízení

Pokud máte chytrý telefon se systémem iOS nebo Android, můžete použít aplikaci Acronis Cyber Protect Home Office k ochraně mobilních dat, například fotografií, videosouborů, kontaktů a kalendáře. Další informace naleznete v části [Acronis Mobile](#).

Před spuštěním zálohování vyberte, kam chcete svoji zálohu uložit: do služby Acronis Cloud nebo místního úložiště ve vašem počítači. Cílové umístění můžete později změnit, ale nemůžete zároveň zálohovat do obou cílových umístění. Chcete-li data zálohovat do úložiště Acronis Cloud, použijte aplikaci Acronis Mobile. Další informace naleznete v části Zálohování mobilního zařízení do úložiště Acronis Cloud.

### ***Jak zálohovat mobilní data do místního úložiště ve vašem počítači***

1. Zkontrolujte, zda:
  - V počítači je nainstalována aplikace Acronis True Image (2017 či novější) nebo Acronis Cyber Protect Home Office.
  - V mobilním zařízení je nainstalována aplikace Acronis Mobile.
  - Vaše mobilní zařízení a váš počítač jsou připojeny ke stejné síti Wi-Fi.
2. Ve vašem počítači:
  - a. Spustíte aplikaci Acronis True Image (2017 či novější) nebo Acronis Cyber Protect Home Office.
  - b. Na bočním panelu klikněte na tlačítko **Záloha** a potom na tlačítko **Přidat zálohu**.
  - c. Klikněte na oblast **Zdroj zálohování** a pak vyberte položku **Mobilní zařízení**.  
Zobrazí se QR kód. Toto okno prosím nezavírejte.
3. Ve vašem mobilním zařízení:
  - a. Spustit Acronis Mobile
  - b. Kliknutím na ikonu plus vytvořte zálohu. Poznámka: Tento krok se nezobrazí při prvním zálohování mobilního zařízení.
  - c. Vyberte počítač jako umístění záloh.
  - d. Klepněte na položku **Naskenovat QR kód**, nasměrujte kameru na QR kód na obrazovce počítače a pak počkejte, dokud nebude mobilní zařízení připojeno k počítači.

- e. Vyberte kategorie dat, která chcete zálohovat, nebo pokud chcete zálohovat všechna data, klepněte na položku **Potvrdit**.
- f. Povolte aplikaci Acronis Mobile přístup k osobním datům.
- g. [volitelný krok] Chcete-li zálohu zašifrovat a ochránit ji, zadejte heslo. V opačném případě klepněte na položku **Přeskočit šifrování**.
- h. Klepněte na tlačítko **Spustit zálohování**.

Po spuštění zálohování můžete sledovat postup v libovolné aplikaci (v počítači nebo mobilním zařízení), ale chyby a výstražné zprávy se zobrazí pouze v mobilní aplikaci.

Můžete zavřít jak aplikaci Acronis Cyber Protect Home Office v počítači, tak i aplikaci Acronis Mobile. Zálohování bude pokračovat na pozadí.

Chcete-li, aby byly změny dat (například nové fotografie) zálohovány automaticky, ujistěte se, že je zapnuto nastavení **Průběžné zálohování**. Je-li toto nastavení vypnuto, jsou nová data zálohována pouze po klepnutí na položku **Zálohovat**. Další informace naleznete v části [Nastavení mobilní aplikace](#).

Změníte-li cílové umístění mobilních záloh z místního úložiště na úložiště Acronis Cloud, dojde k přerušení spojení mezi mobilním zařízením a počítačem a aplikace Acronis Cyber Protect Home Office přestane přidružovat mobilní zálohu v seznamu k mobilnímu zařízení. Budete-li poté chtít změnit umístění zpět na místní úložiště, bude třeba toto spojení obnovit. Spojení se také může přerušit kvůli chybě. Chcete-li spojení obnovit, vyberte mobilní zálohu v seznamu záloh aplikace Acronis Cyber Protect Home Office, klikněte na položku **Znovu připojit** a pak naskenujte QR kód pomocí svého mobilního zařízení. Poté bude zálohování normálně pokračovat se stejným nastavením.

### 4.3.1 Acronis Mobile

---

#### Poznámka

Aplikace Acronis Cloud nemusí být ve vaší oblasti dostupná. Další informace naleznete na adrese: <https://kb.acronis.com/content/4541>

---

Aplikace Acronis Mobile umožňuje zálohovat data do úložiště Acronis Cloud, do místního úložiště ve vašem počítači a v případě jejich ztráty či poškození je obnovit. Možnost zálohovat do cloudového úložiště vyžaduje účet Acronis předplatné úložiště Acronis Cloud.

Další informace o hlavních funkcích aplikace Acronis Mobile a podporovaných zařízeních naleznete v [dokumentaci k aplikaci Acronis Mobile](#).

#### Kde lze tyto aplikace najít?

Další informace o aplikaci Acronis Mobile získáte v obchodě Apple App Store nebo Google Play, kde si můžete aplikaci také stáhnout:

- Acronis Mobile pro systém iOS: <https://go.acronis.com/atimobile/download/iOS>
- Acronis Mobile pro systém Android: <https://go.acronis.com/atimobile/download/Android>

## 4.3.2 Místní cíl pro mobilní zálohy

Při zálohování dat z mobilního zařízení do počítače ukládá aplikace Acronis Mobile zálohy do výchozí složky `C:\ProgramData\Acronis Mobile Backup Data\acronis-local-data\`. Změníte-li výchozí složku, složka `acronis-local-data` se přesune do nově vybraného umístění. Všechna nová mobilní data se začnou zálohovat do nového umístění.

---

### Poznámka

Všechny mobilní zálohy se vždy ukládají do stejné složky a nelze je oddělit.

---

### **Změna místního cíle pro mobilní zálohy**

1. Na bočním panelu klikněte na **Nastavení** a najděte možnost **Umístění mobilních záloh**.
2. V části **Umístění záloh mobilního zařízení** klikněte na možnost **Změnit**. Zobrazí se okno **Změnit umístění**.
3. Klikněte na možnost **Vybrat umístění** a pak vyberte nové umístění pro zálohy. Upozorňujeme, že vybrané umístění se musí nacházet na interním pevném disku.

Chcete-li nové umístění změnit na původní, klikněte na položku **Obnovit výchozí**.

## 4.4 Zálohování dat aplikace Office 365

### 4.4.1 Proč zálohovat data aplikace Office 365?

Ačkoliv je Microsoft Office 365 pro domácnosti sada cloudových služeb, pravidelné zálohy poskytují další úroveň zabezpečení před chybami uživatelů a záměrnými škodlivými akcemi. S pomocí aplikace Acronis Cyber Protect Home Office můžete ochránit poštovní schránky aplikace Microsoft Outlook a data služby Microsoft OneDrive jejich zálohováním do zabezpečeného úložiště Acronis Cloud. Po nahrání do úložiště Acronis Cloud je veškerý obsah kdykoli dostupný z libovolného zařízení. Odstraněné položky můžete ze zálohy obnovit i po uplynutí doby zachování aplikace Office 365.

### 4.4.2 Zálohování dat aplikace Office 365

#### **Data, která můžete zálohovat v poštovní schránce Outlook:**

- Všechny složky
- E-mailové zprávy
- Přílohy

---

## Poznámka

Sdílené a skupinové poštovní schránky zálohovat nelze.

---

### Data, která můžete zálohovat ve službě OneDrive:

- Všechny soubory a složky

### Postup zálohování dat aplikace Office 365:

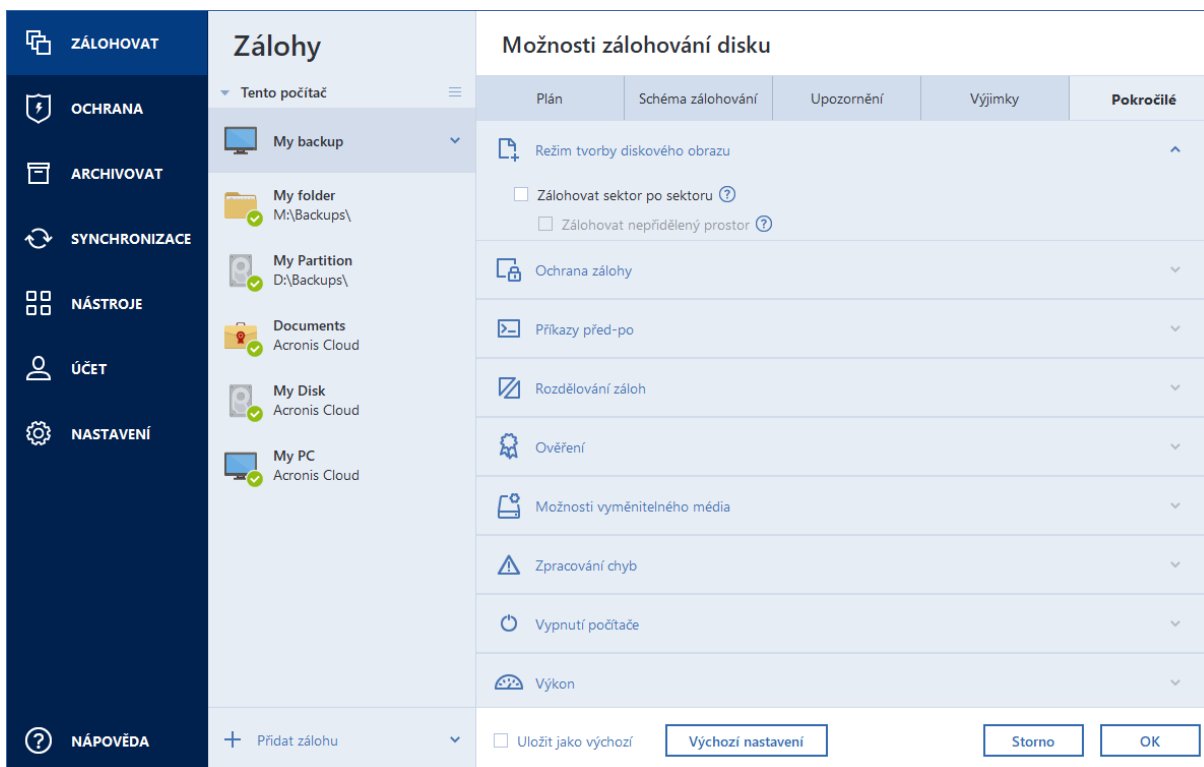
1. Jedním z následujících postupů otevřete aplikaci Online kontrolní panel:
  - Klikněte na odkaz: <https://cloud.acronis.com>.
  - Na bočním panelu Acronis Cyber Protect Home Office klikněte na možnost **Záloha, Přidat zálohu**, pak na oblast **Zdroj zálohy** a nakonec vyberte možnost **Cloudová služba**.
2. Přihlaste se k účtu Acronis.
3. Na bočním panelu klikněte na položku **Zdroje** a možnost **Přidat** a poté vyberte **Microsoft Office 365 pro domácnosti**.
4. Budete-li vyzváni, přihlaste se k účtu Microsoft.
5. V oblasti **Zdroj zálohy** vyberte položky k zálohování:
  - Celý účet
  - Outlook
  - OneDrive
6. Klikněte na tlačítko **Hotovo**.
7. U zálohy můžete prostřednictvím panelu **Vyčištění** nakonfigurovat pravidla čištění. Zálohy můžete také šifrovat a chránit heslem. Poté klikněte na tlačítko **Použít**.
8. Chcete-li spustit zálohování, klikněte na tlačítko **Spustit**.

## 4.5 Možnosti zálohování

Při vytváření zálohy můžete změnit další možnosti a upravit proces zálohování. Chcete-li otevřít okno možností, vyberte zdroj a cíl zálohování a klikněte na tlačítko **Možnosti**.

Možnosti každého typu zálohování (záloha na úrovni disku, záloha na úrovni souborů, online záloha, nonstop záloha) jsou nezávislé, a proto byste je měli nastavovat samostatně.

Po instalaci aplikace jsou všechny možnosti nastaveny na výchozí hodnoty. Můžete je měnit pouze pro aktuální operaci zálohování nebo pro všechny budoucí operace zálohování. Zaškrtnutím políčka **Uložit jako výchozí** použijete upravená nastavení na všechny další operace zálohování.



Chcete-li obnovit výchozí nastavení po instalaci produktu, klikněte na tlačítko **Obnovit výchozí nastavení**. Obnoví se tak nastavení pouze pro aktuální zálohu. Chcete-li obnovit nastavení pro všechny další zálohy, klikněte na tlačítko **Obnovit výchozí nastavení**, zaškrtněte políčko **Uložit nastavení jako výchozí** a klikněte na tlačítko **OK**.

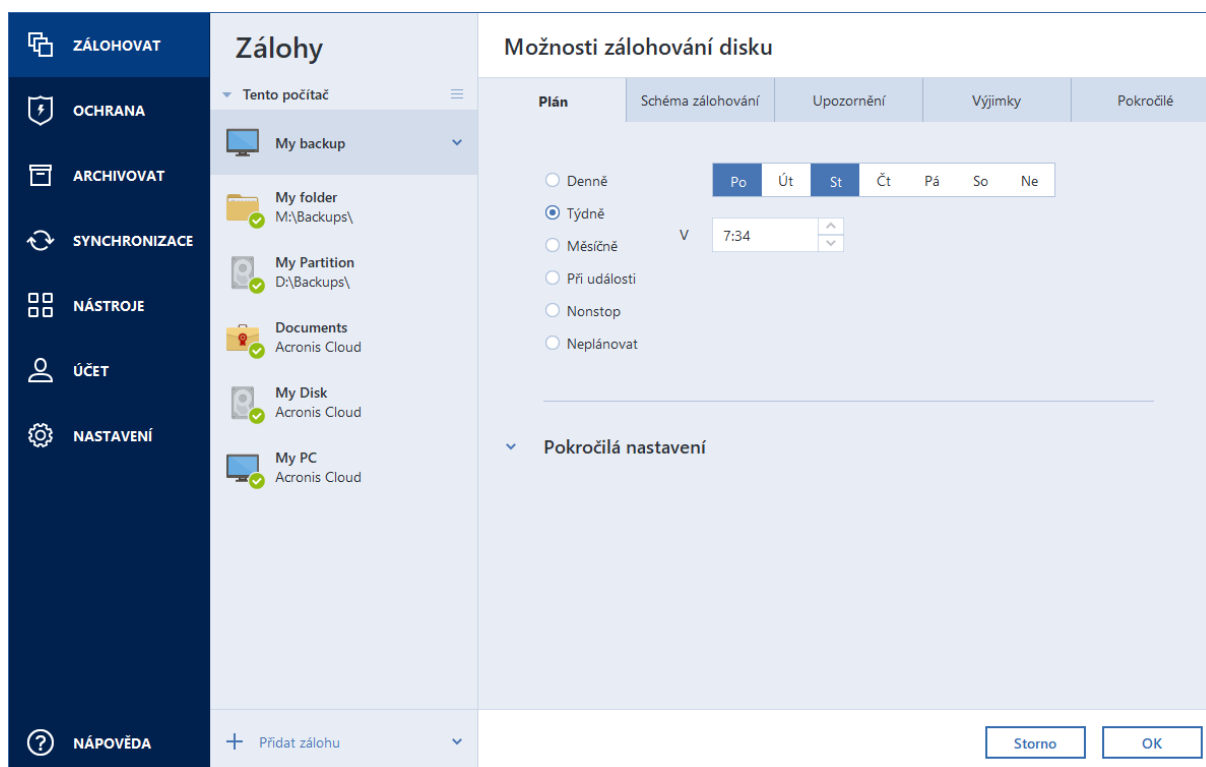
Dále se podívejte na video s pokyny v angličtině na adrese <https://goo.gl/bKZyaG>.

## 4.5.1 Plánování

Umístění: **Možnosti** > **Plánovač**

Na kartě **Plánovač** lze naplánovat zálohování a ověřování.





Můžete zadat plán pravidelně vytvářených nebo ověřovaných záloh:

- **Denně** – operace bude provedena jednou nebo vícekrát denně.
- **Týdně** – operace bude provedena jednou týdně nebo vícekrát týdně ve zvolené dny.
- **Měsíčně** – operace bude provedena jednou nebo vícekrát měsíčně ve zvolené dny.
- **Při události** – operace bude spuštěna při události.
- **Nonstop** – operace se bude spouštět každých pět minut.
- **Neplánovat** – plánovač bude pro aktuální operaci vypnut. V tom případě se zálohování nebo ověření bude spouštět pouze v případě, že kliknete na možnost **Zálohovat nyní** nebo **Ověřit** v hlavním okně.

## Pokročilá nastavení

V okně **Pokročilá nastavení** lze zadat následující pokročilá nastavení zálohování a ověřování:

- **Zálohovat pouze tehdy, je-li počítač zamknutý nebo je-li spuštěn spořič obrazovky** – Zaškrtnutím tohoto políčka odložíte naplánovanou operaci na dobu, kdy počítač nebude používán (bude zobrazen spořič obrazovky nebo bude počítač uzamčen). Při plánování ověření se zaškrtačací políčko změní na **Spouštět ověření jen tehdy, kdy je počítač nečinný**.
- **Vzbudit počítač z režimu spánku/hibernace** – Zaškrtnutím tohoto políčka probudíte spící/hibernující počítač k provedení naplánované operace.
- **Zabránit počítači v přechodu do režimu spánku/hibernace** – Zaškrtnutím tohoto políčka eliminujete situaci, kdy je časově náročné zálohování přerušeno, pokud počítač přejde do režimu spánku nebo hibernace.

- **Spustit zmeškané operace při spuštění systému se zpožděním (v minutách)** – Zaškrtnutím tohoto políčka vynutíte spuštění zmeškané operace při příštím spuštění systému, pokud byl počítač v naplánovaném čase vypnut a operace nebyla provedena.  
Dále můžete nastavit časové zpoždění spuštění zálohování po spuštění systému. Chcete-li například spustit zálohování 20 minut po startu systému, zadejte 20 do odpovídajícího okna.
- **Spustit vynechané operace při připojení externího zařízení** [nepovinné, pokud plánujete zálohování na USB flash disk nebo ověření zálohy, která je umístěna na USB flash disku] – zaškrtnutím tohoto políčka spustíte zmeškanou operaci, když je USB flash disk připojen, pokud byl v plánovaném čase odpojen.

## Parametry denního zálohování

Pro zálohy vytvářené nebo ověřované denně můžete nastavit následující parametry:

- **Každé** – V rozevíracím seznamu vyberte pravidelnost (například každé 2 hodiny).
- **Jednou denně** – Operace se spouští jednou denně v zadaný čas.
- **Dvakrát denně** – Operace se spouští dvakrát denně. Zvolte čas pro každou z těchto dvou operací.

Popis položky **Pokročilá nastavení** naleznete v tématu [Plánování](#).

## Parametry týdenního zálohování

Pro zálohy vytvářené nebo ověřované každý týden můžete nastavit následující parametry:

- **Dny v týdnu** – Vyberte dny, ve kterých se má operace spustit .
- **V** – Vyberte čas spuštění operace.

Popis položky **Pokročilá nastavení** naleznete v tématu [Plánování](#).

## Parametry měsíčního zálohování

Pro zálohy vytvářené nebo ověřované každý měsíc můžete nastavit následující parametry:

- **Každé** – Vyberte v rozevíracím seznamu číslo a den v týdnu. Například výběrem možnosti **Každé první pondělí** spustíte operaci každé první pondělí v měsíci.
- **Ve vybrané dny v měsíci** – Vyberte data zálohování. Operaci můžete spouštět například 10. a poslední den v měsíci.
- **V** – Vyberte čas spuštění operace.

Popis položky **Pokročilá nastavení** naleznete v tématu [Plánování](#).

## Parametry spuštění při události

Pro zálohy vytvořené nebo ověřené při nějaké události můžete nastavit následující parametry:

- **Pouze jednou denně** – Zaškrtněte toto políčko, pokud chcete operaci spustit pouze při prvním výskytu události v aktuálním dni.

- Zadejte událost, která vyvolá vytvoření nebo ověření zálohy:
  - **Když je připojeno externí zařízení** – Operace se spustí pokaždé, když se k počítači připojí stejné externí zařízení (USB flash disk nebo externí pevný disk), které jste dříve použili jako cílové umístění. Upozorňujeme, že systém Windows by měl toto zařízení rozpoznat jako externí.
  - **Při přihlášení uživatele** – Operace se spustí pokaždé, když se aktuální uživatel přihlásí do operačního systému.
  - **Při odhlášení uživatele** – Operace se spustí pokaždé, když se aktuální uživatel odhlásí z operačního systému.
  - **Při vypnutí nebo restartování systému** – Operace se spustí při každém vypnutí nebo restartování počítače.
  - **Spuštění systému se zpožděním (v minutách)** – Operace se spustí při každém spuštění operačního systému po vámi zadané době zpoždění.

Popis položky **Pokročilá nastavení** naleznete v tématu [Plánování](#).

## 4.5.2 Schémata zálohování

Umístění: **Možnosti** > **Schéma zálohování**

Schémata zálohování vám spolu s plánovačem pomohou vytvořit vlastní strategii zálohování. Schémata vám umožňují optimalizovat využití úložišť k zálohování, zvýšit spolehlivost ukládání dat a automaticky odstraňovat zastaralé verze záloh.

---

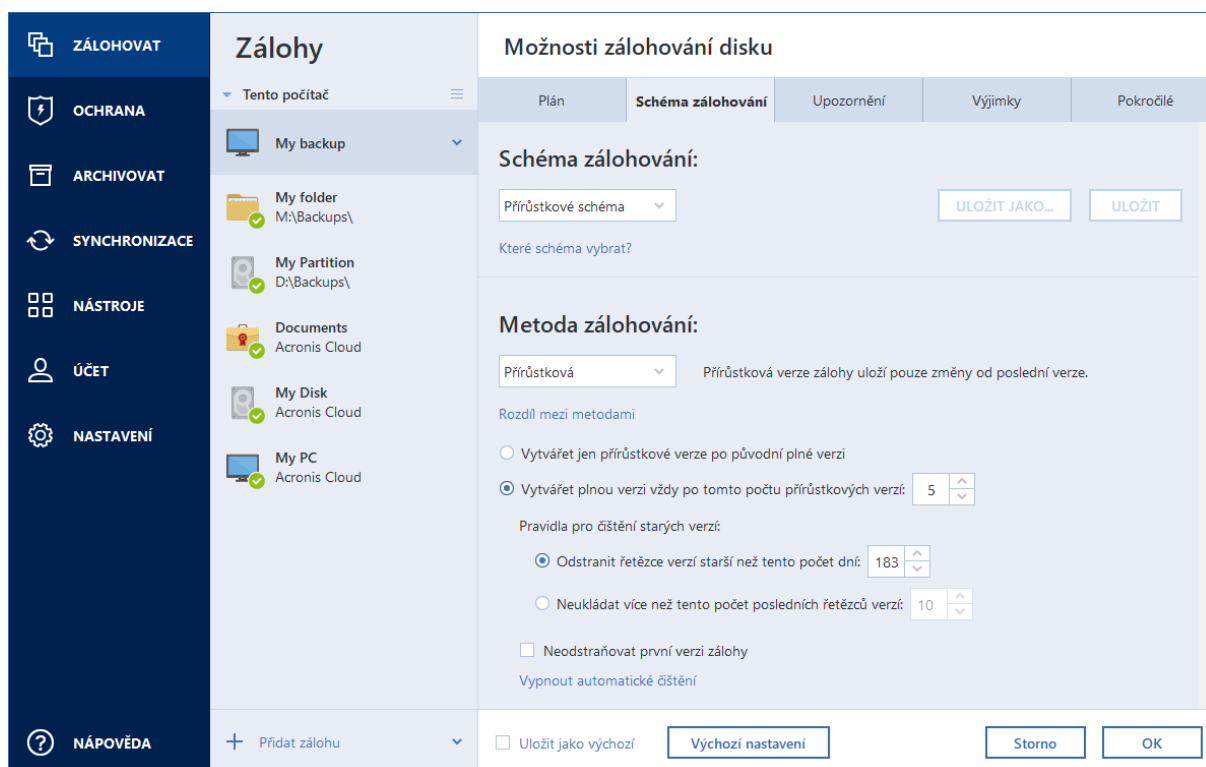
### Poznámka

U online záloh je schéma zálohování přednastavené a nelze jej měnit. Po první plné záloze jsou vytvářeny pouze přírůstkové verze.

---

Schémata zálohování definují následující parametry:

- [metody zálohování](#), které budou použity při vytváření verzí záloh (plné, rozdílové nebo přírůstkové),
- posloupnost verzí záloh vytvořených pomocí různých metod,
- pravidla k vyčištění verzí.



Aplikace Acronis Cyber Protect Home Office umožňuje vybrat z následujících schémat zálohování:

- **Schéma jedné verze** – Toto schéma vyberte, pokud chcete využít nejmenší úložiště zálohy.
- **Schéma řetězce verzí** – Toto schéma je vhodné v celé řadě případů.
- **Přírůstkové schéma** – Vyberte, pokud chcete vytvářet plnou verzi po pěti přírůstkových verzích. Toto je výchozí schéma.
- **Rozdílové schéma** – Vyberte, pokud chcete po počáteční plné záloze vytvářet pouze rozdílové zálohy.
- **Vlastní schéma** – Vyberte, pokud chcete schéma zálohování nastavit ručně.

Můžete snadno měnit schéma zálohování pro předem existující zálohu. Tato situace neovlivní integritu řetězců záloh, takže budete moci obnovit svá data z předchozích verzí záloh.

### Poznámka

Schéma zálohování nelze změnit při zálohování optického média, například DVD nebo BD. V tomto případě aplikace Acronis Cyber Protect Home Office implicitně používá vlastní schéma pouze s plnými zálohami. To proto, že aplikace neumí sloučit zálohy uložené na optických médiích.

## Schéma jedné verze

Toto schéma zálohování je stejné pro zálohu disků i souborů (kromě nastavení plánovače).

Aplikace vytvoří plnou verzi zálohy a přepisuje ji podle plánu, nebo když provedete zálohování ručně. V tomto procesu se stará verze odstraní pouze po vytvoření nové verze.

---

## Poznámka

Zcela první soubor bude zachován pro pomocné účely, nebude však obsahovat žádná vaše data. Neodstraňujte ho.

---

Nastavení plánovače zálohování pro zálohu disku: měsíčně.

Nastavení plánovače zálohování pro zálohu souborů: denně.

Výsledek: máte k dispozici jednu aktuální plnou verzi zálohy.

Požadovaný prostor v úložišti: minimální.

## Schéma řetězce verzí

Toto schéma zálohování se liší u zálohování disků a souborů.

### Řetězec verzí záloh disků

Aplikace nejprve vytvoří plnou verzi zálohy. Tato verze bude uchovávána, pokud ji ručně neodstraníte. Poté aplikace podle plánu (nebo při ručním zálohování) vytvoří: 1 plnou a 5 rozdílových verzí záloh, poté znovu 1 plnou a 5 rozdílových verzí záloh atd. Verze budou uloženy po dobu 6 měsíců. Poté aplikace rozhodne, zda můžou být nejstarší verze zálohy (kromě první plné verze) odstraněny. Záleží to na minimálním množství verzí (osm) a konzistenci řetězce verzí. Aplikace odstraní nejstarší verze jednu po druhé po vytvoření nových verzí stejnou metodou zálohování (například nejstarší rozdílová verze bude odstraněna po vytvoření nejnovější rozdílové verze). Nejprve budou odstraněny nejstarší rozdílové verze, poté – nejstarší plná verze.

Nastavení plánovače zálohování: měsíčně.

Výsledek: budete mít měsíční verze záloh po dobu posledních 6 měsíců a počáteční plnou verzi zálohy, kterou si můžete ponechat déle.

Požadovaný prostor v úložišti: závisí na počtu verzí a jejich velikosti.

### Řetězec verzí záloh souborů

Podle plánu (nebo při ručním zálohování) aplikace vytvoří: 1 plnou a 6 přírůstkových verzí záloh, poté znovu 1 plnou a 6 přírůstkových verzí záloh atd. Verze budou uloženy po dobu 1 měsíce. Poté aplikace rozhodne, zda můžou být nejstarší verze zálohy odstraněny. Záleží to na konzistenci řetězce verzí. Aby se zachovala konzistence, odstraní aplikace nejstarší verze po řetězcích „1 plná + 6 přírůstkových verzí záloh“ až po vytvoření nového podobného řetězce verzí.

Nastavení plánovače zálohování: denně.

Výsledek: máte verze záloh z každého dne posledního měsíce.

Požadovaný prostor v úložišti: závisí na počtu verzí a jejich velikosti.

## Vlastní schémata

Aplikace Acronis Cyber Protect Home Office také umožňuje tvorbu vlastních schémat zálohování. Schémata mohou být založena na předdefinovaných schématech zálohování. Můžete vybrané předdefinované schéma změnit tak, aby vyhovovalo vašim potřebám a poté jej uložit jako nové schéma.

---

### Poznámka

Předdefinovaná schémata zálohování přepsat nelze.

---

Navíc můžete vytvořit vlastní schéma od základů a založit jej na plných, rozdílových nebo přírůstkových zálohách.

Nejprve tedy zaškrtněte políčko u jedné z těchto metod.

- **Plná**

Tuto metodu vyberte, pokud chcete vytvářet pouze plné verze záloh.

- **Přírůstková**

Tuto metodu vyberte, pokud chcete vytvářet řetězce záloh obsahující pouze plné a přírůstkové verze záloh.

Schéma můžete upravit použitím jedné z následujících možností:

- **Po vytvoření plné verze zálohy vytvářet pouze přírůstkové verze** – Chcete-li vytvářet pouze jeden řetězec verzí záloh, zvolte tuto možnost. Pro tuto možnost není dostupné automatické vyčištění.
- **Vytvářet plnou verzi po [n] přírůstkových verzích** – Chcete-li vytvářet několik řetězců verzí záloh, vyberte tuto možnost. Toto schéma zálohování je spolehlivější, vyžaduje ale také více místa na disku.

- **Rozdílová**

Tuto metodu vyberte, pokud chcete vytvářet řetězce záloh obsahující pouze plné a rozdílové verze záloh.

Schéma můžete upravit použitím jedné z následujících možností:

- **Po vytvoření plné verze zálohy vytvářet pouze rozdílové verze** – Chcete-li vytvářet pouze jeden řetězec verzí záloh, zvolte tuto možnost. Pro tuto možnost není dostupné automatické vyčištění.
- **Vytvářet plnou verzi po [n] rozdílových verzích** – Chcete-li vytvářet několik řetězců verzí záloh, vyberte tuto možnost. Toto schéma zálohování je spolehlivější, vyžaduje ale také více místa na disku.

### Zapnout automatické čištění

- **Pravidla pro vyčištění starých verzí** – Chcete-li automaticky odstraňovat zastaralé verze záloh, můžete nastavit jedno z následujících pravidel vyčištění:
  - **Odstranit verze starší než [n] dní** [dostupné pouze pro metodu plného zálohování] – Chcete-li omezit stáří verzí záloh, zvolte tuto možnost. Všechny verze starší než zvolené období budou

automaticky odstraněny.

- **Odstranit řetězce verzí starší než [n] dní** [dostupné pouze pro metody přírůstkového a rozdílového zálohování] – Chcete-li omezit stáří řetězců verzí záloh, zvolte tuto možnost. Nejstarší řetězec verzí se smaže pouze v případě, že je poslední verze zálohy řetězce starší než určené období.
- **Nenechávat uložených více než [n] posledních verzí** [dostupné pouze pro metodu plného zálohování] – Chcete-li omezit maximální počet verzí záloh, zvolte tuto možnost. Když počet verzí přesáhne určitou hodnotu, nejstarší verze zálohy bude automaticky odstraněna.
- **Nenechávat uložených více než [n] posledních řetězců verzí** [dostupné pouze pro metody přírůstkového a rozdílového zálohování] – Chcete-li omezit maximální počet řetězců verzí záloh, zvolte tuto možnost. Když počet řetězců verzí přesáhne určitou hodnotu, nejstarší řetězec verzí záloh bude automaticky odstraněn.
- **Nepřesahovat velikost zálohy [definovaná velikost]** [není k dispozici pro místní zálohy] – Chcete-li omezit maximální velikost zálohy, zvolte tuto možnost. Po vytvoření nové verze zálohy aplikace zkontroluje, zda celková velikost zálohy přesahuje zadanou hodnotu. Pokud ji přesahuje, nejstarší verze zálohy bude odstraněna.
- **Neodstraňovat první verzi zálohy** – Chcete-li ukládat počáteční stav dat, zaškrtněte toto políčko. Aplikace vytvoří dvě počáteční plné verze zálohy. První verze bude vyloučena z automatického vyčištění a bude uchovávána, dokud ji neodstraníte ručně. Pokud vyberete metodu přírůstkovou nebo rozdílovou, první řetězec záloh bude začínat od druhé plné verze zálohy. A pouze třetí verze zálohy bude přírůstková nebo rozdílová. Pokud je toto políčko zaškrtnuté u metody plného zálohování, změní se políčko **Nenechávat uložených více než [n] posledních verzí** na **Nenechávat uložených více než 1+[n] posledních verzí**.

## Správa vlastních schémat zálohování

Pokud v existujícím schématu zálohování cokoliv změníte, lze jej uložit jako nové schéma. V tomto případě bude nutné pro schéma zálohování zadat nový název.

- Existující vlastní schémata lze přepisovat.
- Předdefinovaná schémata zálohování přepsat nelze.
- V názvu schématu lze použít všechny znaky povolené operačním systémem v názvech souborů. Maximální délka názvu schématu zálohování je 255 znaků.
- Nelze vytvořit více než 16 vlastních schémat zálohování.

Po vytvoření vlastního schématu zálohování jej lze použít jako kterékoliv jiné schéma zálohování při konfiguraci zálohování.

Vlastní schéma zálohování lze také použít bez jeho uložení. V tomto případě bude dostupné pouze pro zálohu, ve které bylo vytvořeno, a nebudete jej moci v dalších zálohách použít.

Pokud vlastní schéma zálohování již nepotřebujete, můžete jej odstranit. Chcete-li schéma odstranit, vyberte jej v seznamu schémat zálohování, klikněte na tlačítko **Odstranit** a poté proveďte potvrzení v okně **Odstranit schéma**.

---

## Poznámka

Předdefinovaná schémata zálohování nelze odstranit.

---

## Příklady vlastních schémat

### 1. Zálohování celého počítače „Dvě plné verze“

Příklad: Chcete chránit všechna data ve svém počítači pomocí dvou plných verzí a chcete aktualizovat zálohu jednou měsíčně. Podíváme se, jak to lze provést pomocí vlastního schématu zálohování.

1. Začněte konfigurací zálohy celého počítače. Podrobnosti naleznete v části [Zálohování všech dat v počítači](#).
2. Ujistěte se, že je jako zdroj zálohování zvolen celý počítač.
3. Klikněte na tlačítko **Možnosti**, otevřete kartu **Plán**, klikněte na možnost **Měsíčně** a pak určete den v měsíci (například 20. den). Na základě tohoto nastavení bude v určený den každý měsíc vytvářena záložní verze. Poté zadejte čas spuštění operace zálohování.
4. Otevřete kartu **Schéma zálohování** a zvolte **Vlastní schéma** místo **Přírůstkové schéma**.
5. V poli **Metoda zálohování** vyberte v rozevíracím seznamu položku **Úplná**.
6. Chcete-li omezit počet verzí, klikněte na položku **Neukládat více než [n] posledních verzí**, zadejte nebo vyberte hodnotu „2“ a klikněte na tlačítko **OK**.  
V tomto případě program vytvoří novou úplnou verzi každý měsíc ke 20. dni. Po vytvoření třetí verze bude nejstarší verze automaticky odstraněna.
7. Zkontrolujte, zda jsou veškerá nastavení správná a klikněte na tlačítko **Zálohovat nyní**. Chcete-li, aby první zálohování proběhlo až v čase, který jste zadali do plánovače, klikněte na šipku dolů vpravo od tlačítka **Zálohovat nyní** a v rozevíracím seznamu vyberte položku **Později**.

### 2. Zálohování souborů „Denně přírůstková verze + týdně plná verze“

Příklad: Máte soubory a složky, se kterými pracujete každý den. Potřebujete ukládat denní výsledky práce a chcete mít možnost obnovit stav dat do jakéhokoliv data za poslední tři týdny. Podíváme se, jak lze toto provést pomocí vlastního schématu zálohování.

1. Spusťte konfiguraci zálohování souborů. Další informace naleznete v části [Zálohování souborů a složek](#).
2. Klikněte na tlačítko **Možnosti**, otevřete kartu **Plán**, klikněte na možnost **Denně** a pak zadejte čas spuštění operace zálohování. Pokud například končíte práci každý den ve 20:00, jako čas spuštění operace zadejte tento nebo o trochu pozdější čas (20:05).
3. Otevřete kartu **Schéma zálohování** a zvolte **Vlastní schéma** místo **Přírůstkové schéma**.
4. V poli **Metoda zálohování** vyberte v rozevíracím seznamu položku **Přírůstková**.
5. Klikněte na možnost **Vytvářet plnou verzi vždy po [n] přírůstkových verzích** a zadejte nebo vyberte hodnotu „6“.



V tomto případě aplikace nejprve vytvoří počáteční plnou verzi zálohy (nezávisle na tom, jak proces zálohování nastavíte, první verze zálohy bude vždycky plná) a poté šest přírůstkových verzí den po dni. Potom znovu vytvoří jednu plnou verzi a šest přírůstkových verzí atd. Nové plné verze budou tedy vytvářeny vždy přesně po týdnu.

6. Chcete-li omezit čas uložení verzí, klikněte na možnost **Zapnout automatické čištění**.
7. Klikněte na možnost **Odstranit řetězce verzí starší než [n] dní**, zadejte nebo vyberte hodnotu „21“ a klikněte na tlačítko **OK**.
8. Zkontrolujte, zda jsou veškerá nastavení správná a klikněte na tlačítko **Zálohovat nyní**. Chcete-li, aby první zálohování proběhlo až v čase, který jste zadali do plánovače, klikněte na šipku dolů vpravo od tlačítka **Zálohovat nyní** a v rozevíracím seznamu vyberte položku **Později**.

### 3. Zálohování disku „Plná verze každé 2 měsíce + rozdílová verze dvakrát za měsíc“

Příklad: Potřebujete dvakrát za měsíc zálohovat systémový diskový oddíl a vytvářet novou plnou verzi zálohy každé dva měsíce. Navíc nechcete k uložení verzí zálohy použít více než 100 GB místa na disku. Podíváme se, jak lze toto provést pomocí vlastního schématu zálohování.

1. Spusťte konfiguraci zálohování disků. Další informace naleznete v části [Zálohování diskových oddílů a disků](#).
2. Jako zdroj zálohy vyberte svůj systémový oddíl (obvykle C:).
3. Klikněte na tlačítko **Možnosti**, otevřete kartu **Plán**, klikněte na možnost **Měsíčně** a pak zadejte například 1. a 15. den v měsíci. Nová verze zálohy se bude vytvářet přibližně každé dva týdny. Poté zadejte čas spuštění operace zálohování.
4. Otevřete kartu **Schéma zálohování** a zvolte **Vlastní schéma** místo **Přírůstkové schéma**.
5. V poli **Metoda zálohování** vyberte v rozevíracím seznamu možnost **Rozdílová**.
6. Klikněte na možnost **Vytvářet plnou verzi vždy po [n] rozdílových verzích** a zadejte nebo vyberte hodnotu „3“.

V tom případě aplikace nejprve vytvoří počáteční plnou verzi zálohy (nezávisle na tom, jak proces zálohování nastavíte, první verze zálohy bude vždycky plná) a poté tři rozdílové verze zhruba po dvou týdnech. Potom zase plnou verzi a tři rozdílové verze atd. Každá nová plná verze bude tedy vytvořena za dva měsíce.

7. Chcete-li omezit prostor k uložení verzí, klikněte na možnost **Zapnout automatické čištění**.
8. Klikněte na možnost **Nepřesahovat velikost zálohy [definovaná velikost]**, zadejte nebo zvolte „100“ „GB“ a klikněte na tlačítko **OK**.

---

#### Poznámka

Když celková velikost zálohy přesáhne 100 GB, aplikace Acronis Cyber Protect Home Office vyčistí existující verze zálohy a uvolní tak místo pro další zálohy. Aplikace odstraní nejstarší řetězec záloh skládající se z plné verze zálohy a tří rozdílových verzí zálohy.

---

9. Zkontrolujte, zda jsou veškerá nastavení správná a klikněte na tlačítko **Zálohovat nyní**. Chcete-li, aby první zálohování proběhlo až v čase, který jste zadali do plánovače, klikněte na šipku dolů vpravo od tlačítka **Zálohovat nyní** a v rozevíracím seznamu vyberte položku **Později**.

## 4.5.3 Upozornění na operace zálohování

Umístění: **Možnosti** > **Oznámení**

Někdy může zálohování nebo obnova trvat hodinu i déle. Aplikace Acronis Cyber Protect Home Office vás může upozornit na dokončení operace prostřednictvím e-mailu. Aplikace může zasílat také zprávy zobrazené během operace nebo po jejím dokončení zaslat celý soubor protokolu.

Ve výchozím nastavení jsou všechna upozornění vypnuta.

### Práh volného místa na disku

Upozornění, které se zobrazí v případě, že volné místo v úložišti bude menší než zadaná prahová hodnota, lze nastavit. Pokud po spuštění zálohování aplikace Acronis Cyber Protect Home Office zjistí, že v umístění vybrané zálohy je méně volného místa, než je zadáno, vůbec nezačne samotný proces zálohování a okamžitě vás informuje příslušnou zprávou. Zpráva nabízí tři možnosti – ignorovat ji a pokračovat v zálohování, vyhledat jiné umístění pro zálohu nebo zálohování zrušit.

Pokud se volné místo zmenší v průběhu zálohování, aplikace zobrazí stejnou zprávu se stejnými možnostmi.

Aplikace Acronis Cyber Protect Home Office může sledovat volné místo na následujících úložných zařízeních: místní pevné disky, karty a jednotky USB a sdílené položky v síti (SMB). Tuto možnost nelze zapnout pro servery FTP a jednotky CD/DVD.

#### ***Chcete-li nastavit práh volného místa na disku***

1. Zaškrtněte políčko **Při nedostatku volného místa na disku zobrazovat oznámení**.
2. Zadejte práh volného místa na disku do okna **Zobrazit upozornění, když je na disku méně místa než** .

---

#### **Poznámka**

Pokud je zaškrtnuto políčko **Při zpracování nezobrazovat zprávy a dialogová okna (tichý režim)** v nastavení **Zpracování chyb**, zpráva se nebude zobrazovat.

---

### E-mailové oznámení

1. Zaškrtněte políčko **Posílat upozornění e-mailem o stavech operace**.
2. Konfigurace nastavení e-mailu:
  - Do pole **Komu** zadejte e-mailovou adresu. Je možné zadat více adres oddělených středníky.
  - V poli **Nastavení serveru** zadejte server odchozí pošty (SMTP).
  - Nastavte port serveru odchozí pošty. Implicitně je tento port nastaven na 25.
  - Vyberte požadované šifrování e-mailů.
  - Je-li to vyžadováno, zaškrtněte políčko **Ověření SMTP** a poté do příslušných polí zadejte

uživatelské jméno a heslo.

3. Chcete-li zkontrolovat správnost nastavení, klikněte na tlačítko **Odeslat testovací zprávu**.

#### ***Pokud se odeslání testovací zprávy nezdaří***

1. Klikněte na možnost **Zobrazit rozšířená nastavení**.
2. Konfigurace dalších nastavení e-mailu:
  - V poli **Od** zadejte e-mailovou adresu odesílatele. Pokud si nejste jisti, jakou adresu zadat, zadejte jakoukoli adresu ve standardním formátu, například *aaa@bbb.com*.
  - V případě nutnosti změňte předmět zprávy v poli **Předmět**.  
Chcete-li zjednodušit sledování stavu zálohování, můžete přidat nejdůležitější informace do předmětu e-mailových zpráv. Můžete zadávat následující textové popisky:
    - %BACKUP\_NAME% – název zálohy
    - %COMPUTER\_NAME% – název počítače, kde bylo zálohování spuštěno
    - %OPERATION\_STATUS% – výsledek zálohování nebo jiné operaceMůžete například zadat: *Stav zálohování %BACKUP\_NAME%: %OPERATION\_STATUS% (%COMPUTER\_NAME%)*
  - Zaškrtněte políčko **Přihlásit k serveru příchozí pošty** a zadejte pod ním server příchozí pošty (POP3).
  - Nastavte port serveru příchozí pošty. Implicitně je tento port nastaven na 110.
3. Znovu klikněte na tlačítko **Odeslat testovací zprávu**.

#### ***Další nastavení upozornění***

- **Po úspěšném dokončení operace odeslat upozornění** – Zaškrtněte toto políčko pro odeslání oznámení o dokončení procesu.
- **Odeslat oznámení při selhání operace** – Zaškrtněte toto políčko pro odeslání oznámení o selhání procesu.
- **Odeslat oznámení, když je třeba zásah uživatele** – Zaškrtněte toto políčko pro odeslání oznámení s operačními zprávami.
- **Přidat úplný protokol do oznámení** – Zaškrtněte toto políčko pro odeslání oznámení s úplným protokolem operací.

---

#### **Poznámka**

Na konkrétní zálohu vám budou chodit pouze e-mailová oznámení. Pokud chcete dostávat oznámení o všech zálohách, můžete e-mailová oznámení nastavit na online kontrolním panelu. Další informace naleznete v části [E-mailová oznámení](#). Obě metody fungují nezávisle na sobě a lze je použít současně.

---

## 4.5.4 Vyloučení položek ze zálohy

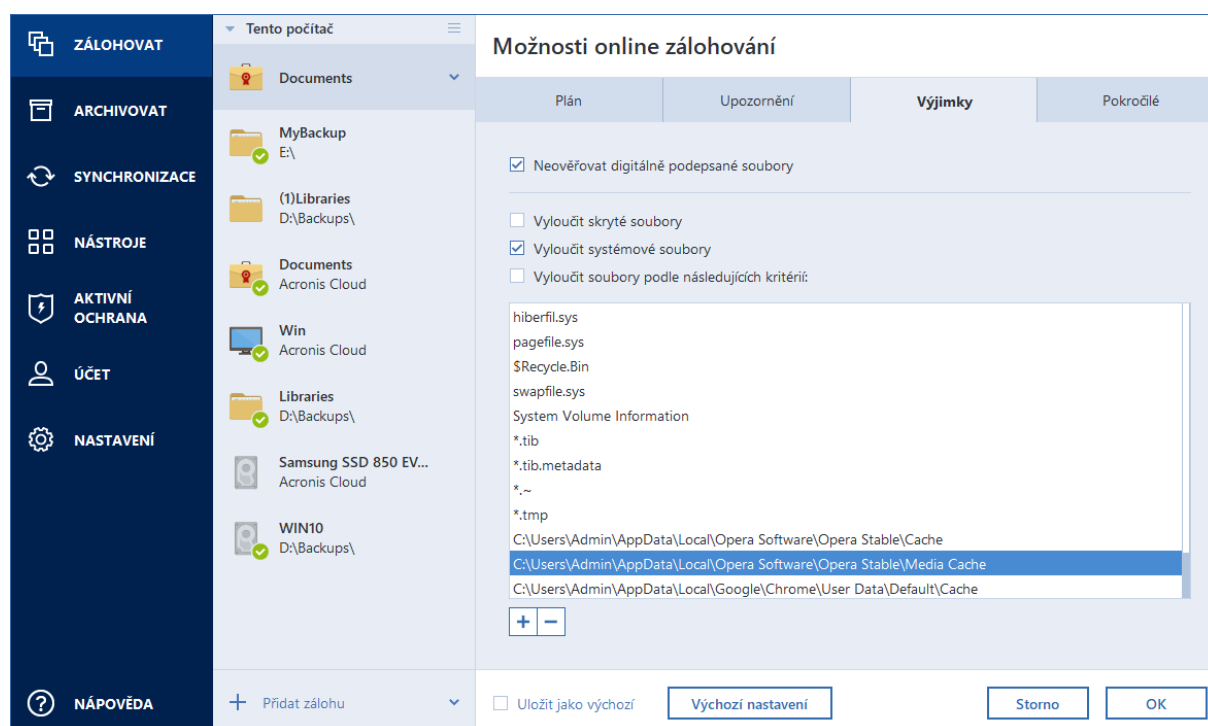
Umístění: **Možnosti** > **Výjimky**

Chcete-li vyloučit nepotřebné soubory ze zálohy, zadejte příslušné typy souborů na kartě **Vyloučení** možností zálohování. Výjimky lze specifikovat pro zálohy disku, zálohy souborů nebo online zálohy.

Vyberete-li pro zálohování určitý soubor, nelze jej vyjmout pomocí nastavení výjimek. Nastavení platí pouze pro soubory nacházející se v oddíle, na disku nebo uvnitř složky vybrané k zálohování.

## Jak používat výchozí nastavení výjimek

Po instalaci aplikace jsou všechny výjimky nastaveny na výchozí hodnoty. Můžete je měnit pouze pro aktuální operaci zálohování nebo pro všechny budoucí operace zálohování. Zaškrtnutím políčka **Uložit jako výchozí** použijete upravená nastavení na všechny další operace zálohování. Chcete-li obnovit výchozí nastavení upravených nastavení na hodnoty po instalaci, klikněte na tlačítko **Obnovit původní nastavení**.



## Co lze vyloučit a jak

Máte následující možnosti jak vyloučit soubory ze zálohování:

- **Neověřovat digitálně podepsané soubory** (dostupné pouze pro ověřené zálohy) – hlavním účelem ověřené zálohy je ochrana vašich osobních souborů. Proto není třeba zálohovat systémové soubory, aplikační soubory ani další soubory, které mají digitální podpis. Chcete-li tyto soubory vyloučit, zaškrtněte příslušné políčko.
- **Vyloučit skryté soubory**– toto políčko zaškrtněte pro vyloučení skrytých souborů a složek ze zálohování na úrovni souborů.
- **Vyloučit systémové soubory**– toto políčko zaškrtněte pro vyloučení systémových souborů a složek ze zálohování na úrovni souborů.

Je možné vyloučit soubory splňující vámi zadaná kritéria. To provedete zaškrtnutím políčka **Vyloučit soubory podle následujících kritérií**, kliknutím na znaménko plus a vložením vylučujícího kritéria.

---

#### **Poznámka**

Vyloučení skrytých a systémových souborů ze záloh systémového oddílu nedoporučujeme.

---

#### **Přidání vylučujícího kritéria**

- Můžete zadat přesný název souboru, který bude ze zálohy vyloučen:
  - *soubor.příp*– všechny takovéto soubory budou ze zálohy vyloučeny.
  - *C:\soubor.příp*– soubor *soubor.příp* na disku C: bude vyloučen.
- Lze použít zástupné znaky (\* a ?):
  - *\*.příp*– všechny soubory s příponou *.příp* budou vyloučeny.
  - *??název.příp*– všechny soubory s příponou *.příp* a šesti písmeny v názvu (začínající libovolnými dvěma symboly – ?? – a končící slovem *název*) budou vyloučeny.
- Chcete-li vyloučit složku ze zálohy na úrovni disku, klikněte na znaménko plus, klikněte na tlačítko se třemi tečkami, přejděte do stromu adresářů, vyberte složku, kterou chcete vyloučit, a pak klikněte na tlačítko **OK**.

Chcete-li odstranit omylem přidané kritérium, vyberte je v seznamu a pak klikněte na znaménko mínus.

## 4.5.5 Režim tvorby diskového obrazu

Umístění: **Možnosti > Rozšířené > Režim tvorby diskového obrazu**

Tato možnost není k dispozici pro zálohy s cílovým umístěním na úložišti Acronis Cloud.

Tyto parametry můžete použít k vytvoření přesné kopie celých diskových oddílů nebo pevných disků (nejen sektorů), které obsahují data. Toto může být užitečné, například pokud chcete zálohovat diskový oddíl nebo disk obsahující operační systém, který aplikace Acronis Cyber Protect Home Office nepodporuje. Nezapomeňte, že tento režim prodlužuje čas zpracování a výsledkem je obvykle větší soubor obrazu.

- Chcete-li vytvořit obraz sektor po sektoru, zaškrtněte políčko **Zálohovat sektor po sektoru**.
- Chcete-li do zálohy zahrnout veškerý nepřidělený prostor na disku, zaškrtněte políčko **Zálohovat nepřidělený prostor**.  
Toto zaškrťovací políčko je k dispozici, pouze pokud je zaškrtnuto políčko **Zálohovat sektor po sektoru**.

## 4.5.6 Ochrana zálohy

Umístění: Kontrolní panel zálohování > **Možnosti > Rozšířené > Ochrana zálohy**

---

### Poznámka

Toto téma lze použít pro místní a síťové zálohy. Informace o ochraně cloudových záloh naleznete v části [Ochrana online zálohování](#).

---

Ve výchozím nastavení není pro zálohu nastavena žádná ochrana heslem. Heslo pro ochranu záloh si však můžete nakonfigurovat.

---

### Poznámka

Možnost ochrany zálohy pro předem existující zálohu změnit nelze.

---

### Jak ochránit zálohu

1. Do příslušného pole zadejte heslo zálohy. Heslo musí obsahovat nejméně sedm znaků a mělo by obsahovat jak písmena (nejlépe velká i malá), tak číslice, aby bylo obtížnější jej uhodnout.
- 

### Poznámka

Heslo nelze obnovit. Zapamatujte si heslo, které jste použili pro ochranu zálohy.

---

2. Pro potvrzení dříve zadaného hesla ho znovu zadejte do příslušného pole.
3. [volitelný krok] Chcete-li zvýšit bezpečnost důvěrných dat, můžete zálohu zašifrovat pomocí šifrovacího algoritmu normy AES (Advanced Encryption Standard). Algoritmus AES je dostupný se třemi délkami klíče – 128, 192 a 256 bitů, aby bylo možné vyvážit podle potřeby výkon a ochranu. Pro většinu případů použití je postačující šifrovací klíč o délce 128 bitů. Čím delší je klíč, tím lépe jsou data chráněna. Klíče o délce 192 a 256 bitů však výrazně zpomalují proces zálohování. Chcete-li použít šifrování AES, vyberte jeden z následujících klíčů:
  - **AES 128**– použít 128bitový šifrovací klíč,
  - **AES 192**– použít 192bitový šifrovací klíč,
  - **AES 256**– použít 256bitový šifrovací klíč.Pokud nechcete zálohu šifrovat, ale chránit ji jen pomocí hesla, vyberte možnost **Žádné**.
4. Po zvolení nastavení zálohování klikněte na tlačítko **OK**.

### Jak získat přístup k záloze chráněné heslem

Aplikace Acronis Cyber Protect Home Office vyžaduje zadání hesla při každém pokusu o úpravu zálohy:

- Obnova dat ze zálohy
- Upravit nastavení
- Připojit
- Přesunout

Pro přístup k této záloze je nutné zadat správné heslo. Z bezpečnostních důvodů neexistuje způsob, jak obnovit ztracená hesla.

## 4.5.7 Ochrana pomocí online zálohování

Umístění: **Možnosti** > **Rozšířené** > **Ochrana zálohy**

Chcete-li data ve službě Acronis Cloud chránit před neoprávněným přístupem, můžete použít šifrování. V takovém případě budou data při zálohování šifrována pomocí algoritmu AES-256 a následně uložena do úložiště Acronis Cloud. K šifrování a dešifrování dat potřebuje aplikace heslo, které je nutné určit při konfiguraci online zálohy. Můžete zadat libovolnou množinu znaků. Nezapomeňte, že u hesla se rozlišuje velikost písmen.

---

### Upozornění!

Heslo online zálohy nelze načíst. Zapamatujte si heslo, které jste použili pro ochranu zálohy.

---

Při pokusu o přístup k šifrovaným datům si aplikace vyžádá zadání hesla.

---

### Poznámka

Nezapomeňte, že není možné nastavit nebo změnit heslo pro již existující online zálohu.

---

## 4.5.8 Příkazy Před/Po pro zálohování

Umístění: **Možnosti** > **Rozšířené** > **Příkazy Před/Po**

Tato možnost není k dispozici pro zálohy s cílovým umístěním na úložišti Acronis Cloud.

Je možné zadat příkazy (nebo dokonce dávkové soubory), které budou automaticky provedeny před a po zálohování.

Například když chcete spustit či zastavit určité procesy systému Windows nebo zkontrolovat data před spuštěním zálohy.

### ***Jak zadat příkazy (dávkové soubory)***

- Zaškrtněte políčko **Použít vlastní příkazy**.
- Vyberte požadovaný příkaz, který bude proveden před spuštěním procesu zálohování v poli **Příkazy před**. Chcete-li vytvořit nový příkaz nebo vybrat nový dávkový soubor, klikněte na tlačítko **Upravit**.
- Vyberte požadovaný příkaz, který bude proveden po skončení procesu zálohování, v poli **Příkaz po**. Chcete-li vytvořit nový příkaz nebo vybrat nový dávkový soubor, klikněte na tlačítko **Upravit**.

Nepokoušejte se prosím spouštět interaktivní příkazy, tj. příkazy vyžadující zadání od uživatele (například „pause“). Ty nejsou podporovány.

## Úprava uživatelských příkazů pro zálohování

Uživatelské příkazy, které se provedou před nebo po procesu zálohování, je možné zadat:

- Do pole **Příkaz** zadejte příkaz nebo jej vyberte ze seznamu. Kliknutím na tlačítko **...** vyberte dávkový soubor.

- V poli **Pracovní adresář** zadejte cestu k provedení příkazu nebo ji vyberte v seznamu dříve zadaných cest.
- Do textového pole **Argumenty** zadejte argumenty provedení příkazu nebo je vyberte ze seznamu.

Vypnutí parametru **Neprovádět operace před dokončením vykonávání příkazu**, který je při výchozím nastavení zapnut u příkazů před spuštěním, umožní procesu zálohování běžet souběžně s prováděním příkazu.

Parametr **Zrušit operaci při selhání uživatelského příkazu** (ve výchozím nastavení zapnut) zruší operaci při výskytu jakýchkoli chyb při provádění příkazů.

Zadaný příkaz lze testovat kliknutím na tlačítko **Testovat příkaz**.

## 4.5.9 Rozdělování záloh

Umístění: **Možnosti > Rozšířené > Rozdělení zálohy**

### Poznámka

Aplikace Acronis Cyber Protect Home Office nemůže rozdělit již existující zálohy. Zálohy lze rozdělit pouze při vytváření.

Tato možnost není k dispozici pro zálohy s cílovým umístěním na úložišti Acronis Cloud.

Větší zálohy lze rozdělit na několik souborů, které dohromady tvoří původní zálohu. Zálohu je také možné rozdělit, aby ji bylo možné vypálit na vyměnitelné médium.

Výchozí nastavení **-Automaticky**. S tímto nastavením bude aplikace Acronis Cyber Protect Home Office postupovat následovně:

### Při zálohování na pevný disk:

- Jestliže je na úložném disku dostatek volného místa a jeho systém souborů odhadovanou velikost souboru podporuje, aplikace vytvoří jediný soubor zálohy.
- Pokud je na úložném disku dostatek volného místa, ale jeho systém souborů odhadovanou velikost souboru nepodporuje, obraz se automaticky rozdělí na několik souborů.
- Jestliže nemáte pro uložení obrazu na pevném disku dostatek místa, zobrazí aplikace upozornění a vyčká na rozhodnutí, jak chcete potíže vyřešit. Můžete se pokusit uvolnit více místa a pokračovat nebo vybrat jiný disk.

### Při zálohování na disk CD-R/RW, DVD-R/RW, DVD+R/RW nebo BD-R/RE:

- Acronis Cyber Protect Home Office požádá o vložení nového disku, jakmile bude ten předchozí zaplněn.

Je také možné vybrat požadovanou velikost souboru v rozevíracím seznamu. Záloha se poté rozdělí do více souborů o zadané velikosti. To je dobré při zálohování na pevný disk s plánem pozdějšího vypálení zálohy na disk CD-R/RW, DVD-R/RW, DVD+R/RW nebo BD-R/RE.



---

## Poznámka

Tvorba obrazů přímo na disk CD-R/RW, DVD-R/RW, DVD+R/RW, BD-R/RE může trvat mnohem déle než na pevný disk.

---

### 4.5.10 Možnosti ověření zálohy

Umístění: **Možnosti** > **Rozšířené** > **Ověření**

Tato možnost není k dispozici pro zálohy s cílovým umístěním na úložišti Acronis Cloud.

Můžete určit následující nastavení:

- **Ověřit zálohu po každém vytvoření** – Výběrem této možnosti zkontrolujete integritu verze zálohy ihned po zálohování. Tuto možnost doporučujeme zapnout při zálohování důležitých dat nebo systémového disku.
  - **Ověřit pouze nejnovější odlišnou verzi zálohy** – Rychlá kontrola poslední části zálohy.
  - **Ověřit celou zálohu**
- **Ověřovat zálohu podle plánu** – Vyberte možnost naplánovat ověřování záloh a kontrolovat, zda jsou stále v pořádku.
  - **Poslední odlišná verze zálohy po dokončení**
  - **Celá záloha po dokončení**

Výchozí nastavení jsou následující:

- **Frekvence** – Jednou měsíčně.
- **Den** – Datum zahájení zálohování.
- **Čas** – Čas zahájení zálohování plus 15 minut.

Zahájení ověření můžete nakonfigurovat také ručně z kontextové nabídky zálohování.

Provedete to tak, že na zálohu kliknete pravým tlačítkem a zvolíte možnost:

- **Ověřit všechny verze**
- **Ověřit nejnovější verzi**

Příklad: Spustíte operaci zálohování 15. července ve 12.00. Verze zálohy je vytvořena ve 12.05. Ověření této zálohy se spustí ve 12.15, pokud v tuto dobu bude počítač v režimu „společně obrazovky“. V opačném případě se ověření nespustí. Za měsíc, 15. srpna ve 12.15, se ověření spustí znovu. Počítač musí být opět v režimu „společně obrazovky“. To stejné se provede 15. září a tak dále.

Výchozí nastavení můžete změnit a určit vlastní plán. Další informace naleznete v části [Plánování](#).

### 4.5.11 Rezervní kopie zálohy

Umístění: **Možnosti** > **Rozšířené** > **Rezervní kopie zálohy**

Tato možnost není k dispozici pro zálohy s cílovým umístěním ve službě Acronis Cloud a pro místní zálohy vytvořené v aplikaci Acronis True Image (2020 či 2021) a Acronis Cyber Protect Home Office.

Rezervní kopie zálohy je nezávislá verze plné zálohy vytvořená okamžitě po normálním zálohování. I když vytváříte přírůstkovou nebo rozdílovou verzi zálohy obsahující pouze změny dat, bude rezervní kopie obsahovat všechna data vybraná pro normální zálohu. Rezervní kopie záloh je možné uložit do systému souborů, na síťový disk nebo USB flash disk.

---

### Poznámka

Nezapomeňte, že média CD/DVD nejsou podporována jako umístění pro rezervní kopie.

---

### ***Jak vytvořit rezervní kopii***

1. Zaškrtněte políčko **Vytvářet rezervní kopie záloh**.
2. Určete umístění kopií záloh.
3. Vyberte formát rezervní kopie. Můžete ji vytvořit jako zálohu Acronis (soubory TIB) nebo jednoduše zkopírovat zdrojové soubory do vybraného umístění beze změny a bez jakékoli úpravy.
4. [Volitelný krok] Chraňte rezervní kopii pomocí hesla.  
Všechny ostatní možnosti zálohy se převezmou ze zdrojové zálohy.

## 4.5.12 Možnosti vyměnitelného média

Umístění: **Možnosti > Rozšířené > Možnosti vyměnitelného média**

Při zálohování na vyměnitelná média z nich můžete vytvořit spouštěcí média tak, že na ně zapíšete další součásti. Nebudete tedy potřebovat další spouštěcí disk.

---

### Upozornění!

Aplikace Acronis Cyber Protect Home Office nepodporuje tvorbu spouštěcího média, pokud flash disk je ve formátu NTFS nebo exFAT. Na disku musí být systém souborů FAT16 nebo FAT32.

---

K dispozici jsou následující nastavení:

- **Umístit aplikaci Acronis Cyber Protect Home Office na médium** – Důrazně doporučujeme zvolit tuto možnost, aby byla podporována rozhraní USB, karta PC Card (dříve PCMCIA) a SCSI spolu s úložnými zařízeními připojenými jejich prostřednictvím.
- **Umístit aplikaci Acronis Cyber Protect Home Office (64-bit) na médium** – Stejná možnost pro 64bitové systémy.
- **Umístit nástroj Systémová zpráva Acronis na médium** – Tuto možnost vyberte, chcete-li vygenerovat systémovou zprávu, která se používá k seskupení informací o systému v případě potíží s aplikací. Generování zprávy bude dostupné před spuštěním aplikace Acronis Cyber Protect Home Office ze spouštěcího média. Vygenerovanou systémovou zprávu lze uložit na USB flash disk.

- **Umístit nástroj Systémová zpráva Acronis (64bitová verze) na médium** – Stejná možnost pro 64bitové systémy.
- **Požádat o vložení prvního média při zálohování na vyměnitelná média** – Tuto možnost vyberte, chcete-li při zálohování na vyměnitelná média zobrazit výzvu **Vložte první médium**. Při použití výchozích nastavení (zvolené možnosti) není zálohování na vyměnitelná média možné bez účasti uživatele, protože aplikace čeká na kliknutí na tlačítko **OK** v okně výzvy. Proto byste při plánování zálohování na vyměnitelné médium měli výzvu vypnout. V tom případě se může zálohování bez problémů spustit, pokud je dostupné vyměnitelné médium (například je vložen disk CD-R/RW).

Pokud máte v počítači nainstalované i jiné produkty společnosti Acronis, budou se spouštěcí verze jejich součástí také nacházet v nabídce.

## 32bitové nebo 64bitové komponenty

Dávejte pozor, které verze aplikace Acronis Cyber Protect Home Office a Systémová zpráva Acronis jsou kompatibilní s vaším počítačem.

	32bitové komponenty	64bitové komponenty
32bitové počítače se systémem BIOS	+	-
64bitové počítače se systémem BIOS	+	+
32bitové počítače se systémem EFI	+	-
64bitové počítače se systémem EFI	-	+

### 4.5.13 Zpracování chyb

Když aplikace Acronis Cyber Protect Home Office narazí při provádění zálohy na chybu, zastaví proces zálohování, zobrazí zprávu a čeká na odpověď, jak chybu zpracovat. Můžete nakonfigurovat zásady zpracování chyb, aby aplikace Acronis Cyber Protect Home Office nezastavila proces zálohování, ale zpracovala chybu podle nastavených pravidel a pokračovala v práci.

#### Poznámka

Toto téma se vztahuje na zálohy, které používají místní nebo síťové cílové složky. Možnosti zpracování chyb pro zálohy využívající jako cílové umístění Acronis Cloud naleznete v tématu [Zpracování chyb při zálohování a replikaci do cloudu](#).

#### Postup nastavení zásad zpracování chyb:

1. Na kontrolním panelu zálohování klikněte na položku > **Možnosti** > **Rozšířené** > **Zpracování chyb**
2. Nastavení zásad zpracování chyb:
  - **Při zpracování nezobrazovat zprávy a dialogová okna (tichý režim)**– po zapnutí této možnosti se budou chyby během operací zálohování ignorovat. Toto je užitečné, když

nemůžete proces zálohování sami řídit.

- **Ignorovat chybné sektory**– tato možnost je dostupná pouze pro zálohy disků a oddílů. Po výběru této možnosti budete moci dokončit zálohu, i když jsou na disku chybné sektory.

Doporučujeme zaškrtnout toto políčko, jestliže váš pevný disk selhává, například pokud:

- Pevný disk během provozu klape nebo rachotí.
- Systém S.M.A.R.T. zjistil na pevném disku problémy a doporučuje disk co nejdříve zálohovat.

Když toto políčko nezaškrtnete, nemusí se zálohování zdařit kvůli možným vadným sektorům na disku.

- **Není-li v zóně ASZ dostatek místa, odstraňte nejstarší zálohu** (ve výchozím nastavení zapnuto) – Doporučujeme toto políčko zaškrtnout při plánování bezobslužného zálohování do zóny Acronis Secure Zone. Pokud ho nezaškrtnete, pak v případě, že bude zóna Acronis Secure Zone během operace zálohování plná, pozastaví aplikace Acronis Cyber Protect Home Office zálohování a bude vyžadovat váš zásah. Toto dialogové okno se zobrazí i v případě, že je zapnuté nastavení **Při zpracování nezobrazovat zprávy a dialogová okna (tichý režim)**.
- **Opakovat pokus, pokud se zálohování nezdaří**– tato možnost umožňuje automaticky opakovat pokus o zálohování, pokud z nějakého důvodu selže. Můžete zadat počet pokusů a interval mezi pokusy. Pokud chyba brání v zálohování přetrvává, zálohu nebude možné vytvořit.

---

#### **Poznámka**

Naplánované zálohovací operace se spustí až po dokončení všech pokusů.

---

3. Klikněte na tlačítko **OK**.

## Zpracování chyb při zálohování a replikaci do cloudu

Aplikaci Acronis Cyber Protect Home Office můžete nakonfigurovat, aby znovu zkusila provést nezdařené zálohování a replikace do cloudu.

#### **Konfigurace počtu opětovných pokusů a intervalu mezi nimi:**

1. Na kontrolním panelu **Zálohování** klikněte na možnost Zálohovat do cloudu, poté na **Možnosti** a přejděte na kartu **Rozšířené**.
2. V části **zpracování chyb** zaškrtněte políčko **Opakovat pokus, pokud se zálohování nezdaří** a zvolte počet pokusů (1 až 99) a interval mezi nimi.
3. Klikněte na tlačítko **OK**.

Nové nastavení se použije na všechny následující operace zálohování a replikace do cloudu u vybraného objektu zálohování.

---

#### **Poznámka**

Naplánované zálohovací operace se spustí až po dokončení všech pokusů o zopakování zálohování.

---

## 4.5.14 Nastavení zabezpečení zálohy na úrovni souborů

Umístění: **Možnosti** > **Rozšířené** > **Nastavení zabezpečení na úrovni souborů**

### Poznámka

Tato možnost je dostupná pouze pro zálohování na úrovni souborů.

Tato možnost není k dispozici pro zálohy s cílovým umístěním na úložišti Acronis Cloud.

Nastavení zabezpečení zálohovaných souborů můžete určit:

- **Zachovat nastavení zabezpečení souborů v zálohách** – zaškrtnutím tohoto políčka zachováte všechny vlastnosti zabezpečení (oprávnění přiřazená ke skupinám nebo uživatelům) zálohovaných souborů pro pozdější obnovení.

Při výchozím nastavení jsou soubory a složky ukládány do zálohy s původním nastavením zabezpečení systému Windows (například oprávnění ke čtení, k zápisu a spouštění a podobně pro každého uživatele nebo skupinu uživatelů, nastavovaná v nabídce **Vlastnosti** -> **Zabezpečení**). Pokud obnovíte zabezpečený soubor nebo složku v počítači bez uživatele, jemuž náleží práva, nemusí být možné tento soubor číst nebo upravovat.

Chcete-li se těmto problémům vyhnout, můžete vypnout zachování nastavení zabezpečení souborů v zálohách. V tomto případě převezmou obnovené soubory a složky oprávnění od složky, do které jsou obnoveny (nadřazená složka nebo disk, pokud obnova probíhá do kořenového adresáře).

Eventuálně můžete nastavení zabezpečení souborů během obnovy zrušit, i když jsou v záloze dostupná. Výsledek bude stejný.

- **V zálohách uchovávat šifrované soubory v dešifrovaném stavu** (výchozí nastavení je vypnuto) – zaškrtněte toto políčko v případě, že jsou v záloze šifrované soubory a chcete je po obnovení zpřístupnit všem uživatelům. Pokud tak neučiníte, bude tyto soubory nebo složky moci číst jen uživatel, který je zašifroval. Dešifrování může být užitečné také v případě, že chcete šifrované soubory obnovit na jiném počítači.

Pokud nepoužíváte funkci šifrování dostupnou v operačních systémech Windows XP a novějších, tuto možnost ignorujte. (Šifrování souborů/složek se nastavuje pomocí položek **Vlastnosti** -> **Obecné** -> **Pokročilé atributy** -> **Šifrovat obsah pro zabezpečení dat**).

## 4.5.15 Vypnutí počítače

Umístění: **Možnosti** > **Rozšířené** > **Vypnutí počítače**

Můžete nakonfigurovat následující možnosti:

- **Při vypnutí počítače zastavit všechny stávající operace** – Když vypnete počítač, zatímco aplikace Acronis Cyber Protect Home Office provádí dlouhodobou operaci, například zálohování disku do cloudu, tato operace zabrání vypnutí počítače. Pokud je toto políčko zaškrtnuté, aplikace Acronis Cyber Protect Home Office automaticky před vypnutím zastaví všechny aktuální operace. Tato operace může trvat přibližně dvě minuty. Při příštím spuštění aplikace Acronis Cyber Protect

Home Office budou zastavené zálohy pokračovat.

- **Po dokončení zálohování vypnout počítač** – Tuto možnost vyberte, pokud proces zálohování, který konfigurujete, může trvat dlouho. V takovém případě nemusíte čekat na dokončení operace. Aplikace provede zálohování a poté automaticky vypne počítač.

Tato možnost je vhodná také při plánování záloh. Například můžete zálohovat každý pracovní den večer a uložit tak všechnu práci. Naplánujte zálohování a zaškrtněte toto políčko. Poté můžete od počítače po skončení práce odejít s tím, že důležitá data budou zálohována a počítač bude vypnutý.

## 4.5.16 Rychlost průběhu zálohování

Umístění pro zálohování do místních destinací: **Možnosti > Rozšířené > Výkon**

Umístění záloh do Acronis Cloud: **Možnosti > Rozšířené > Výkon a síť**

### Úroveň komprese

Úroveň komprese zálohy lze vybrat:

- **Žádná** – data budou kopírována bez jakékoli komprese, přičemž se tím může podstatně zvýšit velikost souboru zálohy.
- **Normální** – doporučená úroveň komprese (výchozí nastavení).
- **Vysoká** – úroveň komprese zálohy je vyšší, ale tvorba zálohy trvá déle.
- **Maximální** – komprese zálohy je maximální, ale tvorba zálohy trvá nejdéle.

---

#### Poznámka

Optimální úroveň komprese dat závisí na typu zálohovaných souborů. Například ani maximální komprese nesníží významně velikost souboru zálohy, pokud obsahuje zkomprimované soubory (JPG, PDF nebo MP3).

---

---

#### Poznámka

Nelze nastavit nebo změnit úroveň komprese pro předem existující zálohu.

---

### Priorita operace

Změna priority procesu zálohování nebo obnovy způsobí, že proces poběží rychleji nebo pomaleji (podle toho, jestli prioritu zvýšíte nebo snížíte) ale také může negativně ovlivnit výkon ostatních spuštěných aplikací. Priorita všech procesů spuštěných v systému určuje využití procesoru a systémových prostředků přiřazených k procesu. Snížení priority operace uvolní více prostředků pro jiné úlohy procesoru. Zvýšení priority zálohování nebo obnovy může urychlit proces přebrání prostředků aktuálně spuštěných procesů. Účinek tohoto nastavení závisí na celkovém využití procesoru a dalších faktorech.

Prioritu operace lze nastavit na jednu ze tří možností:

- **Nízká** (ve výchozím nastavení zapnuto) – proces zálohování nebo obnovy bude fungovat pomaleji, ale výkon ostatních aplikací se zvýší.
- **Normální** – proces zálohování nebo obnovy bude mít stejnou prioritu jako ostatní procesy.
- **Vysoká** – proces zálohování nebo obnovy bude fungovat rychleji, ale výkon ostatních aplikací se sníží. Výběr této možnosti může vyústit ve 100% využití procesoru aplikací Acronis Cyber Protect Home Office.

## Rychlost přenosu síťového připojení

Když zálohujete data do úložiště Acronis Cloud, můžete změnit rychlost připojení používaného aplikací Acronis Cyber Protect Home Office. Nastavte rychlost připojení tak, abyste mohli používat internet a síťové zdroje bez obtěžujícího zpomalování.

Chcete-li nastavit rychlost připojení, vyberte v části **Rychlost přenosu síťového připojení** jednu z následujících možností:

- **Maximální**  
Rychlost přenosu dat je v rámci konfigurace systému maximální.
- **Omezit rychlost nahrávání na**  
Můžete určit maximální hodnotu rychlosti nahrávání dat.

## Snímek zálohy

---

### Upozornění!

Tato možnost je určena pouze pro pokročilé uživatele. Pokud si nejste jisti, kterou možnost vybrat, neměňte výchozí nastavení.

---

Během procesu zálohování disku nebo oddílu, který často zabírá dlouhou dobu, mohou být některé ze zálohovaných souborů používány, uzamčeny nebo nějakým způsobem upravovány. Například můžete pracovat na dokumentu a občas ho uložit. Pokud by aplikace Acronis Cyber Protect Home Office zálohovala soubory po jednom, váš otevřený soubor by se pravděpodobně změnil od spuštění zálohování a pak se uložil do zálohy v odlišném okamžiku. Proto by byla data v záloze nekonzistentní. Aby k této situaci nedocházelo, aplikace Acronis Cyber Protect Home Office vytvoří takzvaný snímek, který zafixuje data k zálohování k určitému okamžiku. To se provede před spuštěním zálohování a zaručuje, že budou data konzistentní.

Vyberte možnost ze seznamu **Snímek zálohy**:

- **Žádný snímek** – Snímek se nevytvoří. Soubory budou zálohovány jeden po druhém jako běžná operace kopírování.
- **Služba VSS** – Tato možnost představuje výchozí nastavení pro zálohování na úrovni disku a zálohy celého počítače a zaručuje konzistenci dat při zálohování.

---

### Upozornění!

Toto je doporučená možnost pouze pro zálohování systému. Váš počítač se nemusí po obnovení ze zálohy vytvořené pomocí jiného typu snímku spustit.

---

- **Snímek Acronis** – Snímek se vytvoří pomocí ovladače Acronis použitého v předchozích verzích aplikace Acronis Cyber Protect Home Office.
- **Služba VSS bez zapisovačů** – Tato možnost je výchozí pro zálohování na úrovni souborů. Zapisovače VSS představují speciální komponenty VSS, které aplikacím oznamují, že bude vytvořen snímek a žádají aplikace, aby připravily svá data na snímek. Zapisovače jsou potřeba pro aplikace, které vykonávají velký počet operací se soubory a vyžadují konzistenci dat, například databáze. Jelikož takové aplikace se neinstalují do domácích počítačů, není zde potřeba používat zapisovače. Navíc se tak omezuje doba nezbytná k zálohování na úrovni souborů.

## 4.5.17 Výběr datového centra pro zálohu

Umístění: **Možnosti** > **Rozšířené** > **Datové centrum**

---

### Poznámka

Tato možnost je dostupná pouze pro online zálohování.

---

Když vytvoříte zálohu do úložiště Acronis Cloud, vaše data se nahrají do jednoho z datových center Acronis umístěných v různých zemích. Nejprve je při vytvoření účtu Acronis určeno nejbližší datové centrum k vašemu umístění. Potom jsou vaše online zálohy a synchronizované soubory standardně ukládány do tohoto datového centra.

Pokud jste v jiné zemi a vaše výchozí datové centrum není nejbližší k vašemu umístění, doporučujeme nastavit datové centrum zálohování ručně. Tím se významně zvýší rychlost nahrávání dat.

---

### Poznámka

Není možné změnit datové centrum pro již existující zálohování.

---

## 4.5.18 Nastavení napájení notebooku

Umístění: **Nastavení** > **Spořič baterie**

---

### Poznámka

Toto nastavení je dostupné pouze v počítačích s bateriemi (přenosné počítače, počítače s nepřerušitelným zdrojem napájení).

---

Dlouho běžící zálohy mohou baterii poměrně rychle vyčerpat. Když pracujete na notebooku a nemáte k dispozici napájení, nebo když se váš počítač přepne po výpadku proudu na nepřerušitelný zdroj napájení, je vhodné spustit úsporu energie baterie.

### ***Jak spořit energii baterie***



- Na bočním panelu klikněte na **Nastavení > Spořič baterie** energie baterie, zaškrtněte pole **Nezálohovat, pokud energie baterie klesne pod** a potom pomocí posuvníku nastavte přesnou úroveň baterie, při které se spustí úsporný režim.

Když je toto nastavení zapnuto a odpojíte napájecí adaptér notebooku nebo po výpadku proudu s počítačem používáte nepřerušitelný zdroj napájení a zbývající energie baterie je rovna nebo nižší než úroveň na bočním panelu, všechny stávající zálohy jsou pozastaveny a naplánované zálohy se nespustí. Jakmile napájecí adaptér znovu připojíte nebo výpadek skončí, pozastavené zálohy budou obnoveny. Spustí se také naplánované zálohy, které byly zmeškány v důsledku tohoto nastavení.

Toto nastavení však neblokuje funkčnost zálohování úplně. Zálohování vždy můžete spustit ručně.

Lokální mobilní zálohování na tomto nastavení nezávisí. Vaše mobilní data jsou zálohována na místní úložiště ve vašem počítači jako obvykle.

## 4.5.19 Sítě Wi-Fi pro zálohování do úložiště Acronis Cloud

Umístění: **Nastavení > Sítě Wi-Fi pro zálohování**

Když zálohujete data do úložiště Acronis Cloud, můžete mít obavy ohledně zabezpečení osobních údajů při přenosu prostřednictvím nezabezpečených sítí Wi-Fi. Abyste zabránili riziku krádeže vašich osobních dat, výrazně doporučujeme používat pouze chráněné Wi-Fi sítě.

### ***Jak chránit data***

1. Na bočním panelu klikněte na **Nastavení > Sítě Wi-Fi pro zálohování** a potom klikněte na **Nastavit síť**.
2. V okně **Sítě Wi-Fi pro zálohování**, které obsahuje všechny aktuálně dostupné a uložené nedostupné Wi-Fi sítě, zaškrtněte pole vedle sítí, které chcete použít k zálohování dat.

Když jsou sítě vybrané a počítač s kteroukoli z nich ztratí spojení, všechny probíhající zálohy se pozastaví a naplánované zálohy se nespustí. Jakmile se počítač ke kterékoli z těchto sítí připojí, pozastavené zálohy se obnoví. Spustí se také naplánované zálohy, které byly zmeškány v důsledku tohoto nastavení.

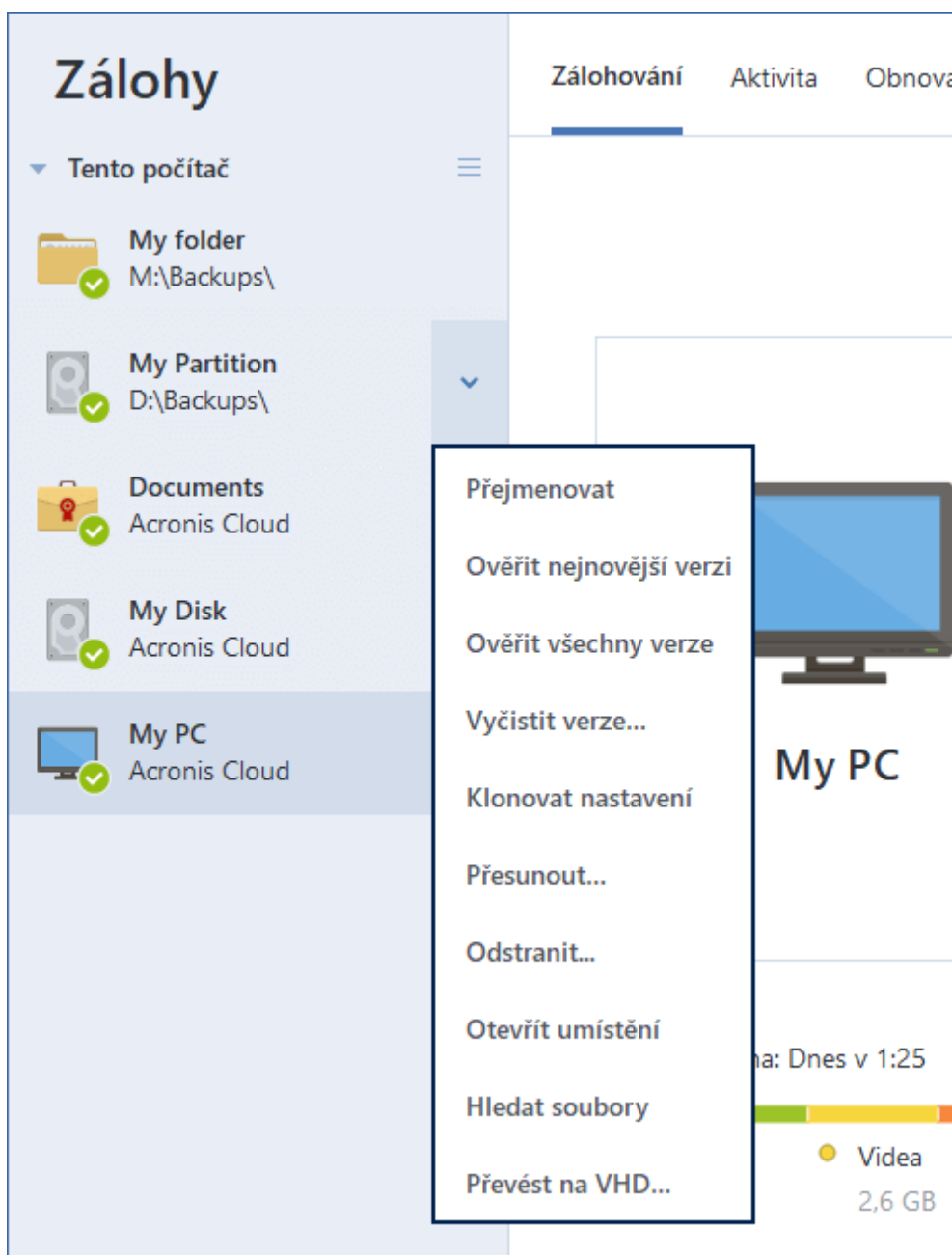
Pokud chcete zálohovat data prostřednictvím nové Wi-Fi sítě, jednoduše ji vyberte v okně **Sítě Wi-Fi pro zálohování**. To můžete udělat vždy, když potřebujete použít novou síť.

Lokální mobilní zálohování na tomto nastavení nezávisí. Vaše mobilní data jsou zálohována na místní úložiště ve vašem počítači jako obvykle.

## 4.6 Operace se zálohami

### 4.6.1 Nabídka Operace zálohování

Nabídka Operace zálohování nabízí rychlý přístup k dalším operacím, které lze provádět s vybranou zálohou.



Nabídka Operace zálohování může obsahovat následující položky:

- **Přejmenovat** (není dostupné pro zálohy služby Acronis Cloud) – umožňuje nastavit nový název zálohy v seznamu. Soubory zálohy nebudou přejmenovány.
- **Změnit konfiguraci** (pro zálohy přidané ručně do seznamu zálohy) – umožňuje konfiguraci nastavení zálohy vytvořené předchozí verzí aplikace Acronis Cyber Protect Home Office. Tato položka se může také objevit při přidávání záloh vytvořených v jiném počítači bez importu jejich nastavení.

Bez nastavení zálohování není možné zálohu zaktualizovat kliknutím na tlačítko **Zálohovat nyní**.  
Také nelze upravit a klonovat nastavení.

- **Změnit konfiguraci** (pro online zálohování) – umožňuje navázat vybranou online zálohu na aktuální počítač. Chcete-li akci provést, klikněte na tuto položku a znovu nakonfigurujte nastavení zálohy. Na jednom počítači může být aktivní pouze jedna online záloha.
- **Ověřit všechny verze** – zahájí ověření všech částí zálohy.
- **Ověřit poslední verzi** – zahájí rychlé ověření poslední části zálohy.
- **Vyčistit verze** – umožňuje odstranit verze záloh, které nepotřebujete.
- **Klonovat nastavení**– vytvoří nové prázdné pole zálohy s nastaveními původního zálohování a názvem **(1) [název původní zálohy]**. Změňte nastavení, uložte ho a poté klikněte na tlačítko **Zálohovat nyní** v poli klonované zálohy.
- **Přesunout**– kliknutím přesunete všechny soubory zálohy do jiného umístění. Následující verze záloh se uloží do nového umístění.  
Pokud změníte cíl zálohování úpravou nastavení zálohování, do nového umístění se uloží pouze nové verze záloh. Předchozí verze záloh zůstanou ve starém umístění.
- **Odstranit** – tento příkaz (v závislosti na typu zálohy) zcela smaže zálohu z jejího umístění nebo vám umožní zvolit, zda chcete smazat celou zálohu nebo pouze pole zálohy. Pokud smažete pole zálohy, zůstanou soubory zálohy ve svém umístění a vy budete moci zálohu přidat do seznamu později. Nezapomeňte, že pokud odstraníte zálohu zcela, odstranění nelze vrátit zpět.
- **Otevřít umístění**– otevře složku obsahující soubory záloh.
- **Hledat soubory**– umožňuje vyhledat konkrétní soubor nebo složku zadáním jejich názvu do pole hledání.
- **Převést do formátu VHD** (pro zálohy na úrovni disku) – umožňuje převést vybranou verzi zálohy aplikace Acronis (soubor TIBX) na virtuální pevné disky (soubory VHD(X)). Původní verze zálohy nebude změněna.

## 4.6.2 Činnost zálohování a statistika

Na kartě **Aktivita** a kartě **Záloha** můžete zobrazit další informace o záloze, například historii zálohy a typy souborů, které záloha obsahuje. Karta **Aktivita** obsahuje seznam operací provedených s vybranou zálohou počínaje jejím vytvořením, provozní stavy a statistiku. Takové informace jsou vhodné v případě, že potřebujete zjistit, co se se zálohou děje v režimu na pozadí, například počet a stav naplánovaných zálohovacích operací, velikost zálohovaných dat, výsledky validace záloh atd.

Když vytvoříte první verzi záloh, karta **Záloha** graficky zobrazí obsah záloh podle typu souborů.

### Karta Aktivita

---

#### Poznámka

Nepřetržité zálohy a mobilní zálohy nemají informační kanál o činnosti.

---

#### ***Jak zobrazit aktivity zálohy***

1. Na bočním panelu klikněte na možnost **Záloha**.
2. V seznamu záloh vyberte zálohu, jejíž historii chcete zobrazit.

3. V pravém panelu klikněte na tlačítko **Aktivita**.

✓ Úspěšně zálohováno dnes v 15:31				
Zálohované	Rychlost	Doba trvání	Data k obnovení	Metoda
1,6 GB	111.0 Mb/s	3 min 54 s	1,6 GB	Plná

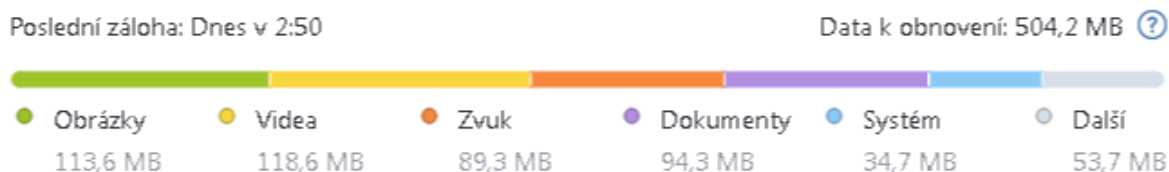
### Co lze zobrazit a analyzovat:

- Operace zálohování a jejich stav (úspěšné, neúspěšné, zrušené, přerušené atd.)
- Operace provedené se zálohami, jejich stav atd.
- Chybové zprávy
- Komentáře zálohy
- Podrobnosti o zálohování, včetně:
  - **Zálohováno**– Velikost dat, která obsahuje poslední verze zálohy.  
V případě záloh na úrovni souborů vypočítává aplikace Acronis Cyber Protect Home Office velikost souborů k zálohování. Hodnota tohoto parametru se u plných verzí záloh rovná hodnotě parametru Data k obnovení. U rozdílových a přírůstkových verzí je hodnota obvykle nižší než u parametru Data k obnovení, protože v tomto případě aplikace Acronis Cyber Protect Home Office dodatečně použije k obnově data z předchozích verzí.  
V případě záloh na úrovni disku aplikace Acronis Cyber Protect Home Office vypočítá velikost sektorů pevného disku, které obsahují data k zálohování. Jelikož sektory mohou obsahovat pevné odkazy na soubory, a to i pro plné verze záloh na úrovni disku, hodnota tohoto parametru může být nižší než u parametru Data k obnovení.
  - **Rychlost** – rychlost zálohovací operace.
  - **Doba trvání**– čas potřebný pro operaci zálohování.
  - **Data k obnovení**– Velikost dat, která lze obnovit z poslední verze zálohy.
  - **Metoda** – metoda operace zálohování (úplná, přírůstková nebo rozdílová).

Další informace naleznete v článku znalostní databáze: <https://kb.acronis.com/content/60104>.

## Karta Záloha

Po vytvoření zálohy můžete zobrazit statistiku typů zálohovaných souborů, které obsahuje poslední verze zálohy:



Ukažte na barevný segment a zobrazte počet souborů a celkovou velikost každé kategorie dat:

- Obrázky
- Video soubory
- Audio soubory
- Dokumenty
- Systémové soubory
- Další typy souborů včetně skrytých systémových souborů

**Data k obnovení** zobrazují velikost původních dat, která jste vybrali k zálohování.

### 4.6.3 Třídění záloh v seznamu

Ve výchozím nastavení jsou zálohy tříděny podle data vytvoření (od nejnovější po nejstarší). Chcete-li změnit pořadí, vyberte vhodný typ třídění v horní části seznamu záloh. Existují následující možnosti:

Příkaz		Popis
Třídít podle	<b>Název</b>	Tento příkaz třídí všechny zálohy podle abecedy. Chcete-li pořadí obrátit, vyberte možnost <b>Z → A</b> .
	<b>Datum vytvoření</b>	Tento příkaz třídí všechny zálohy od nejnovější po nejstarší. Chcete-li pořadí obrátit, vyberte možnost <b>Nejstarší nahoře</b> .
	<b>Datum aktualizace</b>	Tento příkaz třídí všechny zálohy podle data poslední verze. Čím je poslední verze zálohy novější, tím výše bude záloha umístěna v seznamu. Chcete-li pořadí obrátit, vyberte možnost <b>Nejstarší nahoře</b> .
	<b>Velikost</b>	Tento příkaz třídí všechny zálohy podle velikosti (od největší po nejmenší). Chcete-li pořadí obrátit, vyberte možnost <b>Nejmenší nahoře</b> .
	<b>Typ zdroje</b>	Tento příkaz třídí všechny zálohy podle typu zdroje.
	<b>Typ cíle</b>	Tento příkaz třídí všechny zálohy podle typu cíle.

### 4.6.4 Replikace záloh do úložiště Acronis Cloud

#### Proč replikovat?

I když zálohování dat poskytuje ochranu, doporučujeme také všechny místní zálohy replikovat do úložiště Acronis Cloud, což vás chrání před případným poškozením vašeho počítače. Samozřejmě můžete vytvořit dva plány zálohování, jeden pro zálohování do místního počítače a druhý pro zálohování do úložiště Acronis Cloud. Ale automatická replikace šetří čas při nastavování plánů zálohování a vytvoření repliky je rychlejší než vytvoření další zálohy. Replika je kopie zálohy, kterou lze využít jako bezpečnostní opatření a může být přístupná odkudkoli.

## Aktivace replikace

Replikace není k dispozici ve výchozím nastavení. Můžete si ji aktivovat pro jakoukoli místní zálohu disku, oddílu nebo celého počítače používající místní cíl (na externí nebo interní disk), které jste nakonfigurovali v aplikaci Acronis True Image (2020 či 2021) nebo Acronis Cyber Protect Home Office. Replikaci můžete aktivovat na zvláštní kartě plánu zálohování.

### ***Chcete-li aktivovat replikaci zálohy do úložiště Acronis Cloud:***

1. Ze seznamu záloh vyberte zálohu, kterou chcete replikovat, a otevřete kartu **Replika**.
2. Klikněte na tlačítko **Replikovat**. Teď je replikace aktivována a po vytvoření běžné zálohy se spustí. Aplikaci Acronis Cyber Protect Home Office můžete zavřít. Zálohování i replikace budou pokračovat na pozadí.
3. [volitelný krok] Klikněte na položky **Možnosti > Rozšířené > Replikace do úložiště Acronis Cloud**. Zobrazí se datové centrum, do kterého se ukládá replikace zálohy, a můžete zde [nakonfigurovat nastavení](#) vyčištění pro úložiště Acronis Cloud a optimalizovat využívání jeho místa.

## Ochrana replikovaných dat

Replikovaná data se nahrají do úložiště Acronis Cloud prostřednictvím mechanismu Secure Socket Layer (SSL).

V cloudu se data uloží podle vašeho nastavení šifrování. Pokud není nastaveno šifrovací heslo, replikovaná data se uloží nešifrovaná. V ostatních případech se data šifrují pomocí algoritmu AES-256.

## 4.6.5 Ověřování záloh

Proces ověření kontroluje, zda bude možné obnovit data ze zálohy.

Ověření zálohy je například důležité před obnovením systému. Pokud zahájíte obnovení z poškozené zálohy, proces se nezdaří a váš počítač nemusí jít spustit. Doporučujeme ověřit zálohy systémových oddílů ve spouštěčím médiu. Další zálohy mohou být ověřeny v systému Windows. Viz také část [Příprava na obnovení](#) a [Základní pojmy](#).

### ***Jak ověřit celou zálohu v systému Windows***

1. Spustíte aplikaci Acronis Cyber Protect Home Office a na bočním panelu klikněte na možnost **Záloha**.
2. V seznamu záloh klikněte na ikonu šipky dolů vedle zálohy, kterou chcete ověřit, a pak klikněte na možnost **Ověřit**.

### ***Ověření konkrétní verze zálohy nebo celé zálohy v samostatné verzi Acronis Cyber Protect Home Office (spouštěcího média)***

1. Na kartě **Obnova** vyberte zálohu obsahující verzi, kterou chcete ověřit. Pokud záloha není na seznamu, klikněte na možnost **Vyhledat zálohu** a zadejte cestu k záloze. Aplikace Acronis Cyber

Protect Home Office přidá tuto zálohu na seznam.

2. Pravým tlačítkem klikněte na zálohu nebo určitou verzi a poté na možnost **Ověřit archiv**. Tím se otevře **Průvodce ověřením**.
3. Klikněte na tlačítko **Pokračovat**.

## 4.6.6 Zálohování do různých umístění

Změnou cíle zálohování při úpravě nastavení zvolené zálohy můžete verze záloh ukládat do různých cílů. Například poté, co uložíte první plnou zálohu na externí pevný disk USB, můžete změnit cíl zálohování na USB flash disk úpravou nastavení zálohy.

Následující přírůstkové a rozdílové zálohy budou ukládány na USB flash disk.

---

### Poznámka

Nelze pokračovat v zálohování na optický disk.

---

### Poznámka

Acronis Zóna Secure Zone a servery FTP mohou obsahovat pouze celou zálohu.

---

## Rozdělování záloh za běhu

Když v cílovém umístění (CD-R/RW nebo DVD-R/RW) není dost volného místa k dokončení aktuální operace zálohování, aplikace zobrazí výstražnou zprávu.

Dokončit zálohování lze pomocí jednoho z následujících kroků

- Uvolněte na disku místo a potom klikněte na tlačítko **Opakovat**.
- Klikněte na tlačítko **Procházet** a potom vyberte jiné úložiště.
- Kliknutím na **Formátovat** vymažte veškerá data na disku a pokračujte v zálohování.

Když jsou verze zálohy uloženy v jiných umístěních, můžete tato umístění určit během obnovy.

## 4.6.7 Přidání existující zálohy do seznamu

Je možné, že máte zálohy Acronis Cyber Protect Home Office vytvořené v předchozí verzi produktu nebo zkopírované z jiného počítače. Pokaždé, když spustíte aplikaci Acronis Cyber Protect Home Office, vyhledá v počítači tyto zálohy a automaticky je zařadí na seznam záloh.

Pokud některé zálohy nejsou na seznamu uvedeny, můžete je přidat ručně.

### ***Jak ručně přidat zálohy***

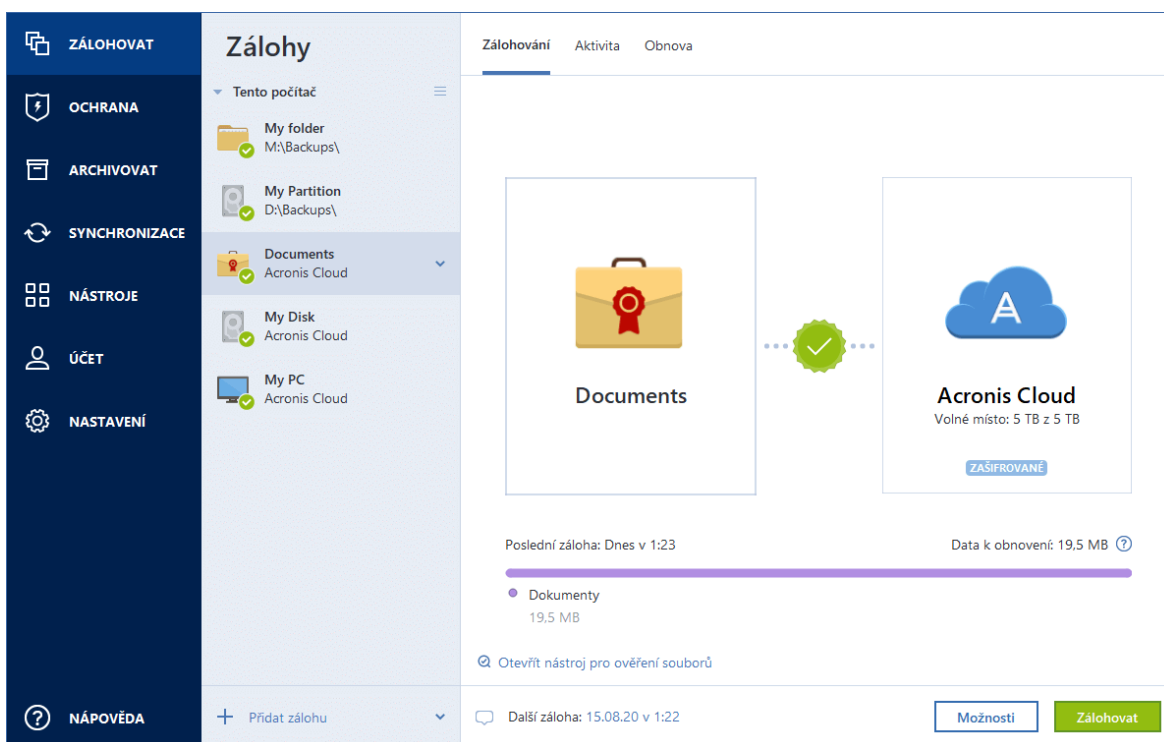
1. V části **Záloha** ve spodní části seznamu záloh klikněte na ikonu šipky a potom klikněte na položku **Přidat existující zálohu**. Aplikace zobrazí okno, ve kterém lze procházením vybrat zálohy v počítači.
2. Vyberte verzi zálohy (soubor TIB) a klikněte na tlačítko **Přidat**.  
Na seznam bude umístěna celá záloha.

## 4.6.8 Ověřená záloha

Pomocí technologie Blockchain dokáže aplikace Acronis Cyber Protect Home Office chránit vaše soubory před neoprávněnými úpravami. To vám přináší záruku, že budete moci obnovit data ze stejného souboru, který byl zálohován. Doporučujeme použít tento typ zálohování k ochraně souborů s právními dokumenty nebo libovolných dalších souborů, které vyžadují ověřenou pravost. Další informace naleznete v části [Používání technologie Blockchain](#).

### Postup vytvoření ověřené zálohy souborů a složek

1. Spustit Acronis Cyber Protect Home Office
2. Na bočním panelu klikněte na možnost **Záloha**.
3. Klikněte na položku **Přidat zálohu**.
4. [Volitelné] Chcete-li přejmenovat zálohu, klikněte na šipku vedle názvu zálohy, klikněte na tlačítko **Přejmenovat** a pak zadejte nový název.
5. Klikněte na oblast **Zdroj zálohy** a poté vyberte možnost **Soubory k ověření**.
6. V zobrazeném okně zaškrtněte políčka vedle souborů a složek, které chcete zálohovat, a klikněte na tlačítko **OK**.



7. Klikněte na oblast **Cíl zálohy** a poté vyberte cíl zálohování:
  - **Acronis Cloud** – přihlaste se ke svému účtu Acronis a klikněte na tlačítko **OK**.  
Nemáte-li ještě účet Acronis, klikněte na tlačítko **Vytvořit účet**, zadejte e-mailovou adresu a heslo a poté klikněte na tlačítko **Vytvořit účet**. Další informace naleznete v části [Účet Acronis](#).
  - **Váš externí disk**– Máte-li k počítači připojený externí disk, můžete ho vybrat ze seznamu.



- **NAS**– Ze seznamu nalezených zařízení NAS vyberte požadované zařízení NAS. Pokud máte pouze jedno zařízení NAS, aplikace Acronis Cyber Protect Home Office jej navrhne použít jako výchozí cílové umístění zálohování.
  - **Procházet**– Vyberte cílové umístění ze stromu složek.
8. [volitelný krok] Kliknutím na možnost **Možnosti** můžete nastavit možnosti zálohy. Další informace naleznete v části [Možnosti zálohování](#).
- Chcete-li vyloučit soubory s digitálním podpisem ze zálohování, zaškrtněte na kartě **Vyloučení** políčko **Neověřovat digitálně podepsané soubory**. Podrobnosti naleznete v části [Vyloučení položek ze záloh](#).
9. [volitelný krok] Klikněte na ikonu **Přidat komentář** a napište komentář na verzi zálohy. Komentáře k zálohám vám pomohou najít zálohu kdykoliv později při obnově dat.
10. Proveďte jednu z následujících akcí:
- Chcete-li provést zálohu okamžitě, klikněte na tlačítko **Zálohovat nyní**.
  - Pokud chcete zálohování spustit později nebo podle plánu, klikněte na šipku dolů napravo od tlačítka **Zálohovat nyní** a poté na tlačítko **Později**.

---

#### Poznámka

Pokud zálohujete data do služby Acronis Cloud, dokončení prvního zálohování může trvat poměrně dlouho. Další zálohování již budou mnohem rychlejší, protože se budou přes internet přenášet pouze změny souborů.

---

Dále se povídejte na video s pokyny v angličtině na adrese <https://goo.gl/WjUoPZ>.

## Používání technologie Blockchain

Aplikace Acronis Cyber Protect Home Office využívá technologii Blockchain k zajištění nejvyšší úrovně zabezpečení zálohovaných souborů. Tato technologie poskytuje záruku, že vaše soubory nebyly upraveny podvodným softwarem a v momentě obnovení obnovíte data z přesně stejného souboru, který jste zálohovali.

### Co je to technologie Blockchain?

Technologie Blockchain představuje databázi, která obsahuje informace o transakcích a jejich sekvenci. Obecně transakce představuje událost, například finanční operaci nebo operaci s různými druhy prostředků. Transakce jsou sdruženy do bloků, které jsou zapsány do databáze jeden po druhém a tvoří řetězec bloků. Každá transakce a každý blok mají své vlastní identifikační číslo. Velmi důležité je, že každý blok ukládá informace o všech předchozích blocích řetězce. Po zapsání do databáze nemůže informace o transakci nikdo žádným způsobem změnit a také nelze upravit pořadí transakce. Jakýkoliv pokus o změnu informací v databázi lze snadno identifikovat pomocí libovolného uživatele databáze, protože neexistují žádné informace o falešné transakci nebo falešném bloku ve všech následných blocích. Tato technologie zaručuje, že jsou data uložená v databázi platná, patří konkrétní osobě a nebyla nikým upravena. Další informace o technologii Blockchain naleznete na adrese [https://en.wikipedia.org/wiki/Blockchain\\_\(database\)](https://en.wikipedia.org/wiki/Blockchain_(database)).

## Jak aplikace Acronis Cyber Protect Home Office využívá technologii Blockchain

Aby mohla aplikace Acronis Cyber Protect Home Office chránit vaše soubory před neoprávněnými úpravami, využívá technologii Acronis Notary. Jedná se o univerzální řešení používání časových razítek a otisků prstů na libovolné datové objekty a datové toky. Jelikož je nepraktické ukládat velké množství dat do databáze technologie Blockchain, odesílá aplikace Acronis Cyber Protect Home Office do služby Acronis Notary pouze kódy hodnoty hash souborů.

Kód hodnoty hash představuje jedinečné číslo o pevné velikosti, které je vytvořeno funkcí hash. Kód matematicky definuje určitou sadu dat, například soubor zálohy. Jakákoliv změna souboru zálohy vede ke změně kódu hodnoty hash. Proto, chcete-li zkontrolovat, zda byl soubor změněn, musíte pouze porovnat kódy hodnoty hash vytvořené v počátečním a aktuálním stavu souboru. Pokud se kódy shodují, máte záruku, že soubor nebyl kýmkoliv upraven.


Když služba Acronis Notary obdrží kódy hodnoty hash vašich souborů, vypočte nový samostatný kód hodnoty hash a odešle jej do databáze Ethereum založené na technologii Blockchain. Další informace o platformě Ethereum naleznete na adrese <https://www.ethereum.org/>.

Jakmile se kód hodnoty hash nachází v databázi, jsou soubory použité k výpočtu tohoto kódu hodnoty hash ověřeny pomocí služby Acronis Notary. Pravost souboru můžete snadno kdykoliv ověřit pomocí postupu popsaného v části [Ověřování pravosti souboru](#). Každý ověřený soubor obsahuje certifikát ověření, což je dokumentující doklad o tom, že je soubor chráněn technologií Blockchain. Certifikát obsahuje obecné informace o souboru a technické podrobnosti, které vám umožňují ručně ověřit pravost souboru. Podrobnosti naleznete v části [Ruční ověření pravosti souboru](#).

## Ověřování pravosti souboru

Pomocí technologie Blockchain dokáže aplikace Acronis Cyber Protect Home Office chránit zálohované soubory před neoprávněnými úpravami. To vám přináší záruku, že budete moci obnovit data z přesně stejného souboru, který byl zálohován.

### ***Jak ověřit pravost souboru v aplikaci Acronis Cyber Protect Home Office***

1. Spustit Acronis Cyber Protect Home Office
2. Na bočním panelu klikněte na možnost **Záloha**.
3. Ze seznamu záloh vyberte ověřenou zálohu, která obsahuje soubor, který chcete ověřit.
4. Na pravém panelu otevřete kartu **Obnova**.
5. Přejděte k požadovanému souboru, klikněte na ikonu Nabídka (  ) a pak klikněte na jednu z následujících možností:
  - **Zobrazit certifikát**– Ve webovém prohlížeči se zobrazí certifikát obsahující podrobné informace o zabezpečení souboru.
  - **Ověřit** – Aplikace Acronis Cyber Protect Home Office zkontroluje pravost souboru.

### ***Postup ověření pravosti souboru v nástroji pro ověření souborů***

1. Pomocí jednoho z následujících způsobů otevřete nástroj pro ověření souborů:
  - Ve webovém prohlížeči otevřete stránku <https://notary.acronis.com/verify>.
  - Na bočním panelu aplikace Acronis Cyber Protect Home Office klikněte na možnost **Záloha**, vyberte ověřenou zálohu a klikněte na pravém panelu na možnost **Otevřít nástroj pro ověření souborů**.
2. V Průzkumníku souborů vyhledejte soubor, který chcete ověřit, a přetáhněte jej do okna webového prohlížeče.

Pokud je ověřené zálohování uloženo do úložiště Acronis Cloud, můžete rovněž ověřit autentizaci zálohovaných souborů ve webové aplikaci úložiště Acronis Cloud.

### ***Jak ověřit pravost souboru v aplikaci Acronis Cloud***

1. Přejděte na stránku <https://www.acronis.com/my/online-backup/webstore/> a poté se přihlaste do svého účtu Acronis.
2. Na bočním panelu klikněte na možnost **Zálohy**.
3. Ze seznamu záloh vyberte ověřenou zálohu, která obsahuje soubor, který chcete ověřit.
4. Přejděte k požadovanému souboru a zaškrtněte jej. Na pravém bočním panelu pak klikněte na možnost **Ověřit**.

## Ruční ověření pravosti souboru

Nejjednodušší způsob, jak ověřit pravost souboru, je použít příkaz **Ověřit** v aplikaci Acronis Cyber Protect Home Office nebo ve webové aplikaci Acronis Cloud. Další informace naleznete v části [Ověřování pravosti souboru](#). Kromě této snadné metody můžete provést ověření krok za krokem sami.

### ***Jak ručně ověřit pravost souboru***

#### **1. krok. Výpočet hodnoty hash MD5 souboru**

1. Spusťte prostředí Windows PowerShell.
2. Například pro výpočet hodnoty hash MD5 pro soubor picture.png umístěný ve složce C:\Users\picture.png zadejte:

```
$(($CertUtil -hashfile "C:\Users\picture.png" MD5)[1] -replace " ", "")
```

Příklad hodnoty hash MD5: eea16ade1edf2750a46bb6bffb2e45a2

3. Zkontrolujte, zda vypočtená hodnota hash MD5 odpovídá elektronickému štítku v poli DATA v ověřovacím certifikátu. Podrobnosti o získání certifikátu souboru naleznete v části [Ověřování pravosti souboru](#).

#### **Krok 2. Zkontrolujte, zda je v distribuované decentralizované databázi blockchain uložena položka ROOT**

1. Otevřete průzkumník databáze blockchain, například <https://etherscan.io/>.
2. Do pole hledání zadejte ID transakce z certifikátu.

3. Zkontrolujte, zda se pole Data v tabulce protokolů událostí rovná hodnotě ROOT v certifikátu.

### **Krok 3. Zkontrolujte, zda je ve stromu uložena hodnota hash**

1. Stáhněte si nástroj pro ovládání příkazové řádky z úložiště Github:  
<https://github.com/acronis/notary-verifyhash/releases>.
2. Postupujte podle následujících pokynů: <https://github.com/acronis/notary-verifyhash>.

## Acronis ASign

### Co je Acronis ASign?

Služba Acronis ASign je online služba, která umožňuje podepsat soubor elektronicky více osobám. Soubor je třeba předběžně nahrát do služby Acronis Cloud pomocí zálohování, archivace nebo synchronizace. Pro další ochranu jsou podepsané soubory ověřeny a chráněny pomocí služby Acronis Notary.

Řešení služby ASign lze použít k podepisování libovolných elektronických dokumentů, včetně různých druhů smluv, dohod, certifikátů, finančních dokumentů a oficiálních dopisů.

### Podepisování souboru

#### ***Jak podepisovat soubor v úložišti Acronis Cloud***

1. Přejděte na stránku <https://www.acronis.com/my/online-backup/webstore/> a poté se přihlaste do svého účtu Acronis.
2. Přejděte k požadovanému souboru, klikněte na jeho název a v otevřené nabídce zvolte možnost **Odeslat k podpisu**.
3. Zadejte e-mailové adresy osob, po kterých chcete, aby podepsali soubor, a pak jim zašlete pozvánky.  
Po podepsání souboru všemi podepisujícími ověří aplikace Acronis Notary soubor a vygeneruje certifikát podpisu.

Úplný popis funkce naleznete v anglické webové nápovědě služby Acronis ASign na adrese <https://www.acronis.com/en-us/support/documentation/ATI2017ASign/>.

## 4.6.9 Čištění záloh, verzí záloh a replik

Pokud chcete odstranit zálohy a verze záloh, které již nepotřebujete, použijte nástroje obsažené v aplikaci Acronis Cyber Protect Home Office.

Aplikace Acronis Cyber Protect Home Office ukládá informace o zálohách v databázi metadat. Odstraněním nepotřebných souborů záloh v Průzkumníku souborů se tedy neodstraní informace o těchto zálohách z databáze. To způsobí chybu, když se aplikace pokusí provádět operace s neexistujícími zálohami.

## Odstranění celé zálohy a její repliky

V části **Záloha** klikněte na tlačítko šipky dolů vedle zálohy, kterou chcete odstranit, pak klikněte na tlačítko **Odstranit**.

Tento příkaz (v závislosti na typu zálohy) zcela smaže zálohu z jejího umístění nebo vám umožní zvolit, zda chcete odstranit celou zálohu nebo pouze pole zálohy. Pokud odstraníte pouze pole zálohy, zůstanou soubory zálohy ve svém umístění a vy budete moci zálohu později přidat do seznamu. Nezapomeňte, že pokud odstraníte zálohu zcela, odstranění nelze vrátit zpět.

Když odstraníte zálohu, společně s ní se odstraní i její replika. Není možné odstranit místní zálohu a přitom zachovat její repliku. Ale můžete odstranit repliku a ponechat si místní zálohu.

## Odstranění celé repliky zálohy

Repliku můžete odstranit společně s původní zálohou nebo samostatně. Pokud ji chcete odstranit se zálohou, odstraňte zálohu podle výše uvedeného postupu.

Chcete-li odstranit repliku bez odstranění zálohy, v části **Záloha** klikněte na ikonu šipky dolů vedle zálohy s replikou, kterou chcete odstranit, pak klikněte na tlačítko **Odstranit repliku**.

## Automatické čištění verzí záloh

1. Přejděte do části **Záloha**.
2. Ze seznamu záloh vyberte zálohu, u které chcete vyčistit verze replik, a klikněte na **Možnosti**.
3. Na kartě **Schéma zálohování** vyberte možnost **Vlastní schéma**, vyberte metodu zálohování a pak klikněte na položku **Zapnout automatické čištění**.
4. Nakonfigurujte pravidla čištění zálohy.  
Další informace naleznete v části [Vlastní schémata](#).

---

### Poznámka

Po vyčištění mohou v úložišti zůstat některé pomocné soubory. Neodstraňujte je.

---

## Automatické čištění verzí replik

1. Přejděte do části **Záloha**.
2. Ze seznamu záloh vyberte zálohu, u které chcete vyčistit verze replik, a klikněte na **Možnosti**.
3. Na kartě **Pokročilé** otevřete kartu **Vyčištění úložiště Acronis Cloud**.
  - Použijte možnost **Neukládat více než ... nejnovějších verzí** a zadejte hodnoty omezující maximální počet uložených verzí replik.
  - Zaškrtněte políčko **Odstranit verze zálohy starší než** a zadejte hodnoty omezující maximální stáří starších verzí. Poslední verze budou zachovány a všechny ostatní verze se automaticky odstraní.

## Ruční zálohování a čištění verzí replik

Pokud chcete odstranit verze záloh, které již nepotřebujete, použijte nástroje obsažené v aplikaci. Pokud odstraníte soubory verzí záloh mimo aplikaci Acronis Cyber Protect Home Office, například v Průzkumníku souborů, bude to mít za následek chyby během práce se zálohami.

Verze následujících záloh nelze odstranit ručně:

- Zálohy uložené na discích CD, DVD, BD nebo Acronis Secure Zone.
- Nonstop zálohy.
- Ověřené zálohy.

### ***Jak vyčistit určité verze záloh***

1. Spustit Acronis Cyber Protect Home Office
2. V části **Záloha** klikněte na tlačítko šipky dolů vedle zálohy, kterou chcete vyčistit, pak klikněte na tlačítko **Vyčistit verze**.  
Otevře se okno **Vyčištění verzí záloh**.
3. Vyberte požadované verze a klikněte na tlačítko **Odstranit**.
4. V žádosti o potvrzení klikněte na příkaz **Odstranit**.

Počkejte na dokončení operace čištění. Po vyčištění mohou v úložišti zůstat některé pomocné soubory. Neodstraňujte je.

### **Čištění verzí, které obsahují závislé verze**

Při výběru verze zálohy k odstranění si pamatujte, že mohou existovat verze na ní závislé. V takovém případě budou závislé verze vybrány k odstranění také, protože obnova dat z takových verzí již nebude možná.

- **Pokud vyberete plnou verzi**– aplikace vybere také všechny závislé přírůstkové a rozdílové verze až po další plnou verzi. Jinými slovy, odstraní se celý řetězec verzí záloh.
- **Pokud vyberete rozdílovou verzi**– aplikace vybere také všechny závislé přírůstkové verze v rámci řetězce verzí záloh.
- **Pokud vyberete přírůstkovou verzi**– aplikace vybere také všechny závislé přírůstkové verze v rámci řetězce verzí záloh.

### **Viz také**

[Plné, přírůstkové a rozdílové zálohy.](#)

[Odebrání dat z Acronis Cloud.](#)

## 4.6.10 Uvolnění místa v Acronis Cloud

1. Přejděte na web <https://www.acronis.com/my/online-backup/webrestore/> a pak se přihlaste ke svému účtu Acronis. Otevře se webová aplikace Acronis Cloud.

2. Na levém bočním panelu webové aplikace klikněte na tlačítko **Účet**.
3. Na řádku **Acronis Cloud** klikněte na možnost **Vyčistit**.
4. Vyberte verze, které chcete odstranit:
  - Verze starší než určité období.
  - Všechny staré verze kromě několika nejnovějších.

---

**Upozornění!**

Buďte opatrní! Odstraněné verze nelze obnovit.

---

Poslední možností čištění je odstranění cloudové zálohy, která už není potřebná. V tom případě bude historie všech verzí zálohy z úložiště Acronis Cloud odstraněna.

## 4.6.11 Odebrání dat z Acronis Cloud

Protože je dostupné místo v úložišti služby Acronis Cloud omezeno, je nutné úložiště Cloud spravovat odstraňováním zastaralých dat nebo dat, která již nepotřebujete. Vyčištění lze provést v aplikaci Acronis Cyber Protect Home Office a rovněž prostřednictvím webové aplikace Acronis Cloud.

### Odstranění celé zálohy

Nejradikálnější možností je odstranění celé zálohy z úložiště Acronis Cloud. Při odstranění zálohy se trvale smažou veškerá data. Odstraněná data nelze obnovit.

V aplikaci **Acronis Cyber Protect Home Office**:

Operaci provedete kliknutím na tlačítko šipky dolů vedle zálohy, kterou chcete odstranit, a poté kliknutím na tlačítko **Odstranit**. Záloha a všechny její verze, nastavení i plán se odstraní.

Ve **webové aplikaci Acronis Cloud**:

1. Přejděte na stránku <https://www.acronis.com/my/online-backup/webstore/> a poté se přihlaste do svého účtu Acronis.
2. Na kartě **Zálohy** přesuňte kurzor nad zálohu, kterou chcete odstranit.
3. Klikněte na velikost zálohy a zobrazí se podrobné zobrazení.
4. V podrobném zobrazení klikněte na příkaz **Odstranit**.

Upozorňujeme, že záloha bude smazána z úložiště Acronis Cloud, její nastavení a plán však v aplikaci Acronis Cyber Protect Home Office zůstanou.

### Odstranění verzí zálohy v cloudu

V aplikaci **Acronis Cyber Protect Home Office**:

1. Operaci provedete kliknutím na tlačítko šipky dolů vedle zálohy verze, kterou chcete odstranit, a poté kliknutím na tlačítko **Vyčistit verze**.

Otevře se seznam verzí záloh.

2. Vyberte verze, které chcete odstranit, a klikněte na tlačítko **Odstranit**.

---

#### **Poznámka**

Aktualizace kvóty cloudu Acronis Cloud může trvat až jeden den.

---

#### **Ve webové aplikaci Acronis Cloud:**

1. Přejděte na stránku <https://www.acronis.com/my/online-backup/webstore/> a poté se přihlaste do svého účtu Acronis.
2. Na kartě **Zálohy** klikněte na velikost zálohy, jejíž verze chcete odstranit.  
Otevře se zobrazení podrobností zálohy.
3. V zobrazení podrobností klikněte na tlačítko **Vyčistit**.  
Můžete vybrat odstranění verzí starších, než je interval vámi zvolený, nebo odstranit všechny verze kromě několika nedávných.
4. Nakonfigurujte, co chcete odstranit, a klikněte na možnost **Vyčistit nyní**.
5. V potvrzovacím dialogovém okně klikněte na tlačítko **Odstranit**.

Po dokončení operace je zobrazen stav procedury vyčištění.

## Odstranění verzí repliky zálohy v cloudu

#### **V aplikaci Acronis Cyber Protect Home Office:**

1. V části **Záloha** vyhledejte místní zálohu, která je replikována do cloudu, klikněte na ikonu šipky dolů a vyberte možnost **Vyčistit verze**.  
Otevře se dialogové okno Vyčištění verzí záloh.
2. V části **Odstranit verze z** vyberte možnost **Acronis Cloud**.  
Zobrazí se seznam verzí replik záloh.
3. Vyberte verze replik, které chcete odstranit, a klikněte na tlačítko **Odstranit**.
4. V potvrzovacím dialogovém okně klikněte na tlačítko **Odstranit**.

---

#### **Poznámka**

Aktualizace kvóty cloudu Acronis Cloud může trvat až jeden den.

---

#### **Ve webové aplikaci Acronis Cloud:**

1. Přejděte na stránku <https://www.acronis.com/my/online-backup/webstore/> a poté se přihlaste do svého účtu Acronis.
2. Na kartě **Zálohy** klikněte na velikost repliky zálohy, jejíž verze chcete odstranit.  
Otevře se zobrazení podrobností repliky zálohy.
3. V zobrazení podrobností klikněte na tlačítko **Vyčistit**.  
Můžete vybrat odstranění verzí starších, než je interval vámi zvolený, nebo odstranit všechny verze kromě několika nedávných.



4. Nakonfigurujte, co chcete odstranit, a klikněte na možnost **Vyčistit nyní**.
5. V potvrzovacím dialogovém okně klikněte na tlačítko **Odstranit**.

Po dokončení operace je zobrazen stav procedury vyčištění.

## Jednorázové smazání

Pokud je vaše úložiště služby Acronis Cloud plné nebo již má málo volného místa, doporučujeme použít nástroj pro vyčištění ve webové aplikaci služby Acronis Cloud. Tento nástroj umožňuje rychlé a snadné uvolnění značného množství místa.

---

### Poznámka

Zálohy můžete vyčistit samostatně po jedné, a to dokonce i šifrované. Bude vyžadováno heslo.

---

1. Přejděte na stránku <https://www.acronis.com/my/online-backup/webrestore/> a poté se přihlaste do svého účtu Acronis.
2. Na kartě **Zálohy** přesuňte kurzor nad zálohu, kterou chcete odstranit.
3. Klikněte na tlačítko **Vyčistit**.
4. V otevřeném okně nakonfigurujte nastavení smazání a klikněte na možnost **Vyčistit nyní**.

Jednorázové vyčištění všech nešifrovaných záloh provedete pomocí následující možnosti:

1. Přejděte na kartu **Účet**.
2. Klikněte na tlačítko **Vyčistit**.

# 5 Obnovení dat

## 5.1 Obnovení disků a diskových oddílů

### 5.1.1 Obnovení systému po havárii

Pokud počítač nelze spustit, doporučujeme nejprve hledat příčinu v tématu [Určování příčiny selhání](#). Pokud je selhání způsobeno poškozením operačního systému, obnovte systém ze zálohy. Proveďte přípravy popsané v části [Příprava na obnovení](#) a poté pokračujte obnovením systému.

#### Určování příčin havárie

Havárie systému může nastat zejména ze dvou důvodů.

- **Selhání hardware**

V tomto případě je lepší předat opravu servisnímu středisku. Můžete však provést některé rutinní testy. Zkontrolujte kabely, konektory, zdroj napájení externích zařízení atd. a potom restartujte počítač. Pokud nastane problém s hardwarem, informaci o tomto selhání zobrazí test při spuštění počítače (POST).

Jestliže sekvence POST neobjeví selhání hardwaru, zobrazte nastavení systému BIOS a zkontrolujte, zda rozpoznal systémový pevný disk. Nastavení systému BIOS je možné zobrazit stisknutím požadované kombinace kláves v průběhu sekvence POST (**Del**, **F1**, **Ctrl+Alt+Esc**, **Ctrl+Esc** nebo nějaká jiná kombinace podle systému BIOS). Během testování při spuštění počítače je obvykle na monitoru zobrazena informace s potřebnou kombinací kláves (například Press DEL to enter Setup.). Stisknutím této kombinace kláves se zobrazí nabídka systému. Spusťte nástroj pro automatické rozpoznání pevného disku, který je obvykle v nastavení „Standard CMOS Setup“ nebo „Advanced CMOS setup“. Jestliže tento nástroj systémový disk nenajde, je disk vadný a je nutné jej vyměnit.

- **Poškození operačního systému (Windows nelze spustit)**

Pokud POST správně zjistí, je příčinou havárie pravděpodobně virus, škodlivý software nebo poškození systémového souboru potřebného ke spuštění. V tomto případě systém obnovte pomocí zálohy systémového disku nebo systémového diskového oddílu. Další informace naleznete v části [Obnovení systému](#).

#### Příprava na obnovení

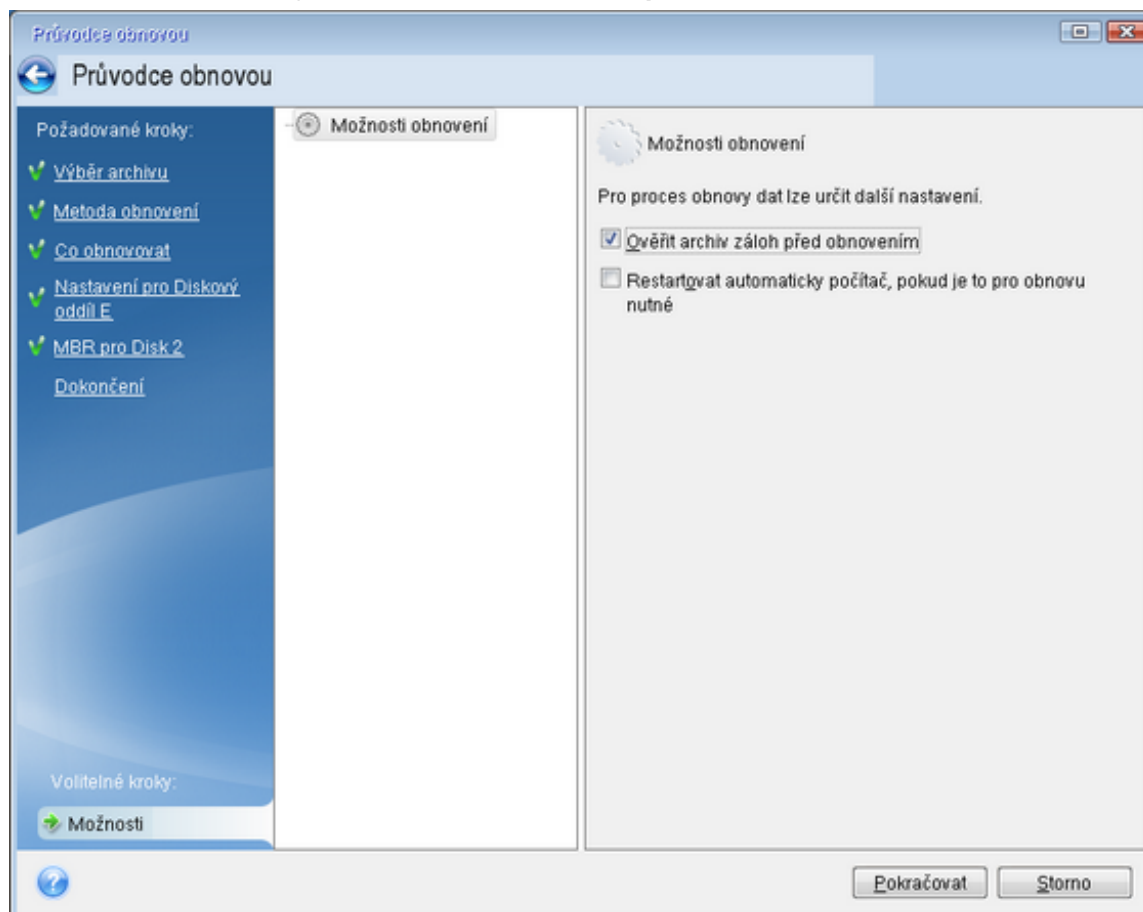
Před obnovením doporučujeme provést následující kroky:

- Jestliže máte podezření, že selhání nastalo z důvodu útoku viru nebo škodlivého softwaru, zkontrolujte, zda počítač neobsahuje viry.
- Při použití spouštěcího média se pokuste provést pokusnou obnovu na jiný pevný disk, pokud jej máte.

- Ověřte obraz při použití spouštěcího média. Záloha čitelná při ověření v systému Windows **nemusí být vždy čitelná v prostředí Linux.**

#### U zaváděcích médií existují dva způsoby ověření zálohy:

- Chcete-li zálohu ověřit ručně, na kartě **Obnovení** klikněte pravým tlačítkem na zálohu a vyberte možnost **Ověřit archiv.**
- Chcete-li zálohu před obnovením ověřit automaticky, u kroku **Možnosti v Průvodci obnovením** zaškrtněte políčko **Ověřit archiv záloh před obnovením.**



- Přiřaďte jedinečné názvy (jmenovky) všem diskovým oddílům na pevných discích. To vám usnadní vyhledání disku obsahujícího zálohy.

Použijete-li spouštěcí médium Acronis, mohou se písmena jednotek v aplikacích lišit od identifikátoru jednotek v systému Windows. Například písmeno D: přiřazené disku na spouštěcím médiu může odpovídat písmenu E: disku ve Windows.

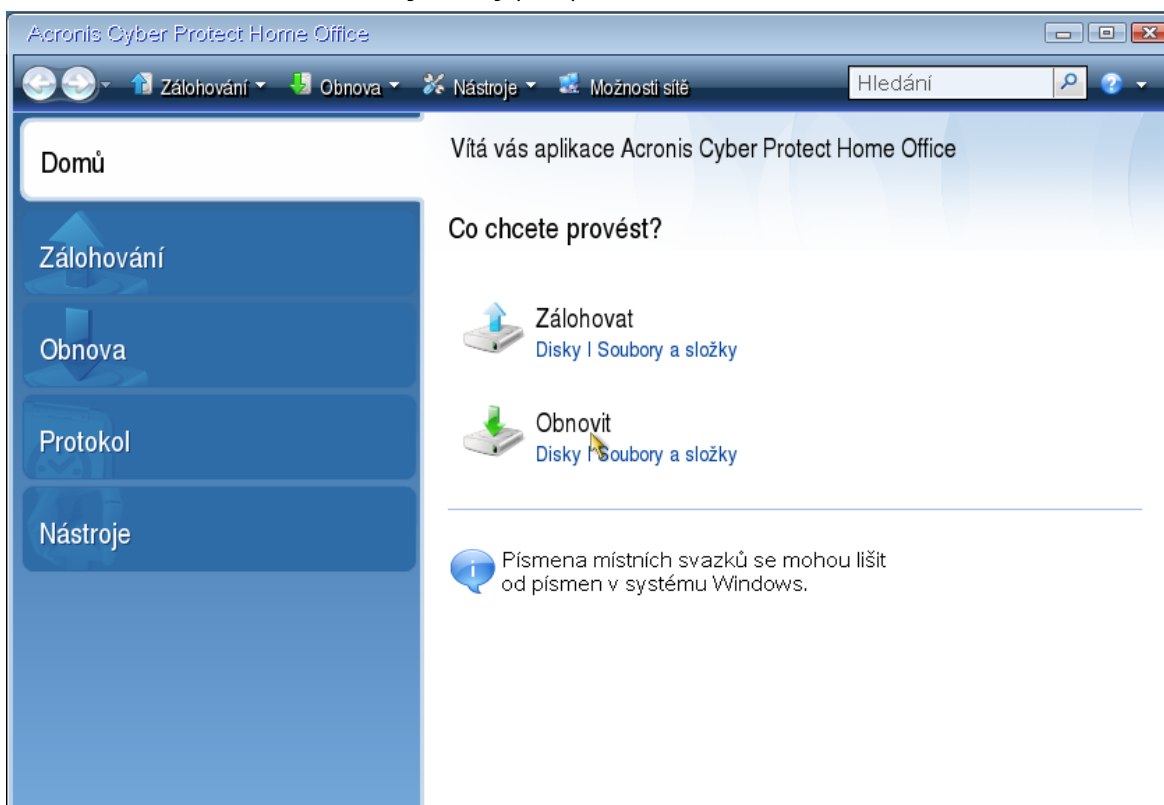
## Obnovení systému na stejný disk

Než začnete, doporučujeme dokončit postup popsany v tématu [Příprava na obnovení](#).

### **Postup obnovy systému**

1. Pokud se záloha, která se má použít pro obnovu, nachází na externím disku, připojte tento disk a zkontrolujte, zda je zapnutý.

2. Uspořádejte pořadí spouštění v systému BIOS tak, aby se systém spustil ze záchranného média (jednotky CD, DVD nebo USB). Viz také [Uspořádání pořadí spouštění v systému BIOS a UEFI BIOS](#). Pokud používáte počítač se systémem UEFI BIOS, věnujte pozornost režimu zavádění spouštěcího média v systému UEFI BIOS. Doporučuje se, aby režim zavádění odpovídal typu systému v záloze. Pokud záloha obsahuje systém BIOS, pak zaveďte spouštěcí médium v režimu BIOS; pokud je systém BIOS typu UEFI, zajistěte, aby byl nastaven režim UEFI.
3. Spusťte systém ze záchranného média a vyberte možnost **Acronis Cyber Protect Home Office**.
4. V okně **Domů** zvolte možnost **Moje disky** pod položkou **Obnovit**.



5. Vyberte zálohu systémového disku nebo diskového oddílu, který se má obnovit. Pokud se záloha nezobrazí, vyberte možnost **Procházet** a zadejte cestu k záloze ručně.

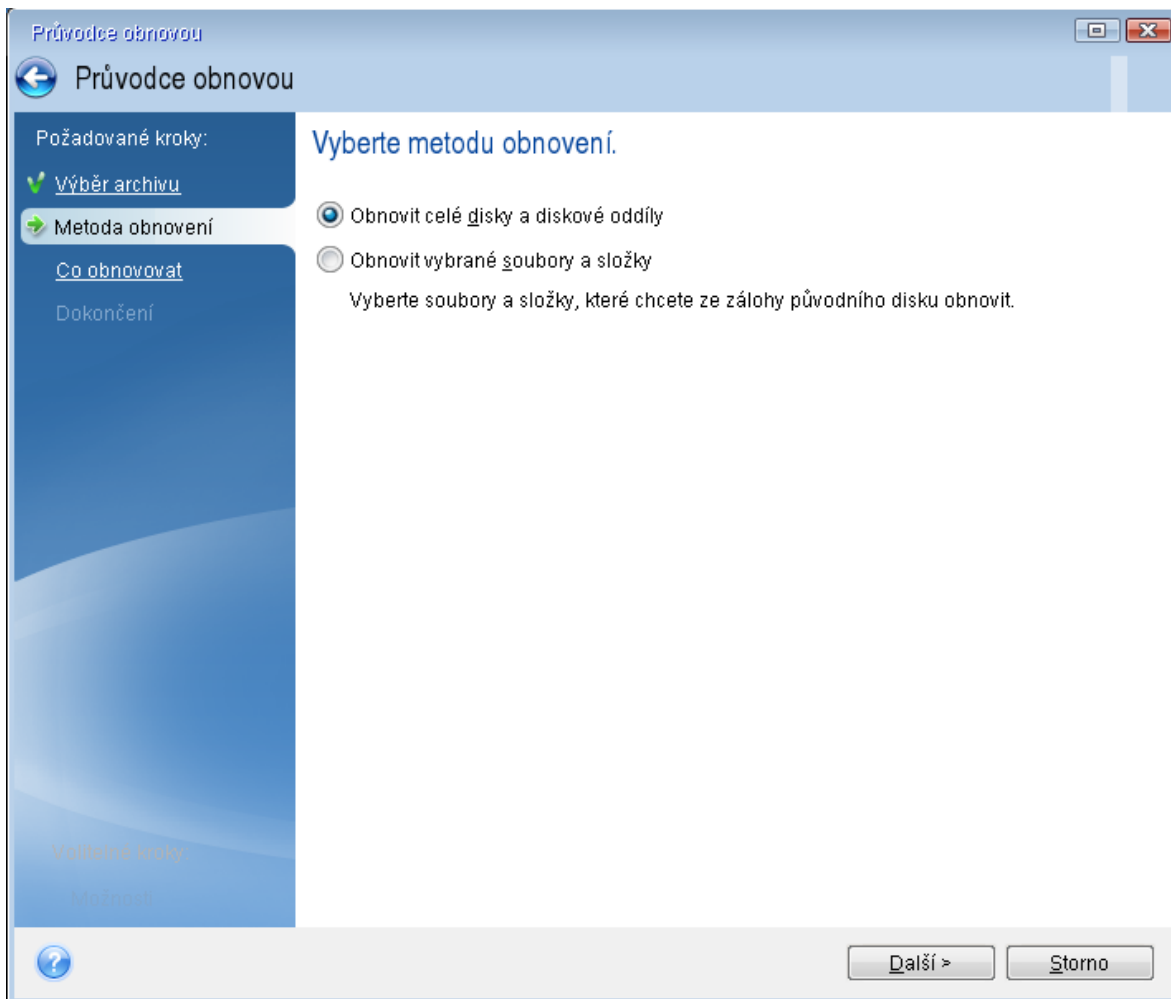
---

#### **Poznámka**

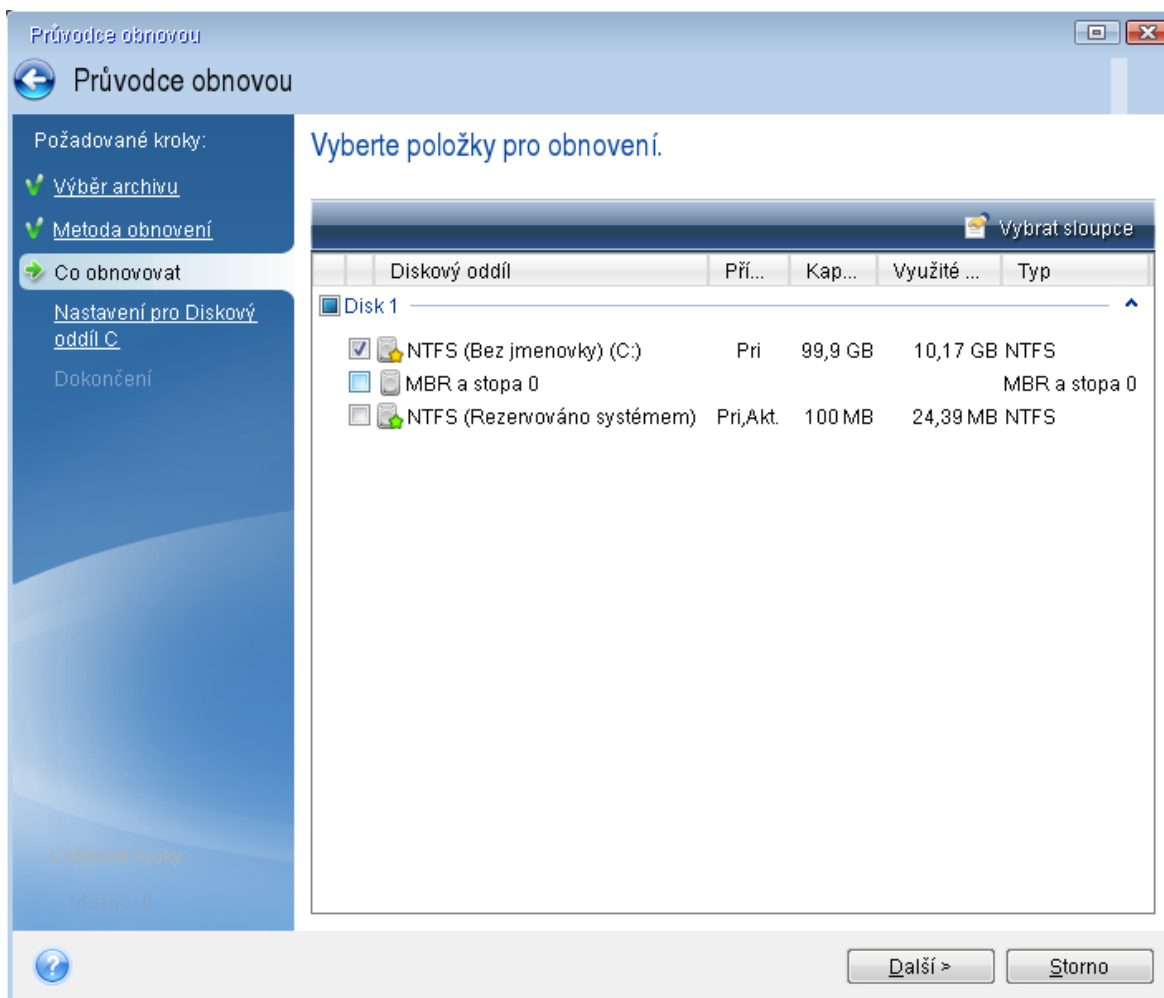
Pokud se záloha nachází na USB disku a disk není správně rozpoznán, zkontrolujte verzi USB portu. Pokud se jedná o port USB 3.0 nebo USB 3.1, zkuste připojit disk k portu USB 2.0.

---

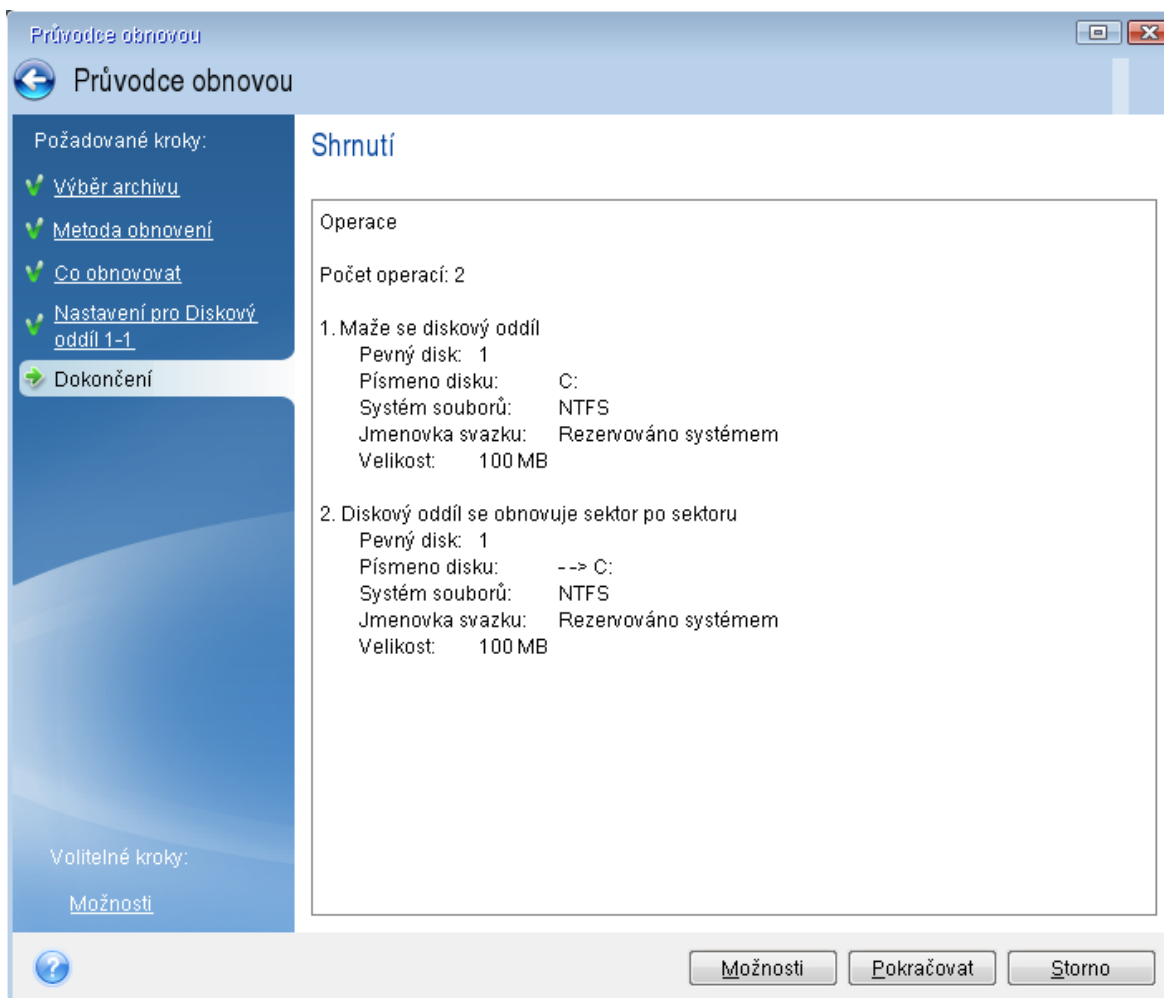
6. V kroku **Metoda obnovení** vyberte možnost **Obnovit celé disky a diskové oddíly**.



7. [Volitelné] V kroku **Bod obnovy** vyberte datum a čas, ze kterého chcete provést obnovu svého systému.
8. Vyberte systémový diskový oddíl (obvykle C) v okně **Co bude obnoveno**. Pokud má systémový diskový oddíl jiné písmeno, vyberte jej pomocí sloupce **Příznaky**. Musí mít příznaky **Pri**, **Akt**. Máte-li oddíl vyhrazený systémem, vyberte jej také.



9. V kroku nastavení diskového oddílu C (písmeno se může lišit) zkontrolujte výchozí nastavení a klikněte na tlačítko **Další** (pokud je správné). V opačném případě před kliknutím na tlačítko **Další** změňte nastavení podle potřeby. Jestliže provádíte obnovení na nový pevný disk s jinou kapacitou, je nutné změnit nastavení.
10. Přečtěte si pozorně souhrn prováděných operací v kroku **Dokončit**. Jestliže jste nezměnili velikost diskového oddílu, musí být velikosti položek **Maže se diskový oddíl** a **Obnovuje se diskový oddíl** shodné. Zkontrolujte nastavení a klikněte na tlačítko **Pokračovat**.



11. Po dokončení operace ukončete samostatnou verzi aplikace Acronis Cyber Protect Home Office, odeberte záchranné médium a spusťte systém z obnoveného systémového diskového oddílu. Zkontrolujte, zda jste obnovili systém Windows do potřebného stavu, a obnovte původní pořadí spouštění.

## Obnovení systému na nový disk při použití spouštěcího média

Než začnete, doporučujeme dokončit přípravu popsanou v tématu [Příprava na obnovení](#). Není nutné formátovat nový disk, protože bude naformátován v procesu obnovení.

### Poznámka

Doporučujeme, aby původní i nový pevný disk pracovaly ve stejném režimu řadiče (například IDE nebo AHCI). Jinak se počítač z nového pevného disku nemusí spustit.

### ***Jak obnovit systém na nový disk***

1. Nainstalujte nový pevný disk na stejné místo v počítači a použijte stejný kabel a stejný konektor, který používal původní disk. Není-li to možné, nainstalujte nový disk tam, kde jej budete používat.
2. Pokud se záloha, která se má použít pro obnovu, nachází na externím disku, připojte tento disk a zkontrolujte, zda je zapnutý.

3. Uspořádejte pořadí spouštění v systému BIOS tak, aby se systém spustil ze spouštěcího média (CD, DVD nebo USB flash disku). Viz také [Uspořádání pořadí spouštění v systému BIOS a UEFI BIOS](#).

Pokud používáte počítač se systémem UEFI BIOS, věnujte pozornost režimu zavádění spouštěcího média v systému UEFI BIOS. Doporučuje se, aby režim zavádění odpovídal typu systému v záloze. Pokud záloha obsahuje systém BIOS, pak zaveďte spouštěcí médium v režimu BIOS; pokud je systém BIOS typu UEFI, zajistěte, aby byl nastaven režim UEFI.

4. Spusťte systém ze spouštěcího média a vyberte možnost **Acronis Cyber Protect Home Office**.
5. V okně **Domů** zvolte možnost **Moje disky** pod položkou **Obnovit**.
6. Vyberte zálohu systémového disku nebo diskového oddílu, který se má obnovit. Pokud se záloha nezobrazí, vyberte možnost **Procházet** a zadejte cestu k záloze ručně.

---

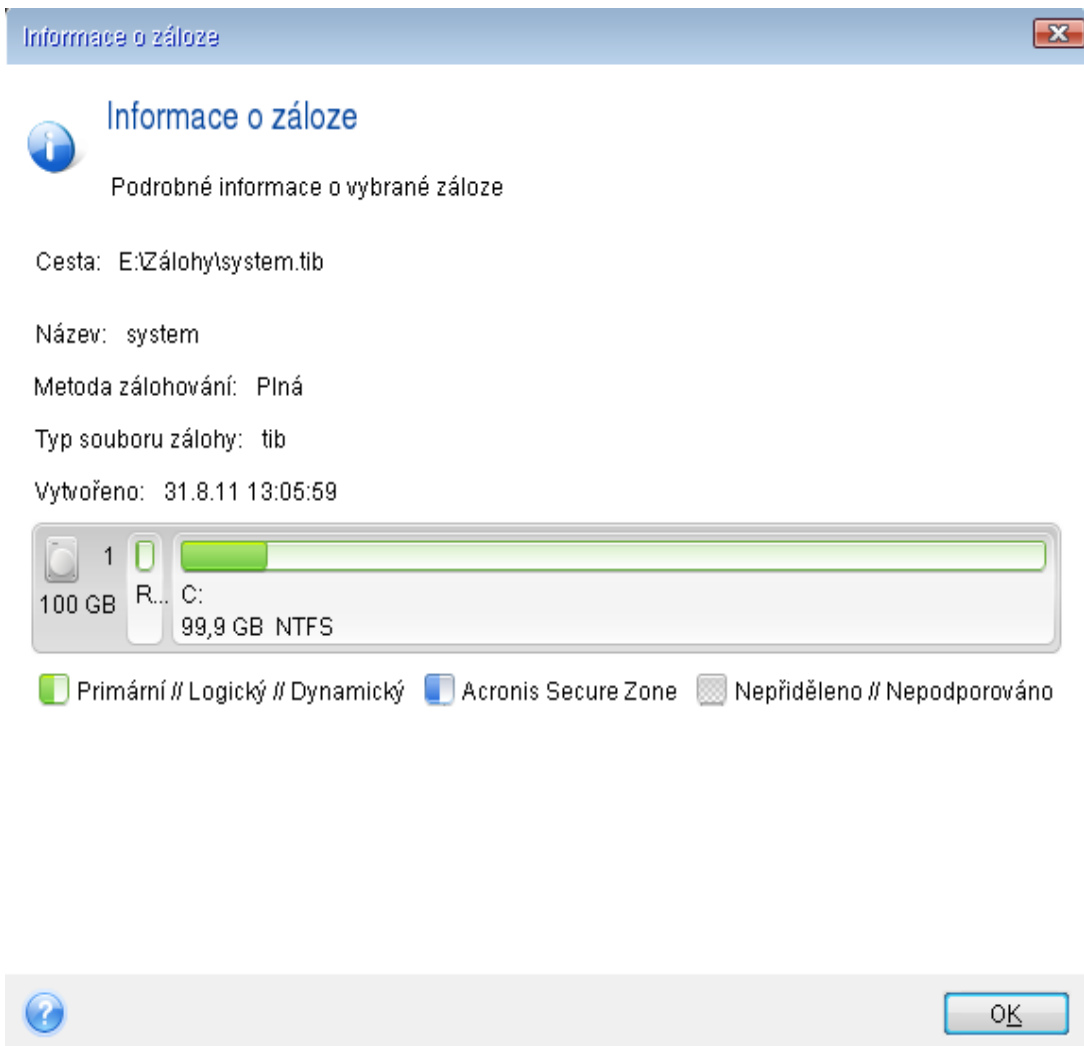
#### **Poznámka**

Pokud se záloha nachází na USB disku a disk není správně rozpoznán, zkontrolujte verzi USB portu. Pokud se jedná o port USB 3.0 nebo USB 3.1, zkuste připojit disk k portu USB 2.0.

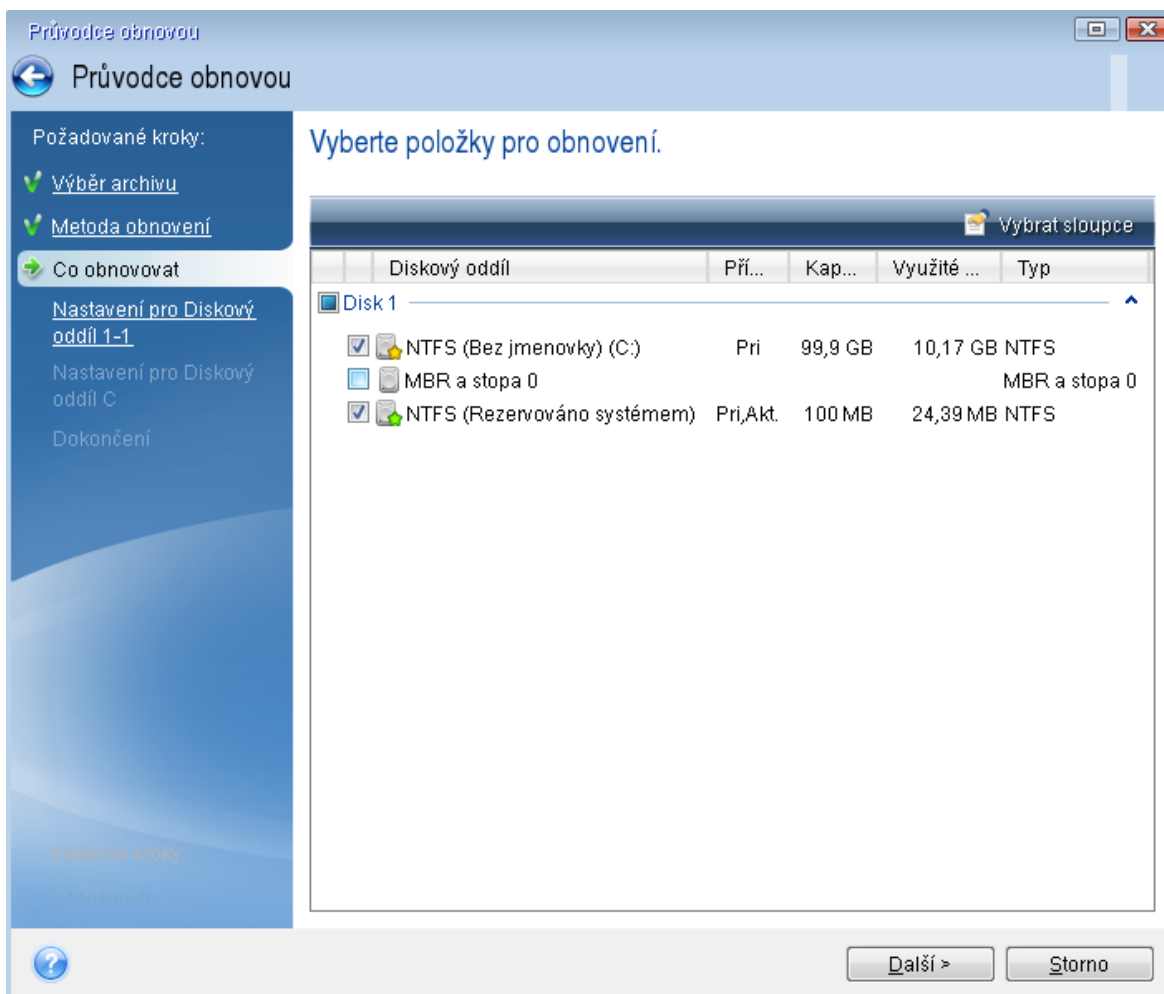
---

7. Pokud máte skrytý diskový oddíl (například diskový oddíl rezervovaný systémem nebo oddíl vytvořený výrobcem počítače), klikněte na panelu nástrojů v průvodci na tlačítko **Podrobnosti**. Zapamatujte si umístění a velikost nového diskového oddílu, je totiž nutné, aby tyto parametry byly na novém disku stejné.





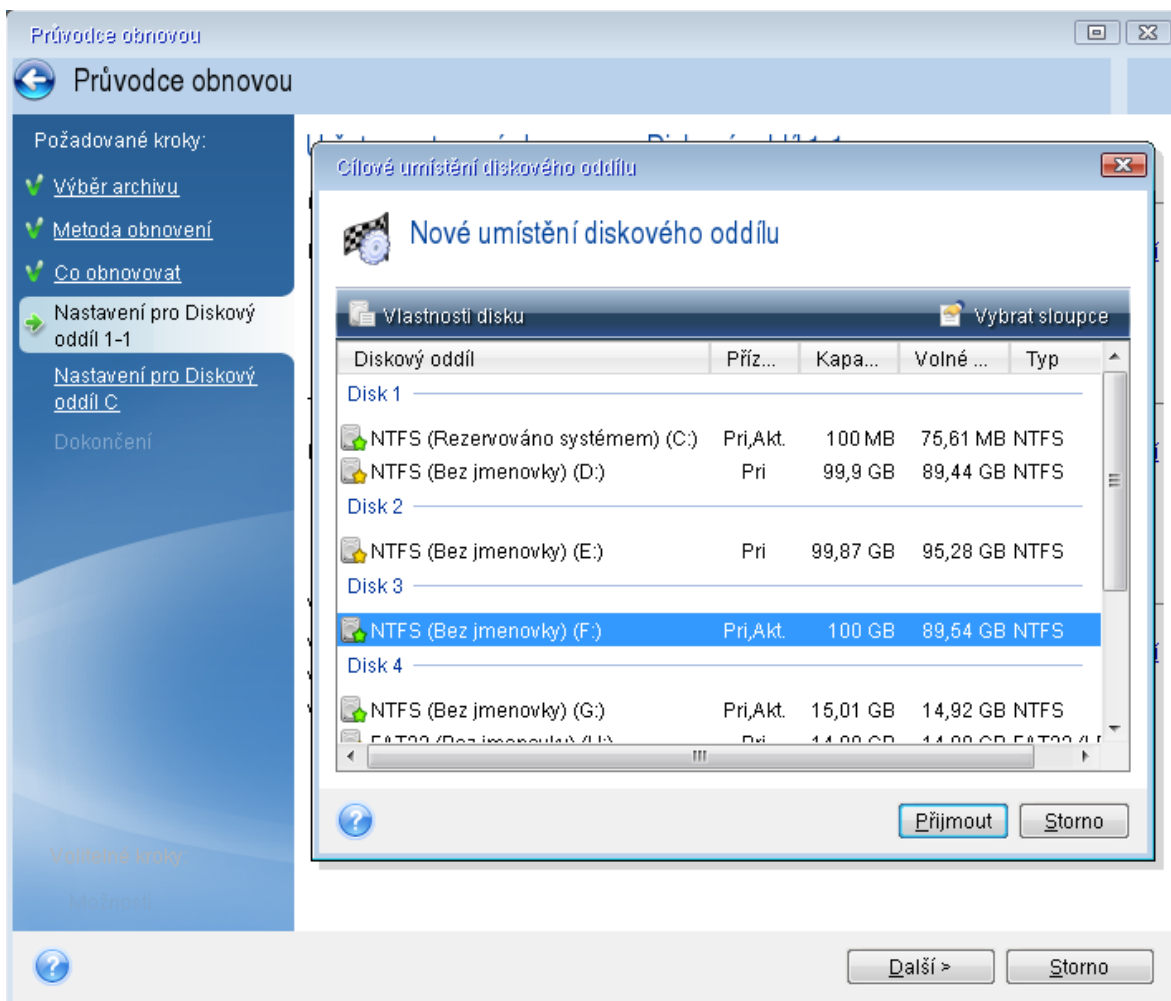
8. V kroku **Metoda obnovení** vyberte možnost **Obnovit celé disky a diskové oddíly**.
9. V kroku **Co obnovovat** zaškrtněte políčka u diskových oddílů, které chcete obnovit. Pokud vyberete celý disk, obnoví se také sektor MBR a stopa 0 disku.



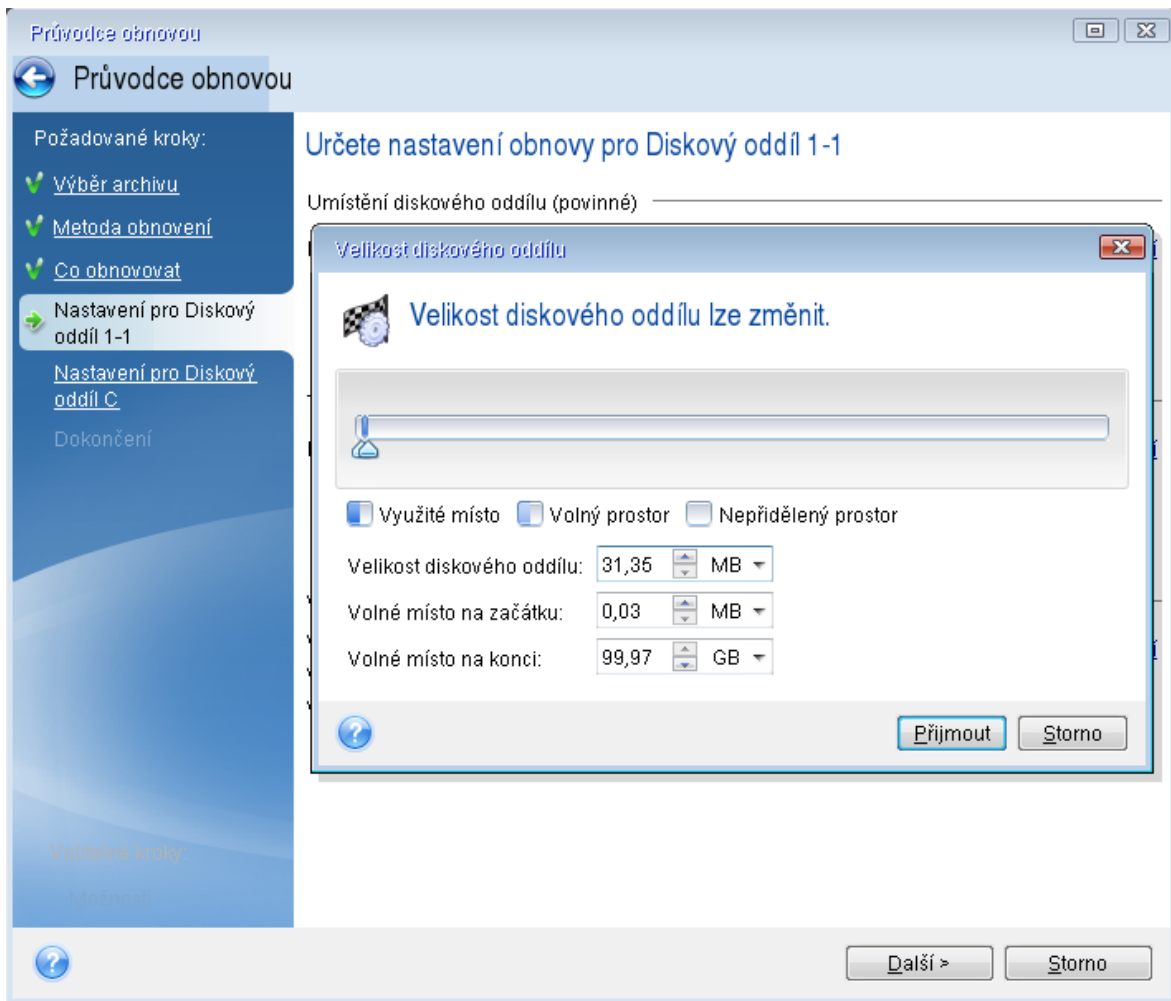
Výběrem diskových oddílů se zobrazí příslušné kroky „Nastavení diskového oddílu...“. Všimněte si, že tyto kroky začínají u diskových oddílů bez přiřazeného písmena (k čemuž obvykle dochází u skrytých diskových oddílů). Diskové oddíly budou seřazeny ve vzestupném pořadí písmen diskových oddílů. Toto pořadí nelze změnit. Pořadí se může lišit od skutečného pořadí diskových oddílů na disku.

10. V kroku nastavení skrytého oddílu (obvykle s názvem Nastavení diskového oddílu 1-1) zadejte následující nastavení:

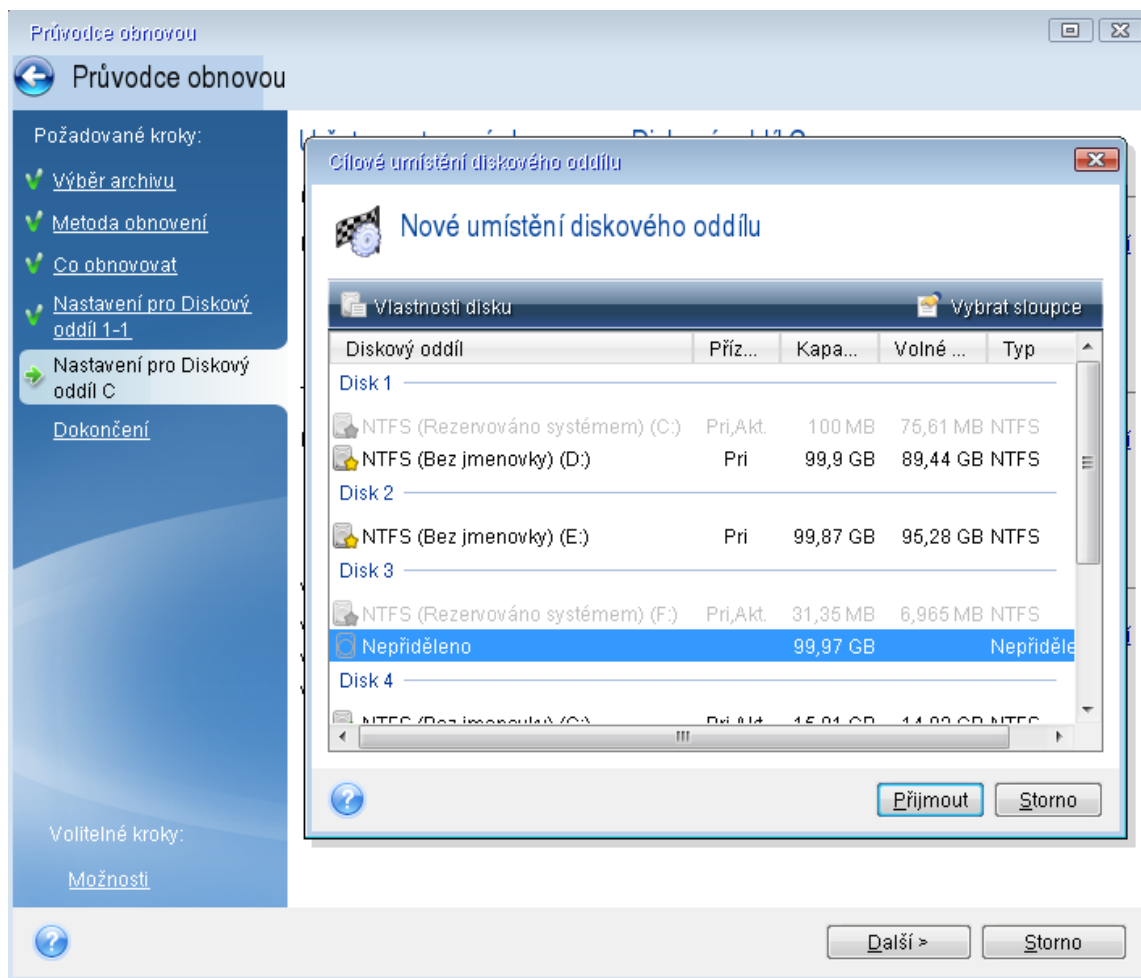
- **Umístění** – klikněte na možnost **Nové umístění**, vyberte nový disk podle přiřazeného názvu nebo kapacity a klikněte na tlačítko **Přijmout**.



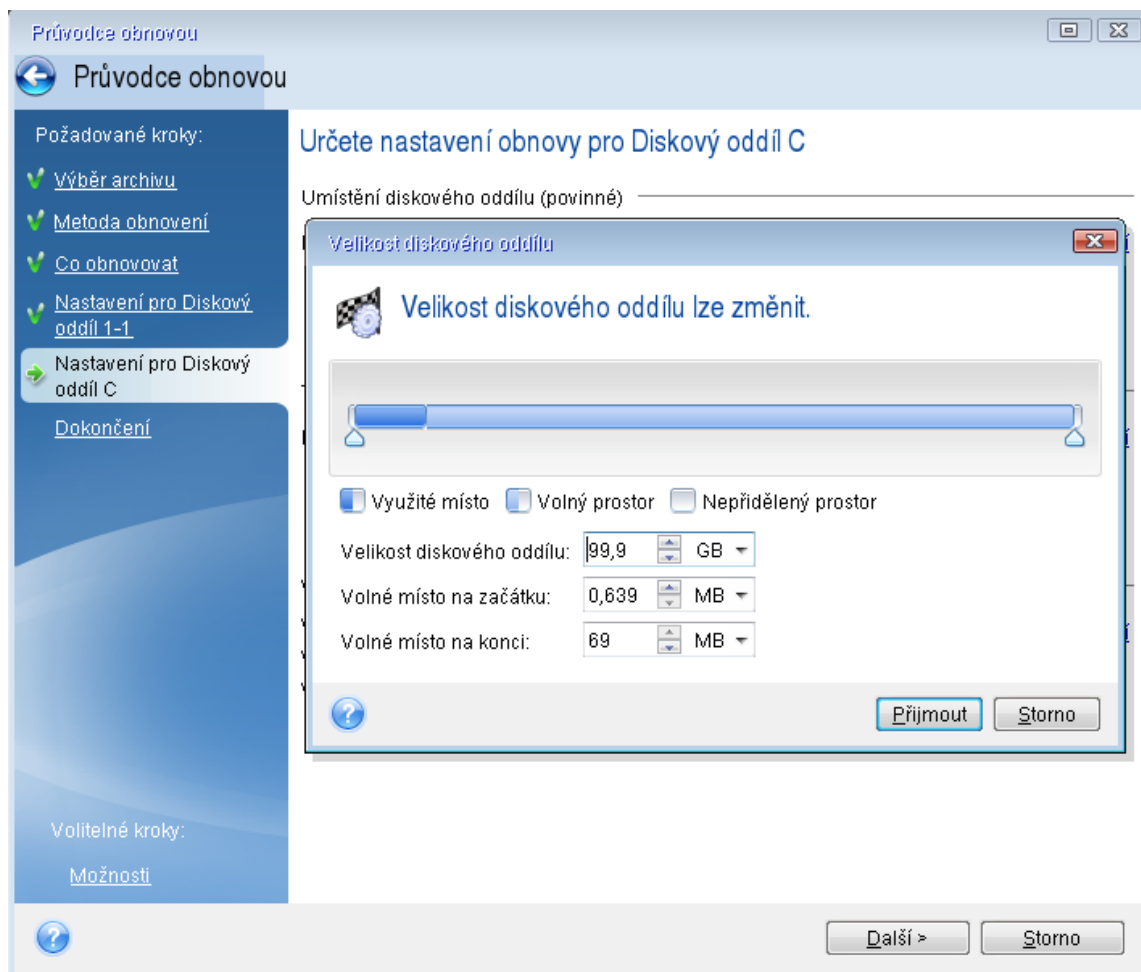
- **Typ** – zkontrolujte typ diskového oddílu a v případě potřeby jej změňte. Zkontrolujte, zda je diskový oddíl rezervovaný systémem (existuje-li) primární a označen jako aktivní.
- **Velikost** – v části Velikost diskového oddílu klikněte na možnost **Změnit výchozí**. Při výchozím nastavení zabírá diskový oddíl celý nový disk. Zadejte správnou hodnotu do pole Velikost diskového oddílu (tato hodnota je uvedena v kroku **Co obnovovat**). Pak tento oddíl přetáhněte do stejného umístění, které bylo uvedeno v okně informací o záloze, je-li to třeba. Klikněte na tlačítko **Potvrdit**.



11. V kroku **Nastavení diskového oddílu C** zadejte nastavení pro druhý diskový oddíl, což je v tomto případě systémový diskový oddíl.
- Klikněte na možnost **Nové umístění** a na cílovém disku vyberte nepřidělené místo, do kterého bude diskový oddíl uložen.



- V případě potřeby změňte typ diskového oddílu. Diskový oddíl rezervovaný systémem musí být primární.
- Zadejte velikost diskového oddílu (při výchozím nastavení má původní velikost). Za diskovým oddílem obvykle není žádné volné místo; proto je možné druhému diskovému oddílu přidělit veškeré nepřidělené místo na novém disku. Klikněte na tlačítko **Přijmout** a potom na tlačítko **Další**.



12. Pozorně si přečtěte shrnutí operací, které se provedou, a klikněte na tlačítko **Pokračovat**.

### Po dokončení obnovy

Před spuštěním počítače odpojte původní disk (je-li připojen). Pokud systém Windows během spuštění „uvidí“ nový i starý disk, způsobí to problémy při spuštění systému Windows. Pokud jste vyměnili starý disk za nový s větší kapacitou, odpojte starý disk před prvním spuštěním.

Vyjměte spouštěcí médium a spusťte v počítači systém Windows. Může se zobrazit upozornění, že byl nalezen nový hardware (pevný disk) a systém Windows je třeba restartovat. Jakmile zkontrolujete, že operační systém funguje správně, obnovte původní pořadí spuštění.

### Acronis Universal Restore

Po obnovení systému na jiný hardware se nemusí podařit spustit cílový počítač. Nový hardware totiž není kompatibilní s nejdůležitějšími ovladači obsaženými v obrazu. Doplněk univerzální obnovy Acronis pomůže zajistit, že cílový počítač půjde spustit. Další informace naleznete v části [Doplněk univerzální obnovy Acronis](#).

## 5.1.2 Obnovení disků a diskových oddílů

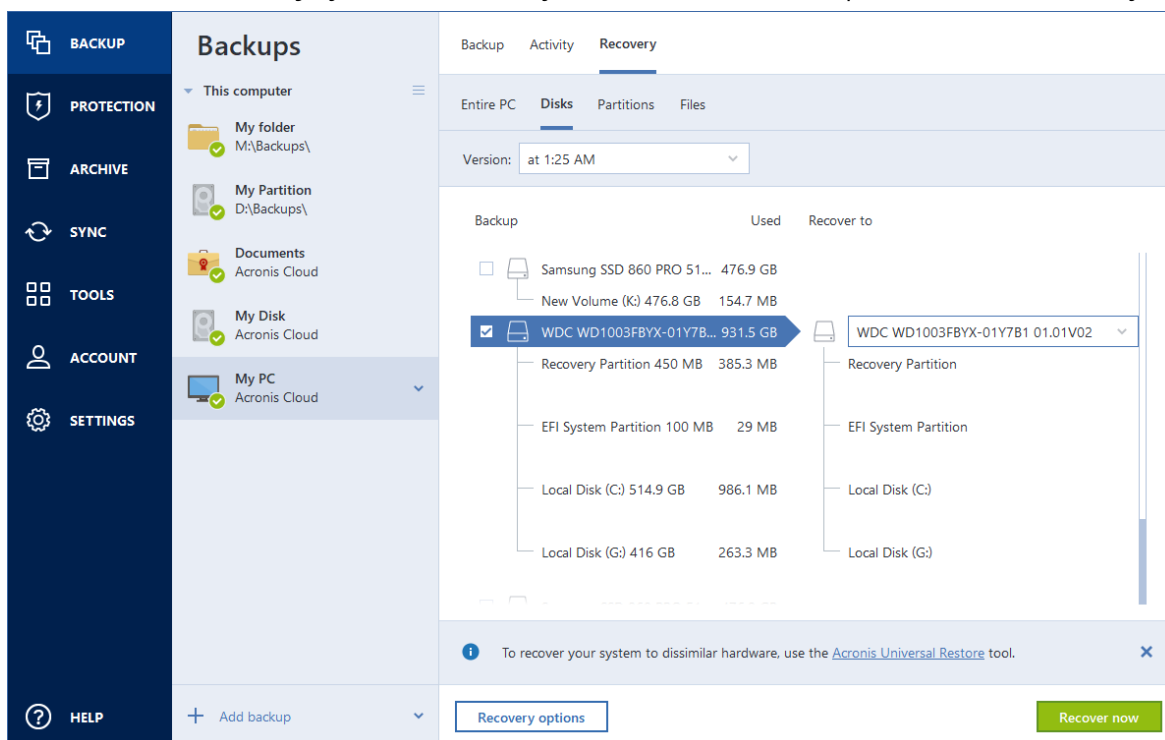
Své disky můžete obnovit ze záloh uložených v místním úložišti, síťovém úložišti nebo v úložišti Acronis Cloud.

### Poznámka

Obnova disků z úložiště Acronis Cloud může trvat dlouhou dobu (v závislosti na rychlosti internetového připojení).

### Jak obnovit diskové oddíly nebo disky

1. Spustit Acronis Cyber Protect Home Office
2. Chcete-li obnovit data z úložiště Acronis Cloud, ujistěte se, že jste přihlášení do účtu Acronis.
3. V části **Zálohování** vyberte zálohu, která obsahuje diskové oddíly nebo disky, které chcete obnovit, otevřete kartu **Obnovení** a poté klikněte na tlačítko **Obnovit disky**.
4. V seznamu **Verze zálohy** vyberte verzi zálohy, kterou chcete obnovit, podle data a času zálohy.



5. Zvolte kartu **Disky** k obnově disků nebo kartu **Oddíly** k obnově konkrétních oddílů. Vyberte objekt, které potřebujete obnovit.
6. V poli cílové umístění obnovy pod názvem diskového oddílu vyberte cílový diskový oddíl. Nevhodné diskové oddíly jsou označeny červeným okrajem. Všechna data v cílovém diskovém oddílu budou ztracena, protože bude nahrazen obnovenými daty a systémem souborů.

### Poznámka

Chcete-li provést obnovu do původního diskového oddílu, musí být v diskovém oddílu alespoň 5 % volného místa. Jinak bude tlačítko **Obnovit nyní** nedostupné.

7. [Volitelné] Chcete-li nastavit další parametry procesu obnovení disku, klikněte na položku **Možnosti obnovy**.
8. Po dokončení výběru spusťte obnovu kliknutím na tlačítko **Obnovit nyní**.

## Vlastnosti diskového oddílu

Obnovujete-li oddíly základního disku, můžete změnit jejich vlastnosti. Chcete-li otevřít okno **Vlastnosti diskového oddílu**, klikněte na tlačítko **Vlastnosti** vedle vybraného cílového oddílu.

The screenshot shows a dialog box titled "Správa diskových oddílů" (Disk Partition Management) with a close button (X) in the top right corner. The dialog is divided into several sections:

- Header:** "Písmeno" (Letter) with a dropdown menu, "Označení" (Label) with a text input field containing "New Volume", and "Typ" (Type) with a dropdown menu showing "Primární" (Primary).
- Progress Bar:** A horizontal bar with a green segment on the left and a grey segment on the right.
- Usage and Size:** "Používané: 1,2 GB" (Used: 1.2 GB) and "Velikost diskového oddílu:" (Disk partition size:). The size is set to "9,0" GB with up/down arrows.
- Unassigned Space:** "Nepřidělené místo" (Unassigned space). The size is set to "7,0" GB with up/down arrows.
- Location:** "Umístit za diskový oddíl" (Place after disk partition) with a dropdown menu.
- Footer:** An information icon (i) followed by the text: "Pomocí aplikace Acronis Disk Director můžete v nepřiřazeném místě vytvářet diskové oddíly. Další informace o aplikaci Acronis Disk Director" (Using the Acronis Disk Director application, you can create disk partitions in unassigned space. For more information about the Acronis Disk Director application). An "OK" button is located in the bottom right corner.

Lze změnit následující vlastnosti diskového oddílu:

- **Písmeno**
- **Označení**
- **Typ**  
Oddíl lze nastavit jako primární, primární aktivní nebo logický.
- **Velikost**



Velikost diskového oddílu změníte přetažením pravého okraje na vodorovném panelu v okně. Konkrétní velikost lze diskovému oddílu přiřadit zadáním příslušné číselné hodnoty do pole **Velikost diskového oddílu**. Dále lze vybrat polohu nealokovaného prostoru – před nebo po oddílu.

## Unified Extensible Firmware Interface (UEFI)

Pomocí aplikace Acronis Cyber Protect Home Office je také možné převádět systémy **BIOS** na rozhraní **UEFI**.

### Co je rozhraní UEFI?

**Unified Extensible Firmware Interface (UEFI)** je specifikace, která nabízí lepší kompatibilitu softwaru nastavením standardní syntaxe pro služby spouštění a služby runtime. Další informace o rozhraní UEFI naleznete na adrese <https://www.uefi.org>.

Rozhraní UEFI podporují následující operační systémy:

- Windows 8 (x86) a novější edice x86 systému Windows.
- Windows Vista SP1 (x64) a novější edice x64 systému Windows.

### Proč rozhraní UEFI?

- **Kompatibilita se systémem BIOS**– pomocí systémů založených na rozhraní UEFI lze stále spouštět operační systémy založené na systému BIOS díky modulu Compatibility Support Module (CSM).
- **Spouštění z velkých disků**– systémy založené na rozhraní UEFI podporují rozložení oddílů GPT, které umožňují použití disků o velikosti větší než 2<sup>32</sup> sektorů.
- **Architektura nezávislá na CPU**– rozhraní UEFI je podobné pro všechny architektury procesorů.
- **Ovladače nezávislé na CPU**– rozhraní UEFI obsahuje technologii EFI Byte Code (EBC) a umožňuje vytváření obrazů EBC (ovladačů), které lze spustit v jakémkoliv systému.
- **Flexibilní prostředí před spuštěním OS**– systémy založené na rozhraní UEFI lze spustit na libovolném hardwaru.
- **Modulární návrh**– rozhraní UEFI umožňuje aktualizace jednotlivých součástí bez vlivu na ostatní.

---

#### Poznámka

Protože je rozhraní UEFI nová technologie, ne všechny systémy jej podporují. Zda váš hardware podporuje rozhraní UEFI zjistíte u výrobce hardwaru.

---

### Jak zapnout rozhraní UEFI v systému BIOS?

Níže je popsán typický postup zapnutí a vypnutí rozhraní UEFI v systému BIOS:

1. Spusťte program pro nastavení systému BIOS stisknutím klávesy ve zprávě na obrazovce během spouštění systému. Obvykle se jedná o klávesy [Del] nebo [F2].
2. Pomocí směrových šipek zobrazte nabídku **Možnosti spouštění**.

3. Vyberte položku **Spouštění UEFI** a vyberte možnost *Zapnout* (nebo *Vypnout*, pokud potřebujete **VYPNOUT** rozhraní UEFI v systému).
4. Vyberte možnost **Uložit a ukončit** a stisknutím klávesy **Enter** uložte změny a spusťte systém.

Pokud potřebujete pomoc se zapnutím rozhraní UEFI, kontaktujte výrobce svého hardwaru.

## Jak migrovat původní systém na větší pevný disk?

Aplikace Acronis Cyber Protect Home Office nyní umožňuje migraci nebo obnovení systému z předešlého archivu na pevné disky větší než 2<sup>32</sup> bajtů (2 TB pro disky s logickými sektory o velikosti 512 bajtů nebo 16 TB pro disky s logickými sektory o velikosti 4 kB (4096 bajtů)).

To lze provést pomocí média Acronis nebo spuštěním operačního systému založeného na systému UEFI s nainstalovanou aplikací Acronis Cyber Protect Home Office:

### **Migrace systému pomocí média Acronis**

1. Spusťte systém z média Acronis.
2. Pokračujte ve spouštění z média výběrem možnosti **Acronis Cyber Protect Home Office (plná verze)** ve spouštěcí nabídce.
3. Vyberte příslušného průvodce (**Obnovit** nebo **Klonovat**) a postupujte podle pokynů.

### **Chcete-li migrovat systém v operačním systému založeném na rozhraní UEFI**

1. Spusťte operační systém Windows s podporou UEFI.
2. Spusťte aplikaci Acronis Cyber Protect Home Office, přejděte na kartu **Záloha a obnova**, klikněte na panelu nástrojů na možnost **Obnovit** a postupujte podle pokynů.

## Rozložení diskových oddílů

Rozložení diskových oddílů určuje, jak operační systém rozděluje diskové oddíly na pevném disku:

- **MBR (Master Boot Record)**– spouštěcí sektor o velikosti 512 bajtů, který je prvním sektorem pevného disku a slouží k uložení hlavní tabulky diskových oddílů.  
Záznam MBR je standardní schéma rozložení a používá se na většině pevných disků. Hlavním omezením záznamu MBR je podpora pevných disků pouze do velikost 2 TB, což znemožňuje použití moderních velkých pevných disků – místo nad 2 TB zůstává pro uživatele nepřístupné.
- **GPT (GUID Partition Table)**– novější standard rozložení tabulky diskových oddílů pevných disků.  
GPT umožňuje velikost disků nebo oddílů až do 9,4 ZB (9,4 x 10<sup>21</sup> bajtů).  
Následující tabulka ukazuje, které operační systémy podporují čtení disků GPT a/nebo spouštění z takových disků:

	Operační systém přečte disky GPT	Operační systém lze spustit z disků GPT
Windows XP x32	ŽÁDNÉ	ŽÁDNÉ
Windows XP x64	ANO	ŽÁDNÉ

Windows Vista x32	ANO	ŽÁDNÉ
Windows Vista x64	ANO	ŽÁDNÉ
Windows Vista x64 SP1 a novější	ANO	ANO
Windows 7 x32	ANO	ŽÁDNÉ
Windows 7 x64	ANO	ANO
Windows 8 x32	ANO	ANO
Windows 8 x64	ANO	ANO
Windows 8,1 x32	ANO	ANO
Windows 8,1 x64	ANO	ANO
Windows 10 x32	ANO	ANO
Windows 10 x64	ANO	ANO
Windows 11	ANO	ANO

Tabulka 1. Cílový disk je větší než 2 TB

Tabulka níže zobrazuje dostupné možnosti, pokud chcete migrovat zdrojový disk na pevný disk větší velikosti (více než 2 TB).

Pokud je váš zdrojový disk typu MBR, musíte si vybrat, zda chcete, aby cílový disk byl také typu MBR, nebo jej chcete převést na typ GPT pomocí aplikace Acronis Cyber Protect Home Office.

Obě možnosti mají své výhody a omezení podle parametrů systému. Většinou se týkají možnosti spouštění z cílového disku a schopnosti využití všeho místa na velkém disku.

	<b>Můj systém se spouští pomocí systému BIOS (Windows nebo Spouštěcí médium Acronis).</b>	<b>Můj systém se spouští pomocí rozhraní UEFI (Windows nebo Spouštěcí médium Acronis).</b>
<b>Můj zdrojový disk MBR a můj OS nepodporuje rozhraní UEFI.</b>	Způsob rozdělení oddílů zůstane po klonování nastaven na MBR. Do klonovaného operačního systému bude nainstalován ovladač Acronis Bus. Také nebudete moci použít prostor na disku nad 2 TB, protože záznam MBR nepodporuje pevné disky větší než 2 TB. Chcete-li využít veškeré místo na disku, je třeba změnit styl oddílů na GPT nebo restartovat aplikaci Acronis Cyber Protect Home Office po dokončení operace a pomocí Správce rozšířené	<i>Můžete vybrat jednu z požadovaných metod migrace:</i> <ul style="list-style-type: none"> <li><b>Kopírovat zdrojové oddíly beze změny</b></li> </ul> Styl bude stále MBR, ale po dokončení operace nebude možné operační systém spustit pomocí rozhraní UEFI. Do klonovaného operačního systému bude nainstalován ovladač Acronis Bus. Také nebudete moci použít prostor na disku nad 2 TB, protože záznam MBR nepodporuje pevné disky větší než 2 TB. Chcete-li využít

	<p>kapacity Acronis nastavit prostor nad 2 TB jako viditelný pro nástroj Přidat nový disk.</p>	<p>veškeré místo na disku, je třeba změnit styl oddílů na GPT nebo restartovat aplikaci Acronis Cyber Protect Home Office po dokončení operace a pomocí Správce rozšířené kapacity Acronis nastavit prostor nad 2 TB jako viditelný pro nástroj Přidat nový disk.</p> <ul style="list-style-type: none"> <li>• <b>Převést styl rozdělení oddílů na GPT</b></li> </ul> <p>Cílový oddíl bude převeden na styl GPT. Lze jej použít jako nesystémový disk, protože operační systém nepodporuje rozhraní UEFI. Bude dostupné veškeré místo na disku.</p>
<p><b>Můj zdrojový disk je MBR a můj OS podporuje rozhraní UEFI.</b></p>	<p>Styl rozdělení oddílů zůstane po migraci MBR. Do klonovaného operačního systému bude nainstalován ovladač Acronis Bus. Nebude možné používat prostor na disku nad 2 TB, protože záznam MBR nepodporuje pevné disky větší než 2 TB. Chcete-li využít veškeré místo na disku, je třeba změnit styl oddílů na GPT nebo restartovat aplikaci Acronis Cyber Protect Home Office po dokončení operace a pomocí Správce rozšířené kapacity Acronis nastavit prostor nad 2 TB jako viditelný pro nástroj Přidat nový disk.</p>	<p>Styl rozdělení oddílů na cílovém disku bude automaticky převeden na GPT. Disk lze použít ke spouštění pomocí rozhraní UEFI. Také bude dostupné veškeré místo na disku.</p>
<p><b>Můj zdrojový disk je typu MBR a OS není Windows nebo je počítač bez OS.</b></p>	<p><i>Můžete vybrat jednu z požadovaných metod migrace:</i></p> <ul style="list-style-type: none"> <li>• <b>Kopírovat zdrojové oddíly beze změny</b></li> </ul> <p>Styl rozdělení zůstane MBR, ale nebudete moci použít prostor na disku nad 2 TB, protože záznam MBR nepodporuje pevné disky větší než 2 TB. Chcete-li využít veškeré místo na disku, je třeba změnit styl oddílů na GPT nebo restartovat aplikaci Acronis Cyber Protect Home Office po dokončení operace a pomocí Správce rozšířené kapacity Acronis nastavit prostor nad 2 TB jako viditelný pro nástroj Přidat nový disk.</p> <ul style="list-style-type: none"> <li>• <b>Převést styl rozdělení oddílů na</b></li> </ul>	<p><i>Můžete vybrat jednu z požadovaných metod migrace:</i></p> <ul style="list-style-type: none"> <li>• <b>Kopírovat zdrojové oddíly beze změny</b></li> </ul> <p>Styl rozdělení zůstane MBR, ale nebudete moci použít prostor na disku nad 2 TB, protože záznam MBR nepodporuje pevné disky větší než 2 TB. Chcete-li využít veškeré místo na disku, je třeba změnit styl oddílů na GPT nebo restartovat aplikaci Acronis Cyber Protect Home Office po dokončení operace a pomocí Správce rozšířené kapacity Acronis nastavit prostor nad 2 TB jako viditelný pro nástroj Přidat nový disk.</p> <ul style="list-style-type: none"> <li>• <b>Převést styl rozdělení oddílů na GPT</b></li> </ul> <p>Cílový oddíl bude převeden na styl GPT. Cílový disk nelze použít ke spouštění, protože není na zdrojovém disku</p>

	<p><b>GPT</b></p> <p>Po dokončení operace bude styl rozdělení oddílů převeden na GPT. Cílový disk nelze použít ke spouštění, protože není na zdrojovém disku nainstalován žádný operační systém Windows. Bude dostupné veškeré místo na disku.</p>	nainstalován žádný operační systém Windows. Také bude dostupné veškeré místo na disku.
<b>Můj zdrojový disk je GPT a můj OS podporuje rozhraní UEFI.</b>	Styl rozdělení oddílů zůstane po migraci GPT. Po dokončení operace nebude možné systém spustit pomocí systému BIOS, protože váš operační systém nepodporuje spouštění z GPT pomocí systému BIOS. Bude dostupné veškeré místo na disku.	Operace nebude mít vliv na rozložení oddílů ani na spustitelnost disku: styl rozložení zůstane i nadále GPT, cílový disk bude možné spustit pomocí rozhraní UEFI. Bude dostupné veškeré místo na disku.
<b>Můj zdrojový disk je typu GPT a operační systém není Windows nebo je počítač bez operačního systému.</b>	Operace nebude mít vliv na rozložení oddílů ani na spustitelnost disku: styl rozložení zůstane i nadále GPT, cílový disk nebude možné spustit. Bude dostupné veškeré místo na disku.	Operace nebude mít vliv na rozložení oddílů ani na spustitelnost disku: styl rozložení zůstane i nadále GPT, cílový disk nebude možné spustit pomocí rozhraní UEFI. Bude dostupné veškeré místo na disku.

## Tabulka 2. Cílový disk je menší než 2 TB

Tabulka níže zobrazuje dostupné možnosti, pokud chcete migrovat zdrojový disk na pevný disk o velikosti menší než 2 TB.

Pokud je váš zdrojový disk typu MBR, musíte si vybrat, zda chcete, aby cílový disk byl také typu MBR, nebo jej chcete převést na typ GPT pomocí aplikace Acronis Cyber Protect Home Office.

Obě možnosti mají své výhody a omezení podle parametrů systému. Většinou se týkají spustitelnosti cílového disku.

	<b>Můj systém se spouští pomocí systému BIOS (Windows nebo Spouštěcí médium Acronis).</b>	<b>Můj systém se spouští pomocí rozhraní UEFI (Windows nebo Spouštěcí médium Acronis).</b>
<b>Můj zdrojový disk MBR a můj OS nepodporuje rozhraní UEFI.</b>	Operace nebude mít vliv na rozložení oddílů ani na spustitelnost disku: styl rozložení zůstane i nadále MBR, cílový disk bude možné spustit pomocí systému BIOS. Bude dostupné veškeré místo na disku.	Po dokončení operace zůstane styl rozdělení MBR, ale operační systém nebude možné spustit pomocí rozhraní UEFI, protože jej váš operační systém nepodporuje.

<p><b>Můj zdrojový disk je MBR a můj OS podporuje rozhraní UEFI.</b></p>	<p>Operace nebude mít vliv na rozložení oddílů ani na spustitelnost disku: styl rozložení zůstane i nadále MBR, cílový disk bude možné spustit pomocí systému BIOS. Bude dostupné veškeré místo na disku.</p>	<p>Cílový oddíl disku bude převeden na styl GPT, což umožní cílový disk spouštět pomocí rozhraní UEFI. Bude dostupné veškeré místo na disku.</p>
<p><b>Můj zdrojový disk je typu MBR a OS není Windows nebo je počítač bez OS.</b></p>	<p><i>Můžete vybrat jednu z požadovaných metod migrace:</i></p> <ul style="list-style-type: none"> <li>• <b>Kopírovat zdrojové oddíly beze změny</b></li> </ul> <p>Styl rozdělení oddílů zůstane MBR. Cílový disk nebude možné spustit, protože ve vašem systému nebyl nalezen operační systém Windows.</p> <ul style="list-style-type: none"> <li>• <b>Převést styl rozdělení oddílů na GPT</b></li> </ul> <p>Cílový disk bude převeden na styl GPT a použit jako nesystémový disk, protože váš operační systém nepodporuje spouštění z GPT pomocí systému BIOS.</p>	<p><i>Můžete vybrat jednu z požadovaných metod migrace:</i></p> <ul style="list-style-type: none"> <li>• <b>Kopírovat zdrojové oddíly beze změny</b></li> </ul> <p>Styl rozdělení oddílů zůstane MBR. Cílový disk nebude možné spustit, protože ve vašem systému nebyl nalezen operační systém Windows.</p> <ul style="list-style-type: none"> <li>• <b>Převést styl rozdělení oddílů na GPT</b></li> </ul> <p>Cílový diskový oddíl bude převeden na styl GPT a použit jako nesystémový disk, protože ve vašem systému nebyl nalezen operační systém Windows.</p>
<p><b>Můj zdrojový disk je GPT a můj OS podporuje rozhraní UEFI.</b></p>	<p>Po dokončení operace zůstane styl rozdělení GPT, systém nebude možné spustit pomocí systému BIOS, protože váš operační systém nepodporuje spouštění z GPT pomocí systému BIOS.</p>	<p>Po dokončení operace zůstane styl rozdělení GPT, operační systém bude možné spustit pomocí rozhraní UEFI.</p>
<p><b>Můj zdrojový disk je typu GPT a operační systém není Windows nebo je počítač bez operačního systému.</b></p>	<p>Po dokončení operace zůstane styl rozdělení GPT, systém nebude možné spustit pomocí systému BIOS, protože operační systém nepodporuje spouštění z GPT pomocí systému BIOS.</p>	<p>Po dokončení operace zůstane styl rozdělení GPT, systém nebude možné spustit, protože ve vašem systému nebyl nalezen žádný operační systém Windows.</p>

## Způsob migrace

Aplikace Acronis Cyber Protect Home Office umožňuje vybrat rozložení diskových oddílů cílového disku po dokončení operace obnovení:

- **MBR (Master Boot Sector)**– spouštěcí sektor o velikosti 512 bajtů, který je prvním sektorem pevného disku a slouží k uložení hlavní tabulky diskových oddílů.
- **GPT (GUID Partition Table)**– standard rozložení tabulky diskových oddílů pevných disků. GPT umožňuje velikost disků nebo oddílů až do 9,4 ZB (9,4 x 10<sup>21</sup> bajtů).

Pomocí tohoto průvodce je možné převést vaše rozložení oddílů při obnovování nebo klonování tak, jak jsou, beze změny rozložení.

- **Kopírovat oddíly beze změny**– pomocí této možnosti lze přesouvat systém tak, jak je, beze změny rozložení oddílů. Pozor, v tomto případě bude všechno místo na disku nad 2 TB nedostupné. Místo na disku nad 2 TB lze přidělit díky nástroji Správce rozšířené kapacity Acronis.
- **Kopírovat oddíly a použít disk jako nesystémový disk GPT**– pomocí této možnosti lze převést diskový oddíl na rozložení disku GPT.

Pomocí aplikace Acronis Cyber Protect Home Office je také možné převádět systémy **BIOS** na rozhraní **UEFI**.

**Systém spouštěný ze systému BIOS, záznam MBR, systém UEFI není podporován**

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

Systém nyní obsahuje:

**Systém:** spouštěný pomocí systému BIOS

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** operační systém Windows, spouštěný pomocí rozhraní UEFI není podporováno.

**Velikost cílového disku:** méně než 2 TB

Pokud systém migrujete na vybraný disk:

**Systém:** spouštěný pomocí systému BIOS

**Styl diskového oddílu:** Záznam MBR

**Operační systém:** operační systém Windows, spouštěný pomocí rozhraní UEFI není podporováno.

**Velikost disku:** je dostupné veškeré místo na disku

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

**Systém spouštěný ze systému BIOS, záznam MBR, systém UEFI je podporován**

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

Systém nyní obsahuje:

**Systém:** spouštěný pomocí systému BIOS

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

**Velikost cílového disku:** méně než 2 TB

Pokud systém migrujete na vybraný disk:

**Systém:** spouštěný pomocí systému BIOS

**Styl diskového oddílu:** Záznam MBR

**Operační systém:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

**Velikost disku:** je dostupné veškeré místo na disku

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## System spouštěný ze systému BIOS, záznam MBR, bez operačního systému Windows

Aplikace Acronis Cyber Protect Home Office umožňuje vybrat rozložení diskových oddílů cílového disku po dokončení operace.

System nyní obsahuje:

**Systém:** spouštěný pomocí systému BIOS

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** bez operačního systému Windows nebo jiného operačního systému

**Velikost cílového disku:** méně než 2 TB

S těmito parametry systému můžete vybrat jednu z následujících možností:

### 1. Kopírovat oddíly beze změny

Na cílovém disku můžete ponechat styl rozložení diskových oddílů MBR.

**Cílový disk po migraci:**

**Systém:** spouštěný pomocí systému BIOS

**Styl diskového oddílu:** Záznam MBR

**Operační systém:** bez operačního systému Windows nebo jiného operačního systému

**Velikost disku:** je dostupné veškeré místo na disku

### 2. Kopírovat oddíly a použít disk jako nesystémový disk GPT

Můžete převést styl rozložení disků na GPT.

**Cílový disk po migraci:**

**Systém:** nelze spouštět pomocí systému BIOS

**Styl diskového oddílu:** GPT

**Operační systém:** bez operačního systému Windows nebo jiného operačního systému

**Velikost disku:** je dostupné veškeré místo na disku



---

### Upozornění!

Po migraci lze cílový disk použít pouze jako nesystémový. Tato možnost není dostupná, pokud je aplikace Acronis Cyber Protect Home Office spuštěna v operačním systému Windows XP x32.

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

---

### System spouštěný ze systému BIOS, GPT, podpora systému UEFI

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

System nyní obsahuje:

**System:** spouštěný pomocí systému BIOS

**Styl diskového oddílu zdroje:** GPT

**Operační systém na zdrojovém disku:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

Pokud systém migrujete na vybraný disk:

**System:** nelze spouštět pomocí systému BIOS

**Styl diskového oddílu:** GPT

**Operační systém:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

**Velikost disku:** je dostupné veškeré místo na disku

---

### Upozornění!

Po migraci nebude možné operační systém z cílového disku spustit pomocí systému BIOS. Pokud chcete po migraci spustit systém z cílového disku, je třeba v systému zapnout spouštění pomocí systému UEFI (viz téma Unified Extensible Firmware Interface (Jednotná rozšiřitelná firmwarová rozhraní)) a poté operaci restartujte.

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

---

### System spouštěný ze systému BIOS, GPT, bez Windows

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

System nyní obsahuje:

**System:** spouštěný pomocí systému BIOS

**Styl diskového oddílu zdroje:** GPT

**Operační systém na zdrojovém disku:** bez operačního systému Windows nebo jiného operačního systému

Pokud systém migrujete na vybraný disk:

**System:** spouštěný pomocí systému BIOS

**Styl diskového oddílu:** GPT

**Operační systém:** bez operačního systému Windows nebo jiného operačního systému

**Velikost disku:** je dostupné veškeré místo na disku

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

**System spouštěný ze systému UEFI, záznam MBR, systém UEFI není podporován**

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

System nyní obsahuje:

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** operační systém Windows, spouštěný pomocí rozhraní UEFI není podporováno.

**Velikost cílového disku:** méně než 2 TB

Pokud systém migrujete na vybraný disk:

**System:** nelze spouštět pomocí rozhraní UEFI

**Styl diskového oddílu:** Záznam MBR

**Operační systém:** operační systém Windows, spouštěný pomocí rozhraní UEFI není podporováno.

**Velikost disku:** je dostupné veškeré místo na disku

---

### Upozornění!

Operační systém možná nepůjde spustit z cílového disku pomocí systému UEFI.

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

**System spouštěný ze systému UEFI, záznam MBR, systém UEFI je podporován**

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

System nyní obsahuje:

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

Pokud systém migrujete na vybraný disk:

Po migraci bude styl rozdělení oddílů převeden na GPT a bude z něj možné spouštět systém.

**Cílový disk po migraci:**

**Systém:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu:** GPT

**Operační systém:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

**Velikost disku:** je dostupné veškeré místo na disku  
Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## Systém spouštěný ze systému UEFI, záznam MBR, bez Windows

Aplikace Acronis Cyber Protect Home Office umožňuje vybrat rozložení diskových oddílů cílového disku po dokončení operace.

Systém nyní obsahuje:

**Systém:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** bez operačního systému Windows nebo jiného operačního systému

**Velikost cílového disku:** méně než 2 TB

S těmito parametry systému můžete vybrat jednu z následujících možností:

### 1. Kopírovat oddíly beze změny

Na cílovém disku můžete ponechat styl rozložení diskových oddílů MBR.

**Cílový disk po migraci:**

**Systém:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu:** Záznam MBR

**Operační systém:** bez operačního systému Windows nebo jiného operačního systému

**Velikost disku:** je dostupné veškeré místo na disku

### 2. Kopírovat oddíly a použít disk jako nesystémový disk GPT

Můžete převést styl rozložení disků na GPT.

**Cílový disk po migraci:**

**Systém:** nelze spouštět pomocí rozhraní UEFI

**Styl diskového oddílu:** GPT

**Operační systém:** bez operačního systému Windows nebo jiného operačního systému

**Velikost disku:** je dostupné veškeré místo na disku

---

### Upozornění!

Po migraci lze cílový disk použít pouze jako nesystémový.

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

### System spouštěný ze systému UEFI, GPT, systém UEFI je podporován

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

System nyní obsahuje:

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu zdroje:** GPT

**Operační systém:** operační systém Windows, spouštění pomocí systému UEFI je podporováno.

Pokud systém migrujete na vybraný disk:

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu:** GPT

**Velikost disku:** je dostupné veškeré místo na disku

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

### System spouštěný ze systému UEFI, GPT, bez Windows

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

System nyní obsahuje:

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu zdroje:** GPT

**Operační systém:** bez operačního systému Windows nebo jiného operačního systému

Pokud systém migrujete na vybraný disk:

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu:** GPT

**Velikost disku:** je dostupné veškeré místo na disku

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## 5.1.3 Obnova dynamických/GPT disků a svazků

### Obnova dynamických svazků

Můžete obnovovat dynamické svazky do následujících umístění na místních pevných discích:

- **Dynamický svazek.**

---

**Poznámka**

Ruční změna velikosti dynamických svazků při obnovení na dynamické disky není podporována. Pokud potřebujete velikost dynamického svazku při obnovení změnit, obnovte jej na základní disk.

---

- **Původní umístění (stejný dynamický svazek).**

Typ cílového svazku se nezmění.

- **Jiný dynamický disk nebo svazek.**

Typ cílového svazku se nezmění. Například při obnovení dynamického prokládaného svazku na dynamický rozložený svazek zůstane cílový svazek rozložený.

- **Nepřidělené místo dynamické skupiny.**

Obnovený svazek bude stejného typu jako v záloze.

- **Základní svazek nebo disk**

Cílový svazek zůstává základní.

- **Obnova od základu.**

Při provádění obnovení dynamických svazků na nový neformátovaný disk (obnova „na holé železo“) se z dynamických svazků stanou základní svazky. Pokud chcete, aby zůstaly dynamické, je nutné cílový disk před obnovením připravit (vytvořit diskové oddíly a naformátovat). To lze provést pomocí nástrojů od externích dodavatelů, například nástroje pro správu disků v systému Windows.

## Obnova základních svazků a disků

- Jestliže obnovíte základní svazek do nepřiděleného místa dynamické skupiny, obnovovaný svazek se stane dynamickým.
- Jestliže obnovíte základní disk na dynamický disk dynamické skupiny skládající se ze dvou disků, obnovovaný disk zůstane základním. Dynamický disk, na který obnova proběhla, změní stav na „Chybí“ a rozložený nebo prokládaný dynamický svazek na druhém disku změní stav na „Selhal“.

## Styl diskového oddílu po obnovení

Styl cílového diskového oddílu závisí na tom, zda váš počítač podporuje rozhraní UEFI a zda je váš operační systém spouštěn systémem BIOS nebo pomocí rozhraní UEFI. Viz následující tabulka:

	<b>Můj systém se spouští pomocí systému BIOS (Windows nebo Spouštěcí médium Acronis).</b>	<b>Můj systém se spouští pomocí rozhraní UEFI (Windows nebo Spouštěcí médium Acronis).</b>
<b>Můj zdrojový disk MBR a můj OS nepodporuje rozhraní UEFI.</b>	Operace nebude mít vliv na rozložení oddílů ani na spustitelnost disku: styl rozložení zůstane i nadále MBR, cílový disk bude možné spustit pomocí systému BIOS.	Po dokončení operace se styl oddílu převede na GPT, ale operační systém nebude možné spustit pomocí rozhraní UEFI, protože jej váš operační systém nepodporuje.

	<b>Můj systém se spouští pomocí systému BIOS (Windows nebo Spouštěcí médium Acronis).</b>	<b>Můj systém se spouští pomocí rozhraní UEFI (Windows nebo Spouštěcí médium Acronis).</b>
<b>Můj zdrojový disk je MBR a můj OS podporuje rozhraní UEFI.</b>	Operace nebude mít vliv na rozložení oddílů ani na spustitelnost disku: styl rozložení zůstane i nadále MBR, cílový disk bude možné spustit pomocí systému BIOS.	Cílový oddíl disku bude převeden na styl GPT, což umožní cílový disk spouštět pomocí rozhraní UEFI. Viz část <a href="#">Příklad obnovení systému UEFI</a> .
<b>Můj zdrojový disk je GPT a můj OS podporuje rozhraní UEFI.</b>	Po dokončení operace zůstane styl rozdělení GPT, systém nebude možné spustit pomocí systému BIOS, protože váš operační systém nepodporuje spouštění z GPT pomocí systému BIOS.	Po dokončení operace zůstane styl rozdělení GPT, operační systém bude možné spustit pomocí rozhraní UEFI.

## Příklad postupu obnovení

Viz část [Příklad obnovení systému UEFI](#).

## Příklad obnovení systému UEFI

Příklad přenosu systému za uvedených podmínek:

- Zdrojový disk je MBR a můj operační systém podporuje systém UEFI.
- Cílový systém je spouštěný ze systému UEFI.
- Původní i nový pevný disk pracuje ve stejném režimu řadiče (například IDE nebo AHCI).

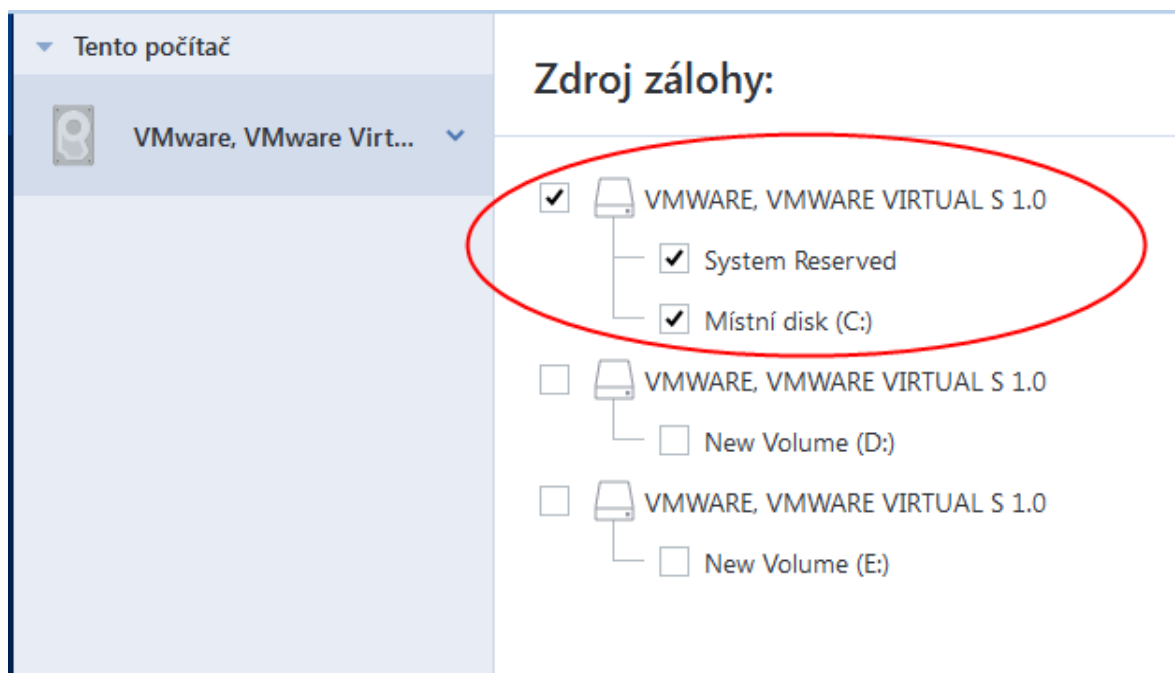
Před zahájením procesu prosím zkontrolujte, zda máte k dispozici:

- **Spouštěcí médium Acronis**

Další informace naleznete v části [Tvorba spouštěcího média Acronis](#).

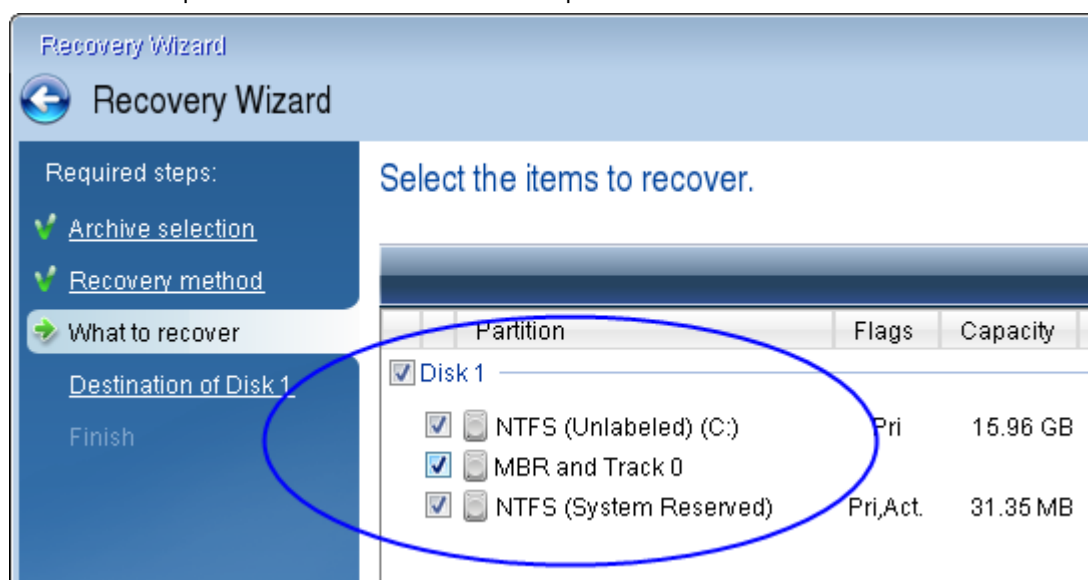
- **Záloha systémového disku vytvořená v režimu disku.**

Chcete-li vytvořit zálohu tohoto typu, přejděte do režimu disku a vyberte pevný disk, který obsahuje váš systémový diskový oddíl. Další informace naleznete v části [Zálohování disků a diskových oddílů](#).



#### **Postup přenosu systému z disku typu MBR do počítače spouštěného ze systému UEFI**

1. Spustíte systém ze spouštěcího média Acronis v módu UEFI a vyberte možnost Acronis Cyber Protect Home Office.
2. Spustíte **Průvodce obnovením** a postupujte podle pokynů uvedených v části [Obnovení systému](#).
3. V kroku **Co se má obnovit** zaškrtnutím políčka vedle názvu disku vyberte celý systémový disk. V níže uvedeném příkladu bude třeba zaškrtnout políčko **Disk 1**:



4. V kroku **Dokončit** klikněte na tlačítko **Pokračovat**.

Po dokončení operace bude cílový disk převeden na styl GPT a bude možné jej spustit v režimu UEFI.

Po obnovení prosím zkontrolujte spuštění počítače v režimu UEFI. Je možné, že budete muset změnit režim spouštění systémového disku v uživatelském rozhraní správce spouštění UEFI.

## 5.1.4 Uspořádání pořadí spouštění v systému BIOS a UEFI BIOS

Chcete-li počítač spustit ze spouštěcího média Acronis, je třeba v pořadí spouštění nastavit toto médium jako první spouštěcí zařízení. Pořadí spouštění se mění v systému BIOS nebo UEFI BIOS v závislosti na rozhraní firmwaru vašeho počítače. Postup je v obou případech velmi podobný.

### ***Jak spustit systém ze spouštěcího média Acronis***

1. Použijete-li jako spouštěcí médium USB flash disk nebo externí disk, zapojte jej do portu USB.
2. Zapněte počítač. V průběhu testu při spuštění počítače (POST) se bude zobrazovat kombinace kláves, které je třeba stisknout, aby mohli vstoupit do systému BIOS nebo UEFI BIOS.
3. Stiskněte uvedenou kombinaci kláves (například **Del**, **F1**, **Ctrl+Alt+Esc**, **Ctrl+Esc**). Otevře se program systému BIOS nebo UEFI BIOS. Program systému se může lišit vzhledem, skupinami položek, názvy atd.

---

#### **Poznámka**

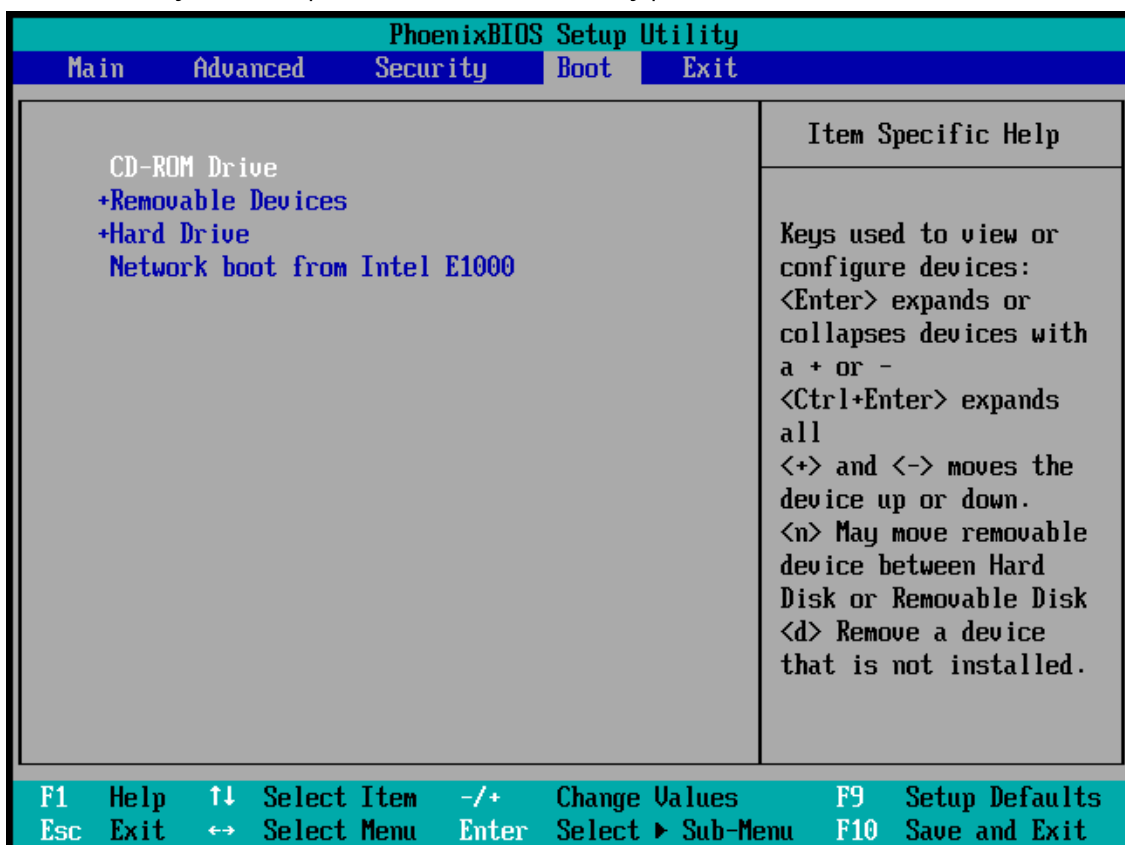
Některé základní desky mají takzvanou spouštěcí nabídku, kterou lze zobrazit stisknutím určité klávesy nebo kombinace kláves, například **F12**. Tato spouštěcí nabídka umožňuje zvolit zařízení, ze kterého chcete systém spustit, ze seznamu spouštěcích zařízení bez změny nastavení systému BIOS nebo UEFI BIOS.

---

4. Použijete-li jako spouštěcí médium disk CD nebo DVD, vložte ho do jednotky CD nebo DVD.
5. Ujistěte se, že je toto spouštěcí médium (CD, DVD nebo USB disk) nastaveno jako první spouštěcí zařízení:
  - a. Pomocí kurzorových šipek na klávesnici se přesuňte se do nastavení pořadí spouštění.
  - b. Umístěte kurzor na zařízení spouštěcího média a posuňte ho v seznamu na první místo.



Pořadí lze obvykle měnit pomocí kláves se znaménky plus a minus.



6. Ukončete BIOS nebo UEFI BIOS a uložte změny, které jste provedli. Počítač se spustí ze spouštěcího média Acronis.

---

#### Poznámka

Pokud se počítač nepodaří spustit z prvního zařízení, pokusí se počítač spustit systém z druhého zařízení v seznamu, a tak dále.

---

### 5.1.5 Obnova disků z úložiště Cloud

Obnova disku z úložiště Acronis Cloud se velmi podobá obnově z obvyčejného pevného disku.

- Pokud se vám daří spustit systém Windows a aplikaci Acronis Cyber Protect Home Office, přečtěte si prosím téma [Obnovení diskových oddílů a disků](#).
- Jestliže systém Windows spustit nelze, přečtěte si článek [Obnova systému z úložiště Acronis Cloud](#).

#### Jak to funguje

Počítač by měl být připojen k internetu pomocí ethernetového kabelu nebo Wi-Fi. Acronis Cyber Protect Home Office podporuje několik protokolů zabezpečení sítě Wi-Fi, včetně WPA-Personal, WPA2-Personal a WPA2-Enterprise.

#### Obnovit do původního umístění

Pokud disk obnovujete do původního umístění, nestahuje Acronis Cyber Protect Home Office do počítače celý disk. Zkontroluje váš disk, vyhledá změny dat a obnoví pouze ty soubory, které se liší od souborů v obrazu disku. Tato technologie výrazně snižuje množství dat potřebné ke stažení, aby bylo možné disk obnovit.

### **Obnova do nového umístění.**

Když obnovujete disk do jiného umístění nebo do nealokovaného prostoru, je tento proces velmi podobný obnově z místního úložiště. Jediný rozdíl spočívá v metodě zápisu dat. Acronis Cyber Protect Home Office stahuje a zapisuje data po jednotlivých blocích, a to nepřetržitě. Tato technologie zvyšuje rychlost obnovy a spolehlivost celého procesu.

## Co se stane, když dojde k přerušení obnovy

Protože obnova disku z úložiště Acronis Cloud používá internetové připojení a obvykle trvá dlouho, je pravděpodobnost jejího přerušení ve srovnání s obnovou z běžných pevných disků vyšší.

Možné důvody přerušení obnovy:

- Internetové připojení bylo ztraceno.
- Spojení s úložištěm Acronis Cloud bylo ztraceno.
- Zrušili jste obnovu, ať již úmyslně nebo omylem.
- Problém s napájením ze sítě.

Pokud se obnova nedokončí z důvodu problémů s připojením, pokusí se aplikace Acronis Cyber Protect Home Office automaticky připojit k aplikaci Acronis Cloud a znovu spustit proces obnovy. V tomto případě doporučujeme zkontrolovat internetové připojení. Pokud se automatické pokusy nezdaří, spusťte po opětovném navázání připojení obnovu ručně.

V ostatních případech spusťte prosím obnovu ručně a ujistěte se, že byla dokončena.

Aplikace Acronis Cyber Protect Home Office bez ohledu na důvod přerušení nespustí obnovu od samého začátku. Obnoví proces a stáhne pouze data, která zatím obnovena nebyla.

## Obnova systému z úložiště Acronis Cloud

---

### **Poznámka**

Obnova disků z úložiště Acronis Cloud může trvat dlouhou dobu (v závislosti na rychlosti internetového připojení).

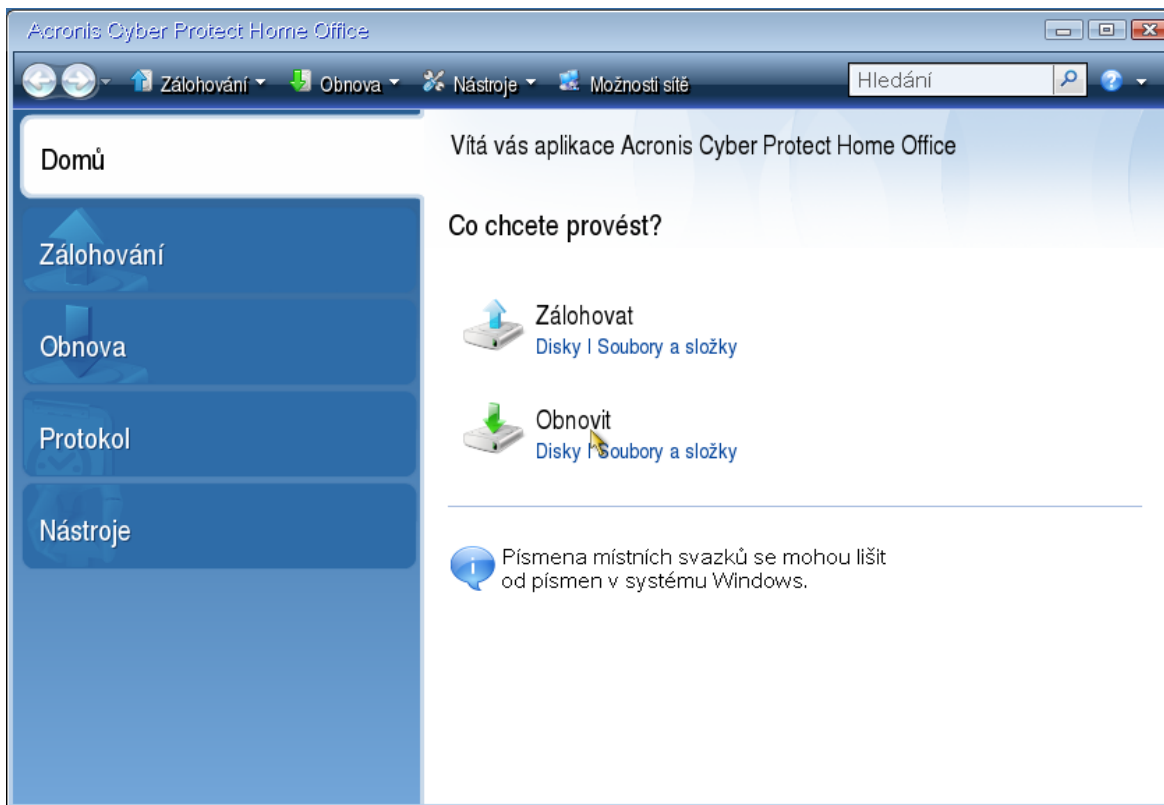
---

Než začnete, doporučujeme dokončit přípravu popsanou v tématu [Příprava na obnovení](#). Pokud obnovujete systém na nový disk, není nutné ho formátovat, protože bude naformátován při procesu obnovení.

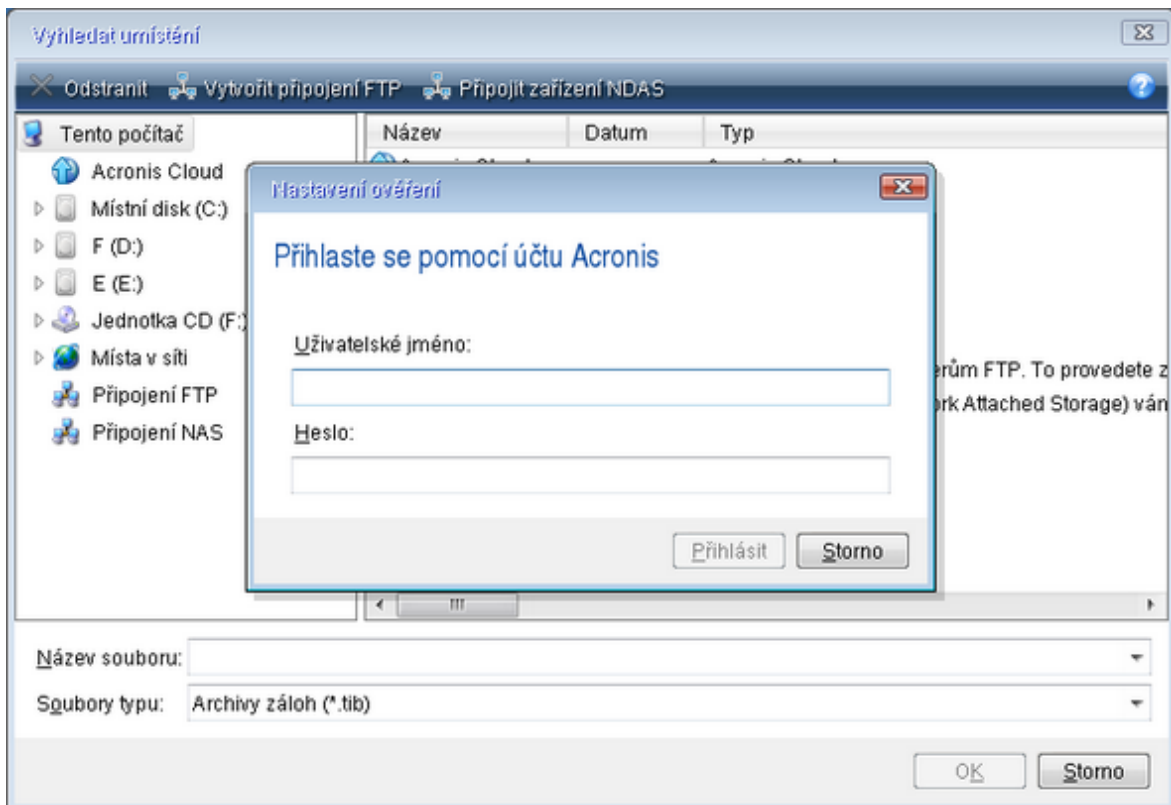
Před zahájením procesu prosím zkontrolujte, zda je počítač připojen k internetu prostřednictvím ethernetového kabelu nebo sítě Wi-Fi.

### **Obnova systémového disku z úložiště Acronis Cloud**

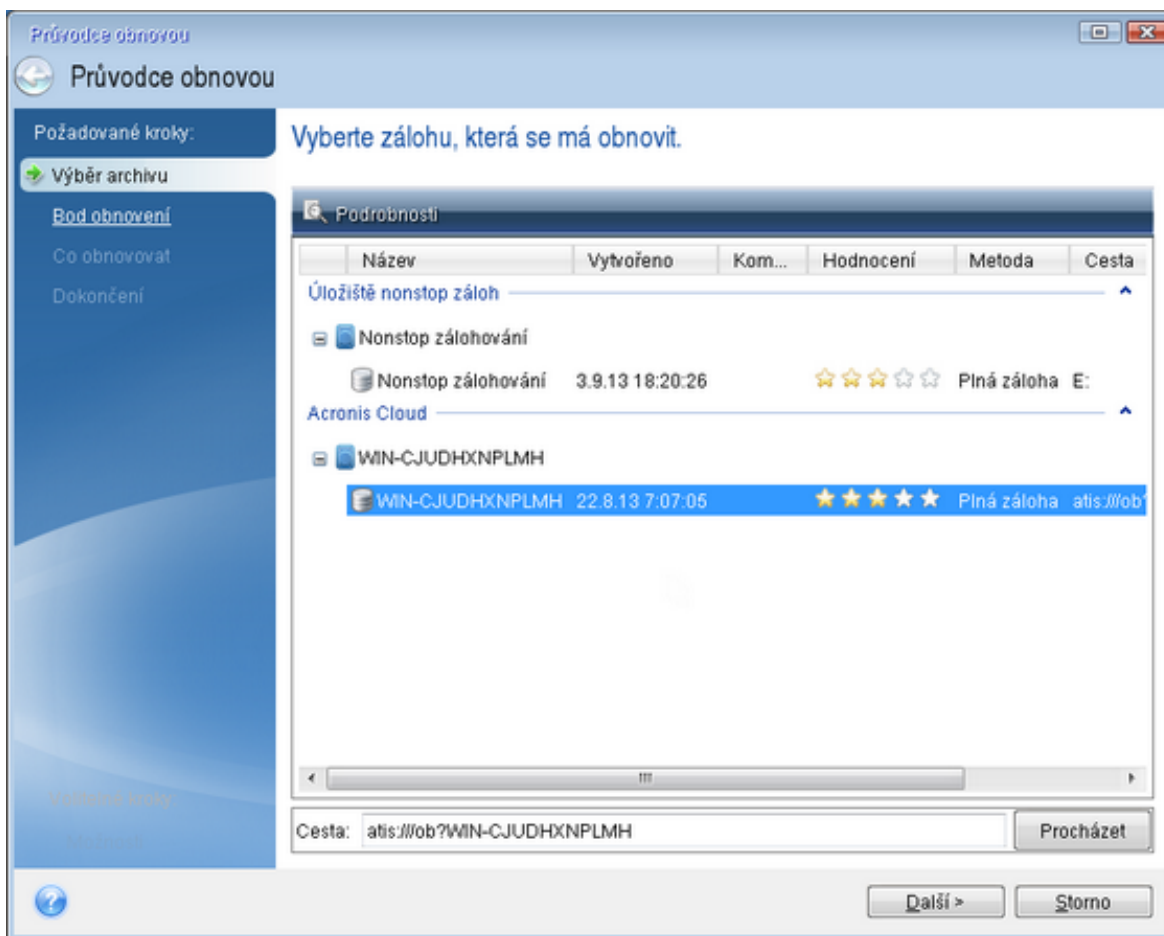
1. Uspořádejte pořadí spouštění v systému BIOS tak, aby se systém spustil ze spouštěcího média Acronis (CD, DVD nebo USB flash disku). Další informace naleznete v tématu [Uspořádání pořadí spouštění v systému BIOS](#).
2. Spusťte systém ze spouštěcího média a vyberte možnost **Acronis Cyber Protect Home Office**.
3. V okně **Domů** zvolte možnost **Moje disky** pod položkou **Obnovit**.



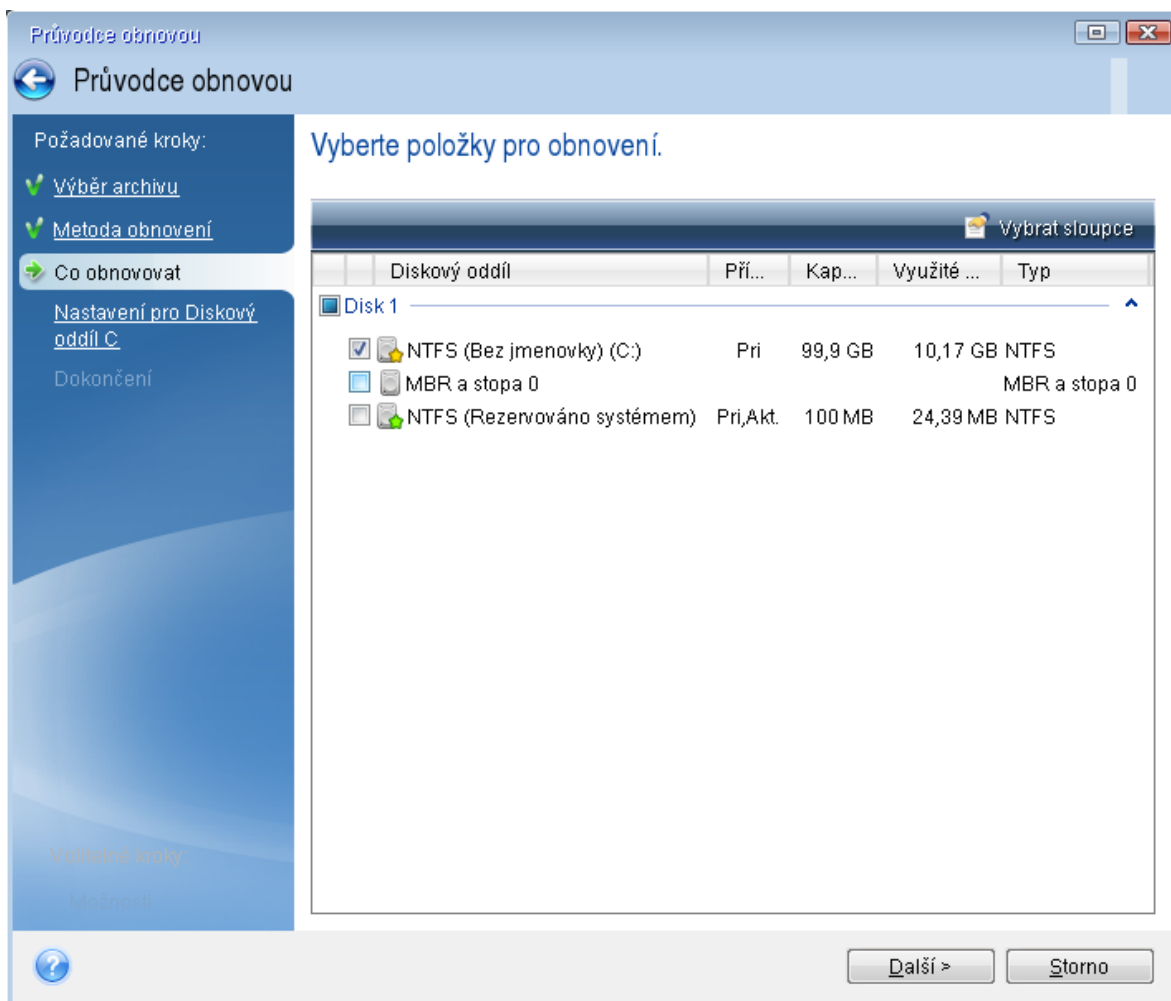
4. Chcete-li přidat online zálohu systémového disku nebo systémového oddílu do seznamu dostupných záloh, klikněte na tlačítko **Procházet**.
5. Ve stromu adresářů otevřeného okna zvolte úložiště Acronis Cloud a zadejte přihlašovací údaje k účtu Acronis.



6. Vyberte zálohu, kterou chcete obnovit, a klepněte na tlačítko **OK**.
7. Během kroku **Výběr archivu** zvolte online zálohu a klikněte na tlačítko **Další**.



8. V kroku **Metoda obnovy** vyberte možnost **Obnovit celé disky a oddíly**.
9. V kroku **Co obnovovat** vyberte systémový oddíl (obvykle C) a oddíl vyhrazený systému (existuje-li). Tyto oddíly můžete rozpoznat také pomocí příznaků **Pri** a **Act**.



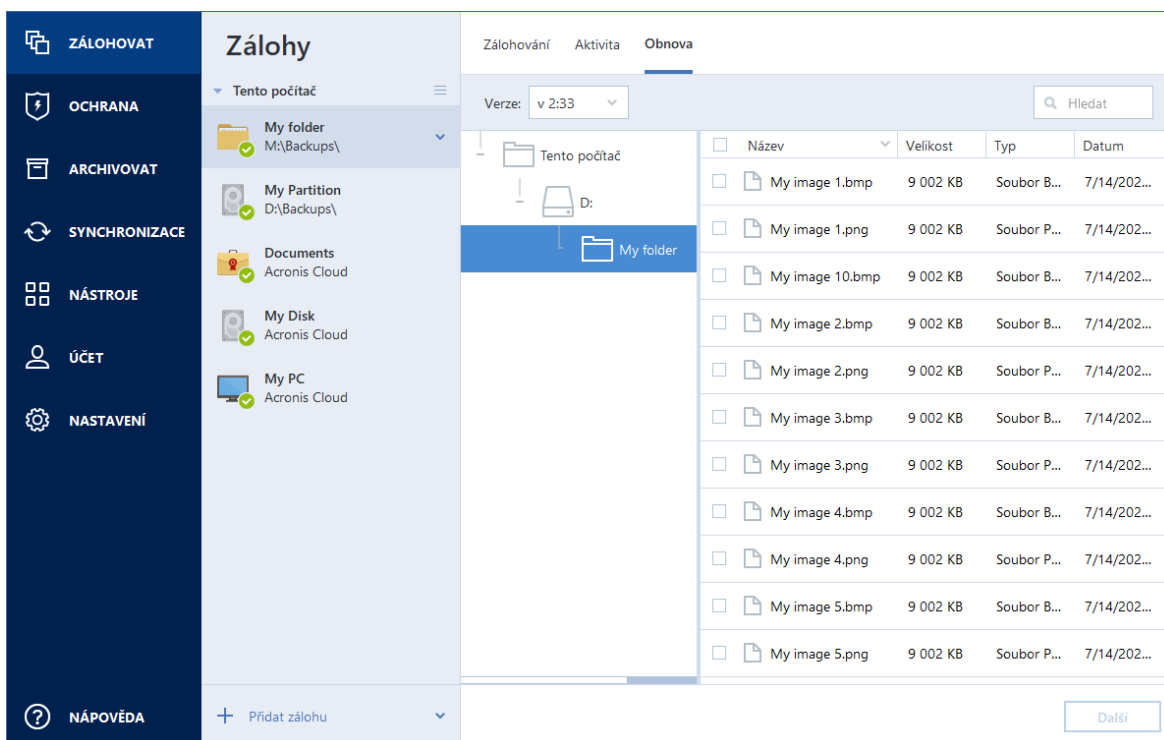
10. V případě potřeby změňte v kroku „Nastavení diskového oddílu C“ (nebo písmene systémového oddílu, pokud se liší) nastavení. Pokud například provádíte obnovení na nový pevný disk s jinou kapacitou, je nutné změnit nastavení.
11. Přečtěte si pozorně souhrn prováděných operací v kroku **Dokončit**. Jestliže jste nezměnili velikost diskového oddílu, musí být velikosti položek **Maže se diskový oddíl** a **Obnovuje se diskový oddíl** shodné. Klikněte na tlačítko **Pokračovat**.
12. Po dokončení obnovení ukončete samostatnou verzi aplikace Acronis Cyber Protect Home Office a odeberte spouštěcí médium. Spusťte obnovený systémový oddíl. Zkontrolujte, zda jste obnovili systém Windows do potřebného stavu, a [obnovte původní pořadí spouštění](#).

## 5.2 Obnova souborů a složek

Zálohované soubory a složky můžete procházet a obnovit v aplikaci Acronis Cyber Protect Home Office, v průzkumníku souborů nebo v úložišti Acronis Cloud. Můžete obnovit soubory a složky ze zálohy na úrovni souborů nebo disku.

### **Postup obnovy dat v Acronis Cyber Protect Home Office**

1. Na bočním panelu klikněte na možnost **Záloha**.
2. Ze seznamu záloh vyberte zálohu obsahující soubory nebo složky, které chcete obnovit, a pak otevřete kartu **Obnovit**.
3. [Volitelné] Na panelu nástrojů v rozevíracím seznamu **Verze** zvolte požadované datum a čas zálohy. Ve výchozím nastavení se obnoví nejnovější záloha.
4. Zaškrtněte políčka příslušných souborů a složek, které chcete obnovit, a klikněte na tlačítko **Další**.



5. [Volitelné] Ve výchozím nastavení se data obnoví do původního umístění. Chcete-li je změnit, klikněte na panelu nástrojů na tlačítko **Procházet** a zvolte požadovanou cílovou složku.
6. [Volitelné] Vyberte možnosti procesu obnovení (prioritu procesu obnovení, nastavení zabezpečení na úrovni souborů a podobně). Chcete-li nastavit možnosti, klikněte na položku **Možnost obnovení**. Zde vybrané možnosti se použijí pouze na aktuální operaci obnovy.
7. Postup obnovy spustíte kliknutím na tlačítko **Obnovit nyní**.  
Vybraná verze souboru se stáhne do zadaného cílového umístění.  
Obnovu můžete zastavit kliknutím na tlačítko **Storno**. Zrušená obnova může způsobit změny v cílové složce.

### **Obnova dat v Průzkumníku souborů**

1. Dvakrát klikněte na příslušný soubor TIB a potom vyhledejte soubor nebo složku, které chcete obnovit.
2. Soubor nebo složku zkopírujte na pevný disk.

---

### Poznámka

Kopírované soubory ztrácejí atribut „Komprimované“ a „Zašifované“. Pokud chcete tyto atributy zachovat, je vhodné zálohu obnovit.

---

### Postup obnovy dat v Acronis Cloud

1. Na levém bočním panelu klikněte na možnost **ZÁLOHY**.
2. V seznamu Zálohy vyberte cloudovou zálohu obsahující soubory nebo složky, které chcete obnovit.
3. V seznamu souborů a složek vyberte ty, které chcete obnovit.
4. [Volitelné] Může obnovit konkrétní verzi souboru (nikoliv složky). Provedete to tak, že na pravém bočním panelu kliknete na tlačítko **Verze** a poté na ikonu stahování na řádku požadované verze.
5. Chcete-li zahájit obnovení, na pravém bočním panelu klikněte na možnost **STÁHNOUT**. Vybraná data se zkopírují do výchozí složky stahování.

---

### Poznámka

Pokud jste vybrali několik souborů a složek, budou umístěny do archivu zip.

---

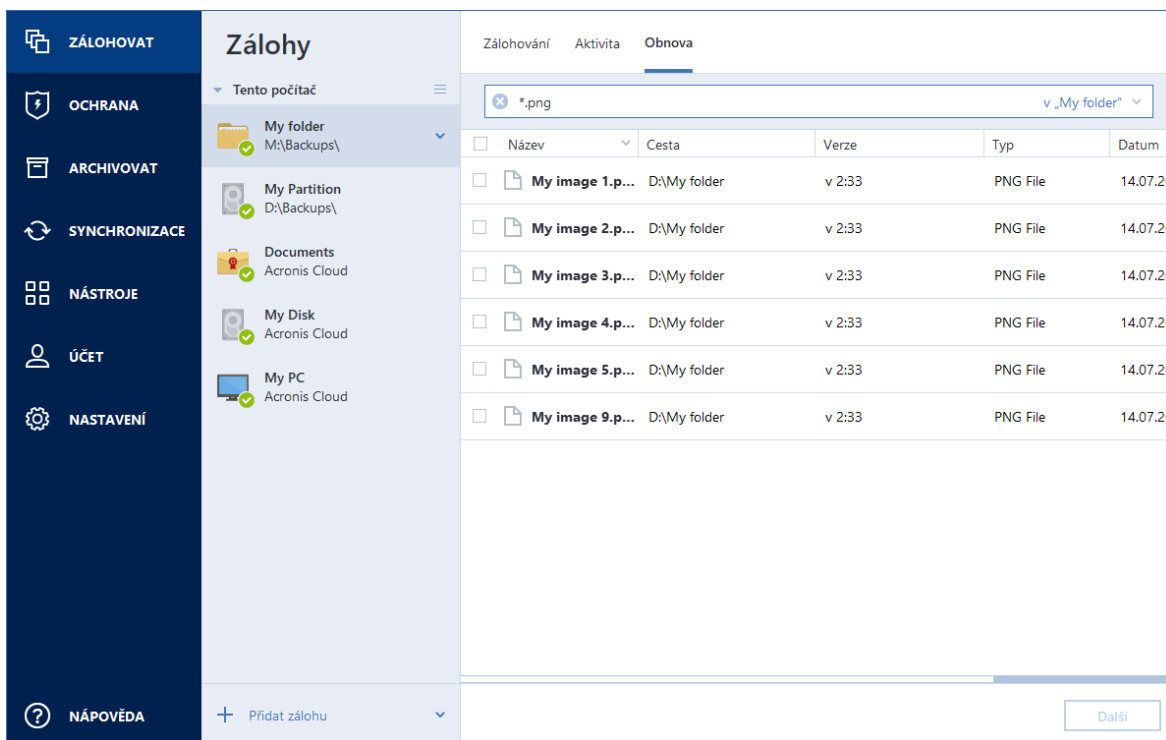
## 5.3 Hledání obsahu zálohy

Při obnovení dat z místních záloh můžete hledat konkrétní soubory a složky uložené ve vybraných zálohách.

### Jak hledat soubory a složky

1. Spustíte obnovení dat dle popisu v části [Obnovení oddílů a disků](#) nebo [Obnovení souborů a složek](#).
2. Při výběru souborů a složek k obnovení zadejte název souboru nebo složky do pole **Hledání**. Program zobrazí výsledky vyhledávání.  
Můžete také použít běžné zástupné znaky systému Windows: \* a ?. Například můžete vyhledat všechny soubory s příponou **EXE** zadáním textu **\*.exe**. Když zadáte **moje???.exe**, vyhledají se všechny soubory s příponou EXE, jejichž název se skládá ze sedmi znaků a začíná textem „moje“.





3. Ve výchozím nastavení aplikace Acronis Cyber Protect Home Office prohledá složku zvolenou v předchozím kroku. Chcete-li do hledání zahrnout celou zálohu, klikněte na šipku dolů a pak klikněte na položku **v celé záloze**.

Chcete-li se vrátit k předchozímu kroku, odstraňte hledaný text a pak klikněte na ikonu křížku.

4. Po dokončení hledání vyberte soubory, které chcete obnovit a pak klikněte na tlačítko **Další**.

#### Poznámka

Dávejte pozor na sloupec Verze. Soubory a složky, které patří do odlišných verzí záloh nelze obnovit zároveň.

## 5.4 Obnova dat aplikace Office 365

Aplikace Acronis Cyber Protect Home Office umožňuje chránit osobní účet aplikace Office 365 před ztrátou e-mailových zpráv, souborů a složek, informací o profilu a jiných dat. Máte-li data účtu zálohována v cloudu, můžete je prohlížet a obnovit konkrétní položky.

### 5.4.1 Jaké položky lze obnovit?

#### Následující položky lze obnovit ze zálohy poštovní schránky:

- Celou poštovní schránku
- E-mailové zprávy
- Přílohy

#### Následující položky lze obnovit ze zálohy úložiště OneDrive:

- Celé úložiště OneDrive
- Jakékoliv zálohované soubory a složky

## 5.4.2 Obnova dat aplikace Office 365

### *Jak prohlížet a obnovit data*

1. Jedním z následujících postupů otevřete aplikaci Online kontrolní panel:
  - Klikněte na odkaz: <https://cloud.acronis.com>.
  - Na bočním panelu aplikace Acronis Cyber Protect Home Office klikněte na položku **Účet** a poté na možnost **Otevřít online kontrolní panel**.
2. Přihlaste se k účtu Acronis.
3. Na bočním panelu klikněte na položku **Zdroje**, vyhledejte pole zálohy aplikace Office 365 a klikněte na tlačítko **Obnovit**.
4. Prohlédněte si seznam záloh. V případě potřeby použijte filtr a vyhledejte zálohu podle obsahu.
5. Po výběru zálohy klikněte na tlačítko **Obnovit...** a vyberte data, která chcete obnovit:
  - Celé úložiště OneDrive nebo konkrétní soubory a složky.
  - Celou poštovní schránku nebo konkrétní zprávy.

Pokud se rozhodnete obnovit konkrétní položky, online kontrolní panel otevře seznam zálohovaných položek. Můžete je prohlížet, zobrazit jejich obsah a vyhledat konkrétní položku (u některých typů dat není tato možnost k dispozici).

Po výběru položek můžete zvolit operaci, která se provede (v závislosti na typu dat nemusejí být některé operace dostupné):

- **Zobrazit obsah**– kliknutím zobrazíte podrobnosti o položce nebo ji otevřete v plné velikosti.
  - **Poslat jako e-mail**– kliknutím pošlete zprávu vybraným příjemcům.
  - **Zobrazit verze**– kliknutím zobrazíte verze položky.
  - **Obnovit**– kliknutím zadáte umístění položek, které chcete obnovit. U některých položek můžete rovněž obnovit oprávnění ke sdílení.
  - **Stáhnout**– kliknutím stáhnete vybraný soubor.
6. Klikněte na tlačítko **Spustit obnovu**.

## 5.5 Možnosti obnovy

Možnosti procesu obnovy disku či diskového oddílu a souborů je možné nakonfigurovat. Po instalaci aplikace jsou všechny možnosti nastaveny na výchozí hodnoty. Můžete je měnit pouze pro aktuální operaci obnovení nebo pro všechny budoucí operace obnovení. Zaškrtnutím políčka **Uložit nastavení jako výchozí** použijete upravené nastavení pro všechny další operace obnovení.

Možnosti obnovení disku a možnosti obnovy souborů jsou zcela nezávislé a měli byste je nastavovat odděleně.

Chcete-li obnovit výchozí nastavení po instalaci produktu, klikněte na tlačítko **Obnovit výchozí nastavení**.

## 5.5.1 Režim obnovy disku

Umístění: **Možnosti obnovení** > **Rozšířené** > **Režim obnovy disku**

Pomocí této možnosti je možné vybrat režim obnovy disku pro zálohy diskových obrazů.

- **Obnova sektor po sektoru**– toto políčko zaškrtněte, pokud chcete obnovit využitě i nevyužitě sektory disků nebo diskových oddílů. Tato možnost bude efektivní pouze tehdy, když k obnovení vyberete zálohu vytvořenou sektor po sektoru.

## 5.5.2 Příkazy Před/Po pro obnovu

Umístění: **Možnosti obnovení** > **Rozšířené** > **Příkazy Před/Po**

Příkazy (nebo dokonce dávkové soubory), které budou automaticky provedeny před a po obnově, lze zadat.

Například chcete spustit či zastavit určité procesy systému Windows nebo zkontrolovat přítomnost možných virů v datech před obnovením.

Jak zadat příkazy (dávkové soubory):

- Vyberte požadovaný příkaz, který bude proveden před spuštěním procesu obnovení v poli **Příkazy před**. Chcete-li vytvořit nový příkaz nebo vybrat nový dávkový soubor, klikněte na tlačítko **Upravit**.
- Vyberte požadovaný příkaz, který bude proveden po skončení procesu obnovení v poli **Příkaz po**. Chcete-li vytvořit nový příkaz nebo vybrat nový dávkový soubor, klikněte na tlačítko **Upravit**.

Nepokoušejte se prosím spouštět interaktivní příkazy, tj. příkazy vyžadující zadání od uživatele (například „pause“). Ty nejsou podporovány.

## Úprava uživatelských příkazů pro obnovu

Je možné zadat uživatelské příkazy, které se provedou před nebo po obnově:

- Do textového pole **Příkaz** zadejte příkaz nebo jej vyberte ze seznamu. Kliknutím na tlačítko ... vyberte dávkový soubor.
- Do textového pole **Pracovní adresář** zadejte cestu pro provedení příkazu nebo ji vyberte v seznamu dříve zadaných cest.
- Do textového pole **Argumenty** zadejte argumenty provedení příkazu nebo je vyberte ze seznamu.

Vypnutí parametru **Neprovádět operace před dokončením vykonávání příkazu**, který je ve výchozím nastavení zapnut, umožní procesu zálohování běžet souběžně s prováděním příkazů.

Parametr **Zrušit operaci při selhání uživatelského příkazu** (ve výchozím nastavení zapnut) zruší operaci při výskytu jakýchkoli chyb při provádění příkazů.

Zadaný příkaz lze testovat kliknutím na tlačítko **Testovat příkaz**.

### 5.5.3 Možnosti ověřování

Umístění: **Možnosti obnovení > Rozšířené > Ověření**

- **Ověřit zálohu před obnovením**– Tuto možnost povolte, chcete-li provést kontrolu integrity zálohy před obnovením.
- **Zkontrolovat systém souborů po obnovení**– Tuto možnost povolte, chcete-li provést kontrolu integrity systému souborů na obnoveném diskovém oddílu.

---

#### Poznámka

Kontrolu lze provést pouze u systémů souborů FAT16/32 a NTFS.

---

#### Poznámka

Pokud je během obnovy vyžadováno restartování (například při obnově systémového diskového oddílu do původního umístění), systém souborů se nezkontroluje.

---

### 5.5.4 Restartování počítače

Umístění: **Možnosti obnovení > Rozšířené > Restartování počítače**

Pokud chcete, aby se počítač restartoval automaticky, když je to nezbytné pro obnovu, zaškrtněte políčko **Restartovat automaticky počítač, pokud je to nutné k provedení obnovy**. Toho lze využít, když je třeba obnovit diskový oddíl uzamknutý operačním systémem.

### 5.5.5 Možnosti obnovy souborů

Umístění: **Možnosti obnovení > Rozšířené > Možnosti obnovy souborů**

Je možné vybrat následující možnosti obnovy souborů:

- **Obnovovat soubory s původním nastavením zabezpečení** – pokud bylo při zálohování zachováno nastavení zabezpečení souborů (viz část [Nastavení zabezpečení zálohy na úrovni souborů](#)), můžete si vybrat, zda je chcete obnovit, nebo zda soubory zdědí nastavení zabezpečení složky, do které budou obnoveny. Tato možnost je účinná pouze při obnovení souborů ze záloh souborů či složek.
- **Nastavit aktuální datum a čas pro obnovené soubory**– je možné určit, zda se má obnovit datum a čas souborů ze zálohy nebo přiřadit k souborům aktuální datum a čas. Při výchozím nastavení se přiřadí výchozí datum a čas souboru ze zálohy.

### 5.5.6 Možnosti přepsání souborů

Umístění: **Možnosti obnovení > Rozšířené > Možnosti přepsání souborů**

Zvolte, co si přejete provést v případě, že aplikace v cílové složce nalezne soubor se stejným názvem, jako má soubor v záloze.

---

## Poznámka

Tato možnost je k dispozici pouze při obnově souborů a složek (nikoli disků a oddílů).

---

Chcete-li přepsat soubory na pevném disku pomocí souborů ze zálohy, označte zaškrťovací políčko **Přepsat stávající soubory**. Pokud dojde ke zrušení zaškrtnutí políčka, budou na disku zachovány nejaktuálnější soubory a složky.

Pokud si některé soubory nepřejete přepisovat:

- Zaškrtnutím políčka **Skryté soubory a složky** vypnete přepisování všech skrytých souborů a složek. Tato možnost je k dispozici pro zálohování na úrovni souborů do místních cílových umístění a sdílených síťových složek.
- Zaškrtnutím políčka **Systémové soubory a složky** vypnete přepisování všech systémových souborů a složek. Tato možnost je k dispozici pro zálohování na úrovni souborů do místních cílových umístění a sdílených síťových složek.
- Zaškrtnutím políčka **Novější soubory a složky** vypnete přepisování novějších souborů a složek.
- Kliknutím na možnost **Přidat určité soubory a složky** spravujete seznam vlastních souborů a složek, které nechcete přepsat. Tato možnost je k dispozici pro zálohování na úrovni souborů do místních cílových umístění a sdílených síťových složek.
  - Chcete-li vypnout přepisování určitých souborů, klikněte na znaménko plus a vytvořte tak výjimku.
  - Při určování kritérií lze použít běžné zástupné znaky systému Windows. Například můžete zachovat všechny soubory s příponou **.exe** přidáním masky **\*.exe**. Masku **Moje???.exe** ponechá všechny soubory s příponou **.exe**, jejichž název se skládá ze sedmi znaků a začíná znaky „Moje“.

Chcete-li odstranit kritérium, vyberte ho v seznamu a pak klikněte na znaménko minus.

## 5.5.7 Rychlost průběhu obnovování

Umístění: **Možnosti obnovení > Rozšířené > Výkon**

Můžete nakonfigurovat následující nastavení:

### Priorita operace

Změna priority procesu zálohování nebo obnovy způsobí, že proces poběží rychleji nebo pomaleji (podle toho, jestli prioritu zvýšíte nebo snížíte) ale také může negativně ovlivnit výkon ostatních spuštěných aplikací. Priorita všech procesů spuštěných v systému určuje využití procesoru a systémových prostředků přiřazených k procesu. Snížení priority operace uvolní více prostředků pro jiné úlohy procesoru. Zvýšení priority zálohování nebo obnovy může urychlit proces přebrání prostředků aktuálně spuštěných procesů. Účinek tohoto nastavení závisí na celkovém využití procesoru a dalších faktorech.

Prioritu operace lze nastavit na jednu ze tří možností:

- **Nízká** (ve výchozím nastavení zapnuto) – proces zálohování nebo obnovy bude fungovat pomaleji, ale výkon ostatních aplikací se zvýší.
- **Normální** – proces zálohování nebo obnovy bude mít stejnou prioritu jako ostatní procesy.
- **Vysoká** – proces zálohování nebo obnovy bude fungovat rychleji, ale výkon ostatních aplikací se sníží. Výběr této možnosti může vyústit ve 100% využití procesoru aplikací Acronis Cyber Protect Home Office.

## 5.5.8 Upozornění na operace obnovy

Umístění: **Možnosti obnovy > Oznámení**

Někdy může zálohování nebo obnova trvat hodinu i déle. Aplikace Acronis Cyber Protect Home Office vás může upozornit na dokončení operace prostřednictvím e-mailu. Aplikace může zasílat také zprávy zobrazené během operace nebo po jejím dokončení zaslat celý soubor protokolu.

Ve výchozím nastavení jsou všechna upozornění vypnuta.

### Práh volného místa na disku

Lze nastavit upozornění, které se zobrazí v případě, že volné místo v úložišti obnovy bude menší než zadaná prahová hodnota. Pokud po spuštění zálohování aplikace Acronis Cyber Protect Home Office zjistí, že v umístění vybrané zálohy je méně volného místa, než je zadáno, vůbec nezačne samotný proces obnovy a okamžitě vás informuje příslušnou zprávou. Zpráva nabízí tři možnosti – ignorovat ji a pokračovat v obnově, vyhledat jiné umístění pro obnovu nebo obnovu zrušit.

Pokud se volné místo zmenší v průběhu obnovy, aplikace zobrazí stejnou zprávu se stejnými možnostmi.

#### ***Chcete-li nastavit práh volného místa na disku***

- Zaškrtněte políčko **Při nedostatku volného místa na disku zobrazovat oznámení**.
- Do pole **Velikost** zadejte prahovou hodnotu a vyberte jednotku.

Aplikace Acronis Cyber Protect Home Office může sledovat volné místo na následujících úložných zařízeních:

- místní pevné disky,
- karty a jednotky USB,
- Sdílené síťové složky (SMB)

---

#### **Poznámka**

Pokud je zaškrtnuto políčko **Při zpracování nezobrazovat zprávy a dialogová okna (tichý režim)** v nastavení **Zpracování chyb**, zpráva se nebude zobrazovat.

---

#### **Poznámka**

Tuto možnost nelze zapnout pro jednotky CD/DVD.

---

## E-mailové oznámení

1. Zaškrtněte políčko **Posílat upozornění e-mailem o stavech operace**.
2. Konfigurace nastavení e-mailu:
  - Do pole **Komu** zadejte e-mailovou adresu. Můžete zadat více e-mailových adres oddělených středníkem.
  - V poli **Nastavení serveru** zadejte server odchozí pošty (SMTP).
  - Nastavte port serveru odchozí pošty. Ve výchozím nastavení je tento port 25.
  - Je-li to vyžadováno, zaškrtněte políčko **Ověření SMTP** a poté do příslušných polí zadejte uživatelské jméno a heslo.
3. Chcete-li zkontrolovat správnost nastavení, klikněte na tlačítko **Odeslat testovací zprávu**.

### ***Pokud se odeslání testovací zprávy nezdaří***

1. Klikněte na možnost **Zobrazit rozšířená nastavení**.
2. Konfigurace dalších nastavení e-mailu:
  - V poli **Od** zadejte e-mailovou adresu odesílatele. Pokud si nejste jisti, jakou adresu zadat, zadejte jakoukoli adresu ve standardním formátu, například *aaa@bbb.com*.
  - V případě nutnosti změňte předmět zprávy v poli **Předmět**.
  - Zaškrtněte políčko **Přihlásit k serveru příchozí pošty**.
  - V poli **Server POP3** zadejte server příchozí pošty (POP3).
  - Nastavte port serveru příchozí pošty. Ve výchozím nastavení je tento port 110.
3. Znovu klikněte na tlačítko **Odeslat testovací zprávu**.

### ***Další nastavení upozornění***

- Chcete-li odeslat upozornění o dokončení procesu, zaškrtněte políčko **Po úspěšném dokončení operace odeslat upozornění**.
- Chcete-li odeslat upozornění o selhání procesu, zaškrtněte políčko **Při selhání operace odeslat upozornění**.
- Chcete-li odeslat upozornění se zprávami o operaci, zaškrtněte políčko **Odeslat upozornění, když je třeba interakce uživatele**.
- Chcete-li odeslat upozornění s úplným protokolem o operacích, zaškrtněte políčko **Přidat protokol k upozornění**.

## 6 Archivace dat

### 6.1 Co je archivace dat?

Archivace dat je nástroj umožňující přesouvání velkých a málo používaných souborů do úložiště Acronis Cloud, do zařízení NAS, na externí pevný disk nebo na USB flash disk. Při každém spuštění nástroj analyzuje data ve vybraných složkách a navrhuje nahrání nalezených souborů do úložiště Acronis Cloud nebo jejich přesunutí do místního úložiště. Můžete vybrat soubory a složky, které mají být archivovány. Po přesunutí do archivu se místní kopie souborů odstraní. Odkazy na soubory se ukládají do jedinečného umístění, které se nazývá Acronis Drive. Umístění můžete otevřít jako běžnou složku v Průzkumníku souborů. Dvojitým kliknutím na odkaz na soubor otevřete soubor jako by byl uložen v místní složce. Pokud je soubor archivován v úložišti Acronis Cloud, bude nejprve stažen zpět do počítače. Můžete ho také otevřít a spravovat přímo v úložišti Acronis Cloud.

Archivace dat má následující vlastnosti:

- **Úspora volného místa v úložišti**

Úložiště moderních velkokapacitních pevných disků je zpravidla obsazeno uživatelskými daty, jako jsou fotografie a dokumenty, nikoli operačním systémem či aplikacemi. Protože většina z těchto dat je používána pouze občas, není třeba je uchovávat na místním disku. Archivace dat umožňuje uvolnit místo v úložišti pro často používané soubory.

- **Archivace v cloudu a místní archivace**

Můžete si zvolit typ cíle pro váš archiv: Úložiště Acronis Cloud nebo místní úložiště, například interní pevný disk, externí pevný disk, zařízení NAS nebo USB flash disk. Vždy, když jako cíl vyberete úložiště Acronis Cloud, vybraná data se uloží do stejného cloudového archivu. Místní archivy jsou na sobě nezávislé a mohou mít různé názvy, cílová umístění, nastavení šifrování a tak podobně, i když můžete jako cílové umístění vybrat stávající archiv místo vytvoření nového. Počet místních archivů není omezen.

- **Snadný přístup do cloudového archivu z libovolného zařízení**

Když archivujete soubory do úložiště Acronis Cloud, můžete je prostřednictvím aplikace Acronis Cyber Protect Home Office, mobilní aplikace Acronis Cyber Protect Home Office nebo webové aplikace Acronis Cloud otvírat z jakéhokoli zařízení se systémem Windows, macOS, iOS nebo Android (včetně tabletů a chytrých telefonů).

- **Ochrana dat v cloudovém archivu**

Data uložená v úložišti Acronis Cloud jsou chráněna před poškozením a havárií. V případě selhání místního pevného disku můžete například soubory stáhnout na nový pevný disk. Navíc jsou data ukládána v zašifrovaném stavu. Můžete si být jisti, že kromě vás nemá k datům nikdo přístup.

- **Sdílení souborů**

Když jsou soubory nahrány do úložiště Acronis Cloud, můžete vytvořit veřejné odkazy a jejich prostřednictvím sdílet soubory s přáteli nebo je posílat na fóra a sociální síť.

- **Verze souborů**



Pokud byly soubory několikrát změněny a nahrány do úložiště Acronis Cloud, aplikace Acronis Cyber Protect Home Office uchovává všechny změny v různých verzích souborů. Můžete si vybrat předchozí verzi a stáhnout si ji do zařízení.

## 6.2 Co je vyloučeno z archivů?

Z důvodu zmenšení velikosti archivu a zamezení možnosti poškození systému aplikace Acronis Cyber Protect Home Office ve výchozím nastavení vyčleňuje z archivů následující data:

- pagefile.sys
- swapfile.sys
- Složka Temp
- Složka System Volume Information
- Koš
- Dočasná data webového prohlížeče:
  - Dočasné soubory internetu
  - Mezipaměť
- Soubory TIB
- Soubory TIB.METADATA
- Soubory TMP
- Soubory ~

Viz kompletní seznam souborů ve znalostní databázi: <https://kb.acronis.com/content/58297>.

## 6.3 Archivace v cloudu vs. online zálohování

Když archivujete data do úložiště Acronis Cloud, je to podobné jako online zálohování, ale existuje zde několik rozdílů.

	Online zálohování	Archivace do cloudu
Účel funkce	Ochrana dat pro případ poškození operačního systému, selhání hardwaru a ztráty jednotlivých souborů	Čištění místního úložného zařízení a přesouvání dat do úložiště Acronis Cloud.
Ochrana dat	<ul style="list-style-type: none"> <li>• Celková ochrana dat v počítači, především operačního systému</li> <li>• Ochrana často používaných souborů</li> </ul>	Ochrana málo používaných a starých souborů, převážně osobních dokumentů, fotografií atd.
Výběr zdrojových dat	Ruční výběr	Ruční výběr automaticky vyhledaných souborů

	Online zálohování	Archivace do cloudu
Manipulace se zdrojovými daty	Zdrojová data jsou uchovávána v původním umístění.	Zdrojová data jsou odstraňována z původního umístění. Tím je zaručeno, že se vaše data v případě krádeže pevného disku nebo notebooku nedostanou do nesprávných rukou.
Četnost změn dat	Data, která mají být zálohována, se často mění. Obvykle má záloha mnoho verzí, které jsou čas od času aktualizovány.	Data, která mají být archivována, se mění málokdy. Soubory mají pouze několik verzí.

## 6.4 Archivace dat

Archivace dat slouží k uvolnění úložného prostoru přesunutím starých a málo používaných souborů do úložiště Acronis Cloud nebo místního úložiště. Další informace naleznete v části [Co je archivace dat](#).

### ***Jak archivovat data***

1. Spustíte aplikaci Acronis Cyber Protect Home Office a přejděte do části **Archivovat**.
2. [Volitelný krok] Základy archivace dat naleznete na snímcích Začínáme.
3. Proveďte jeden z následujících úkonů:
  - Chcete-li analyzovat soubory ve výchozí uživatelské složce systému Windows, která je obvykle uložena v umístění C:\Users\[uživatelské jméno], klikněte na položku **Analyzovat domovskou složku**.
  - Chcete-li analyzovat soubory ve vlastní složce, klikněte na šipku dolů, klikněte na položku **Vybrat jinou složku** a vyberte složku, kterou chcete analyzovat.

Aplikace Acronis Cyber Protect Home Office analyzuje soubory ve vašem počítači. Upozorňujeme, že tento proces může trvat několik minut.
4. V levé části vyberte kategorii dat. Potom v pravé části vyberte soubory a složky, které chcete archivovat.

Při výběru vyhledaných souborů je můžete třídit například podle velikosti nebo stáří (datum poslední úpravy). Chcete-li soubory třídit, klikněte na záhlaví příslušného sloupce.
5. Klikněte na tlačítko **Vybrat cíl** a pak vyberte možnost Acronis Cloud nebo vlastní místní cíl pro archivované soubory.
6. [volitelný krok] Klikněte na položku **Možnosti** a nastavte možnosti archivace včetně položek **Datové centrum** a **Šifrování**. Další informace naleznete v části [Možnosti šifrování archivu](#).
7. Klikněte na tlačítko **Archivovat**.
8. Potvrďte, že chcete soubory přesunout do archivu a automaticky je odstranit z počítače.

Dále se povídejte na video s pokyny v angličtině na adrese <https://goo.gl/eEkNj2>.

## 6.4.1 Možnosti archivace dat

### Datové centrum

Když archivujete soubory do úložiště Acronis Cloud, nahrají se do jednoho z datových center Acronis umístěných v různých zemích. Nejprve je při vytvoření účtu Acronis určeno nejbližší datové centrum k vašemu umístění. Potom jsou vaše archivované soubory standardně ukládány do tohoto datového centra.

Pokud jste v jiné zemi a vaše výchozí datové centrum není nejbližší k vašemu umístění, doporučujeme nastavit datové centrum archivu ručně. Tím se významně zvýší rychlost nahrávání dat.

---

#### Poznámka

Datové centrum nelze po spuštění archivace změnit.

---

#### *Chcete-li zvolit datové centrum*

1. Při konfiguraci první archivace klikněte na položku **Možnosti**.
2. Vyberte zemi, která je nejbližší vašemu aktuálnímu umístění.

### Šifrování

Chcete-li chránit archivovaná data před neoprávněným přístupem, můžete archiv zašifrovat pomocí standardizovaného kryptografického algoritmu AES (Advanced Encryption Standard) s klíčem o délce 256 bitů.

---

#### Poznámka

Pro již existující archiv nelze nastavit nebo změnit možnost šifrování archivu.

---

Jak šifrovat archiv:

1. Při konfiguraci první archivace klikněte na položku **Možnosti**.
2. Zaškrtněte políčko **Zašifrovat archiv pomocí algoritmu AES-256**.
3. Do příslušného pole zadejte heslo archivu. Heslo musí obsahovat nejméně sedm znaků a mělo by obsahovat jak písmena (nejlépe velká i malá), tak číslice, aby bylo obtížnější jej uhodnout.

---

#### Poznámka

Heslo nelze obnovit. Zapamatujte si heslo, které jste použili pro ochranu archivu.

---

Aplikace Acronis Cyber Protect Home Office vyžaduje zadání hesla při každém pokusu o úpravu archivu. Pro přístup k tomuto archivu je nutné zadat správné heslo.

## 6.5 Přístup k archivovaným souborům

Po úspěšné archivaci soubory najdete zde:

- **Průzkumník souborů**

Spusťte Průzkumník souborů a klikněte v části Oblíbené na položku **Úložiště Acronis Drive**. Se soubory můžete pracovat v režimu pouze ke čtení. Chcete-li upravit soubor, zkopírujte ho nejprve do jiné složky.

- **Acronis Cloud** (platí pouze pro cloudový archiv)

Otevřete webovou aplikaci Acronis Cloud jedním z následujících způsobů:

- Spusťte aplikaci Acronis Cyber Protect Home Office, klikněte na položku **Archivovat** a potom klikněte na položku **Zobrazit ve webovém prohlížeči**.
- Přejděte na stránku <https://www.acronis.com/my/online-backup/webrestore/> a pak se přihlaste do svého účtu.

## 7 Sdílení dat

Soubory a složky uložené v zálohách a archivech v úložišti Acronis Cloud můžete sdílet.

1. Na bočním panelu Acronis Cyber Protect Home Office klikněte na možnost **Účet**.
2. V části **Úložiště služby Acronis Cloud Storage** klikněte na tlačítko **Procházet data**. Prohlížeč vás přesměruje na stránku úložiště Acronis Cloud.
3. V závislosti na tom, co chcete sdílet, postupujte následovně:
  - Chcete-li sdílet soubor nebo složku ze zálohy, na levém bočním panelu klikněte na položku **ZÁLOHY**. Zaškrtněte požadovaný soubor nebo složku.
  - Chcete-li sdílet soubor nebo složku z archivu, na levém bočním panelu klikněte na položku **ARCHIVY**. Zaškrtněte požadovaný soubor nebo složku.
4. Na pravém bočním panelu klikněte na možnost **Sdílet odkaz**.
5. [Volitelné] Můžete nakonfigurovat možnosti sdílení. Provedete to tak, že v okně odkazu kliknete na možnost **Nastavení odkazu**. Můžete použít heslo, nastavit datum vypršení platnosti a omezit počet stahování.
6. V okně odkazu klikněte na možnost **Kopírovat odkaz** a okno zavřete.

Nyní můžete tento odkaz sdílet. Chcete-li sdílené soubory zobrazit, na levém bočním panelu klikněte na možnost **SDÍLENÍ**. Zde můžete vybrat soubor a na pravém bočním panelu kopírovat jeho odkaz, nakonfigurovat nastavení odkazu nebo jej odstranit.

## 8 Ochrana rodinných dat

### 8.1 Co je ochrana rodinných dat?

Ochrana rodinných dat je unifikované multiplatformní řešení umožňující sledování a kontrolu stavu ochrany všech počítačů, chytrých telefonů a tabletů sdílejících jeden účet. Protože uživatelé těchto zařízení musí být přihlášení ke stejnému účtu, jsou obvykle členy jedné rodiny. Obecně může tuto funkci používat každý z nich, ale jeden ze členů rodiny je obvykle technologicky zkušenější než ostatní. Je tedy rozumné přenést zodpovědnost za ochranu rodinných dat na něj.

Chcete-li sledovat a kontrolovat stav ochrany rodinných zařízení, používejte webovou aplikaci Online kontrolní panel dostupnou z jakéhokoli počítače připojeného k internetu. Pomocí této webové aplikace váš rodinný IT správce může:

- Kontrolovat aktuální stavy všech záloh na všech rodinných zařízeních se systémem Windows, macOS, iOS nebo Android.
- Přidat do seznamu nové zařízení
- Ručně spouštět všechny zálohy v libovolném počítači
- Vytvářet nové zálohy libovolného typu (celý počítač, na úrovni souborů, na úrovni disku) na počítačích PC a Mac.
- Měnit nastavení existujících záloh.
- Obnovovat data z jakékoli zálohy nacházející se v úložišti Acronis Cloud, včetně záloh z počítačů PC a Mac nebo zařízení se systémem iOS a Android.
- Řešit některé problémy související s produkty

### 8.2 Přidání nového zařízení do aplikace Online kontrolní panel

Chcete-li využívat všech výhod aplikace Online kontrolní panel, včetně vzdálené správy záloh, musíte nejprve přidat svá zařízení na seznamu zařízení.

#### **Chcete-li přidat nové zařízení**

1. Nainstalujte do zařízení Mac aplikaci Acronis Cyber Protect Home Office.
  - Instalační soubory pro operační systémy Windows a macOS můžete stáhnout na webových stránkách společnosti Acronis.
  - Chcete-li aplikaci Acronis Cyber Protect Home Office nainstalovat do zařízení se systémem iOS nebo Android, postupujte podle pokynů v tématu Instalace aplikace Acronis Cyber Protect Home Office pro mobilní zařízení.
2. Spusťte aplikaci Acronis Cyber Protect Home Office a přihlaste se ke svému účtu.

Případně můžete zařízení přidat prostřednictvím rozhraní aplikace Online kontrolní panel.

#### **Chcete-li přidat nové zařízení prostřednictvím aplikace Online kontrolní panel**

1. V zařízení, které chcete přidat, otevřete aplikaci Online kontrolní panel na adrese: <https://cloud.acronis.com>.
2. Přihlaste se pomocí účtu.
3. Na kartě **Zdroje** klikněte na položku **Přidat**.
4. Stáhněte si aplikaci Acronis Cyber Protect Home Office a nainstalujte ji.
5. Spusťte aplikaci Acronis Cyber Protect Home Office a přihlaste se ke stejnému účtu Acronis.

## 8.3 Vzdálené zálohování dat

S webovou aplikací Online kontrolní panel můžete nakonfigurovat a spustit zálohování na jakémkoli počítači (PC či Mac) se stejným účtem.

### ***Před zálohováním se ujistěte, že máte přístup k počítači***

1. Otevřete aplikaci Online kontrolní panel na adrese: <https://cloud.acronis.com>.
2. Přihlaste se pomocí účtu.
3. Na kartě **Zdroje** vyhledejte počítač, který chcete zálohovat.
  - Nedaří-li se vám počítač najít, je třeba jej nejprve přidat na seznam. Nainstalujte do počítače aplikaci Acronis Cyber Protect Home Office, spusťte ji a poté se přihlaste pomocí svého účtu. Podrobnosti naleznete v tématu [Přidání nového zařízení](#).
  - Je-li počítač offline, ujistěte se, že je zapnutý a připojený k internetu.

### ***Chcete-li v počítači vytvořit první zálohu***

1. Otevřete aplikaci Online kontrolní panel a poté vyhledejte počítač, který obsahuje data, jež chcete zálohovat.
2. Klikněte na možnost **Povolit zálohu** a poté nakonfigurujte nastavení nové zálohy, včetně následujících položek:
  - Typ zálohy (celý počítač, na úrovni disku nebo na úrovni souborů)
  - Data k zálohování
  - Cíl zálohy
  - Plán
  - Pravidla zachování
  - Šifrování dat
3. Po nakonfigurování zálohy klikněte na tlačítko **Použít** a poté **Spustit**.

### ***Chcete-li vytvořit novou verzi existující zálohy***

1. Otevřete aplikaci Online kontrolní panel a poté vyhledejte počítač, který obsahuje data, jež chcete zálohovat.
2. Klikněte na tlačítko **Zálohovat nyní** a poté vyberte zálohu, kterou chcete aktualizovat.

### ***Chcete-li změnit nastavení existující zálohy***

1. Otevřete aplikaci Online kontrolní panel a poté vyhledejte počítač, který je zdrojem zálohy.
2. Klikněte na ikonu ozubeného kolečka a položku **Záloha** a poté vyhledejte zálohu, u níž chcete změnit konfiguraci.
3. Klikněte na ikonu ozubeného kolečka vedle názvu zálohy a poté klikněte na jednu z následujících položek:
  - Chcete-li změnit hlavní nastavení, klikněte na položku **Upravit**.
  - Chcete-li změnit další možnosti, klikněte na položku **Možnosti zálohy**.
4. Klikněte na tlačítko **Uložit změny**.

#### ***Chcete-li vytvořit novou zálohu***

1. Otevřete aplikaci Online kontrolní panel a poté vyhledejte počítač, který obsahuje data, jež chcete zálohovat.
2. Klikněte na ikonu ozubeného kolečka a položku **Záloha**.
3. Klikněte na položku **Přidat plán zálohování**.
  - Chcete-li vytvořit zálohu s předdefinovaným nastavením, klikněte na tlačítko **Použít**. Celý počítač se zálohuje do úložiště Acronis Cloud.
  - Chcete-li vytvořit zálohu s vlastním nastavením, klikněte na položku **Vytvořit novou**, změňte nastavení a poté klikněte na tlačítko **Použít**.
4. Chcete-li spustit zálohování, klikněte na tlačítko **Spustit**.

## 8.4 Obnova dat pomocí aplikace Online kontrolní panel

Webová aplikace Online kontrolní panel umožňuje obnovovat data z jakékoli online zálohy nahrané z rodinných zařízení včetně počítačů PC a Mac, chytrých telefonů a tabletů.

#### ***Chcete-li obnovit data z online zálohy***

1. Otevřete aplikaci Online kontrolní panel na adrese: <https://cloud.acronis.com>.
2. Přihlaste se pomocí účtu.
3. Na kartě **Zdroje** najděte zařízení, které je zdrojem dat, jež chcete obnovit. Je-li zařízení offline, ujistěte se, že je zapnuté a připojené k internetu.
4. Obnovujete-li data:
  - Z počítače – klikněte na položku **Obnovit**. Otevře se webová aplikace Acronis Cloud, v níž můžete procházet a obnovit svá data. Další informace naleznete v části Obnovení dat z online záloh.
  - Z mobilního zařízení – klikněte na položku **Obnovit**. V levém panelu vyberte verzi zálohy podle data a času zálohování. Poté v pravém panelu vyberte položky, které chcete obnovit, a klikněte na možnost **Stáhnout**.



## 8.5 E-mailová oznámení

Operace zálohování může někdy trvat dlouhou dobu. Chcete-li sledovat stav záloh a dostávat informace o jejich dokončení, můžete si na online kontrolním panelu nakonfigurovat e-mailová oznámení.

### ***Jak konfigurovat e-mailová oznámení***

1. Na online kontrolním panelu otevřete nabídku E-mailová oznámení. To lze provést dvěma způsoby:
  - Na online kontrolním panelu klikněte na ikonu účtu v pravém horním rohu a zvolte položku **E-mailová oznámení**.
  - V aplikaci Acronis Cyber Protect Home Office klikněte na možnost **Nastavení** a poté na položku **Změnit nastavení e-mailových oznámení**.
2. V části **Posílat e-mailová oznámení o** zvolte informace, které vás zajímají:
  - Chyby
  - Upozornění
  - Úspěšné zálohy
3. Do textového pole **E-mailové adresy příjemců** zadejte cílovou e-mailovou adresu. Je možné zadat více adres oddělených středníky.
4. [Volitelný krok] V poli **Předmět** změňte předmět e-mailového oznámení.  
Můžete použít následující proměnné:
  - [computer\_name] – název počítače
  - [operation\_status] – stav, při kterém byla operace dokončena
  - [backup\_name] – název zálohyVýchozí předmět je [computer\_name] – [operation\_status] – [backup\_name].

Po uložení nastavení budete ze serverů Acronis dostávat informace o všech zálohách ve všech rodinných zařízeních s operačním systémem Windows nebo macOS.

## 9 Ochrana

Acronis Cyber Protect Home Office poskytuje následující ochranu vašich dat:

- Služba Active Protection je nepřetržitě spuštěna na pozadí a chrání počítač v reálném čase, zatímco vy pracujete jako obvykle.
- Antivirové kontroly se spouští na vyžádání a provádějí hloubkové vyhledávání škodlivého softwaru v celém systému.
- Vyhodnocování bezpečnostních rizik je každodenní kontrola spouštěná na pozadí, která odhaluje bezpečnostní rizika ve vašem systému a aplikacích a následně vyhodnocuje jejich závažnost.

---

### Poznámka

Ochranu můžete zapínat a vypínat pouze v uživatelském rozhraní aplikace Acronis Cyber Protect Home Office. Proces nemůžete ukončit ručně prostřednictvím správce úloh ani jiného externího nástroje.

---

### 9.1 Kontrolní panel ochrany

Kontrolní panel ochrany obsahuje statistické údaje o procesech služby **Active protection**, **antivirové ochrany** a **vyhodnocení bezpečnostních rizik**, poskytuje kontrolu nad stavem ochrany a přístup k jejím nastavením.

Chcete-li získat přístup ke kontrolnímu panelu ochrany, klikněte na možnost **Ochrana** na bočním panelu aplikace Acronis Cyber Protect Home Office.

Na kartě **Přehled** v kontrolním panelu můžete:

- Zobrazit statistiku o stavu služby Active Protection.
- Zobrazit počet detekovaných problémů, položek v karanténě a výjimek z ochrany.
- Zobrazit nejnovější zprávu z **antivirové kontroly**. Chcete-li si tuto položku zobrazit, klikněte na **Zpráva o kontrole**.
- Zobrazit čas další naplánované kontroly.
- Ručně spustit úplnou nebo rychlou **antivirovou kontrolu**. Provedete to kliknutím na tlačítko **Spustit úplnou kontrolu** nebo **Spustit rychlou kontrolu**.
- Zobrazit nejnovější zprávu se zjištěnými bezpečnostními riziky a spustit z ní novou kontrolu. Chcete-li si tuto položku zobrazit, klikněte na **Zjištěná bezpečnostní rizika**.
- Zastavit celou ochranu na předem definované období (30 minut, 1 hodinu, 4 hodiny, do restartování). Provedete to kliknutím na tlačítko **Vypnout ochranu** a výběrem období.

---

### Poznámka

Vypnutím ochrany deaktivujete službu Active Protection. Naplánované kontroly na vyžádání se nespustí.

---

Na kartě **Aktivita** v kontrolním panelu můžete zobrazit protokol změn, které jste použili na stav a nastavení ochrany.

## 9.2 Active protection

Aby mohla aplikace Acronis Cyber Protect Home Office chránit váš počítač před škodlivým softwarem v reálném čase, využívá technologii Acronis Active Protection.

Služba Active Protection nepřetržitě kontroluje počítač, zatímco vy můžete pracovat jako obvykle. Kromě vašich souborů služba Acronis Active Protection chrání soubory aplikace Acronis Cyber Protect Home Office, vaše zálohy a hlavní spouštěcí záznamy pevných disků.

Služba Active Protection se skládá z několika úrovní ochrany, které se aktivují nezávisle na sobě:

- Ochrana proti ransomwaru
- Ochrana v reálném čase
- Webové filtrování

### 9.2.1 Ochrana proti ransomwaru

Ransomware šifruje soubory a výměnou za šifrovací klíč vyžaduje výkupné. Malware těžící kryptoměnu provádí na pozadí matematické výpočty, čímž snižuje výpočetní výkon a síťový provoz vašeho počítače.

Když je služba **ochrany proti ransomwaru** zapnutá, sleduje procesy spuštěné v počítači v reálném čase. Když zjistí proces třetí strany, který se pokusí zašifrovat vaše soubory nebo těžít kryptoměnu, služba vás o tom informuje a zeptá se, zda chcete procesu povolit pokračovat nebo jej zablokovat.

Chcete-li procesu povolit pokračování v aktivitě, klikněte na položku **Důvěřovat**. Pokud si nejste jisti, zda je proces bezpečný a legální, doporučujeme kliknout na položku **Karanténa**. Poté bude proces umístěn do **karantény** a jakákoli další aktivita tohoto procesu bude zablokována.

Po zablokování procesu doporučujeme zkontrolovat, zda nebyly vaše soubory jakýmkoli způsobem šifrovány nebo poškozeny. Pokud k tomu došlo, klikněte na položku **Obnovit upravené soubory**. Aplikace Acronis Cyber Protect Home Office prohledá následující oblasti a pokusí se najít nejnovější verze souborů k obnovení.

- Kopii dočasného souboru, které byly předběžně vytvořeny během procesu ověřování
- Místní zálohy
- Zálohy v cloudu

Jestliže aplikace Acronis Cyber Protect Home Office najde kvalitní dočasnou kopii, obnoví soubor z této kopie. Pokud dočasné kopie souboru nejsou pro obnovu vhodné, Acronis Cyber Protect Home Office vyhledá místní a cloudové záložní kopie, porovná data vytvoření kopií v obou umístěních a obnoví soubor z nejnovější dostupné, nepoškozené kopie.

---

## Poznámka

Acronis Cyber Protect Home Office nepodporuje obnovení souborů ze záloh chráněných heslem.

---

Chcete-li aplikaci Acronis Cyber Protect Home Office nakonfigurovat, aby soubory po zablokování procesu automaticky obnovila, v nastavení služby Active Protection zaškrtněte políčko **Automaticky obnovit soubory po zablokování procesu**. Viz téma [Konfigurace služby Active Protection](#).

## 9.2.2 Ochrana v reálném čase

Když je **ochrana v reálném čase** zapnutá, nepřetržitě kontroluje soubory, se kterými pracujete, s cílem ochránit počítač před podezřelou aktivitou, viry a dalšími nebezpečími v reálném čase.

Ochrana v reálném čase se dodává s následujícími doplňujícími možnostmi ochrany:

- Behaviorální analýza – služba Active Protection používá funkci behaviorální heuristiky k identifikaci škodlivých procesů. Porovnává řetězec akcí prováděných procesem s řetězcem událostí zaznamenaných v databázi vzorů škodlivého chování. Tento přístup umožňuje službě Active Protection detekovat nový malware na základě jeho typického chování.
- Ochrana před bezpečnostními dírami – služba Active Protection analyzuje chování procesů spuštěných na počítači a detekuje neobvyklou činnost. Brání infikovaným procesům v šíření a využívání zranitelností dalšího softwaru instalovaného v systému. Služba Active Protection používání několik způsobů ochrany před bezpečnostními dírami:
  - Ochrana paměti detekuje a omezuje oprávnění podezřelých modifikací ke spouštění aplikací v paměťových stránkách. Škodlivé procesy aplikují takové modifikace na vlastnosti stránky a umožňují tak spouštění kódů prostředí z nespustitelných oblastí paměti, jako jsou zásobníky a haldy.
  - Ochrana před eskalací oprávnění detekuje a brání pokusům o rozšíření oprávnění prováděným neautorizovaným kódem nebo aplikací. Eskalace oprávnění je používána škodlivým kódem k získání úplného přístupu k napadenému počítači a pak k provedení citlivých a kritických úkolů. Neautorizovanému kódu není povoleno přistupovat ke kritickým systémovým zdrojům, ani modifikovat nastavení systému.
  - Ochrana před injekcí kódu detekuje a brání škodlivé injekcí kódu do vzdálených procesů. Injektáž kódu se používá ke skrytí škodlivých záměrů aplikace mezi běžné či nečinné procesy, aby se tak vyhnula zjištění produkty na ochranu proti malwaru.

Můžete si vybrat jeden z následujících typů kontroly:

- Zjišťování pomocí funkce **Inteligentně při přístupu** znamená, že program pracuje na pozadí a aktivně a nepřetržitě prohledává počítačový systém na přítomnost virů a jiných škodlivých hrozeb po celou dobu, po kterou je systém zapnutý. Malware bude detekován v obou případech. Jak při zpracování souboru, tak při různých operacích se souborem, například při jeho otevření ke čtení/úpravám.
- Zjišťování pomocí funkce **Při spuštění** znamená, že spustitelné soubory budou kontrolovány pouze v okamžiku jejich spuštění, aby bylo zajištěno, že jsou v pořádku a nezpůsobí žádné poškození vašeho počítače nebo dat. Kopírování infikovaného souboru zůstane bez povšimnutí.

Výsledky kontrol v reálném čase můžete zobrazit na kartě **Aktivita** na kontrolním panelu Ochrana.

### 9.2.3 Webové filtrování

Malware se často šíří prostřednictvím škodlivých nebo napadených webů a používá metodu infekce zvanou „Drive-by download“ (instalace softwaru bez vědomí uživatele).

Webové filtrování vás pomáhá chránit před potenciálně škodlivými webovými stránkami a nedůvěryhodnými webovými zdroji tím, že blokuje přístup, když se je pokusíte otevřít. Webové filtrování určuje, které webové stránky jsou potenciálně škodlivé, pomocí databáze aktualizací ochrany. Databáze webového filtrování rovněž zahrnuje informace o webových stránkách, které obsahují podvody a phishingové adresy URL. Pravidla definovaná v databázi můžete upravit pomocí konfigurace výjimek ze seznamu webového filtrování.

Webové filtrování má dva režimy provozu:

- **Kompletní zablokování**– přístup na webové stránky bude kompletně zablokován.
- **Pouze oznámení**– zobrazí se oznámení, avšak uživatelé budou moci na webové stránky přejít.

### 9.2.4 Konfigurace služby Active Protection

Chcete-li získat přístup k nastavení služby Active Protection, na postranním panelu klikněte na tlačítko **Ochrana**, poté na možnost **Nastavení** a přejděte na kartu **Active Protection**.

#### ***Jak konfigurovat službu Ochrana proti ransomwaru:***

1. Zapnutím přepínače **Ochrana proti ransomwaru** aktivujete ochranu proti ransomwaru. Po zapnutí chrání váš počítač před potenciálně škodlivými aplikacemi a procesy, které běží na pozadí.
2. Vyberte možnosti, které chcete povolit.
  - **Automatické obnovení souborů po zablokování procesu**– I když byl proces zablokován, stále existuje možnost, že vaše soubory byly upraveny. Pokud je toto políčko zaškrtnuto, aplikace Acronis Cyber Protect Home Office následujícím způsobem soubory obnoví. Acronis Cyber Protect Home Office prohledá následující oblasti a pokusí se najít nejnovější verze souborů k obnovení.
    - Kopii dočasného souboru, které byly předběžně vytvořeny během procesu ověřování
    - Místní zálohy
    - Zálohy v cloudu

Jestliže aplikace Acronis Cyber Protect Home Office najde kvalitní dočasnou kopii, obnoví soubor z této kopie. Pokud dočasné kopie souboru nejsou pro obnovu vhodné, Acronis Cyber Protect Home Office vyhledá místní a cloudové záložní kopie, porovná data vytvoření kopií v obou umístěních a obnoví soubor z nejnovější dostupné, nezměněné kopie.

---

### Poznámka

Acronis Cyber Protect Home Office nepodporuje obnovení souborů ze záloh chráněných heslem.

---

- **Chránit soubory zálohy před ransomwarem** – aplikace Acronis Cyber Protect Home Office ochrání vlastní procesy a vaše zálohy před ransomwarem. Vaše archivy jsou také chráněny.
  - **Chránit sdílené síťové složky a zařízení NAS** – Acronis Cyber Protect Home Office bude monitorovat a chránit síťové složky a zařízení NAS, ke kterým máte přístup. Můžete rovněž zadat umístění obnovy pro soubory postižené útokem ransomwaru.
  - **Chránit počítač před nelegální těžbou kryptoměn** – Toto políčko zaškrtněte, pokud počítač chcete chránit před malwarem pro těžbu kryptoměn.
3. Klikněte na tlačítko **OK**.

### **Konfigurace ochrany v reálném čase:**

1. Zapnutím přepínače **Ochrana v reálném čase** aktivujete ochranu v reálném čase. Ochrana v reálném čase po zapnutí u všech souborů, se kterými pracujete, kontroluje, zda neobsahují malware.
2. Zvolte, kdy se soubory mají kontrolovat.
  - **Inteligentně při přístupu** – monitorují se všechny aktivity systému a soubory se kontrolují, jakmile k nim přistoupíte.
  - **Při spuštění** – kontrolují se pouze spustitelné soubory při jejich spuštění s cílem zajistit, aby nepoškodily váš počítač.
3. Z rozbalovacího seznamu vyberte, co se provede s odstraněnými objekty.
  - **Zablokování a oznámení** – proces s podezřením na škodlivou aktivitu bude zablokován a vy obdržíte oznámení.
  - **Karanténa** – proces s podezřením na škodlivou aktivitu bude zablokován a soubor bude přesunut do složky karantény.
4. Povolte další možnosti ochrany.
  - **Detekce škodlivého chování v procesech** – umožňuje službě Active Protection detekovat nový malware na základě jeho typického chování a blokovat jej.
  - **Zjištění škodlivých procesů a zabránění jejich zneužití v systému (experimentální funkce)** – umožňuje službě Active Protection detekovat a blokovat procesy, které se snaží využít chyby a zranitelnosti jiných procesů v systému.

---

### Poznámka

Všechny zjištěné objekty jsou okamžitě zablokovány. Nebudou přesunuty do karantény ani přidány do seznamu zjištěných problémů.

---

### **Konfigurace webového filtrování:**

1. Chcete-li získat ochranu pro potenciálně škodlivým webovým stránkám a nedůvěryhodným webovým zdrojů, zapněte **filtrování webů**.

2. V rozevírací nabídce **Akce při detekci škodlivé adresy URL** vyberte akce, které se provedou při zjištění škodlivých adres URL.
  - **Kompletní zablokování**– přístup na webové stránky bude kompletně zablokován.
  - **Blokovat a upozorňovat**– webové stránky budou zablokovány s možností na ně přejít.
3. Chcete-li nakonfigurovat seznam důvěryhodných nebo blokových webových stránek, klikněte na možnost **Spravovat výjimky**.
  - a. Adresu URL přidáte do seznamu kliknutím na tlačítko **Přidat URL**.
  - b. Zadejte platný název adresy URL. Její doména se přidá do výjimek.

---

#### **Poznámka**

Se všemi adresami ze zadané domény bude zacházeno jako s důvěryhodnými nebo blokovánými. Pokud například zadáte xyz.com jako důvěryhodnou doménu, všechny cesty a dílčí domény v doméně xyz.com budou považovány za důvěryhodné.

---

- c. V rozevírací nabídce zvolte možnost **Povoleno** nebo **Blokováno**. Na povolených webových stránkách se nebudou provádět kontroly za účelem odhalení hrozeb. Blokové webové stránky se neotevřou nebo při pokusu o jejich otevření obdržíte oznámení.
- d. Klikněte na tlačítko **Přidat URL**.
- e. Klikněte na tlačítko **Použít**.

## 9.3 Antivirové kontroly

**Antivirová kontrola** je jednou ze součástí ochrany proti virům a malwaru aplikace Acronis Cyber Protect Home Office. Chrání váš počítač tím, že na vyžádání provádí kontrolu výskytu malwaru – ručně nebo v předem definovaných intervalech, které můžete nakonfigurovat.

Můžete si vybrat ze dvou typů kontroly.

- **Úplná** kontrola bude vyhledávat viry v celém počítači. Při úplné kontrole se malware vyhledává kontrolou všech souborů a procesů (nebo podmnožiny souborů a procesů), kromě vyloučených souborů a složek, které jste nadefinovali v seznamu vyloučených položek.
- **Rychlá** kontrola kontroluje pouze konkrétní soubory a složky. Při rychlé kontrole se malware vyhledává kontrolou konkrétních složek, které se považují za nejpravděpodobnější zdroj virů.

Můžete si také vybrat, co se bude kontrolovat: archivované soubory, externí disky nebo pouze nové a změněné soubory.

---

#### **Poznámka**

Acronis Cyber Protect Home Office je nakonfigurována tak, aby zabránila spuštění režimu spánku, pokud probíhá kontrola.

---

Pokud je vytížení procesoru vysoké, ve výchozím nastavení se sníží priorita antivirových kontrol, aby ostatní aplikace mohly fungovat správně. Tím se kontrola zpomalí. Deaktivací této možnosti můžete kontroly urychlit.

Pokud chcete zobrazit okno **Podrobná zpráva o kontrole** uvádějící podrobnosti o antivirové kontrole, klikněte na tlačítko **Zpráva o kontrole**.

## 9.3.1 Konfigurace antivirových kontrol

### Nastavení antiviru

Zde můžete nakonfigurovat hlavní funkce **antiviru**. Můžete například zvolit **akci při detekci**, definovat **typ kontroly**, nastavit **plán**, vybrat, co se bude kontrolovat atd.

Chcete-li získat přístup k nastavení **antiviru**, na postranním panelu klikněte na tlačítko **Ochrana**, poté na možnost **Nastavení** a přejděte na kartu **Antivirus**.

#### **Postup konfigurace akce při detekci:**

Vyberte možnosti, které chcete povolit.

- **Karanténa** – tato volba je nastavena implicitně. Když aplikace Acronis Cyber Protect Home Office detekuje potenciální malwarovou hrozbu, zastaví proces a podezřelý soubor přesune do složky karantény.
- **Pouze oznámení**– když je detekován podezřelý proces, obdržíte oznámení o potenciální malwarové hrozbě.

#### **Postup konfigurace typu kontroly:**

Vyberte typ kontroly, kterou chcete provést:

- **Úplná** – Tato volba je nastavena implicitně. Aplikace Acronis Cyber Protect Home Office zkontroluje celý počítač.
- **Rychlá** – Aplikace Acronis Cyber Protect Home Office zkontroluje pouze konkrétní složky, které jsou považovány za nejpravděpodobnější zdroj hrozeb.

#### **Postup naplánování antivirových kontrol:**

Zaškrtnutím jednoho z políček nakonfigurujete dobu, kdy se má proces kontroly zahájit.

- **Denně**– kontrola se bude spouštět každý den v zadanou dobu.
- **Týdně**– kontrola se bude spouštět v určitý den v týdnu. Nastavte den v týdnu a čas.
- **Měsíčně**– kontrola se bude spouštět v určitý den v měsíci.
- **Při spuštění systému**– kontrola proběhne při každém spuštění systému.
- **Neplánovat**– kontrola se nebude spouštět v plánovanou konkrétní dobu.

#### **Postup konfigurace cílů kontroly:**

Zaškrtněte následující políčka:

- **Neskenujte archivy o velikosti větší než**. Pomocí šipek vyberte hodnotu.
- **Kontrolovat externí disky**



- **Kontrolovat sdílené síťové složky a zařízení NAS**
- **Pouze kontrola nových a změněných souborů**

**Konfigurace chování systému během antivirových kontrol:**

Někdy před dokončením antivirové kontroly může dojít k vypnutí systému. Pro takové případy zaškrtnutím políčka **Při spuštění spustit zmeškané úlohy** nakonfigurujte aplikaci Acronis Cyber Protect Home Office tak, aby po opětovném spuštění systému kontrolu obnovila.

Kromě toho můžete povolit možnost **Zabránit režimu hibernace nebo spánku**, která zabrání vypnutí počítače, pokud probíhá kontrola.

Prioritu antivirových kontrol lze v případě přetížení procesoru snížit, aby ostatní aplikace mohly fungovat správně. Tato možnost je ve výchozím nastavení zapnuta, což může kontrolu zpomalit. Chcete-li kontroly urychlit, zrušte zaškrtnutí políčka **Upřednostnit ostatní aplikace**.

Po nakonfigurování antivirové kontroly klikněte na tlačítko **OK**.

## 9.4 Vyhodnocení bezpečnostních rizik

Vyhodnocení bezpečnostních rizik je jednou ze součástí ochrany proti virům a malwaru aplikace Acronis Cyber Protect Home Office. Je to každodenní kontrola spouštěná na pozadí, která odhaluje bezpečnostní rizika ve vašem systému a aplikacích a následně vyhodnocuje jejich závažnost. Kontrolu lze v případě potřeby také spustit ručně.

---

### Poznámka

Aktualizace databáze bezpečnostních rizik vyžaduje stabilní internetové připojení.

---

### Postup zobrazení bezpečnostních rizik:

1. Na levém bočním panelu klikněte na možnost **OCHRANA**.
2. Na kartě **Přehled** v části **Vyhodnocení bezpečnostních rizik** klikněte na možnost **Zjištěná bezpečnostní rizika**. Zobrazí se zpráva.
3. Chcete-li spustit novou kontrolu, klikněte na tlačítko **Spustit kontrolu**.
4. [Volitelné] Chcete-li zobrazit okno **Podrobné informace**, klikněte na ikonu vedle názvu bezpečnostního rizika.
5. [Volitelné] Chcete-li zobrazit podrobný popis bezpečnostního rizika, klikněte na šipku vedle jeho názvu. Zobrazí se webová stránka, na které jsou tyto informace zobrazeny.
6. Chcete-li vyřešit zjištěné problémy, nainstalujte nejnovější aktualizace zasažených aplikací. Následně znovu proveďte kontrolu, abyste se ujistili, že bezpečnostní rizika byla opravena. Pokud problémy přetrvávají, znamená to, že některé aplikace i nadále mohou vystavit váš systém riziku. Za účelem úplné ochrany dat vytvořte zálohu operačního systému a zapněte ochranu proti malwaru.

### Postup konfigurace vyhodnocení bezpečnostních rizik:

1. Na levém bočním panelu klikněte na možnost **OCHRANA** a poté **Nastavení**.
2. Přejděte na kartu **Vyhodnocení bezpečnostních rizik** a zapnutím nebo vypnutím přepínače aktivujte nebo deaktivujte kontrolu bezpečnostních rizik.

## 9.5 Správa zjištěných problémů

Seznam zjištěných problémů se vyplní, pokud je v antivirové kontrole nakonfigurována akce při detekci na možnost **Zablokování a oznámení**: Seznam byste si měli prostudovat a rozhodnout, zda budete položkám důvěřovat nebo je přesunete do karantény.

### **Kontrola a správa zjištěných problémů:**

1. Na kontrolním panelu **Ochrana** klikněte na položku **Zjištěné problémy**.
2. Zaškrtněte políčko u problému v seznamu a zvolte, jak se má zpracovat.
  - Chcete-li soubor nebo proces přidat na seznam výjimek z ochrany, klikněte na položku **Důvěřovat**.

---

#### **Poznámka**

Pokud se rozhodnete souboru nebo procesu důvěřovat, bude z budoucích antivirových kontrol vyloučen.

---

- Chcete-li soubor nebo proces přesunout do karantény, klikněte na položku **Karanténa**.
3. Klikněte na tlačítko **Close** (Zavřít).

Detekované problémy můžete řešit také kliknutím na panel **Ochrana** na postranním panelu Acronis Cyber Protect Home Office a potom na **Nastavení**. Potom přejděte na kartu **Pokročilé**. V části **Detekované problémy** klikněte na **Spravovat**.

## 9.6 Správa souborů v karanténě

Na základě vašeho nastavení mohou služba Active Protection a antivirové kontroly přesunout zablokované soubory do karantény. Karanténa je zvláštní úložiště sloužící k izolování napadených a podezřelých souborů, kterým byl zablokován přístup k vašemu počítači a datům. Umístíte-li soubor aplikace do karantény, minimalizujete tím riziko, že by zablokovaná aplikace prováděla potenciálně škodlivé činnosti.

Ve výchozím nastavení jsou soubory v karanténě uchovány 30 dní a poté se z počítače odstraní. Soubory v karanténě můžete před uplynutím této doby zkontrolovat a rozhodnout se, zda si je ponecháte nebo odstraníte. Výchozí období uchování souborů v karanténě lze také změnit.

### **Obnova nebo odstranění souborů z karantény:**

1. Na kontrolním panelu **Ochrana** klikněte na položku **Karanténa**.
2. V seznamu karantény zvolte položku.

- Chcete-li ji vrátit do původního umístění, klikněte na možnost **Obnovit**.
  - Chcete-li ji odstranit, klikněte na příkaz **Odstranit z počítače**.
3. Klikněte na tlačítko **Close** (Zavřít).

#### ***Nastavení období pro automatické odstranění souborů z karantény:***

1. Na panelu **Ochrana** klikněte na možnost **Nastavení** a poté na kartu **Rozšířené**.
2. V části **Karanténa** vyberte počet dní, po který se položky uchovávají v karanténě.
3. Klikněte na tlačítko **OK**.

## 9.7 Konfigurace výjimek z ochrany

Služba Active Protection a antivirové kontroly používají k určení potenciálních nebezpečí databázi ochrany. Pokud některým spustitelným souborům a složkám důvěřujete, můžete je přidat na seznam výjimek z ochrany, aby je aplikace Acronis Cyber Protect Home Office během kontroly přeskočila.

#### ***Přidání souboru nebo složky na seznam výjimek z ochrany***

1. Na kontrolním panelu **Ochrana** klikněte na možnost **Výjimky z ochrany**.
2. V nabídce **Přidat výjimku** zvolte, jakou položku chcete vyjmout.
  - **Přidat soubor**– k vyloučení spustitelných nebo jiných souborů z kontroly.
  - **Přidat složku**– k vyloučení složek z kontroly.
3. Vyhledejte položku, kterou chcete vyloučit a klikněte na tlačítko **Otevřít**.
4. Přidejte další položku k vyloučení nebo seznam aktualizujte kliknutím na tlačítko **Uložit**.

#### ***Odebrání souborů nebo složek ze seznamu výjimek z ochrany***

1. Na kontrolním panelu **Ochrana** klikněte na možnost **Výjimky z ochrany**.
2. V seznamu výjimek z ochrany zaškrtněte políčka u položek, které chcete odstranit, a klikněte na tlačítko **Odebrat**.
3. Kliknutím na tlačítko **Uložit** seznam aktualizujte.

Postup konfigurace výjimek z ochrany pro webové filtrování naleznete v části [Konfigurace služby Active Protection](#).

## 9.8 Ochrana pro aplikace Zoom, Cisco Webex a Microsoft Teams

Aplikace Zoom, Cisco Webex Meetings a Microsoft Teams se často využívají pro webové konference a komunikaci. Funkce ochrany před ransomwarem aplikace Acronis Cyber Protect Home Office ve výchozím nastavení tyto aplikace pro spolupráci následujícím způsobem chrání.

- Ochrana procesů aplikace před instalací kódů
- Zamezení škodlivým operacím v procesech aplikace

## 9.9 Stahování aktualizací ochrany

Aplikace Acronis Cyber Protect Home Office stahuje aktualizace ochrany ve výchozím nastavení automaticky. Můžete zkontrolovat stav databází a komponent ochrany nebo deaktivovat automatické stahování aktualizací ochrany.

### ***Postup kontroly stavu aktualizací ochrany:***

1. Na panelu **Ochrana** klikněte na **Nastavení** a poté na možnost **Rozšířené**.
2. Ve spodní části vyhledejte sekci **Aktualizace ochrany**.  
Ve spodní části sekce se zobrazí nejnovější verze databáze a datum stažení.

### ***Postup deaktivace automatického stahování aktualizací ochrany:***

---

#### **Poznámka**

Za účelem zajištění maximální ochrany nedoporučujeme automatické aktualizace ochrany deaktivovat.

---

1. Na panelu **Ochrana** klikněte na **Nastavení** a poté na možnost **Rozšířené**.
2. Ve spodní části vyhledejte sekci **Aktualizace ochrany**.
3. Zrušte zaškrtnutí políčka **Stahovat aktualizace ochrany automaticky**.

### ***Stažení nejnovějších aktualizací ochrany:***

Pokud je automatické stahování aktualizací ochrany deaktivováno, můžete aktualizace zkontrolovat a stáhnout ručně.

1. Na panelu **Ochrana** klikněte na **Nastavení** a poté na možnost **Rozšířené**.
2. Ve spodní části vyhledejte sekci **Aktualizace ochrany**.
3. Klikněte na možnost **Zkontrolovat aktualizace**. Tato možnost je k dispozici, když není zaškrtnuté políčko **Stahovat aktualizace ochrany automaticky**.
4. Pokud aktualizace ochrany nejsou nejnovější, klikněte na příkaz **Aktualizovat**.

# 10 Synchronizace dat

## 10.1 Funkce synchronizace

Hlavní rysy synchronizace:

- Stejná data – dokumenty, fotografie, videa atd. – můžete mít na všech počítačích. Vaše data jsou snadno dosažitelná kdykoli a kdekoli. Už si nemusíte posílat e-maily nebo s sebou všude nosit USB disk.
- Můžete vytvořit tolik synchronizací, kolik bude potřeba.
- Služba Acronis Cloud zachovává synchronizované soubory i verze těchto souborů. Takto se budete moci vrátit k předchozí verzi souboru, kdykoli to bude potřeba.

---

### Poznámka

K používání této funkce je vyžadováno předplatné úložiště Acronis Cloud. Další informace naleznete v části Informace o předplatném.

---

- Do cloudu lze přistupovat také pomocí webového prohlížeče bez nutnosti instalace naší aplikace.
- Pro vytvoření přímé synchronizace mezi dvěma nebo více počítači není nutné předplatné služby Acronis Cloud.

## 10.2 Co lze a nelze synchronizovat

Synchronizovat můžete data uložená ve dvou nebo více složkách. Uvažme, kde tyto složky mohou být umístěny a jaká mohou obsahovat data.

### 10.2.1 Typy úložišť

Proces synchronizace může být vytvořen mezi:

- dvěma nebo více složkami ve dvou nebo více počítačích,
- Jeden nebo několik počítačů a aplikace Acronis Cloud.  
Úložiště Acronis Cloud vždy obsahuje nejnovější verze synchronizovaných souborů. V úložišti Acronis Cloud navíc nelze vybrat složku pro synchronizaci, tato složka se vytvoří automaticky.

V rámci jednoho procesu synchronizace můžete přiřadit pouze jednu synchronizovanou složku v každém počítači.

---

### Poznámka

Pro synchronizaci nemůžete vybrat samostatný soubor. Chcete-li synchronizovat soubor, vyberte pro synchronizaci složku, která soubor obsahuje.

---

### 10.2.2 Typy dat

**Synchronizovat je možné následující data:**

- Soubory (fotografie, hudbu, videa, dokumenty a další), kromě těch uvedených níže.

---

#### **Poznámka**

Synchronizovány jsou pouze původní atributy souborů systémů FAT32 a NTFS. Pokud synchronizované složky náleží různým systémům souborů, aplikace synchronizuje pouze atributy podporované oběma systémy.

---

- Další složky uvnitř synchronizované složky (tedy synchronizované podložky) a jejich obsah.

#### **Není možné synchronizovat následující data:**

- Disky a diskové oddíly
- Systémové soubory a složky
- Skryté soubory a složky
- dočasné soubory a složky,
- registr systému,
- Databáze
- data e-mailových aplikací (včetně aplikace Microsoft Outlook a dalších),
- další data, která nelze zobrazit jako samostatné soubory nebo složky (například kontakty v adresáři),
- Knihovny systému Windows (dokumenty, hudbu apod.)




## 10.3 Ikony synchronizace

Při práci se synchronizací se setkáte se speciálními ikonami. Ikony nabízejí následující informace:

- Typ a aktuální stav synchronizace (ikony se zobrazují v oznamovací oblasti)
- Aktuální stav synchronizovaných souborů a složek (ikony se zobrazují v Průzkumníku souborů).




### 10.3.1 Oznamovací oblast

Ikony stavu synchronizace:



<b>Ikona</b>	<b>Popis</b>
	Synchronizace pracuje v normálním režimu.
	Synchronizace byla pozastavena.
	Během poslední synchronizace se vyskytla chyba.

### 10.3.2 Průzkumník souborů

Ikony stavu synchronizace souborů a složek:

Ikona	Popis
	Soubor nebo složka jsou synchronizovány.
	Synchronizace souboru nebo složky momentálně probíhá.
	Soubor nebo složka nebyly synchronizovány z důvodu chyby.

Ikony typu synchronizace pro synchronizované složky:

Ikona	Popis
	Synchronizace s úložištěm Acronis Cloud.
	Synchronizace mezi počítači synchronizovanými pomocí místní sítě.

## 10.4 Vytvoření synchronizace

Než začnete s vytvářením nové synchronizace, ujistěte se, že jsou splněny následující podmínky:

- Máte Acronis účet.
- Pokud plánujete zahrnout cloud Acronis Cloud do své synchronizace, musíte mít předplatné úložiště Acronis Cloud. Další informace naleznete v části "Informace o předplatném" (str. 34).
- V každém počítači je nainstalována aplikace Acronis Cyber Protect Home Office nebo Acronis True Image (2012 či pozdější).
- Pokud jsou vaše počítače propojeny místní sítí, zkontrolujte, že je toto místní propojení navázáno.
- Každý počítač je připojen k internetu.

### **Synchronizace souborů a složek**

1. Na bočním panelu klikněte na možnost **Synchronizace**.
2. Nejste-li ještě přihlášení, zadejte přihlašovací údaje k účtu Acronis.
3. Klikněte na tlačítko **Přidat synchronizaci**.
4. Rozhodněte se, zda chcete zahrnout úložiště Acronis Cloud do své nové synchronizace a pak vyberte odpovídající typ synchronizace.
5. Vyberte složku, kterou chcete synchronizovat a pak klikněte na tlačítko **OK**.
6. Chcete-li se připojit k této synchronizaci, spusťte aplikaci Acronis Cyber Protect Home Office v ostatních počítačích, v části Synchronizace vyberte tuto synchronizaci, klikněte na tlačítko **Připojit k synchronizaci** a vyberte složku, kterou chcete synchronizovat.

## 10.5 Nastavte ukládání verzí v online úložišti.

Aplikace Acronis Cyber Protect Home Office nabízí možnost vrátit změny provedené v souborech následkem synchronizace. Pokud zjistíte, že jeden ze souborů obsahuje nežádoucí změnu, můžete zobrazit předchozí verze tohoto souboru a potom se vrátit ke správné verzi. Další informace naleznete v tématu [Návrat k předchozí verzi](#).

Všechny verze uložené v úložišti služby Acronis Cloud, která je dostupná přes internet. Chcete-li používat úložiště služby Acronis Cloud, je nutné mít službu Acronis Cloud předplacenou. Další informace naleznete v tématu [Informace o předplatném](#).

Chcete-li odstranit zastaralé verze, spusťte ve webové aplikaci služby Acronis Cloud operaci vyčištění. Další informace naleznete v části [Jak uvolnit místo v úložišti Acronis Cloud](#).

---

### Upozornění!

Pokud používáte zkušební verzi aplikace Acronis Cyber Protect Home Office, všechny uložené verze včetně posledních se po vypršení zkušebního období z úložiště Cloud odstraní.

---

### 10.5.1 Návrat k předchozí verzi souboru

Pokud ukládáte historii synchronizace do služby Acronis Cloud, můžete aktuální verzi synchronizovaného souboru vrátit na předcházející verzi. To je užitečné, pokud chcete vrátit nežádoucí operaci synchronizace.

#### ***Jak se vrátit k předchozí verzi souboru***

1. V části **Synchronizace** vyhledejte pole synchronizace s potřebným souborem. Poté klikněte na odkaz **Acronis Cloud**.
2. Po otevření seznamu synchronizovaných položek ve vašem webovém prohlížeči vyberte soubor, který chcete vrátit do předchozí verze. Poté klikněte na ikonku ozubeného kola vpravo. V nabídce vyberte položku **Zobrazit verze**.
3. Vyberte verzi, ke které se chcete vrátit. Zobrazí se přesné datum a čas dané verze. Aktuální verze se vrátí do stavu, ve kterém byla v tomto bodě a čase.
4. Pokračujte kliknutím na tlačítko **Obnovit**. Vybraná verze se stane nejnovější verzí v úložišti Cloud. Poté bude stažena do počítače, který synchronizaci vlastní.

## 10.6 Jak obnovit smazaný soubor

Někdy se může stát, že omylem odstraníte soubor ze synchronizace. Potom potřebujete soubor obnovit. To je možné provést u synchronizací, které uchovávají verze souborů v úložišti Acronis Cloud.

smazaný soubor nesmí být odstraněn během čištění úložiště Cloud.

Jak obnovit smazaný soubor:



1. Spustit Acronis Cyber Protect Home Office
2. Na bočním panelu klikněte na možnost **Synchronizace**, vyberte synchronizaci obsahující soubory, které chcete obnovit, a poté klikněte na odkaz **Acronis Cloud**.
3. Klikněte na kartu **Files** a vyberte synchronizaci, ze které byl soubor odstraněn.
4. Jakmile vyberete synchronizaci, zobrazí se seznam souborů a složek.
5. Zaškrtněte políčko **Show deleted** a potom vyberte odstraněný soubor, který chcete obnovit.
6. Kliknutím na tlačítko **Recover** obnovte odstraněný soubor do jeho složky.

## 10.7 Odstranění synchronizace

1. Na bočním panelu klikněte na možnost **Synchronizace**.
2. Nejste-li ještě přihlášení, zadejte přihlašovací údaje k účtu Acronis.
3. Ze seznamu synchronizace vyberte tu, kterou chcete odstranit, klikněte na ikonu šipky a pak klikněte na tlačítko **Odstranit**.

Tato činnost pouze naruší spojení mezi synchronizovanými složkami. Soubory, které byly synchronizovány, zůstanou ve svém umístění a nebudou žádným způsobem upraveny.

# 11 Klonování a migrace disku

Tato operace kopíruje veškerý obsah jednoho pevného disku na jiný. Tento postup může být nutný například v případě, kdy chcete naklonovat operační systém, aplikace a data na nový disk s větší kapacitou. To lze provést dvěma způsoby:

- [Použít nástroj Klonování disků.](#)
- [Provést zálohu starého disku a poté jej obnovit na novém disku.](#)

## 11.1 Nástroj pro klonování disku

Pomocí nástroje pro klonování disku můžete klonovat pevný disk kopírováním diskových oddílů na jiný pevný disk.

Než začnete, přečtěte si následující informace:

- Chcete-li naklonovat systém na pevný disk o vyšší kapacitě, doporučujeme nainstalovat cílový (nový) disk tam, kde jej chcete použít, a zdrojový disk do jiného umístění, například do externího USB úložiště. To je důležité především u přenosných počítačů.

---

### Poznámka

Doporučujeme, aby původní i nový pevný disk pracovaly ve stejném režimu řadiče (například IDE nebo AHCI). Jinak se počítač z nového pevného disku nemusí spustit.

---

---

### Poznámka

Pokud disk se systémem Windows naklonujete na externí pevný disk USB, systém z něj nemusí být možné spustit. Doporučujeme jej naklonovat raději na interní disk SSD nebo HDD.

---

- Nástroj Klonování disku nepodporuje systémy s více možnostmi spuštění.
- V oknech aplikace jsou poškozené diskové oddíly označeny červeným kroužkem s bílým křížkem v levém horním rohu. Před zahájením klonování musíte provést kontrolu těchto disků na výskyt chyb a nalezené chyby opravit pomocí příslušného nástroje operačního systému.
- Z důvodu bezpečnosti důrazně doporučujeme vytvořit zálohu celého původního disku. Tímto způsobem můžete zachránit data, pokud se během klonování původního pevného disku něco přihodí. Informace o vytváření takovéto zálohy naleznete v tématu [Zálohování diskových oddílů a disků](#). Po vytvoření zálohy ji ověřte.

### 11.1.1 Průvodce klonováním disku

Než začnete, doporučujeme vám přečíst si obecné informace o nástroji [Klonování disků](#). Pokud používáte počítač se systémem UEFI BIOS a rozhodnete se začít postup klonování pomocí spouštěcího média, věnujte pozornost režimu zavádění spouštěcího média v systému UEFI BIOS. Doporučuje se, aby režim zavádění odpovídal typu systému v záloze. Pokud záloha obsahuje systém BIOS, pak zaveďte spouštěcí médium v režimu BIOS; pokud je systém BIOS typu UEFI, zajistěte, aby byl nastaven režim UEFI.

## **Jak klonovat disk**

1. Spustit Acronis Cyber Protect Home Office
2. V bočním panelu klikněte na možnost **Nástroje** a pak na možnost **Klonovat disk**.
3. V kroku **Režim klonování** vyberte režim přenosu.
  - **Automatický**– doporučen ve většině případů.
  - **Ruční**– Ruční režim nabízí uživateli více možností při přenosu dat. Ruční režim může být užitečný, pokud potřebujete změnit rozvržení diskových oddílů.

---

### **Poznámka**

Pokud aplikace najde dva disky, z nichž jeden je rozdělený na diskové oddíly a druhý ne, automaticky rozpozná jako zdrojový disk ten disk, který je rozdělen na diskové oddíly, a nerozdělený disk jako cílový disk. V takovém případě budou další kroky přeskočeny a zobrazí se okno **Souhrn**.

---

4. V kroku **Zdrojový disk** vyberte disk, který chcete klonovat.

---

### **Poznámka**

Aplikace Acronis Cyber Protect Home Office nepodporuje klonování dynamických disků.

---

5. V kroku **Cílový disk** vyberte cílový disk pro klonovaná data.

Pokud vybraný cílový disk obsahuje oddíly, bude nutné potvrdit smazání těchto oddílů. Vezměte na vědomí, že samotné trvalé odstranění dat bude provedeno, pouze pokud kliknete na tlačítko **Pokračovat** v posledním kroku průvodce.

---

### **Poznámka**

Pokud některý z disků neobsahuje žádný diskový oddíl, aplikace jej automaticky rozpozná jako cílový a tento krok přeskočí.

---

6. [Tento krok je dostupný pouze v případě, že je na zdrojovém disku nainstalován operační systém]. V kroku **Využití disku** zvolte, jak se bude klon používat.
  - **Nahradit disk v tomto počítači**—data systémového disku se zkopírují a klon bude fungovat jako spouštěcí. Tento klon použijte při výměně systémového disku za nový v tomto počítači.
  - **Použit na jiném počítači**—data systémového disku se zkopírují a klon bude fungovat jako spouštěcí. Tento klon použijte k přenosu všech dat do jiného počítače na spouštěcím disku.
  - **Použit jako datový disk**—data disku se zkopírují. Použit tento klon jako nespouštěcí datovou jednotku.
7. [Tento krok je dostupný pouze v ručním režimu klonování]. V kroku **Metoda přesouvání** zvolte metodu přesouvání dat.
  - **Zachování**– pro každý původní diskový oddíl bude vytvořen nový stejného typu a velikosti, se stejným systémem souborů a jmenovkou. Nepoužité místo na disku zůstane nepřiděleno.
  - **Proporcionální**– prostor na novém disku bude rozdělen poměrným způsobem mezi

klonované diskové oddíly.

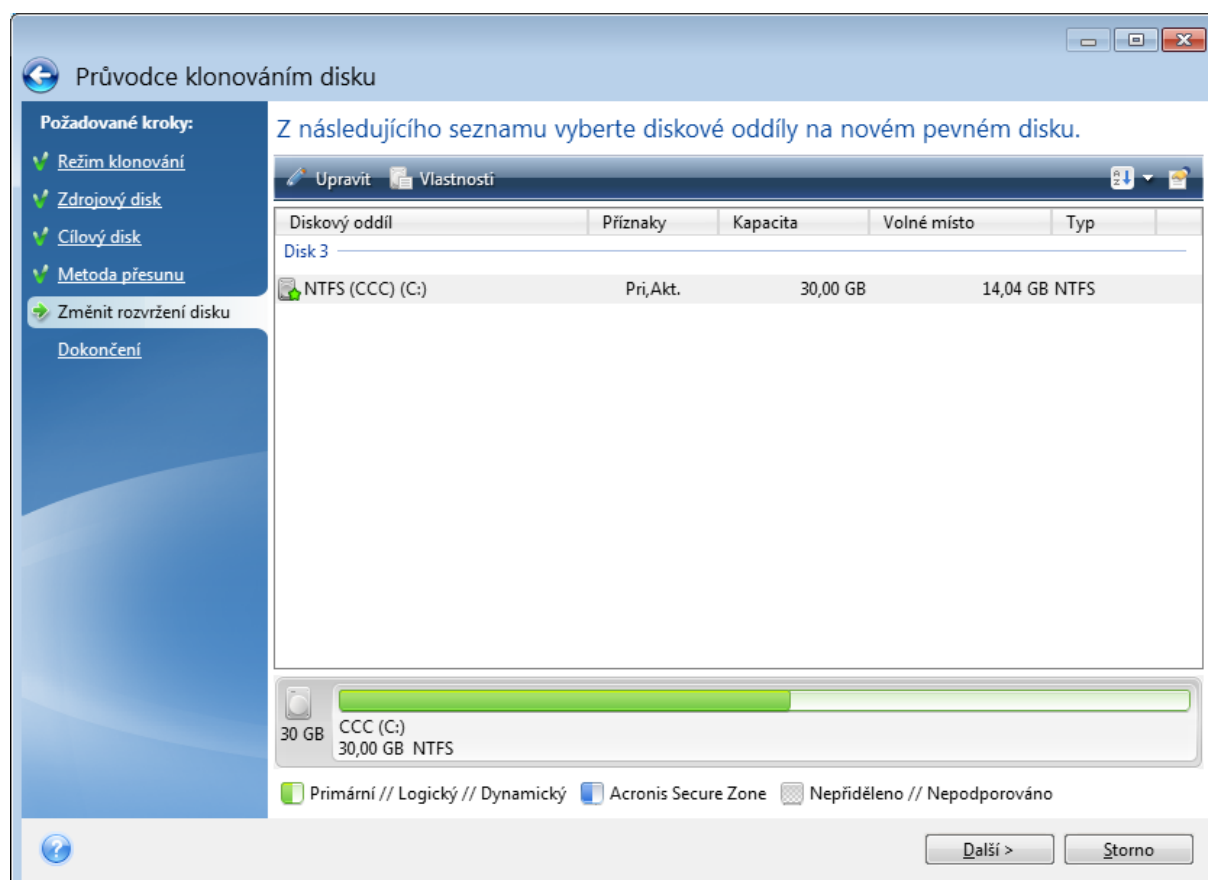
- **Ruční**– uživatel sám zadá novou velikost a další parametry.
8. [Tento krok je dostupný pouze v ručním režimu klonování]. V kroku **Změnit rozvržení disku** můžete upravit nastavení oddílů, které budou vytvořeny na cílovém disku. Další informace naleznete v části [Ruční vytváření oddílů](#).
  9. [Volitelný krok] V kroku **Co se má vyloučit** můžete určit soubory a složky, které nechcete klonovat. Podrobnosti naleznete v části [Vyloučení položek z klonování](#).
  10. V kroku **Dokončit** ověřte, zda nakonfigurovaná nastavení odpovídají vašim potřebám a pak klikněte na tlačítko **Pokračovat**.

Pokud dojde z nějakého důvodu k zastavení klonování, budete muset postup znovu nakonfigurovat a spustit. Neztratíte data, protože aplikace Acronis Cyber Protect Home Office během klonování neupravuje původní disk ani na něm uložená data.

Ve výchozím nastavení aplikace Acronis Cyber Protect Home Office po dokončení procesu klonování vypne počítač. To umožní změnu nadřazených/podřazených přepínačů a odstranění jednoho z disků.

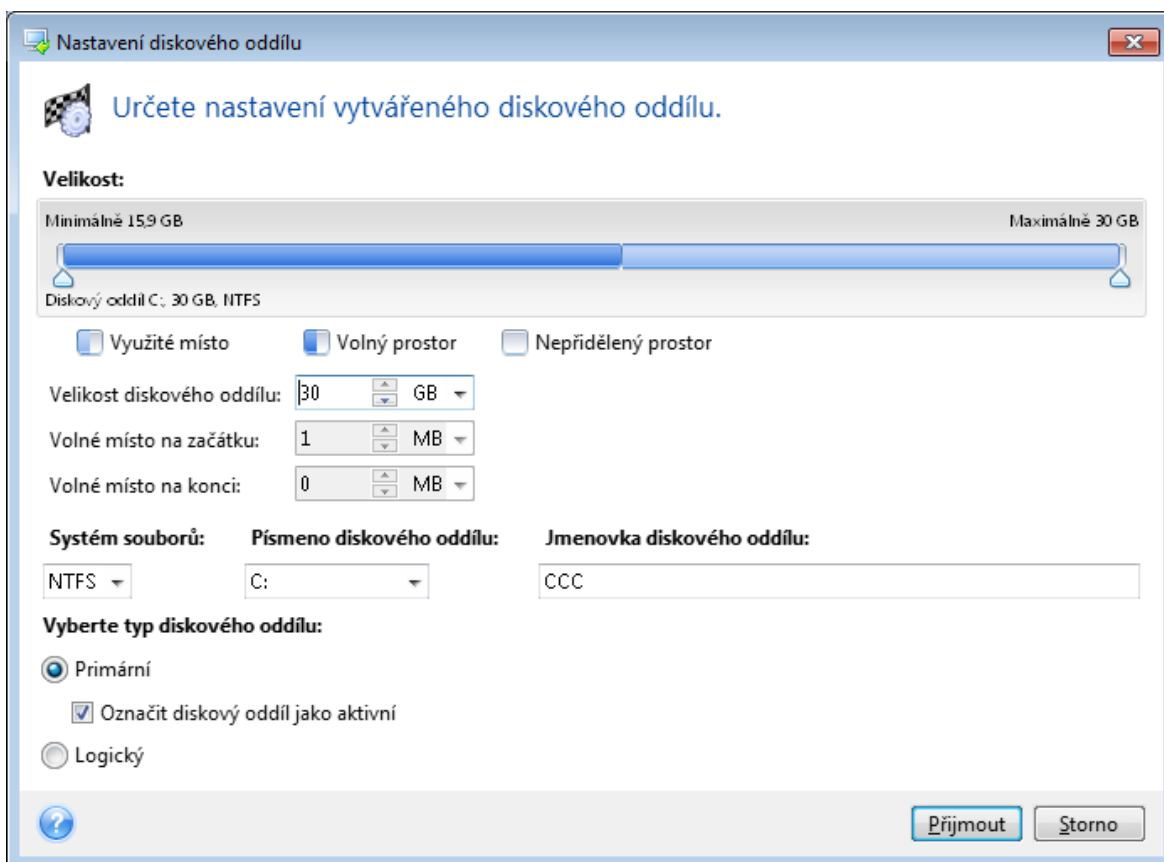
## 11.1.2 Ruční rozdělení na diskové oddíly

Metoda ručního přenosu umožňuje změnit velikost diskových oddílů na novém disku. Při výchozím nastavení aplikace změní jejich velikost proporcionálně.



### ***Jak upravit diskový oddíl***

1. Vyberte diskový oddíl a klikněte na tlačítko **Upravit**. Tím zobrazíte okno Nastavení diskového oddílu.



2. Zadejte pro diskový oddíl následující nastavení:

- Velikost a umístění
- Systém souborů
- Typ oddílu (dostupné pouze pro disky MBR)
- Písmeno a jmenovka diskového oddílu

Další informace naleznete v části [Nastavení diskového oddílu](#).

3. Klikněte na tlačítko **Potvrdit**.

---

### Upozornění!

Kliknutí na jakýkoli předchozí krok na bočním panelu v tomto okně způsobí zrušení všech změn velikosti a umístění, které jste provedli, proto je budete muset určit znovu.

---

## 11.1.3 Vyloučení položek z klonování

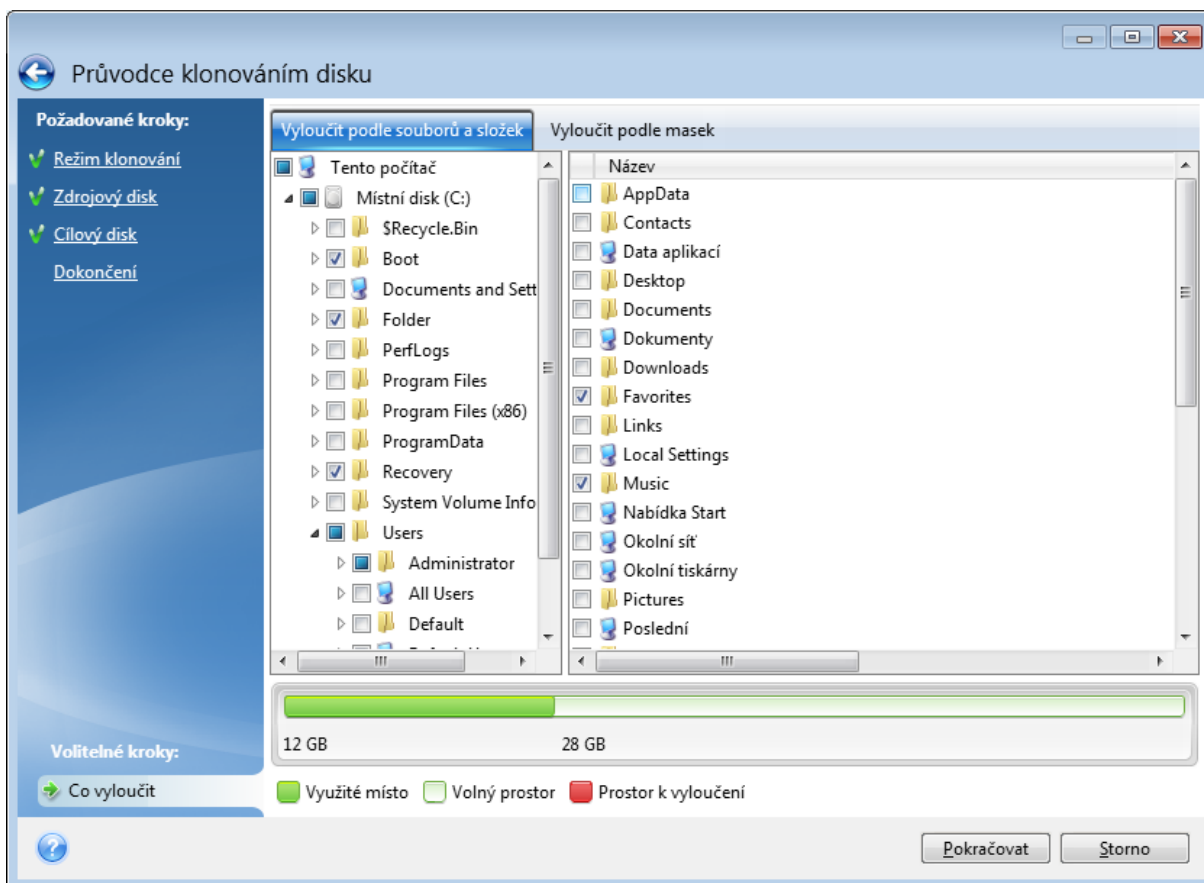
Pokud ze zdrojového disku určité soubory klonovat nechcete (cílový disk je například menší než zdrojový), můžete se je v kroku **Co se má vyloučit** rozhodnout vyloučit.

---

### Poznámka

Vyloučení skrytých a systémových souborů z klonování systémového oddílu nedoporučujeme.

---



### Soubory a složky můžete vyloučit dvěma způsoby:

- **Vyloučit podle souborů a složek**– na této kartě lze vybrat konkrétní soubory a složky ze stromu složek.
- **Vyloučit podle masek**– na této kartě lze vyloučit skupinu souborů podle masky, nebo jednotlivé soubory podle názvu či cesty.  
Chcete-li přidat kritérium vyloučení, klikněte na tlačítko **Přidat**, zadejte název souboru, cestu nebo masku a poté klikněte na tlačítko **OK**. Můžete přidat libovolný počet souborů i masek.

### Příklad kritérií vyloučení:

- Můžete zadat konkrétní názvy:
  - *soubor.příp*– všechny takovéto soubory budou z klonování vyloučeny.
  - *C:\soubor.příp*– soubor *soubor.příp* na disku C: bude vyloučen.
- Lze použít zástupné znaky (\* a ?):
  - *\*.příp*– všechny soubory s příponou *.příp* budou vyloučeny.
  - *??název.příp*– všechny soubory s příponou *.příp* a šesti písmeny v názvu (začínající libovolnými dvěma symboly – ?? – a končící slovem *název*) budou vyloučeny.
- Můžete zadat cestu k souboru:
  - *C:\moje obrázky*– složka *Moje obrázky* na disku C: bude vyloučen.

Kritéria vyloučení lze upravovat a odstraňovat pomocí odpovídajících tlačítek na pravém panelu.

## 11.1.4 Způsob migrace

Aplikace Acronis Cyber Protect Home Office umožňuje vybrat rozložení diskových oddílů cílového disku po dokončení operace klonování:

- **MBR (Master Boot Sector)**– spouštěcí sektor o velikosti 512 bajtů, který je prvním sektorem pevného disku a slouží k uložení hlavní tabulky diskových oddílů.
- **GPT (GUID Partition Table)**– standard rozložení tabulky diskových oddílů pevných disků. GPT umožňuje velikost disků nebo oddílů až do 9,4 ZB (9,4 x 10<sup>21</sup> bajtů).

Pomocí tohoto průvodce je možné převést vaše rozložení oddílů při operaci klonování nebo je klonovat tak, jak jsou, beze změny rozložení.

- **Kopírovat oddíly beze změny**– pomocí této možnosti lze přesouvat systém tak, jak je, beze změny rozložení oddílů. Pozor, v tomto případě bude všechno místo na disku nad 2 TB nedostupné. Místo na disku nad 2 TB lze přidělit díky nástroji Správce rozšířené kapacity Acronis.
- **Kopírovat oddíly a použít disk jako nesystémový disk GPT**– pomocí této možnosti lze převést diskový oddíl na rozložení disku GPT.

Pomocí aplikace Acronis Cyber Protect Home Office je také možné převádět systémy **BIOS** na rozhraní **UEFI**. Další informace naleznete v tématu [Unified Extensible Firmware Interface \(Jednotná rozšiřitelná firmwarová rozhraní\)](#).

### System spouštěný ze systému BIOS, záznam MBR, systém UEFI není podporován

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

**System nyní obsahuje:**

**System:** spouštěný pomocí systému BIOS

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** operační systém Windows, spouštěný pomocí rozhraní UEFI není podporováno.

**Velikost cílového disku:** méně než 2 TB

**Pokud systém migrujete na vybraný disk:**

**System:** spouštěný pomocí systému BIOS

**Styl diskového oddílu:** Záznam MBR

**Operační systém:** operační systém Windows, spouštěný pomocí rozhraní UEFI není podporováno.

**Velikost disku:** je dostupné veškeré místo na disku

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## System spouštěný ze systému BIOS, záznam MBR, systém UEFI je podporován

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

System nyní obsahuje:

**System:** spouštěný pomocí systému BIOS

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

**Velikost cílového disku:** méně než 2 TB

Pokud systém migrujete na vybraný disk:

**System:** spouštěný pomocí systému BIOS

**Styl diskového oddílu:** Záznam MBR

**Operační systém:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

**Velikost disku:** je dostupné veškeré místo na disku

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## System spouštěný ze systému BIOS, záznam MBR, bez operačního systému Windows

Aplikace Acronis Cyber Protect Home Office umožňuje vybrat rozložení diskových oddílů cílového disku po dokončení operace.

System nyní obsahuje:

**System:** spouštěný pomocí systému BIOS

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** bez operačního systému Windows nebo jiného operačního systému

**Velikost cílového disku:** méně než 2 TB

S těmito parametry systému můžete vybrat jednu z následujících možností:

### 1. Kopírovat oddíly beze změny

Na cílovém disku můžete ponechat styl rozložení diskových oddílů MBR.

**Cílový disk po migraci:**



**Systém:** spouštěný pomocí systému BIOS

**Styl diskového oddílu:** Záznam MBR

**Operační systém:** bez operačního systému Windows nebo jiného operačního systému

**Velikost disku:** je dostupné veškeré místo na disku

## 2. Kopírovat oddíly a použít disk jako nesystémový disk GPT

Můžete převést styl rozložení disků na GPT.

### Cílový disk po migraci:

**Systém:** nelze spouštět pomocí systému BIOS

**Styl diskového oddílu:** GPT

**Operační systém:** bez operačního systému Windows nebo jiného operačního systému

**Velikost disku:** je dostupné veškeré místo na disku

---

### Upozornění!

Po migraci lze cílový disk použít pouze jako nesystémový. Tato možnost není dostupná, pokud je aplikace Acronis Cyber Protect Home Office spuštěna v operačním systému Windows XP x32.

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## Systém spouštěný ze systému BIOS, GPT, podpora systému UEFI

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

### Systém nyní obsahuje:

**Systém:** spouštěný pomocí systému BIOS

**Styl diskového oddílu zdroje:** GPT

**Operační systém na zdrojovém disku:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

### Pokud systém migrujete na vybraný disk:

**Systém:** nelze spouštět pomocí systému BIOS

**Styl diskového oddílu:** GPT

**Operační systém:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

**Velikost disku:** je dostupné veškeré místo na disku

---

### Upozornění!

Po migraci nebude možné operační systém z cílového disku spustit pomocí systému BIOS. Pokud chcete po migraci spustit systém z cílového disku, je třeba v systému zapnout spouštění pomocí systému UEFI (viz téma Unified Extensible Firmware Interface (Jednotná rozšiřitelná firmwarová rozhraní)) a poté operaci restartujte.

---

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## System spouštěný ze systému BIOS, GPT, bez Windows

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

System nyní obsahuje:

**System:** spouštěný pomocí systému BIOS

**Styl diskového oddílu zdroje:** GPT

**Operační systém na zdrojovém disku:** bez operačního systému Windows nebo jiného operačního systému

Pokud systém migrujete na vybraný disk:

**System:** spouštěný pomocí systému BIOS

**Styl diskového oddílu:** GPT

**Operační systém:** bez operačního systému Windows nebo jiného operačního systému

**Velikost disku:** je dostupné veškeré místo na disku

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## System spouštěný ze systému UEFI, záznam MBR, systém UEFI není podporován

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

System nyní obsahuje:

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** operační systém Windows, spouštěný pomocí rozhraní UEFI není podporováno.

**Velikost cílového disku:** méně než 2 TB

Pokud systém migrujete na vybraný disk:

**System:** nelze spouštět pomocí rozhraní UEFI

**Styl diskového oddílu:** Záznam MBR

**Operační systém:** operační systém Windows, spouštěný pomocí rozhraní UEFI není podporováno.

**Velikost disku:** je dostupné veškeré místo na disku

---

### Upozornění!

Operační systém možná nepůjde spustit z cílového disku pomocí systému UEFI.

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## System spouštěný ze systému UEFI, záznam MBR, systém UEFI je podporován

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

System nyní obsahuje:

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

Pokud systém migrujete na vybraný disk:

Po migraci bude styl rozdělení oddílů převeden na GPT a bude z něj možné spouštět systém.

**Cílový disk po migraci:**

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu:** GPT

**Operační systém:** operační systém Windows, spouštění pomocí rozhraní UEFI je podporováno.

**Velikost disku:** je dostupné veškeré místo na disku

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## System spouštěný ze systému UEFI, záznam MBR, bez Windows

Aplikace Acronis Cyber Protect Home Office umožňuje vybrat rozložení diskových oddílů cílového disku po dokončení operace.

System nyní obsahuje:

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu zdroje:** Záznam MBR

**Operační systém na zdrojovém disku:** bez operačního systému Windows nebo jiného operačního systému

**Velikost cílového disku:** méně než 2 TB

S těmito parametry systému můžete vybrat jednu z následujících možností:

### 1. Kopírovat oddíly beze změny

Na cílovém disku můžete ponechat styl rozložení diskových oddílů MBR.

#### Cílový disk po migraci:

**Systém:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu:** Záznam MBR

**Operační systém:** bez operačního systému Windows nebo jiného operačního systému

**Velikost disku:** je dostupné veškeré místo na disku

### 2. Kopírovat oddíly a použít disk jako nesystémový disk GPT

Můžete převést styl rozložení disků na GPT.

#### Cílový disk po migraci:

**Systém:** nelze spouštět pomocí rozhraní UEFI

**Styl diskového oddílu:** GPT

**Operační systém:** bez operačního systému Windows nebo jiného operačního systému

**Velikost disku:** je dostupné veškeré místo na disku

---

#### Upozornění!

Po migraci lze cílový disk použít pouze jako nesystémový.

---

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## Systém spouštěný ze systému UEFI, GPT, systém UEFI je podporován

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

Systém nyní obsahuje:

**Systém:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu zdroje:** GPT

**Operační systém:** operační systém Windows, spouštění pomocí systému UEFI je podporováno.

Pokud systém migrujete na vybraný disk:

**Systém:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu:** GPT

**Velikost disku:** je dostupné veškeré místo na disku

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## System spouštěný ze systému UEFI, GPT, bez Windows

V tomto kroku průvodce je třeba vybrat cílový pevný disk.

System nyní obsahuje:

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu zdroje:** GPT

**Operační system:** bez operačního systému Windows nebo jiného operačního systému

Pokud system migrujete na vybraný disk:

**System:** spouštěný pomocí rozhraní UEFI

**Styl diskového oddílu:** GPT

**Velikost disku:** je dostupné veškeré místo na disku

Další informace o procesu migrace naleznete v tématu [Způsob migrace](#).

## 11.2 Migrace systému z pevného disku na disk SSD

Nejprve zkontrolujte, zda aplikace Acronis Cyber Protect Home Office rozpozná váš nový disk SSD v systému Windows i v rámci spouštěcího média Acronis. Pokud nastane problém, další informace naleznete v části [Co dělat v případě, že aplikace Acronis Cyber Protect Home Office nerozpozná disk SSD](#).

### 11.2.1 Velikost SSD

Vzhledem k tomu, že mají disky SSD obvykle menší kapacitu než disky HDD, může obsazené místo na starém disku přesáhnout velikost disku SSD. V takovém případě není migrace možná.

Chcete-li snížit množství dat na systémovém disku, zkuste následující:

- Přesuňte datové soubory ze starého pevného disku do jiného umístění, například na jiný pevný disk (interní či externí).
- Vytvořte archivy ZIP datových souborů (například dokumentů, obrázků, zvukových souborů atd.) a poté odstraňte původní soubory.
- Vyčistěte pevný disk pomocí nástroje pro vyčištění disku systému Windows.

K zajištění stabilního provozu je nutné, aby měl system Windows k dispozici několik GB volného místa na systémovém diskovém oddílu.

### 11.2.2 Kterou metodu migrace použít

Pokud se váš disk skládá z jednoho oddílu (skryté oddíly rezervované pro system se nepočítají), můžete zkusit provést migraci na disk SSD pomocí nástroje Klonování. Další informace naleznete v tématu [Klonování pevného disku](#).

Doporučujeme ovšem ve většině případů používat metodu zálohování a obnovy. Tato metoda poskytuje při migraci více kontroly a je flexibilnější. Viz téma [Migrace na disk SSD pomocí metody zálohování a obnovy](#).

## 11.2.3 Co dělat v případě, že aplikace Acronis Cyber Protect Home Office nerozezná váš disk SSD

Někdy aplikace Acronis Cyber Protect Home Office nemusí rozeznat disk SSD.

V takovém případě zkontrolujte, zda je disk SSD rozpoznán v systému BIOS.

Pokud systém BIOS ve vašem počítači nezobrazí disk SSD, zkontrolujte, zda jsou správně zapojeny datové a napájecí kabely. Je také možné zkusit aktualizovat systém BIOS a ovladače SATA. Pokud tato doporučení nepomohou, obraťte se na podporu výrobce vašeho disku SSD.

### ***Pokud systém BIOS vašeho počítače zobrazuje disk SSD***

1. Do pole Hledat nebo Spustit (v závislosti na operačním systému) zadejte `cmd` a pak stiskněte klávesu **Enter**.
2. Do příkazového řádku zadejte následující příkazy:

```
diskpart  
list disk
```

Na obrazovce se zobrazí disky připojené k vašemu počítači. Zjistěte číslo vašeho disku SSD. Ke zjištění čísla disku můžete použít velikost disku.

3. Chcete-li vybrat tento disk, spusťte následující příkaz:

```
select disk N
```

N je číslo vašeho disku SSD.

4. Chcete-li odebrat všechny informace z disku SSD a přepsat tabulku MBR výchozí, spusťte následující příkaz:

```
clean  
exit  
exit
```

Spusťte aplikaci Acronis Cyber Protect Home Office a zkontrolujte, zda rozpozná disk SSD. Pokud disk SSD rozpozná, pomocí nástroje Přidat nový disk vytvořte na disku jeden diskový oddíl zabírající veškeré místo na disku. Během tvorby diskového oddílu se ujistěte, že se před oddílem nachází 1 MB volného místa. Další informace naleznete v části nápovědy [Přidání nového pevného disku](#).

### ***Kontrola, zda Acronis spouštěcí médium rozpozná disk SSD***

1. Spusťte systém ze spouštěcího média Acronis.

2. Výběrem možnosti **Nástroje -> Přidat nový disk** v hlavní nabídce se zobrazí okno **Výběr disku** s informacemi o všech pevných discích ve vašem počítači. Pomocí tohoto okna zkontrolujte, zda je disk SSD rozpoznán v prostředí obnovy.
3. Pokud se v okně zobrazuje váš disk SSD, pouze klikněte na možnost **Storno**.

Jestliže spouštěcí médium nerozpozná disk SSD a řadič disku SSD je v režimu AHCI, je možné vyzkoušet změnu tohoto režimu na IDE (nebo ATA u některých výrobců systémů BIOS) a zkontrolovat, zda se problém vyřeší.

---

### Upozornění!

Pozor! Po změně režimu nespouštějte systém Windows – může dojít k závažným systémovým problémům. Před spuštěním systému Windows je nutné režim vrátit zpět na AHCI.

---

Pokud po změně režimu řadiče spouštěcí médium rozpozná disk SSD, je možné pro obnovu nebo klonování v rámci spouštěcího média použít následující postup:

1. Vypněte počítač.
2. Spusťte systém BIOS a změňte režim řadiče z AHCI na IDE (nebo ATA u některých výrobců systémů BIOS).
3. Spusťte systém ze spouštěcího média Acronis.
4. Obnovte nebo naklonujte disk.
5. Zobrazte nastavení systému BIOS a změňte režim IDE zpátky na AHCI.
6. Spusťte systém Windows.

## Co dělat v případě, že předchozí pokyny nepomohly

Můžete také vytvořit média na bázi prostředí WinPE. To může poskytnout nezbytné ovladače. Další informace naleznete v tématu [Tvorba spouštěcího média Acronis](#).

### 11.2.4 Migrace na disk SSD pomocí metody zálohy a obnovení

Následující postup je možné použít pro všechny podporované operační systémy. Tento postup si nejprve ukážeme na jednoduchém případě: váš disk obsahuje jediný oddíl. Upozorňujeme, že systémový disk Windows 7 a novějšího systému může obsahovat skrytý oddíl vyhrazený systémem.

Doporučujeme systém přesunout na prázdný disk SSD, který neobsahuje oddíly (místo na disku není alokované). Nezapomeňte, že je-li disk SSD nový a dosud nepoužívaný, oddíly neobsahuje.

#### ***Jak přesunout systém na disk SSD***

1. Spustit Acronis Cyber Protect Home Office
2. Pokud jste tak ještě neučinili, vytvořte spouštěcí médium Acronis. V části **Nástroje** klikněte na tlačítko **Vytvořit spouštěcí médium** a postupujte podle pokynů na obrazovce.
3. Zazálohujte celý systémový disk (v režimu zálohy disku) na jiný pevný disk než váš systémový disk a disk SSD.

4. Vypněte počítač a vyjměte systémový pevný disk.
5. Připojte disk SSD do slotu, ve kterém se nacházel pevný disk.

---

**Poznámka**

U některých značek disků SSD může být nutné vložit disk SSD do slotu PCI Express.

---

6. Spusťte systém ze spouštěcího média Acronis.
7. Ověřením zálohy se ujistěte, že je záloha použitelná k obnově. To provedete kliknutím na možnost **Obnovení** na levém panelu a výběrem zálohy. Klikněte pravým tlačítkem myši, vyberte možnost **Ověřit zálohu** v místní nabídce a poté klikněte na **Provést**.
8. Po dokončení ověření klikněte pravým tlačítkem myši na zálohu a v místní nabídce vyberte příkaz **Obnovit**.
9. V kroku Metoda obnovení vyberte možnost **Obnovit celé disky a diskové oddíly** a poté klikněte na možnost **Další**.
10. V kroku Co obnovovat vyberte systémový disk.
11. Klikněte na možnost **Nové umístění** a poté vyberte jako nové umístění vašeho systémového disku disk SSD a klikněte na **Přijmout**.
12. V dalším kroku kliknutím na **Pokračovat** spustíte obnovení.
13. Po dokončení obnovení ukončete samostatnou verzi aplikace Acronis Cyber Protect Home Office.
14. Spusťte systém z disku SSD a ověřte, že systém Windows i aplikace fungují v pořádku.

Pokud váš systémový pevný disk obsahuje také skrytý diskový oddíl pro obnovení nebo diagnostiku, jako to mu je u většiny notebooků, bude nutné použít jiný postup. Během obnovení na disk SSD bude ve většině případů nutné změnit velikost diskových oddílů ručně. Další informace najdete v tématu [Obnovení disku se skrytým diskovým oddílem](#).



## 12 Nástroje

Nástroje Acronis obsahují nástroje na ochranu, připojování, klonování disků, zabezpečení soukromí a správu disků.

### ***Nástroje na ochranu***

- "Acronis Universal Restore" (str. 238)
- "Acronis Startup Recovery Manager" (str. 203)
- "Tvůrce médií Acronis" (str. 190)
- "Acronis Secure Zone" (str. 210)
- "Try&Decide" (str. 205)

### ***Klonování disku***

- "Nástroj pro klonování disku" (str. 175)

### ***Zabezpečení a soukromí***

- "Acronis DriveCleanser" (str. 220)
- "Vyčištění systému" (str. 225)

### ***Správa disků***

- "Přidání nového pevného disku" (str. 215)

### ***Připojení obrazu***

- "Připojení diskového obrazu" (str. 234)
- "Odpojení diskového obrazu" (str. 236)

## 12.1 Tvůrce médií Acronis

Tvůrce médií Acronis umožňuje vytvořit z USB flash disku, externího disku nebo z prázdného disku CD či DVD spouštěcí médium. Pokud systém Windows nelze spustit, spusťte pomocí spouštěcího média samostatnou verzi aplikace Acronis Cyber Protect Home Office a počítač obnovte.

### **Můžete vytvořit několik typů spouštěcího média:**

- **Spouštěcí médium Acronis**

Tento typ se doporučuje pro většinu uživatelů.

- **Média založená na prostředí WinPE s doplňkem Acronis**

Spouštění aplikace Acronis Cyber Protect Home Office v předinstalačním prostředí může zajistit lepší kompatibilitu s hardwarem vašeho počítače, protože předinstalační prostředí používá ovladače systému Windows.

Doporučujeme tento typ média vytvořit, pokud vám se spuštěním počítače nepomohlo spouštěcí médium Acronis.

Při použití této možnosti je třeba mít nainstalovanou jednu z následujících součástí:

- Windows Automated Installation Kit (AIK)

Tato součást je nutná k vytvoření prostředí WinPE 3.0.

- Windows Assessment and Deployment Kit (ADK)

Tato součást je nutná k vytvoření prostředí WinPE 4.0, WinPE 5.0 a WinPE 10.0.

- **Média založená na prostředí WinRE s doplňkem Acronis**

Tento typ spouštěcích médií je podobný médiím WinPE, má však důležitou výhodu – nemusíte stahovat software Windows ADK nebo AIK z webu společnosti Microsoft. Prostor obnovy Windows je již součástí systému Windows Vista a novějších verzí systému Windows. Acronis Cyber Protect Home Office používá tyto soubory ze systému k vytvoření médií založených na WinRE. Podobně jako u médií WinPE můžete přidat ovladače pro zajištění lepší kompatibility s vaším hardwarem. Nicméně média WinRE mohou být použita pouze na počítači, na kterém byla vytvořena nebo na počítači se stejným operačním systémem.

### Poznámky

- Při každé aktualizaci aplikace Acronis Cyber Protect Home Office doporučujeme znovu vytvořit nové spouštěcí médium.
- Pokud nepoužíváte optické médium, musí být na médiu systém souborů FAT16 nebo FAT32.
- Tvůrce médií Acronis podporuje pouze prostředí x64 WinPE 3.0, WinPE 4.0, WinPE 5.0 a WinPE 10.0.
- Váš počítač musí splňovat tyto předpoklady:
  - Pro WinPE 3,0 alespoň 256 MB RAM
  - Pro WinPE 4,0 alespoň 512 MB RAM
  - Pro WinPE 5,0 alespoň 1 GB RAM
  - Pro WinPE 10.0 alespoň 512 MB RAM
- Pokud Tvůrce médií Acronis nerozpozná váš USB flash disk, můžete vyzkoušet postup popsany v článku znalostní databáze Acronis na adrese <https://kb.acronis.com/content/1526>.
- Při spouštění ze spouštěcího média nemůžete provádět zálohování na disky nebo diskové oddíly se systémy souborů Ext2/Ext3/Ext4, ReiserFS a Linux SWAP.
- Při spuštění ze spouštěcího média a používání samostatné verze aplikace Acronis Cyber Protect Home Office nemůžete obnovovat soubory a složky zašifrované funkcemi pro šifrování dostupnými v operačních systémech Windows XP a novějších. Další informace naleznete v tématu [Nastavení zabezpečení zálohy na úrovni souborů](#). Zálohy šifrované pomocí funkce šifrování aplikace Acronis Cyber Protect Home Office však obnovit lze.
- Pokud se rozhodnete vytvořit spouštěcí médium na disku, který již obsahuje sadu Survival Kit, Tvůrce médií Acronis se pomocí spouštěcího média pokusí přepsat a aktualizovat pouze skrytý oddíl bez formátování celého disku.

## 12.1.1 Jak vytvořit spouštěcí médium Acronis

1. Připojte USB flash disk či externí disk (HDD/SSD) nebo vložte prázdný disk CD či DVD.
2. Spustit Acronis Cyber Protect Home Office
3. V části **Nástroje** klikněte na možnost **Program pro tvorbu záchranných médií**.
4. Zvolte metodu vytvoření.
  - **Jednoduchý**– tato možnost je nejjednodušší. Acronis Cyber Protect Home Office vybere optimální typ média pro váš počítač. Používáte-li systém Windows 7 nebo novější, vytvoří se médium WinRE.
  - **Pokročilý**– tato volba umožňuje vybrat typ média. To znamená, že můžete vytvořit spouštěcí médium nejenom pro svůj počítač, ale také pro počítač s jinou verzí systému Windows. Další informace naleznete v části Program pro tvorbu médií [Acronis](#).

Vyberete-li médium založené na systému Linux, zvolte součásti Acronis, které mají být na médium uloženy. Zajistěte, aby vybrané součásti byly kompatibilní s architekturou cílového počítače. Další informace naleznete v části [Nastavení vyměnitelných médií](#).

Pokud vyberete médium založené na prostředí WinRE nebo WinPE:

- Vyberte typ architektury média – 32bitové nebo 64bitové. 32bitové spouštěcí médium může fungovat pouze na 32bitových počítačích, zatímco 64bitové médium je kompatibilní s 32bitovými i 64bitovými počítači.
- Vyberte si sadu nástrojů, kterou chcete použít pro vytvoření spouštěcího média. Pokud zvolíte software Windows AIK nebo ADK a nemáte vybranou sadu nainstalovanou ve svém počítači, budete si ji muset nejprve stáhnout z webu Microsoft, pak nainstalovat požadované součásti – Nástroje pro nasazení a prostředí Windows Preinstallation Environment (Windows PE).

Pokud soubory prostředí WinPE již máte na svém počítači a jsou uloženy v jiné složce než výchozí, zadejte pouze jejich umístění a zásuvný modul Acronis bude přidán do stávající bitové kopie prostředí WinPE.
- Pro zajištění lepší kompatibility s vaším hardwarem můžete vybrat ovladače, které se mají přidat na médium.

5. Vyberte cílové umístění pro médium:

- **CD**
- **DVD**
- **Externí disk**
- **USB flash disk**

Má-li váš disk nepodporovaný systém souborů, navrhne jej aplikace Acronis Cyber Protect Home Office naformátovat na systém souborů FAT.

---

### Upozornění!

Zformátováním se trvale vymažou všechna data na disku.

---

- **Soubor obrazu ISO**

Bude třeba zadat název a cílovou složku souboru ISO.

Po vytvoření obrazu ISO jej můžete vypálit na disk CD nebo DVD. Například v systémech Windows 7 a novějších to lze provést pomocí integrovaného nástroje pro vypalování.

V Průzkumníku souborů dvakrát klikněte na vytvořený soubor obrazu ISO a poté klikněte na možnost **Vypálit**.

- **Soubor obrazu WIM** (k dispozici pouze pro médium založené na prostředí WinPE)

Aplikace Acronis Cyber Protect Home Office přidá k souboru WIM doplněk Acronis Plug-in ze sady Windows AIK nebo Windows ADK. Bude třeba zadat název a cílovou složku nového souboru WIM.

Chcete-li vytvořit spouštěcí médium pomocí souboru WIM, musíte ho nejprve převést na soubor ISO. Podrobnosti naleznete v části [Vytvoření souboru ISO ze souboru WIM](#).

---

#### **Poznámka**

Pokud tvůrce médií Acronis na této jednotce rozpozná dříve nainstalovanou sadu Acronis Survival Kit, pokusí se pomocí spouštěcího média přepsat a aktualizovat pouze skrytý oddíl bez formátování celé jednotky.

---

6. Klikněte na tlačítko **Pokračovat**.

## 12.1.2 Parametry spuštění spouštěcího média Acronis

Zde můžete nastavit parametry spuštění spouštěcího média Acronis tak, aby možnosti spuštění spouštěcího média byly lépe kompatibilní s různým hardwarem. Je dostupných několik možností (nouse, nomouse, noapic atd.). Tyto parametry jsou vhodné pro pokročilé uživatele. Pokud při spuštění ze spouštěcího média Acronis nastanou nějaké problémy s hardwarovou kompatibilitou, je nejlepší obrátit se na technickou podporu společnosti Acronis.

### ***Jak přidat parametry spuštění***

1. Zadejte příkaz do pole **Parametry**. Můžete zadat několik příkazů oddělených mezerami.
2. Pokračujte kliknutím na tlačítko **Další**.

Další parametry lze použít před zavedením jádra Linuxu

### **Popis**

Následující parametry lze použít k načtení jádra Linuxu ve zvláštním režimu:

- **acpi=off**

Vypne **ACPI** a může pomoci při problémech s určitou hardwarovou konfigurací.

- **noapic**

Vypne APIC (Advanced Programmable Interrupt Controller) a může pomoci při problémech s určitou hardwarovou konfigurací.

- **nousb**

Vypne načítání USB modulů.

- **nousb2**

Vypne podporu USB 2.0. Zařízení standardu USB 1.1 při použití této volby stále fungují. Tato volba umožňuje používat USB jednotky v režimu USB 1.1 v případě, že v režimu USB 2.0 nefungují.

- **quiet**

Tento parametr je implicitně zapnutý a zprávy spuštění se nezobrazují. Po jeho odstranění se při načítání jádra Linuxu budou zobrazovat zprávy spuštění a před spuštěním programu je nabídnuto použití příkazového [prostředí](#).

- **nodma**

Vypne DMA u všech jednotek disků IDE. Zabraňuje zamrznutí jádra při použití určitého hardwaru.

- **nofw**

Vypne podporu FireWire (IEEE1394).

- **nopcmcia**

Vypne detekci PCMCIA hardwaru.

- **nomouse**

Vypne podporu myši.

- **[název modulu]=off**

Vypne modul (např. **sata\_sis=off**).

- **pci=bios**

Vynutí používání PCI BIOSu místo přímého přístupu k hardwarovým zařízením. Tento parametr lze použít, například když počítač nemá standardní hostitelský most PCI.

- **pci=nobios**

Zakáže používání PCI BIOSu a povolí pouze metody přímého přístupu k hardwaru. Tento parametr lze použít například v případě, že se při zavádění vyskytnou chyby, které pravděpodobně způsobuje BIOS.

- **pci=biosirq**

K získání tabulky směrování přerušení se použijí volání PCI systému BIOS. Tato volání často způsobují na některých počítačích problémy, ale na jiných počítačích je to jediný způsob, jak získat tabulku směrování přerušení. Tuto volbu použijte, pokud jádro nemůže alokovat IRQ nebo objevilo na základní desce sekundární PCI sběrnice.

- **vga=ask**

Získá seznam režimů videa dostupných pro vaši grafickou kartu a umožní vybrat režim videa nejvhodnější pro grafickou kartu a monitor. Tuto možnost vyzkoušejte, pokud automaticky zvolený režim videa není pro váš hardware vhodný.

### 12.1.3 Přidání ovladačů do stávající bitové kopie WIM

Někdy základní disk WinPE s doplňkem Acronis Plug-in nemá ovladače pro váš konkrétní hardware, například pro řadiče úložných zařízení. Nejsnazší způsob jejich přidání je vybrat režim Pokročilý v aplikaci [tvůrce záchranných spouštěcích médií](#) a zadat ovladače, které chcete přidat. Můžete přidat ovladače ručně do stávajícího souboru WIM, než vytvoříte soubor ISO pomocí zásuvného modulu Acronis.

---

#### Upozornění!

Pozor! Je možné přidat pouze soubory ovladačů s příponou INF.

---

Následující postup je založen na článku MSDN, který je dostupný na adrese <https://technet.microsoft.com/>.

#### **Chcete-li vytvořit vlastní diskový obraz WindowsPE**

1. Pokud nemáte doplněk Acronis Plug-in se souborem WIM, spusťte **tvůrce záchranných spouštěcích médií** a vytvořte jej tak, že **soubor WIM** vyberete jako cíl pro média založená na WinPE. Další informace naleznete v části [Tvorba spouštěcího média Acronis](#).
2. V závislosti na verzi sady Windows AIK a Windows ADK proveďte jeden z následujících postupů:
  - V nabídce **Start** klikněte na možnost **Microsoft Windows AIK**, poté klikněte pravým tlačítkem myši na možnost **Příkazový řádek nástrojů systému Windows PE** a zvolte možnost **Spustit jako správce**.
  - V nabídce **Start** klikněte na možnost **Microsoft Windows AIK**, klikněte pravým tlačítkem myši na možnost **Příkazový řádek nástrojů pro nasazení** a potom zvolte možnost **Spustit jako správce**.
  - V nabídce **Start** klikněte na možnost **Windows Kits**, klikněte na položku **Windows ADK**, klikněte pravým tlačítkem myši na možnost **Deployment and Imaging Tools Environment** a potom zvolte možnost **Spustit jako správce**.
3. Vytvořte složku se soubory Windows PE spuštěním skriptu Copype.cmd. Například na příkazovém řádku napište:

```
copype amd64 C:\winpe_x64
```

4. Zkopírujte soubor WIM například do složky C:\winpe\_x64\. Implicitně má tento soubor název AcronisBootablePEMedia.wim.
5. Připojte základní diskový obraz k místní složce pomocí nástroje DISM. Napište:

```
Dism /Mount-Wim /WimFile:C:\winpe_x64\AcronisBootablePEMedia.wim /index:1  
/MountDir:C:\winpe_x64\mount
```

6. Přidejte váš ovladač hardwaru pomocí příkazu DISM s parametrem /Add-Driver. Chcete-li například přidat ovladač Mydriver.inf umístěný ve složce C:\drivers\, napište:

```
Dism /image:C:\winpe_x64\mount /Add-Driver /driver:C:\drivers\mydriver.inf
```

7. Předchozí krok opakujte u každého ovladače, který je třeba přidat.
8. Proveďte změny pomocí příkazu DISM:

```
Dism /Unmount-Wim /MountDir:C:\winpe_x64\mount /Commit
```

9. Vytvořte bitovou kopii PE (soubor ISO) z výsledného souboru WIM. Podrobnosti naleznete v části Vytvoření souboru ISO ze souboru WIM.

## 12.1.4 Vytvoření souboru ISO ze souboru WIM

Chcete-li vytvořit spouštěcí médium pomocí souboru WIM, musíte ho nejprve převést na soubor ISO.

### ***Vytvoření obrazu PE (soubor ISO) z výsledného souboru WIM***

1. V závislosti na verzi sady Windows AIK a Windows ADK proveďte jeden z následujících postupů:
  - V nabídce **Start** klikněte na možnost **Microsoft Windows AIK**, poté klikněte pravým tlačítkem myši na možnost **Příkazový řádek nástrojů systému Windows PE** a zvolte možnost **Spustit jako správce**.
  - V nabídce **Start** klikněte na možnost **Microsoft Windows AIK**, klikněte pravým tlačítkem myši na možnost **Příkazový řádek nástrojů pro nasazení** a potom zvolte možnost **Spustit jako správce**.
  - V nabídce **Start** klikněte na možnost **Windows Kits**, klikněte na položku **Windows ADK**, klikněte pravým tlačítkem myši na možnost **Deployment and Imaging Tools Environment** a potom zvolte možnost **Spustit jako správce**.
2. Vytvořte složku se soubory Windows PE spuštěním skriptu Copype.cmd. Například na příkazovém řádku napište:

```
copype amd64 C:\winpe_x64
```

3. Nahradte výchozí soubor boot.wim ve složce Windows PE nově vytvořeným souborem WIM (například AcronisBootablePEMedia.wim). Pokud se soubor AcronisBootablePEMedia.wim nachází na disku C:\, pak:

V případě rozhraní WinPE 3.0 zadejte:

```
copy c:\AcronisBootablePEMedia.wim c:\winpe_x64\ISO\sources\boot.wim
```

V případě rozhraní WinPE 4.0, WinPE 5.0 nebo WinPE 10.0 zadejte:

```
copy "c:\AcronisBootablePEMedia.wim" c:\winpe_x64\media\sources\boot.wim
```

4. Použijte nástroj **Oscdimg**. Chcete-li vytvořit soubor ISO, zadejte:

```
oscdimg -n -bc:\winpe_x64\etfsboot.com c:\winpe_x64\ISO c:\winpe_x64\winpe_x64.iso
```

Případně, chcete-li vytvořit médium spustitelné na počítačích se systémem BIOS i UEFI, zadejte:

```
oscdimg -m -o -u2 -udfver102 -bootdata:2#p0,e,bc:\winpe_x64\fwfiles\etfsboot.com#pEF,e,bc:\winpe_x64\fwfiles\efisys.bin c:\winpe_x64\media c:\winpe_x64\winpe_x64.iso
```

5. Vypalte soubor ISO na disk CD pomocí nástroje od jiného výrobce, získáte tím spouštěcí disk Windows PE s aplikací Acronis Cyber Protect Home Office.

## 12.2 Kontrola, že spouštěcí médium lze v případě potřeby použít

Abyste v případě potřeby měli maximální šance na úspěšné obnovení počítače, je nutné zjistit, zda lze počítač ze spouštěcích médií spustit. Navíc je nutné zkontrolovat, zda spouštěcí médium rozpozná všechna zařízení vašeho počítače, například pevné disky, myš, klávesnici nebo síťový adaptér.

Pokud jste zakoupili krabicovou verzi produktu se spouštěcím diskem CD a neprovedli jste aktualizaci aplikace Acronis Cyber Protect Home Office, můžete vyzkoušet tento disk CD. V opačném případě vytvořte nové spouštěcí médium. Další informace naleznete v části [Tvorbá spouštěcího média Acronis](#).

### 12.2.1 Jak testovat spouštěcí média

#### Poznámka

Pokud pro ukládání záloh využíváte externí pevné disky, před spuštěním spouštěcího CD je třeba je připojit. Jinak je aplikace nemusí rozpoznat.

1. Nastavte počítač tak, aby se spouštěl ze spouštěcího média. Poté nastavte zařízení se spouštěcím médiem (jednotku CD-ROM/DVD-ROM nebo disk USB) jako první spouštěcí zařízení. Podrobnosti naleznete v části [Uspořádání pořadí spuštění v systému BIOS](#).
2. Pokud máte spouštěcí CD, spusťte z něj systém stisknutím libovolné klávesy při zobrazení výzvy „Press any key to boot from CD“. Pokud do pěti sekund nestisknete nějakou klávesu, bude nutné počítač restartovat.
3. Po zobrazení spouštěcí nabídky zvolte položku **Acronis Cyber Protect Home Office**.



---

**Poznámka**

Pokud vaše bezdrátová myš nefunguje, zkuste ji nahradit drátovou myší. Stejně doporučení se týká i klávesnice.

---

**Poznámka**

Pokud nemáte náhradní myš ani klávesnici, kontaktujte podporu Acronis. Sestaví pro vás vlastní spouštěcí CD, které bude obsahovat ovladače pro váš model myši a klávesnice. Nalezení příslušných ovladačů a tvorba vlastního spouštěcího CD může zabrat mnoho času. Pro některé modely to navíc nemusí být možné.

---

4. Po spuštění aplikace doporučujeme vyzkoušet obnovu některých souborů ze zálohy. Test obnovy vám umožní se ujistit, že spouštěcí CD lze použít pro obnovu. Navíc můžete zkontrolovat, zda aplikace nalezne všechny pevné disky ve vašem systému.

---

**Poznámka**

Pokud máte pevný disk navíc, doporučujeme provést pokusnou obnovu systémového diskového oddílu na tento disk.

---

## 12.2.2 Jak testovat obnovu a zkontrolovat ovladače a síťový adaptér

1. Pokud máte zálohy souborů, spusťte průvodce obnovením kliknutím na možnosti **Obnova** -> **Obnova souborů** na panelu nástrojů.

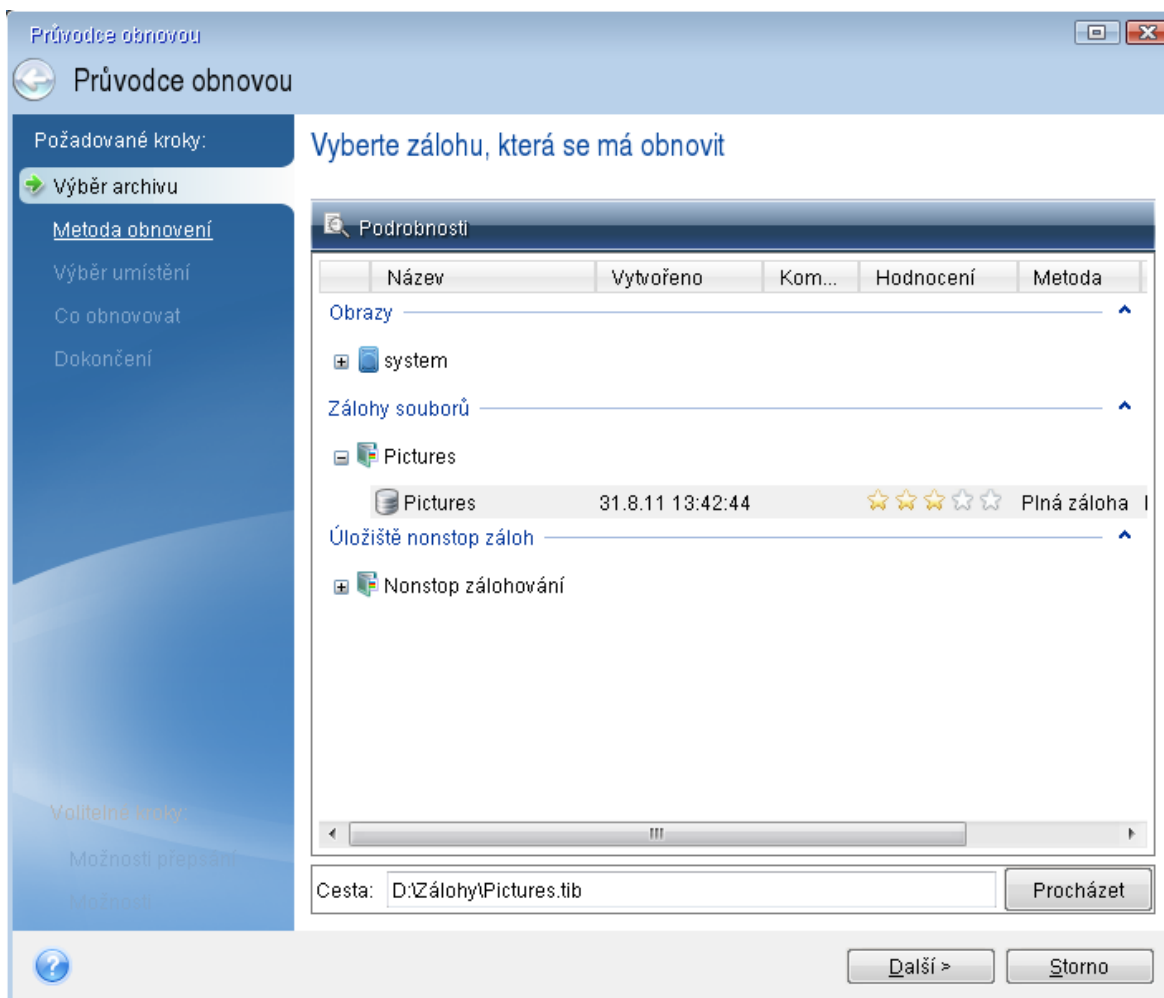
---

**Poznámka**

Pokud máte pouze jeden disk a zálohu diskového oddílu, spustí se průvodce obnovením také a proces obnovy bude podobný. V takovém případě je třeba v kroku **Metoda obnovení** zvolit možnost **Obnovit vybrané soubory a složky**.

---

2. V kroku **Umístění archivu** vyberte zálohu a poté klikněte na tlačítko **Další**.



3. Při obnově souborů pomocí spouštěcího CD budete moci pro obnovované soubory vybrat pouze nové umístění. Proto v kroku **Výběr umístění** pouze klikněte na tlačítko **Další**.
4. Po otevření okna **Cílové umístění** zkontrolujte, zda jsou ve složce **Tento počítač** zobrazeny všechny disky.

---

#### **Poznámka**

Pokud ukládáte zálohy v síti, ověřte také, zda je síť dostupná.

---

#### **Poznámka**

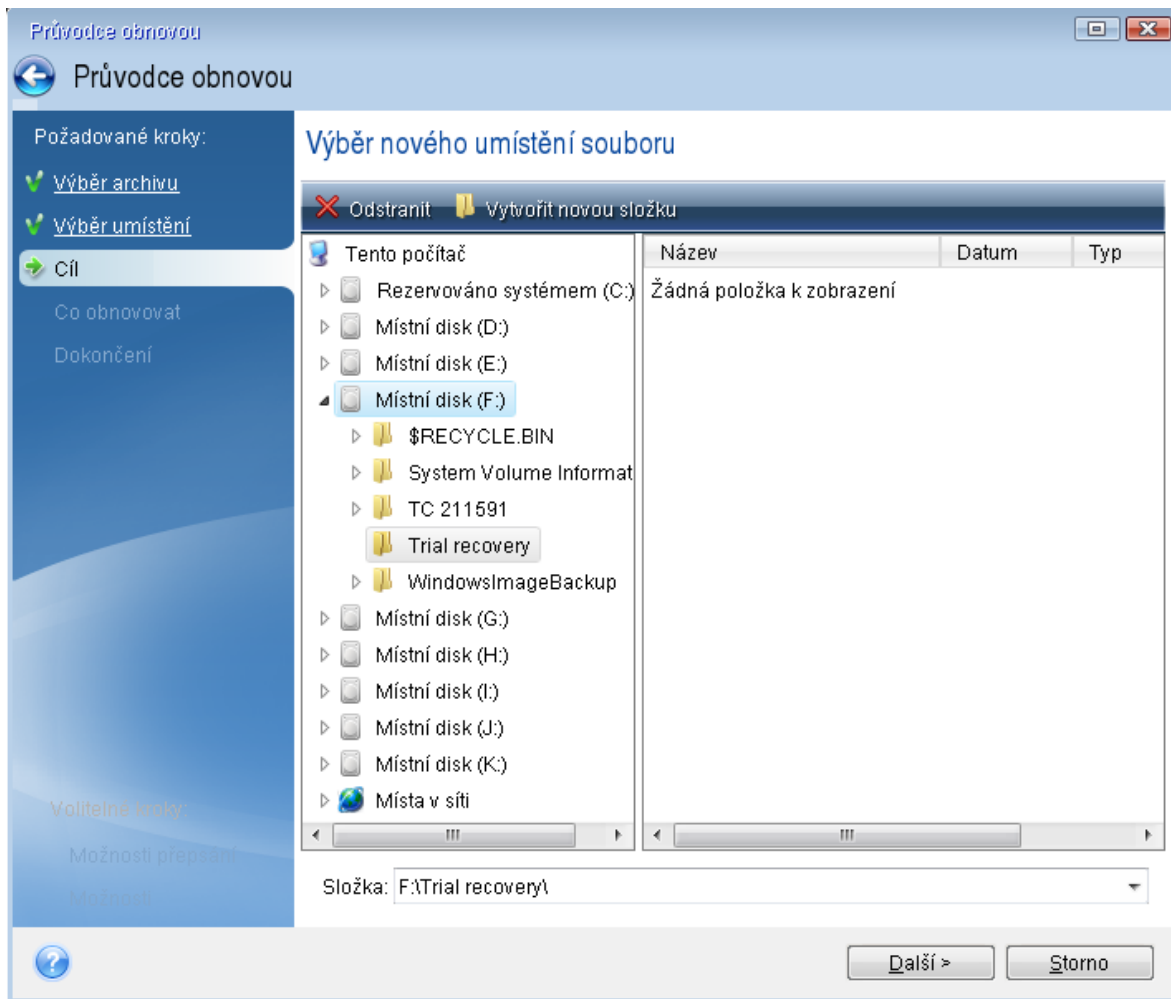
Pokud nejsou v síti viditelné žádné počítače, ale ikona **Síť** se v okně **Tento počítač** zobrazuje, zadejte nastavení sítě ručně. To provedete otevřením okna **Nástroje > Možnosti > Síťové adaptéry**.

---

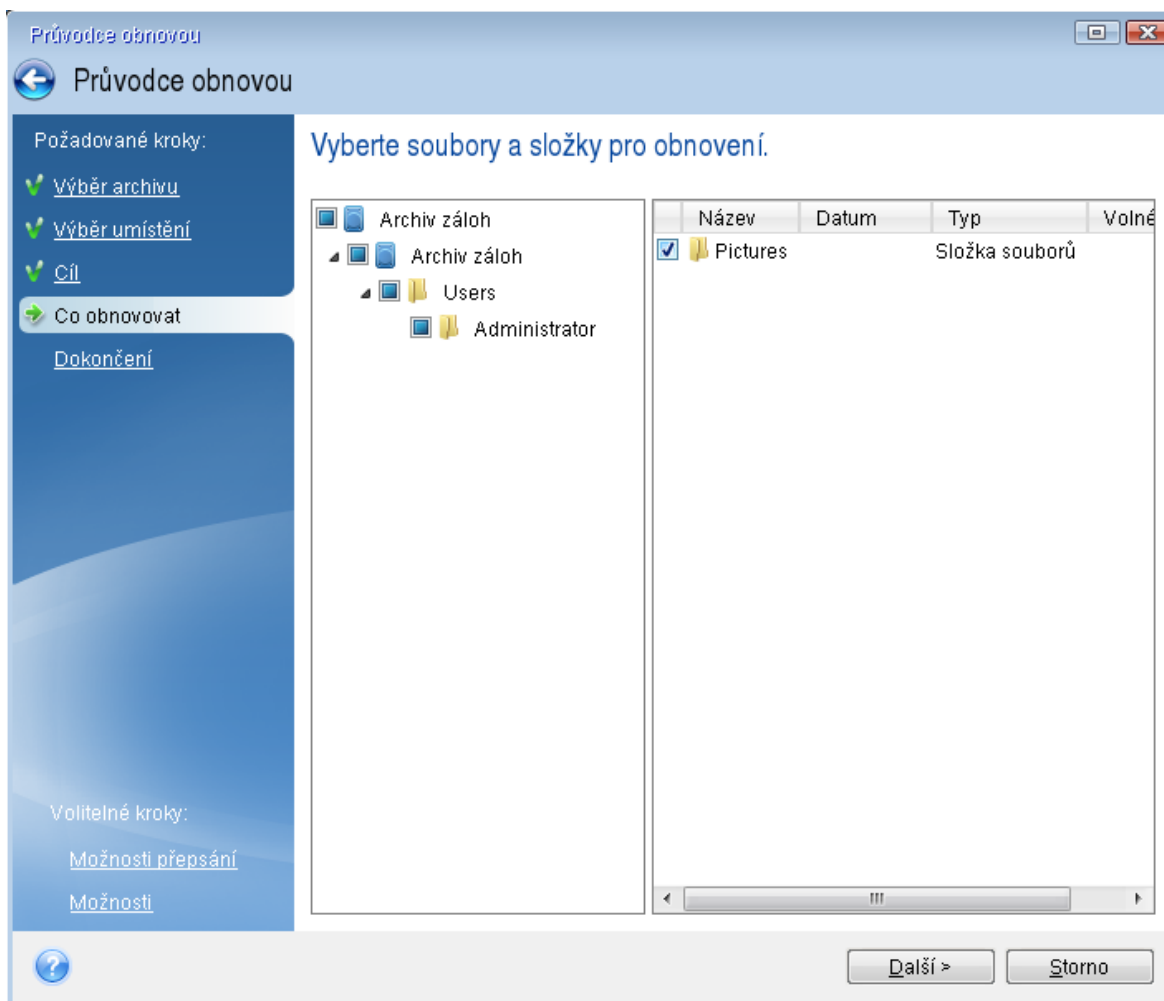
#### **Poznámka**

Pokud není ikona **Síť** v okně **Tento počítač** dostupná, je možná problém se síťovou kartou nebo s jejím ovladačem dodávaným s aplikací Acronis Cyber Protect Home Office.

---



5. Vyberte cílové umístění pro soubory a poté klikněte na tlačítko **Další**.
6. Pomocí zaškrťovacích políček několik souborů pro obnovu vyberte a poté klikněte na tlačítko **Další**.



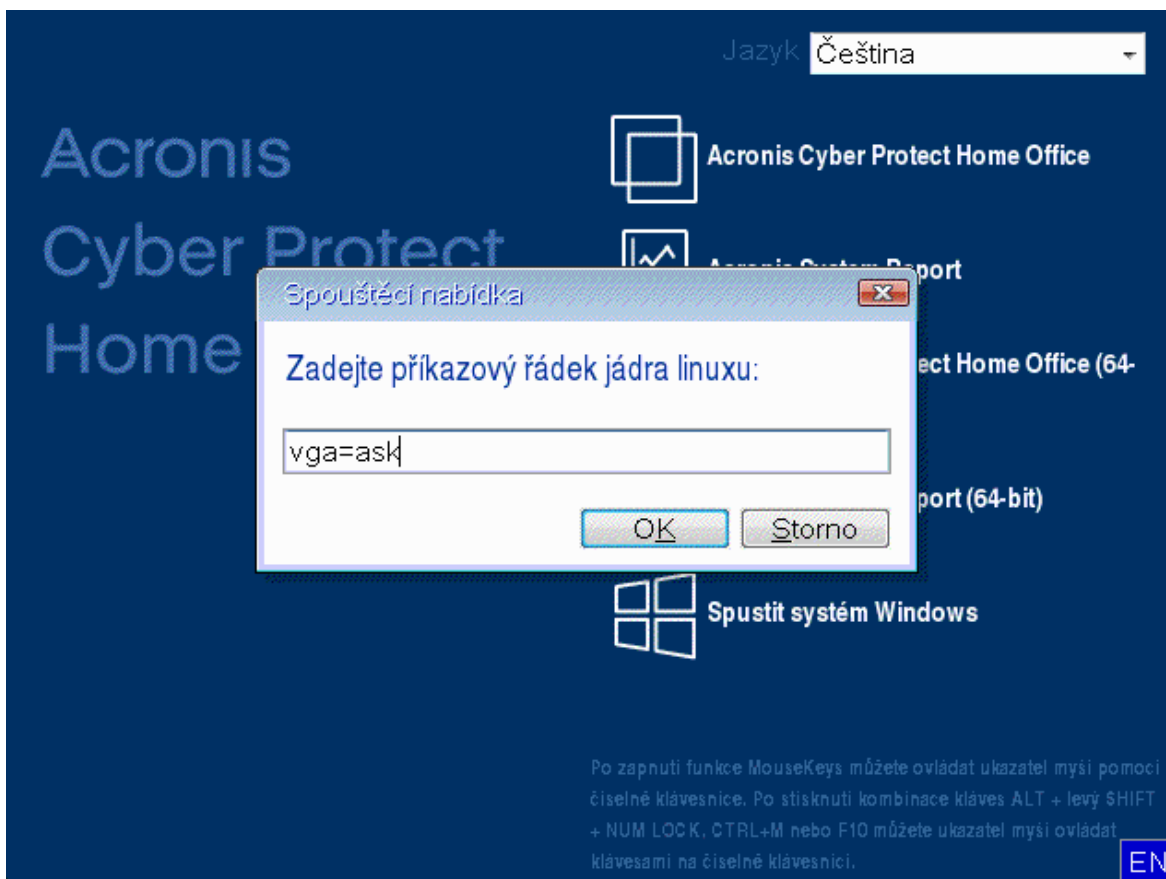
7. Kliknutím na tlačítko **Pokračovat** v okně Shrnutí spustíte obnovu.
8. Po dokončení obnovy ukončete samostatnou verzi aplikace Acronis Cyber Protect Home Office.

Nyní si můžete být jisti, že vám spouštěcí CD v případě potřeby pomůže.

### 12.2.3 Výběr grafického režimu při spouštění ze spouštěcího média

Při spouštění ze spouštěcího média se automaticky vybere optimální grafický režim podle specifikací vaší grafické karty a monitoru. Někdy však aplikace může vybrat nesprávný režim, který není pro váš hardware vhodný. V takovém případě můžete jiný režim vybrat následujícím způsobem:

1. Zahajte spouštění ze spouštěcího média. Po zobrazení spouštěcí nabídky přejedte myší na položku **Acronis Cyber Protect Home Office** a stiskněte klávesu F11.
2. Po zobrazení příkazového řádku zadejte „vga=ask“ (bez uvozovek) a klikněte na tlačítko **OK**.



3. Výběrem možnosti **Acronis Cyber Protect Home Office** ve spouštěcí nabídce bude pokračovat spouštění ze spouštěcího média. Chcete-li zobrazit dostupné grafické režimy, stiskněte při zobrazení příslušné zprávy klávesu Enter.
4. Vyberte režim vhodný pro váš monitor a zadejte jeho číslo na příkazovém řádku. Například zadáním hodnoty 338 vyberete režim 1600×1200×16 (viz obrázek níže).

```

333 1024x768x16 VESA      334 1152x864x16 VESA      335 1280x960x16 VESA
336 1280x1024x16 VESA    337 1400x1050x16 VESA    338 1600x1200x16 VESA
339 1792x1344x16 VESA    33A 1856x1392x16 VESA    33B 1920x1440x16 VESA
33C  320x200x32 VESA     33D  320x400x32 VESA     33E  640x400x32 VESA
33F  640x480x32 VESA     340  800x600x32 VESA     341 1024x768x32 VESA
342 1152x864x32 VESA     343 1280x960x32 VESA     344 1280x1024x32 VESA
345 1400x1050x32 VESA    346 1600x1200x32 VESA    347 1792x1344x32 VESA
348 1856x1392x32 VESA    349 1920x1440x32 VESA    34A 1366x768x8 VESA
34B 1366x768x16 VESA     34C 1366x768x32 VESA     34D 1680x1050x8 VESA
34E 1680x1050x16 VESA    34F 1680x1050x32 VESA    350 1920x1200x8 VESA
351 1920x1200x16 VESA    352 1920x1200x32 VESA    353 2048x1536x8 VESA
354 2048x1536x16 VESA    355 2048x1536x32 VESA    356  320x240x8 VESA
357  320x240x16 VESA     358  320x240x32 VESA     359  400x300x8 VESA
35A  400x300x16 VESA     35B  400x300x32 VESA     35C  512x384x8 VESA
35D  512x384x16 VESA     35E  512x384x32 VESA     35F  854x480x8 VESA
360  854x480x16 VESA     361  854x480x32 VESA     362 1280x720x8 VESA
363 1280x720x16 VESA     364 1280x720x32 VESA     365 1920x1080x8 VESA
366 1920x1080x16 VESA    367 1920x1080x32 VESA    368 1280x800x8 VESA
369 1280x800x16 VESA     36A 1280x800x32 VESA     36B 1440x900x8 VESA
36C 1440x900x16 VESA     36D 1440x900x32 VESA     36E  720x480x8 VESA
36F  720x480x16 VESA     370  720x480x32 VESA     371  720x576x8 VESA
372  720x576x16 VESA     373  720x576x32 VESA     374  800x480x8 VESA
375  800x480x16 VESA     376  800x480x32 VESA     377 1280x768x8 VESA
378 1280x768x16 VESA     379 1280x768x32 VESA
Enter a video mode or "scan" to scan for additional modes: _

```

5. Vyčkejte, dokud se nespustí aplikace Acronis Cyber Protect Home Office a zkontrolujte, zda vám kvalita zobrazení uvítacího okna vyhovuje.

Chcete-li vyzkoušet jiný grafický režim, ukončete aplikaci Acronis Cyber Protect Home Office a opakujte předchozí postup.

Jakmile naleznete pro váš hardware optimální grafický režim, můžete vytvořit nové spouštěcí médium, které jej automaticky vybere.

To provedete spuštěním Tvůrce spouštěcích médií Acronis, výběrem požadovaných součástí média, zadáním čísla režimu s předponou „0x“ (v tomto případě 0x338) na příkazovém řádku v kroku Parametry spuštění spouštěcího média a nakonec vytvořením média obvyklým způsobem.

## 12.3 Acronis Startup Recovery Manager

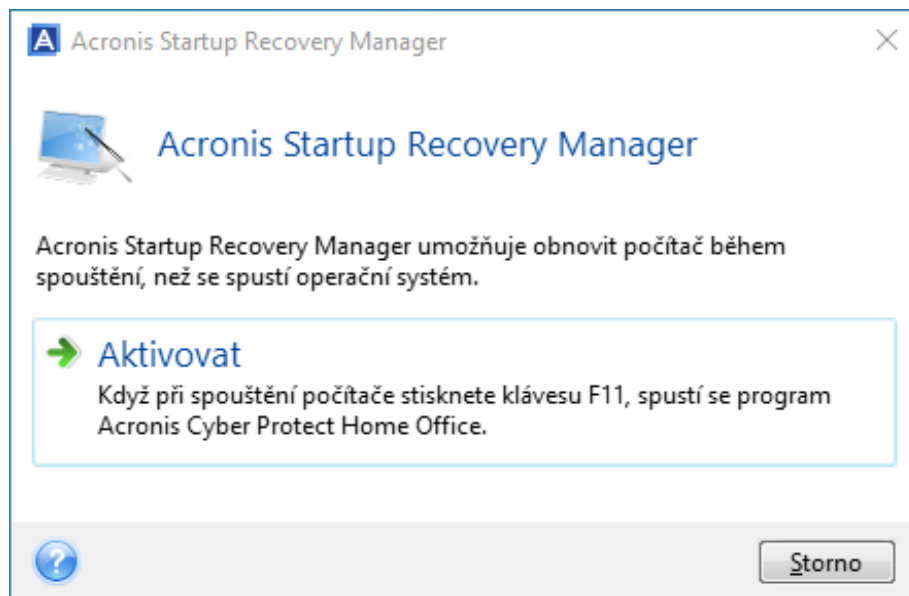
Acronis Startup Recovery Manager umožňuje spustit Acronis Cyber Protect Home Office bez načtení operačního systému. Pomocí této funkce můžete používat aplikaci Acronis Cyber Protect Home Office samostatně k obnovení poškozených diskových oddílů, dokonce i v případě, že operační systém nelze spustit. Na rozdíl od spuštění z vyměnitelného média Acronis nepotřebujete ke spuštění aplikace Acronis Cyber Protect Home Office žádné zvláštní médium ani připojení k síti.

### Poznámka

Správce Acronis Startup Recovery Manager nelze používat v tabletech se systémem Windows.

### **Aktivování aplikace Acronis Startup Recovery Manager**

1. Spustit Acronis Cyber Protect Home Office
2. V části **Nástroje** klikněte na položku **Všechny nástroje** a pak dvakrát klikněte na položku **Aktivovat správce Acronis Startup Recovery Manager**.
3. V zobrazeném okně klikněte na příkaz **Aktivovat**.



Když dojde k selhání, vypněte počítač a jakmile uvidíte zprávu "Stiskem klávesy F11 spustíte Acronis Startup Recovery Manager", stiskněte klávesu F11. Tím spustíte samostatnou verzi aplikace Acronis Cyber Protect Home Office, která se pouze mírně liší od úplné verze.

#### **Deaktivování aplikace Acronis Startup Recovery Manager**

1. Spustit Acronis Cyber Protect Home Office
2. V části **Nástroje** klikněte na položku **Všechny nástroje** a pak dvakrát klikněte na položku **Aktivovat správce Acronis Startup Recovery Manager**.
3. V zobrazeném okně klikněte na příkaz **Deaktivovat**.

### 12.3.1 Další informace

Písmena disků v samostatném programu Acronis Cyber Protect Home Office se mohou občas lišit od písmen přiřazených systémem Windows. Například písmeno D: přiřazený disk v samostatném programu Acronis Cyber Protect Home Office může odpovídat písmenu E: disku ve Windows. Při správné identifikaci disků a diskových oddílů vám mohou pomoci jmenovky disků, informace o velikosti diskových oddílů, systémech souborů, kapacitách disků, výrobcích a oddílech.

Když je spuštěn režim Try&Decide, není možné používat dříve aktivovaný správce Acronis Startup Recovery Manager. Restartování počítače v režimu Try vám umožní znovu používat správce Acronis Startup Recovery Manager.

#### **Má aplikace Acronis Startup Recovery Manager vliv na ostatní zaváděcí programy?**

Když je správce Acronis Startup Recovery Manager aktivován, přepíše hlavní zaváděcí záznam (Master Boot Record - MBR) svým vlastním zaváděcím kódem. Pokud máte nainstalované nějaké správce spouštění (boot managery) od jiných výrobců, budete je muset po aktivaci správce Startup Recovery Manager znovu zapnout. V případě zaváděčů Linuxu (například LiLo a GRUB) byste mohli zvážit jejich instalaci do zaváděcího záznamu kořenového (nebo zaváděcího) diskového oddílu Linuxu místo MBR ještě před aktivací správce Acronis Startup Recovery Manager.

Spouštěcí mechanismus UEFI se liší od mechanismu systému BIOS. Všechny zaváděcí programy operačního systému nebo jiné spouštěcí programy mají svou vlastní spouštěcí proměnnou, která definuje cestu k odpovídajícímu zaváděcímu programu. Všechny zaváděcí programy jsou uloženy ve zvláštním oddílu, který se nazývá systémový oddíl EFI. Když aplikaci Acronis Startup Recovery Manager aktivujete v systému spouštěném z rozhraní UEFI, změní spouštěcí sekvenci tím, že zapíše svou vlastní spouštěcí proměnnou. Tato proměnná se přidá do seznamu ostatních proměnných, aniž by je změnila. Jelikož jsou všechny zaváděcí programy nezávislé a navzájem se neovlivňují, není před nebo po aktivaci aplikace Acronis Startup Recovery Manager třeba nic měnit.

## 12.4 Try&Decide

Když zapnete režim Try&Decide, počítač je v režimu Try. Potom můžete provádět různé potenciálně nebezpečné operace bez starostí o poškození operačního systému, aplikací nebo dat. Když režim Try&Decide vypnete, můžete rozhodnout, zda chcete použít změny v počítači nebo zda je chcete zrušit.

### 12.4.1 Kdy je režim Try&Decide užitečný

Než se pokusíte o následující operace, doporučujeme režim Try&Decide zapnout:

- Změna systémového nastavení, pokud si nejste jisti, jak toto nastavení může počítač ovlivnit.
- Instalace aktualizací systému, ovladačů atd.
- Instalace neznámých aplikací.
- Otevírání e-mailových příloh od neznámých odesílatelů.
- Návštěva internetových stránek, které mohou obsahovat problematický obsah.

---

#### **Poznámka**

Nezapomeňte, že pokud při práci ve zkušebním režimu stáhnete e-mail z poštovního serveru POP, vytvoříte nové soubory nebo upravíte stávající dokumenty a potom se rozhodnete provedené změny zahodit, tyto e-maily, soubory ani změny dokumentů se neuloží. V takovém případě uložte nové soubory a upravené dokumenty například na USB flash disk a před zrušením změn disk odpojte.

---

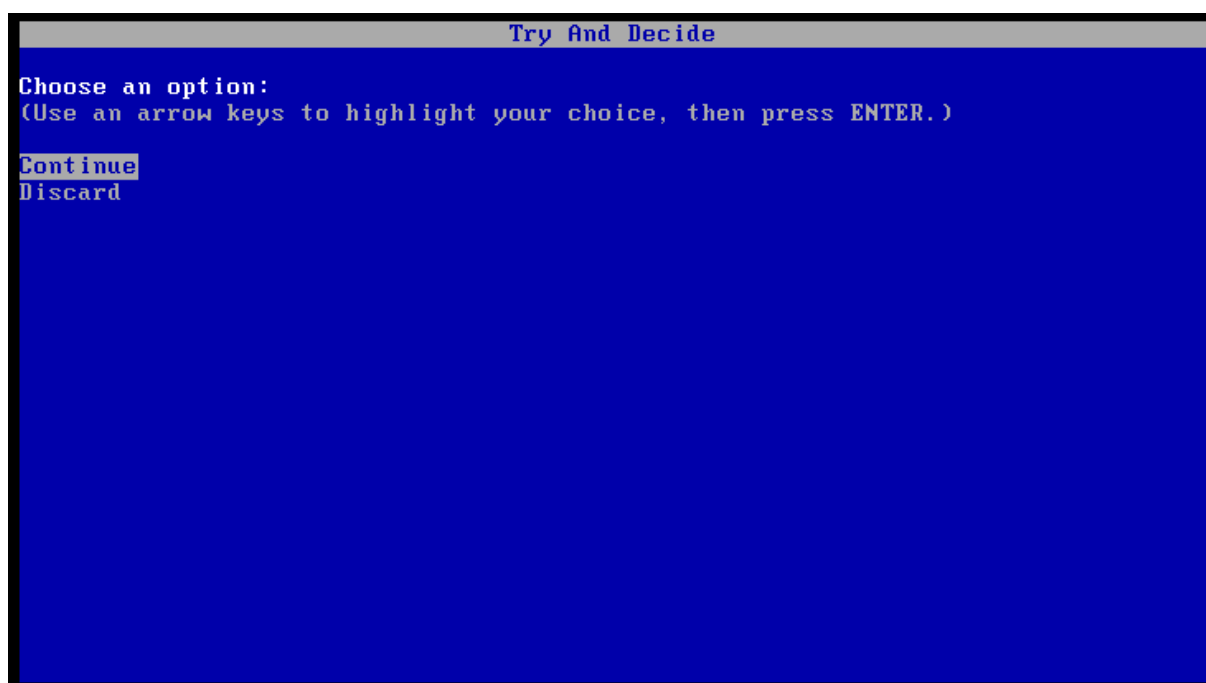


## 12.4.2 Jak režim Try&Decide funguje po restartování počítače

Režim Try&Decide můžete nechat spuštěný, jak dlouho chcete, protože tento režim „přetrvává“ i mezi restartováním operačního systému.

Jestliže se počítač při práci v režimu Try z nějakého důvodu restartuje, zobrazí se před spuštěním operačního systému dialogové okno, kde lze vybrat, zda se má režim zastavit a změny zrušit nebo se má v tomto režimu pokračovat. Tím je umožněno zrušit změny, které způsobily pád systému. Pokud však na druhou stranu provedete restartování například po instalaci aplikace, můžete po spuštění systému Windows pokračovat v práci v režimu Try.

Při každém restartování počítače v režimu Try bude do úložiště vybraného k ukládání virtuálních změn přidáno až 500 MB provozních dat režimu Try&Decide.



## 12.4.3 Omezení při používání režimu Try&Decide

Pokud používáte systém Windows 7, Windows 8 nebo Windows 10, aplikace může v režimu Try poměrně intenzivně využívat volné místo, i když je počítač nečinný. Je tomu tak kvůli aktivitám údržby, například indexování, které je spuštěno na pozadí.

Při práci v režimu Try se výkon systému může snížit. Proces aplikace změn může navíc trvat dlouho, obzvláště pokud necháte režim Try zapnutý na konci dne.

Režim Try&Decide nemůže sledovat změny diskových oddílů, proto v režimu Try není možné provádět virtuální operace s diskovými oddíly, například měnit jejich velikost nebo rozložení. Kromě toho nelze současně používat režim Try&Decide a defragmentaci disku nebo nástroje pro kontrolu chyb na disku, protože tak můžete způsobit neopravitelné poškození systému souborů a znemožnit spuštění systémového disku.

Při spuštění režimu Try není možné používat dříve aktivovaného správce Acronis Startup Recovery Manager. Restartování počítače v režimu Try vám umožní znovu používat správce Acronis Startup Recovery Manager.

Nelze současně používat nonstop zálohování a režim Try&Decide. Spuštěním režimu Try zastavíte nonstop zálohování. Nonstop zálohování se znovu spustí po ukončení režimu Try.

Při spuštění režimu Try není možné používat režim úspory energie Hibernace.

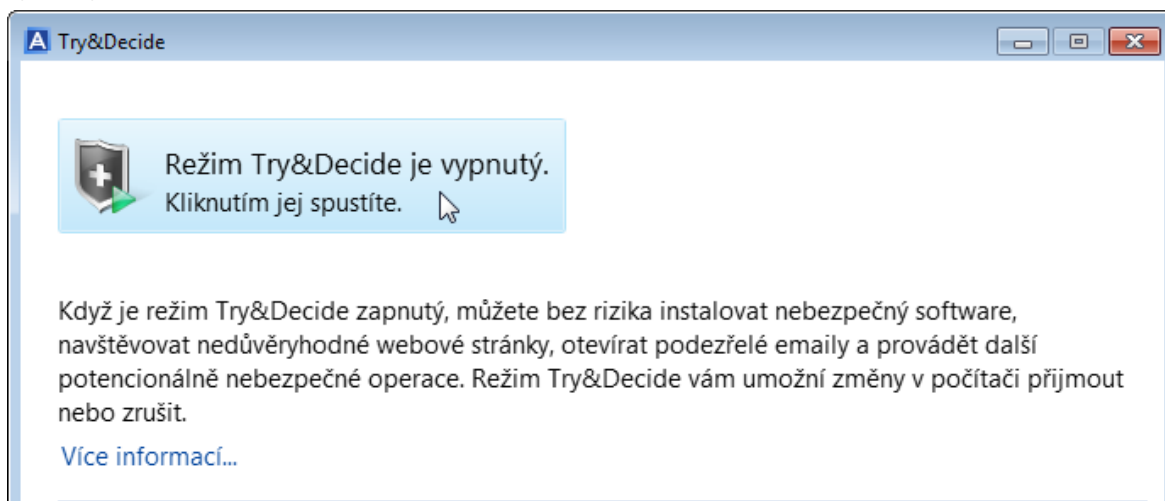
Režim Try&Decide nelze použít k ochraně dynamických disků.

Je-li diskový oddíl systému zašifrovaný nástrojem BitLocker, nemůže režim Try&Decide pracovat.

Režim Try&Decide nedokáže chránit zónu Acronis Secure Zone nebo ji využívat jako úložiště pro virtuální změny.

## 12.4.4 Používání funkce Try&Decide

1. Spustit Acronis Cyber Protect Home Office
2. V části **Nástroje** klikněte na položku **Try&Decide**.
3. V případě nutnosti nastavte možnosti režimu Try&Decide. Další informace naleznete v části [Možnosti a upozornění režimu Try&Decide](#).
4. Zkušební režim spustíte kliknutím na ikonu **Try&Decide**. Aplikace začne sledovat všechny změny provedené v operačním systému a souborech a dočasně bude všechny změny ukládat na vybraný disk.

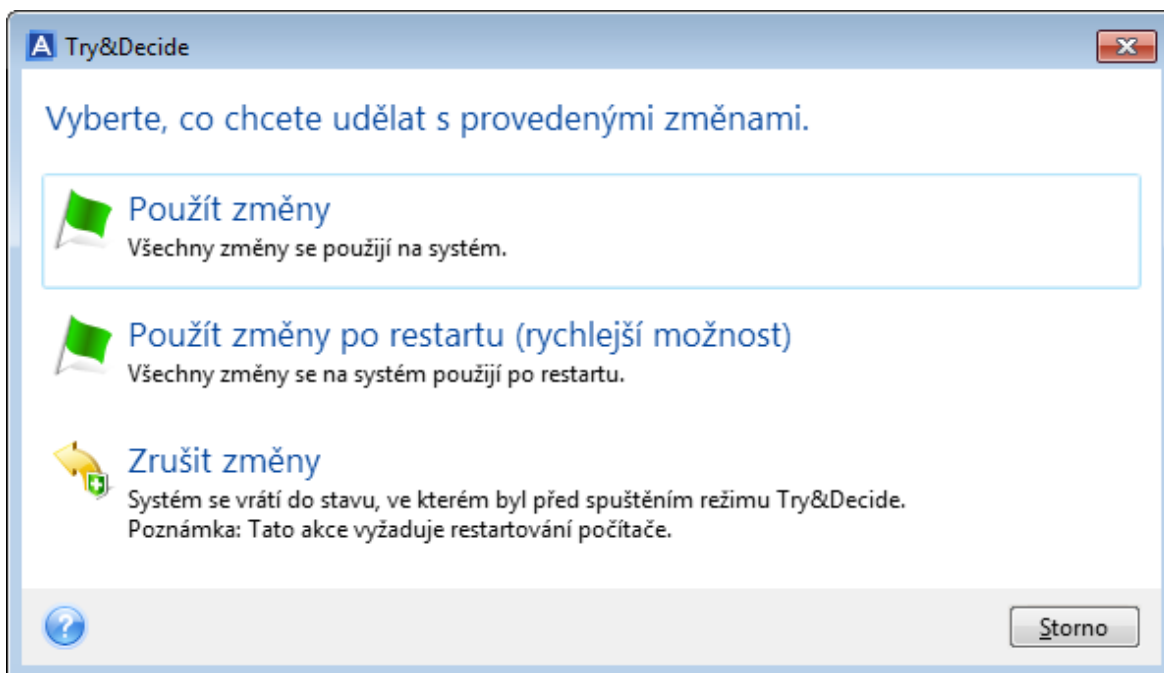


5. Proveďte všechny změny, které jste chtěli vyzkoušet.

### Poznámka

Je-li diskový prostor pro použití změn v umístění vybraném pro ukládání virtuálních změn minimální, aplikace se zeptá, zda má změny použít nebo zrušit. Pokud výstrahu ignorujete, aplikace po zaplnění disku automaticky restartuje systém a změny zruší.

6. Chcete-li ukončit zkušební režim, klikněte v okně Try&Decide na ikonu **Try&Decide**.



7. Vyberte jednu z následujících možností:

- Chcete-li změny provedené v systému zachovat, klikněte na tlačítko **Použít změny**.
- Použití změny můžete urychlit výběrem možnosti **Použít změny po restartu**. Po kliknutí na toto tlačítko režim Try&Decide restartuje počítač a použije změny během zavádění.
- Jestliže chcete vrátit systém do stavu, ve kterém byl před spuštěním zkušebního režimu, vyberte možnost **Zrušit změny**. Když tuto možnost vyberete, zobrazí se vyskakovací okno s následujícími možnostmi: **Restartovat a zahodit změny** a **Nerestartovat**. Když vyberete možnost **Nerestartovat** zůstane režim Try&Decide aktivní a změny se nezruší.

#### Poznámka

Když vyberete možnost **Zrušit změny** a restartujete počítač, na němž je nainstalováno více operačních systémů, nebudete moci zavést jiný operační systém než ten, který byl použitý pro práci v režimu Try. Po druhém restartování se obnoví původní záznam MBR a bude možné zavést i ostatní operační systémy.

## 12.4.5 Možnosti a upozornění režimu Try&Decide

V okně Try&Decide můžete měnit možnosti režimu Try&Decide. Chcete-li obnovit výchozí nastavení, klikněte na tlačítko Obnovit výchozí nastavení.

### Chráněné diskové oddíly

Chcete-li toto nastavení změnit:

1. Klikněte na písmeno diskového oddílu vedle názvu nastavení. Otevře se okno Výběr diskového oddílu.
2. Vyberte diskové oddíly, které chcete chránit, a pak klikněte na tlačítko **OK**.

Při výchozím nastavení chrání režim Try&Decide systémový diskový oddíl (disk C), ale můžete vybrat i jiné diskové oddíly v systému.

## Úložiště pro virtuální změny

Chcete-li toto nastavení změnit:

1. Klikněte na písmeno diskového oddílu vedle názvu nastavení. Otevře se okno Úložiště pro virtuální změny.
2. Vyberte diskový oddíl, který chcete používat jako úložiště pro virtuální změny, a klikněte na tlačítko **OK**.

Ve výchozím nastavení režim Try&Decide ukládá informace na volné místo na disku C.

---

### Poznámka

Při výběru ochrany více diskových oddílů nelze pro ukládání virtuálních změn použít žádný z diskových oddílů, které se mají chránit. Nelze vybrat ani externí pevný disk.

---

## Upozornění

Výchozí nastavení upozornění lze změnit kliknutím na tlačítko **Změnit nastavení upozornění**. Otevře se okno Nastavení.

- Podle zbývajících volných míst na disku – pokud volné místo v úložišti pro virtuální změny klesne pod určenou hodnotu, zobrazí aplikace upozornění.
- Po uplynutí času od spuštění režimu Try&Decide – aplikace vás upozorní v případě, že režim Try&Decide bude spuštěn déle, než bylo zadáno.

## 12.4.6 Try&Decide: typické případy použití

Režim Try&Decide vám může pomoci v různých případech, například:

### Vyzkoušení softwaru

Někdy je užitečné zapnout režim Try před instalací nového softwaru. Doporučujeme jej například zapnout, když chcete provádět následující akce:

- Vybrat antivirový software.  
Jsou známy případy, kdy instalace antivirového softwaru poškodila funkčnost aplikací nebo tyto aplikace nebylo po instalaci antiviru vůbec možné spustit. Můžete otestovat zkušební verzi antivirového softwaru. Jestliže se vyskytnou nějaké problémy, zrušte změny a zkuste antivirový software od jiného výrobce.
- Nainstalovat zkušební verzi aplikace.  
Je také známo, že funkce „Přidat nebo odebrat programy“ v okně Ovládací panely systému Windows nezajistí úplné odstranění odinstalovaných aplikací. Pokud se vám nainstalovaná aplikace nelíbí, zrušte změny v systému. V takovém případě si můžete být jisti, že režim Try&Decide odstraní aplikaci beze stopy.

- Instalovat podezřelý software.  
Nedůvěřujete-li výrobcí softwaru, který chcete instalovat, nebo je-li zdroj softwaru neznámý, zapněte před instalací tohoto softwaru režim Try. Pokud dojde k problémům, zrušte změny provedené v režimu Try.

## Obnova souborů

Omylem jste smazali některé soubory a vysypali koš. Potom jste si vzpomněli, že smazané soubory obsahovaly důležitá data a pokusíte se je pomocí příslušného softwaru obnovit. Někdy však můžete při obnově smazaných souborů něco provést nesprávně a celou situaci ještě zhoršit. Můžete tedy postupovat následovně:

- Zapněte režim Try.
- Spusťte nástroj pro obnovení smazaných souborů.
- Jakmile nástroj projde disk a nalezne záznamy odstraněných souborů nebo složek, zobrazí seznam nalezených položek (pokud jsou) a nabídne vám uložení všeho, co lze obnovit. Vždy je však možnost, že vyberete špatný soubor a při jeho obnově může nástroj přepsat soubor, který jste chtěli obnovit. Bez použití režimu Try&Decide je taková chyba fatální a soubor je pravděpodobně nenávratně ztracen.
- Nyní však můžete změny provedené v režimu Try jednoduše zrušit a po opětovném zapnutí režimu Try můžete zkusit soubory obnovit znovu. Tyto pokusy lze opakovat, dokud nebudete s obnovou souborů dostatečně spokojeni.

## Soukromí v síti

Předpokládejme, že nechcete, aby někdo věděl, které webové servery jste navštívili nebo které stránky jste otevřeli – každý má právo na soukromí. Problémem však je, že systém kvůli usnadnění a urychlení surfování ukládá tyto a další informace: načtené soubory cookie, provedené vyhledávací dotazy, zadané adresy URL atd., zvláště ve skrytých souborech. Takové informace se při odstranění dočasných souborů Internetu, vymazání souborů cookie a historie otevřených stránek pomocí nástrojů prohlížeče neodstraní zcela. Špehové mohou tyto informace zobrazit pomocí speciálního softwaru.

Zapněte režim Try a surfujte na internetu dle libosti. Chcete-li následně odstranit všechny stopy své činnosti, zrušte změny provedené v režimu Try.

## 12.5 Acronis Secure Zone

Acronis Secure Zone je speciální bezpečný oddíl, který si můžete vytvořit v počítači pro ukládání záloh. Acronis Secure Zone používá systém souborů FAT32.

Když vytvoříte zónu Acronis Secure Zone, zobrazí se v Průzkumníku souborů v části **Jiné**. Zónu Acronis Secure Zone můžete procházet jako běžný diskový oddíl.

Pokud je zóna Acronis Secure Zone chráněna heslem, vyžadují všechny operace kromě zobrazení podrobností o verzi zadání hesla.

## 12.5.1 Acronis Vyčištění zóny Secure Zone

Pokud v zóně Acronis Secure Zone není dostatek místa na novou zálohu, můžete:

- Zrušit operaci zálohování, zvětšit velikost zóny Acronis Secure Zone a poté znovu spustit zálohování.
- Zrušit operaci zálohování, ručně odstranit některé zálohy ze zóny Acronis Secure Zone a poté znovu spustit zálohování.
- Potvrďte, že chcete automaticky odstranit nejstarší zálohu stejného typu (na úrovni souborů nebo disku) spolu se všemi přírůstkovými či rozdílovými verzemi. Nebude-li poté k dispozici stále dostatek volného místa, požádá aplikace Acronis Cyber Protect Home Office o potvrzení a odstraní další plnou zálohu. To se bude opakovat, dokud nebude dostatek volného místa pro novou zálohu. Pokud po odstranění všech předchozích záloh stále nebude dostatek místa, zálohování se zruší.

### ***Jak zabránit přeplnění zóny:***

1. Vyberte naplánovanou zálohu.
2. Klikněte na **Možnosti**.
3. Na kartě **Pokročilé** rozbalte část **Zpracování chyb**.
4. Zaškrtněte políčko **Odstranit nejstarší zálohu, pokud není v zóně ASZ dostatek místa**.
5. Klikněte na tlačítko **OK**.

Další informace naleznete v části [Zpracování chyb](#).

V režimu Try nelze použít Acronis Secure Zone jako úložiště změn virtuálního systému. Použitá data budou po ukončení režimu Try&Decide automaticky odstraněna.

Aplikace Acronis Cyber Protect Home Office automaticky neodstraní verze nonstop záloh ze zóny Acronis Secure Zone. Tyto verze lze odstranit pouze ručně. Další informace naleznete v tématu datové úložiště Nonstop zálohování [Acronis](#).

## 12.5.2 Vytváření a řízení Acronis Secure Zone

1. Klikněte na tlačítko **Start** -> **Acronis** (složka produktu) -> **Acronis Secure Zone** .  
Otevře se průvodce Správa zóny Acronis Secure Zone.
2. Provedte jednu z následujících akcí:  
Chcete-li vytvořit zónu Acronis Secure Zone, určete její [umístění](#) a [velikost](#).  
Chcete-li zónu Acronis Secure Zone upravit, vyberte akci:
  - [Zvětšit nebo zmenšit velikost](#)
  - [Odebrat](#)
  - [Změnit heslo](#)

Dále postupujte podle jednotlivých kroků v průvodci.

3. V kroku **Dokončit** klikněte na tlačítko **Pokračovat**.

#### Poznámka

Tato operace může vyžadovat restartování počítače.

## 12.5.3 Umístění zóny Acronis Secure Zone

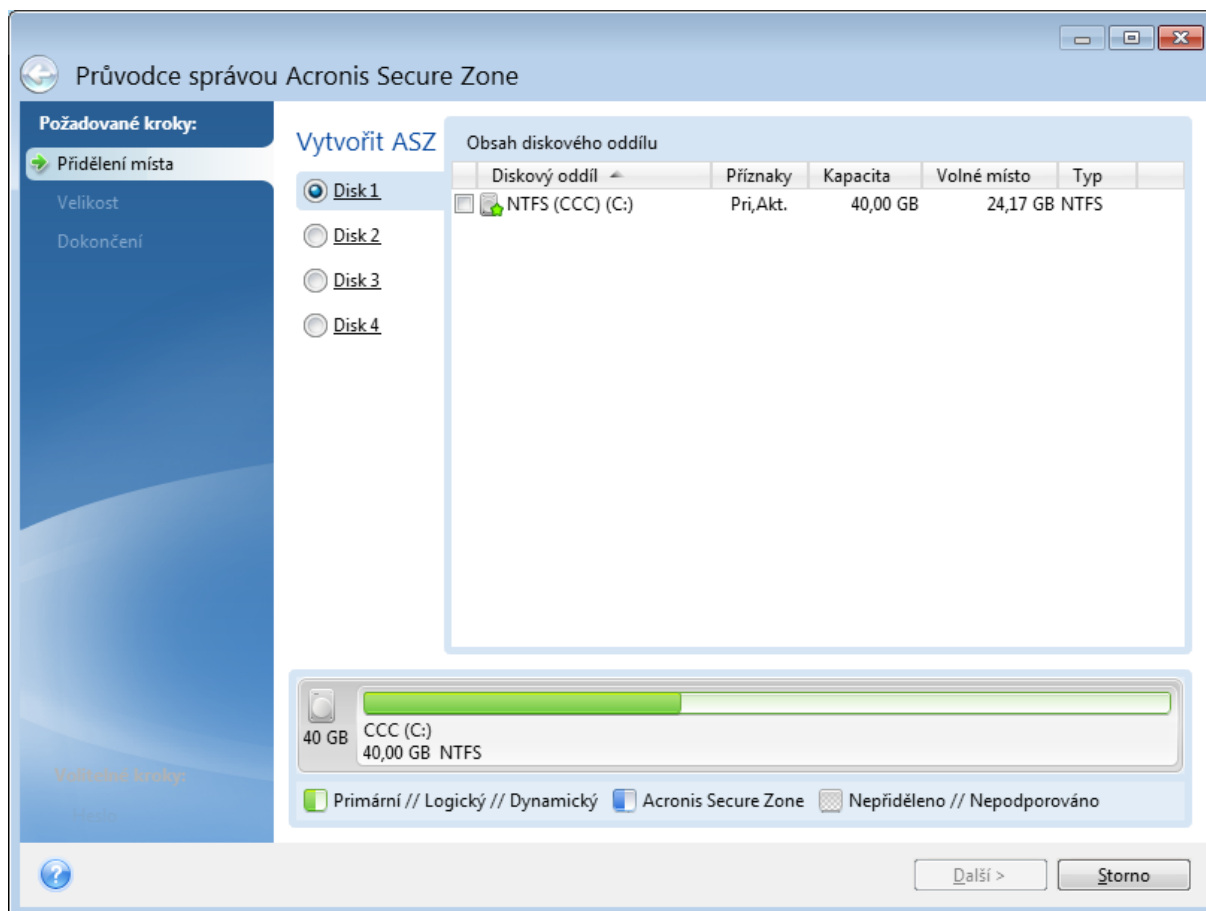
### Jak zadat umístění zóny Acronis Secure Zone

1. Vyberte pevný disk, na kterém chcete zónu Acronis Secure Zone vytvořit.
2. Vyberte jeden nebo více diskových oddílů, ze kterých bude nepřídělené nebo volné místo odebráno. Velikost vybraných diskových oddílů bude podle potřeby změněna, aby se uvolnil prostor pro zónu Acronis Secure Zone.

#### Poznámka

Zónu Acronis Secure Zone nelze vytvořit na dynamických discích a diskových svazcích.

3. Klikněte na tlačítko **Další**.

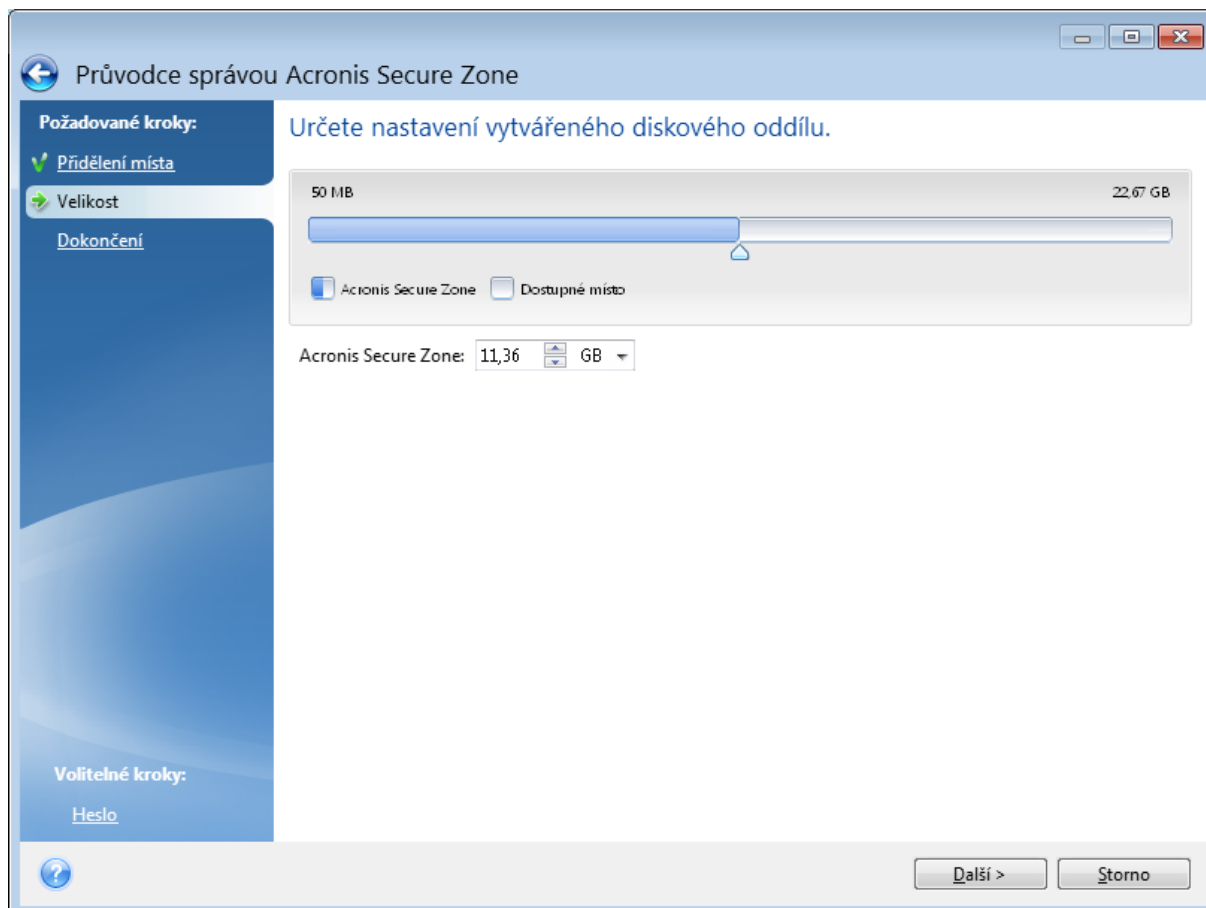


### Jak zvětšit či zmenšit velikost zóny Acronis Secure Zone

1. Vyberte diskové oddíly, jejichž volné místo bude použito ke zvětšení zóny Acronis Secure Zone nebo které získají volné místo po zmenšení zóny Acronis Secure Zone. Je možné vybírat i diskové oddíly s nepřiděleným místem.
2. Klikněte na tlačítko **Další**.

## 12.5.4 Velikost Acronis Secure Zone

Chcete-li zvolit velikost zóny Acronis Secure Zone, přetáhněte posuvník do vhodné pozice nebo zadejte přesnou hodnotu.



Minimální velikost je přibližně 50 MB v závislosti na geometrii pevného disku. Maximální velikost odpovídá volnému místu na disku plus celkovému volnému místu na všech diskových oddílech vybraných v předchozím kroku.

Při tvorbě či zvětšení Acronis Secure Zone využije aplikace nejprve nepřidělené místo. Jestliže není k dosažení požadované velikosti nepřiděleného místa dostatek, budou vybrané diskové oddíly zmenšeny. Změna velikosti diskových oddílů může vyžadovat restartování počítače.

Při zmenšení Acronis Secure Zone se nepřidělené místo, které pevný disk obsahoval, přidělí vybraným diskovým oddílům společně s místem uvolněným z Acronis Secure Zone. Na disku tedy nezbude žádné nepřidělené místo.



## Upozornění!

Zmenšení nebo zvětšení systémového diskového oddílu na minimální velikost může znemožnit spuštění operačního systému.

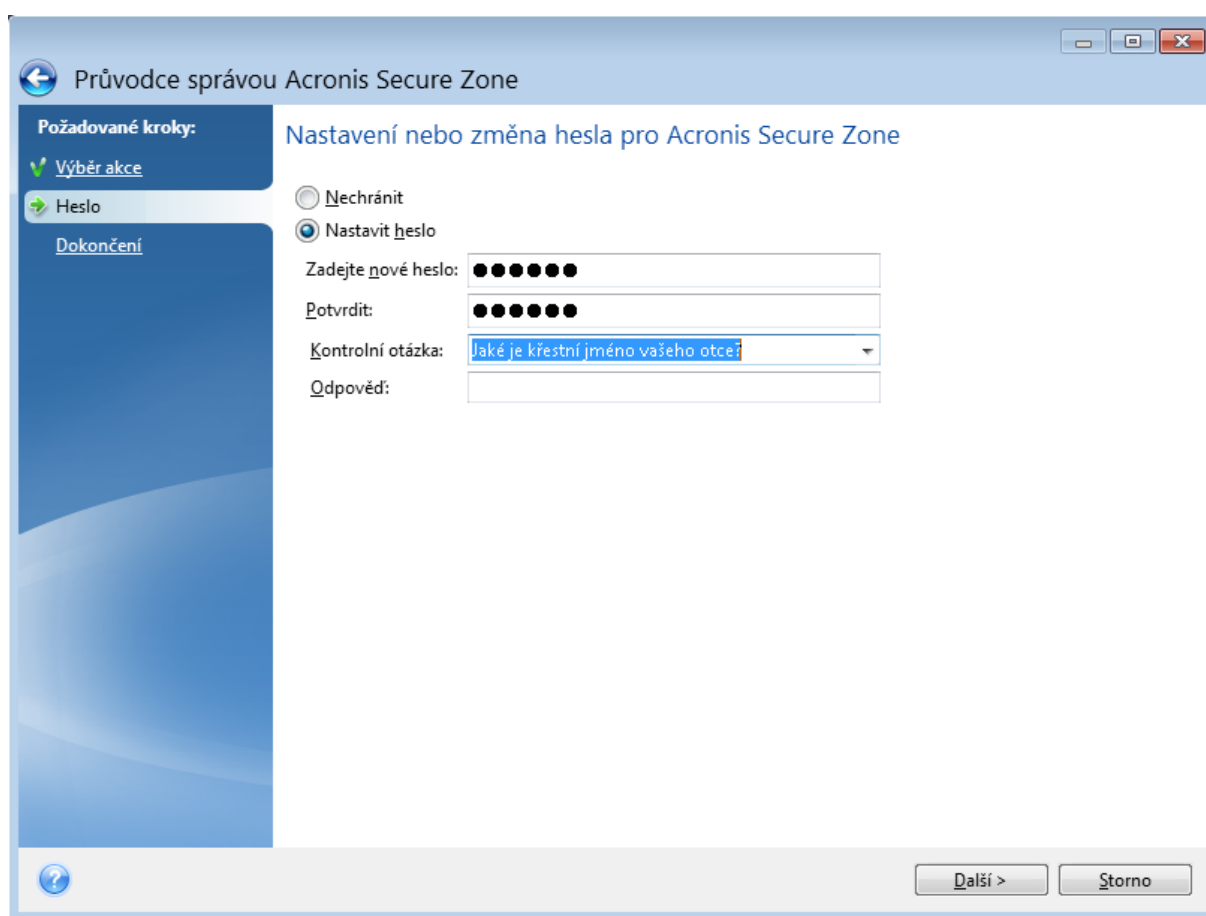
## 12.5.5 Ochrana zóny Acronis Secure Zone

Můžete nastavit heslo pro ochranu zóny Acronis Secure Zone, abyste zabránili neautorizovanému přístupu.

Program si vyžádá heslo u každé operace související se zónou Acronis Secure Zone, například při zálohování a obnově, připojení diskových obrazů nebo ověřování záloh v zóně Acronis Secure Zone, změně velikosti a odstranění zóny Acronis Secure Zone.

### ***Jak nastavit heslo do zóny Acronis Secure Zone***

1. Vyberte možnost **Nastavit heslo**.
2. Do pole **Heslo** zadejte heslo.
3. Do pole **Potvrdit** zadejte stejné heslo znovu.
4. [volitelný krok] Můžete také zvolit kontrolní otázku, na kterou zadáte odpověď v případě, že zapomenete heslo. V seznamu vyberte tajnou otázku a zadejte odpověď na ni.
5. Pokračujte kliknutím na tlačítko **Další**.



The screenshot shows a window titled "Průvodce správou Acronis Secure Zone". On the left, a sidebar lists "Požadované kroky:" with "Výběr akce", "Heslo", and "Dokončení". The main area is titled "Nastavení nebo změna hesla pro Acronis Secure Zone" and contains two radio buttons: "Nechránit" (unselected) and "Nastavit heslo" (selected). Below are four input fields: "Zadejte nové heslo:" (masked with 8 dots), "Potvrdit:" (masked with 8 dots), "Kontrolní otázka:" (a dropdown menu with "Jaké je křestní jméno vašeho otce?" selected), and "Odpověď:" (empty). At the bottom right, there are "Další >" and "Storno" buttons.

---

### Poznámka

Oprava nebo aktualizace programu Acronis Cyber Protect Home Office heslo neovlivní. Pokud je však program odstraněn a znovu nainstalován, zatímco zóna Acronis Secure Zone zůstane na disku, provede se obnovení hesla zóny Acronis Secure Zone.

---

## 12.5.6 Odstraňuje se Acronis

---

### Upozornění!

Acronis Při odstranění Secure Zone se automaticky trvale odstraní všechny zálohy uložené v této zóně.

---

Zvolte si diskové oddíly, k nimž chcete přidat místo, které bude odstraněním Acronis Secure Zone uvolněno. Pokud vyberete více diskových oddílů, místo se rozdělí mezi diskové oddíly úměrně jejich velikosti.

Možnost odebrat zónu Acronis Secure Zone můžete vybrat také při odinstalování aplikace.

## 12.6 Přidání nového pevného disku

Pokud nemáte dost místa pro svá data, můžete buď nahradit starý disk novým s vyšší kapacitou, nebo můžete prostě jen přidat nový disk pro ukládání dat a systém ponechat na starém disku.

### ***Jak přidat nový pevný disk***

1. Vypněte počítač a pak nainstalujte nový disk.
2. Zapněte počítač.
3. Klikněte na tlačítko **Start > Acronis** (složka produktu) > **Přidat nový disk**.
4. Postupujte podle jednotlivých kroků v průvodci.
5. V kroku **Dokončit** se ujistěte, zda nakonfigurované rozložení disku vyhovuje vašim potřebám, a potom klikněte na tlačítko **Pokračovat**.

### 12.6.1 Výběr pevného disku

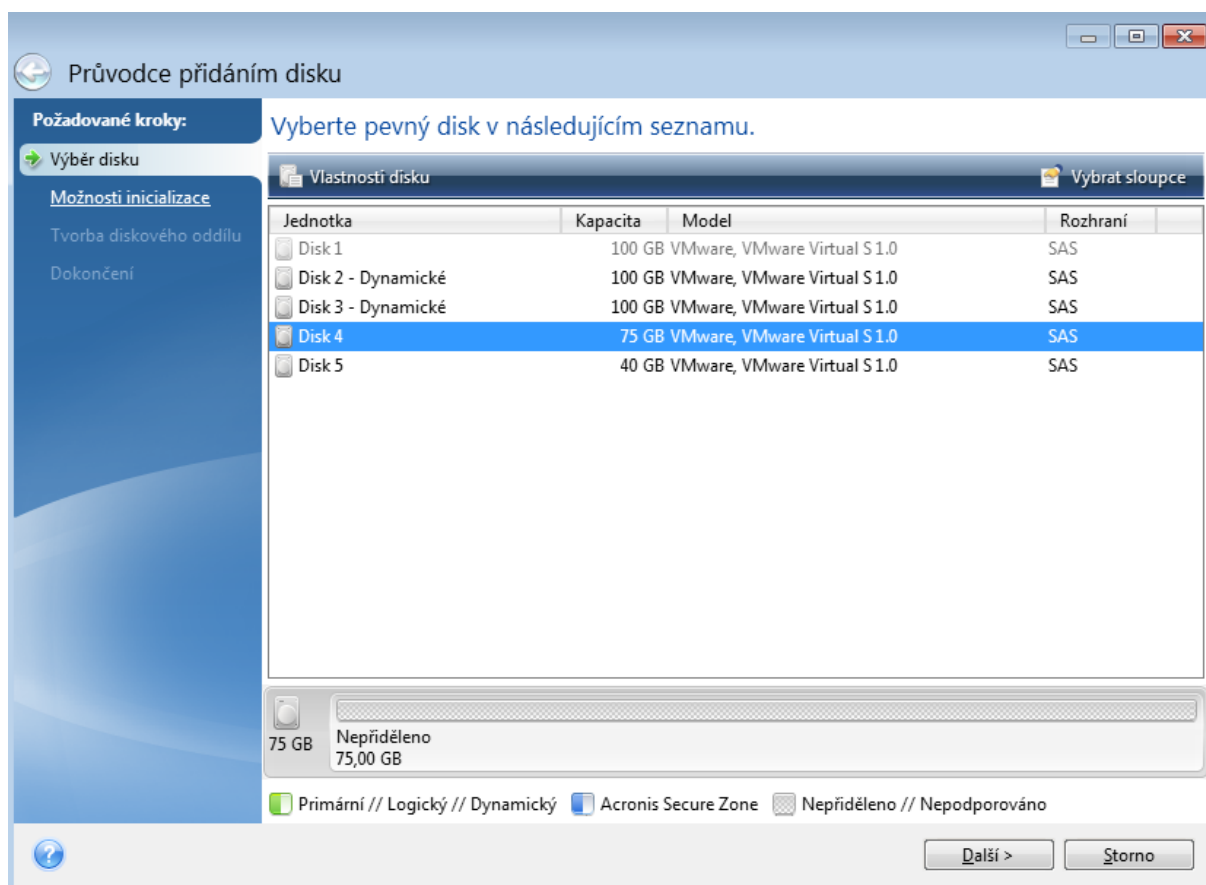
Vyberte si disk, který jste do počítače přidali. Pokud jste přidali více disků, vyberte jeden z nich a klikněte na tlačítko **Další**. Další disky můžete přidat později novým spuštěním průvodce Přidat nový disk.

---

### Poznámka

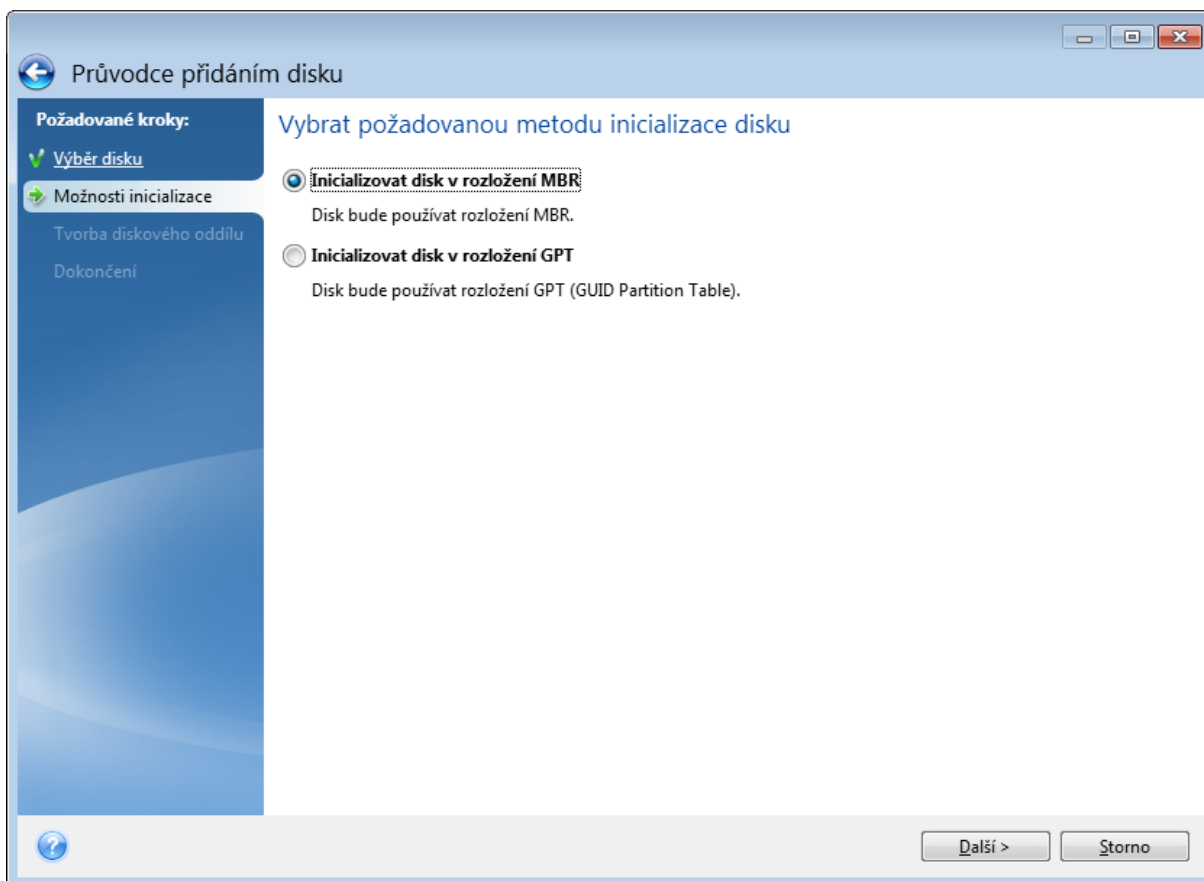
Pokud jsou na novém disku nějaké diskové oddíly, zobrazí aplikace Acronis Cyber Protect Home Office varování, že tyto oddíly budou odstraněny.

---



## 12.6.2 Výběr metody inicializace

Acronis Cyber Protect Home Office podporuje vytváření oddílů MBR i GPT. Tabulka GPT (GUID Partition Table) je nová metoda dělení disků na diskové oddíly, která oproti staré metodě MBR nabízí různé výhody. Pokud operační systém podporuje disky GPT, můžete nový disk inicializovat jako disk GPT.



- Chcete-li přidat disk GPT, klikněte na příkaz **Inicializovat disk v rozložení GPT**.
- Chcete-li přidat disk MBR, klikněte na příkaz **Inicializovat disk v rozložení MBR**.

Po výběru požadované metody inicializace klikněte na tlačítko **Další**.

### 12.6.3 Tvorba diskových oddílů

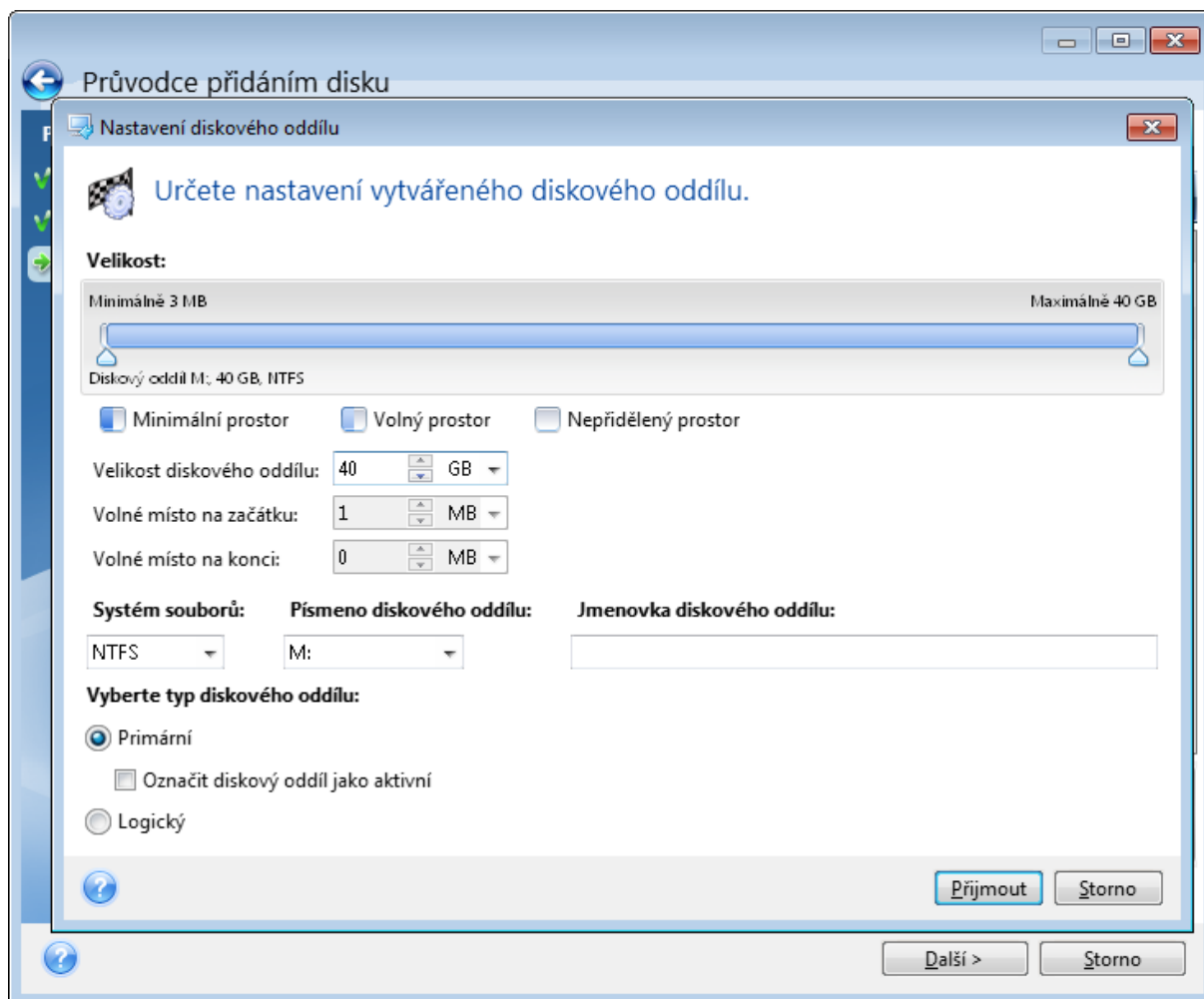
Chcete-li používat místo na pevném disku, je nutné rozdělit jej na oddíly. Tvorba oddílů je proces, při kterém se pevný disk rozdělí na logické části zvané diskové oddíly. Každý diskový oddíl může fungovat jako samostatný disk s přiřazeným písmenem, vlastním systémem souborů atd.

#### ***Jak vytvořit nový diskový oddíl***

1. V kroku průvodce **Vytváření diskového oddílu** vyberte nepřiřazený prostor a klikněte na tlačítko **Vytvořit nový diskový oddíl**.
2. Určete následující nastavení vytvářeného diskového oddílu:
  - Velikost a umístění
  - Systém souborů
  - Typ oddílu (dostupné pouze pro disky MBR)
  - Písmeno a jmenovka diskového oddílu

Další informace naleznete v části [Nastavení diskového oddílu](#).

3. Klikněte na tlačítko **Potvrdit**.



## Nastavení diskového oddílu

### Velikost

#### ***Zvětšit diskový oddíl lze pomocí jednoho z následujících kroků***

- Najedte myší na hranici diskového oddílu. Když se ukazatel změní na oboustrannou šipku, přetažením ukazatele můžete velikost oddílu zvětšit nebo zmenšit.
- Zadejte požadovanou velikost oddílu v poli **Velikost diskového oddílu**.

#### ***Přemístit diskový oddíl lze pomocí jednoho z následujících kroků***

- Přetáhněte diskový oddíl na nové místo.
- Zadejte požadovanou velikost oddílu v poli **Volné místo na začátku** nebo **Volné místo na konci**.

---

## Poznámka

Když vytváříte diskové oddíly, program si před vytvořenými oddíly může vyhradit volný diskový prostor pro potřeby systému.

---

## Systém souborů

Diskový oddíl může zůstat neformátovaný nebo pro něj můžete vybrat jeden z následujících typů systémů souborů:

- **NTFS** je nativní systém souborů pro operační systémy Windows NT, Windows 2000, Windows XP a novější. Vyberte jej, pokud používáte některý z těchto systémů. Nezapomeňte, že systémy Windows 95/98/Me a MS-DOS nemohou mít k diskovým oddílům NTFS přístup.
- **FAT 32** je vylepšená 32bitová verze systému souborů FAT podporující svazky o velikosti až 2 TB.
- **FAT 16** je původní systém souborů DOS. Rozpozná jej většina operačních systémů. Pokud je však disk větší než 4 GB, není možné jej systémem souborů FAT16 naformátovat.
- **Ext2** je původní systém souborů pro Linux. Je dostatečně rychlý, ale nejedná se o žurnálující souborový systém.
- **Ext3** – oficiálně představený s operačním systémem Red hat Linux verze 7.2; Ext3 je žurnálující systém souborů pro Linux. Je zpětně i dopředně kompatibilní se systémem Ext2. Obsahuje několik žurnálujících režimů a širokou meziplatformovou kompatibilitu na 32 i 64bitových architekturách.
- **Ext4** je nový systém souborů pro Linux. Oproti ext3 má určitá vylepšení. Je plně zpětně kompatibilní s ext2 a ext3. Ext3 má nicméně jen částečnou dopřednou kompatibilitu s ext4.
- **ReiserFS** je žurnálující systém souborů pro Linux. Obecně lze říci, že je spolehlivější a rychlejší než Ext2. Tento typ zvolte pro datový diskový oddíl Linuxu.
- **Linux Swap** je odkládací diskový oddíl pro Linux. Vyberte jej, pokud chcete přidat více odkládacího prostoru pro Linux.

## Písmeno diskového oddílu

Vyberte písmeno, které má být přiřazeno diskovému oddílu. Pokud je vybrána možnost **Automaticky**, aplikace přiřadí první nepoužité písmeno v abecedním pořadí.

## Jmenovka diskového oddílu

Jmenovka diskového oddílu je název přiřazený diskovému oddílu, který usnadňuje jeho rozpoznání. Například oddíl s operačním systémem může mít název Systém, diskový oddíl obsahující data může být označen jako Data atd. Název diskového oddílu je volitelný atribut.

## Typ oddílu (tato nastavení jsou dostupná pouze pro disky MBR)

Nový diskový oddíl lze definovat jako primární nebo logický.

- **Primární** – tento parametr vyberte, pokud chcete z tohoto diskového oddílu spouštět systém. V ostatních případech je vhodné vytvořit nový diskový oddíl jako logickou jednotku. Na každé

jednotce mohou být maximálně čtyři primární diskové oddíly nebo tři primární diskové oddíly a jeden rozšířený diskový oddíl.

---

#### **Poznámka**

Jestliže máte několik primárních diskových oddílů, může být aktivní jen jeden, přičemž ostatní primární diskové oddíly se skryjí a operační systém je nevidí.

---

- **Označit diskový oddíl jako aktivní**– toto políčko zaškrtněte, chcete-li na tento diskový oddíl nainstalovat operační systém.
- **Logický**– tento parametr vyberte, pokud na tento diskový oddíl nechcete instalovat a spouštět z něj operační systém. Logická jednotka je část fyzické jednotky disku, která byla rozdělena na oddíly a přidělena jako samostatná jednotka, ale funguje jako samostatný disk.

## 12.7 Nástroje zajišťující bezpečnost a soukromí

### 12.7.1 Acronis DriveCleanser

Nástroj Acronis DriveCleanser umožňuje trvale odstranit všechna data na vybraných pevných discích a diskových oddílech. K tomuto odstranění můžete použít některý z předdefinovaných algoritmů, nebo vytvořit algoritmus vlastní. Další informace naleznete v tématu [Výběr algoritmu](#).

#### Proč tuto funkci potřebuji?

Když naformátujete starý pevný disk, abyste ho poté vyřadili, informace se neodstraní trvale a lze je ještě získat. Vaše osobní údaje takto mohou skončit v nesprávných rukou. Abyste tomu zabránili, doporučujeme použít nástroj Acronis DriveCleanser v případech, kdy:

- Měníte starý pevný disk za nový a nemáte v úmyslu starý disk dále používat.
- Dáte starý pevný disk příbuznému nebo kamarádovi.
- Starý disk prodáváte.

#### Jak používat nástroj Acronis DriveCleanser

##### ***Jak trvale odstranit data z disku***

1. Klikněte na tlačítko **Start** → **Acronis** (složka produktu) → **AcronisDriveCleanser**.  
Spustí se průvodce nástrojem Acronis DriveCleanser.
2. V kroku **Výběr zdroje** vyberte disky a diskové oddíly, které chcete vymazat. Další informace naleznete v tématu [Výběr zdroje](#).
3. V kroku **Výběr algoritmu** vyberte algoritmus, který chcete k odstranění dat použít. Další informace naleznete v tématu [Výběr algoritmu](#).
4. [volitelný krok] Můžete si vytvořit vlastní algoritmus. Další informace naleznete v tématu [Tvorba vlastního algoritmu](#).

5. [volitelný krok] V kroku **Operace po odstranění dat** vyberte, co se má stát s diskovými oddíly a diskem, až budou data trvale odstraněna. Další informace naleznete v tématu [Operace po odstranění dat](#).
6. V kroku **Dokončit** se ujistěte, že je nakonfigurované nastavení správné. Abyste proces spustili, zaškrtněte políčko **Nevratně vymazat vybrané diskové oddíly** a klikněte na tlačítko **Pokračovat**.

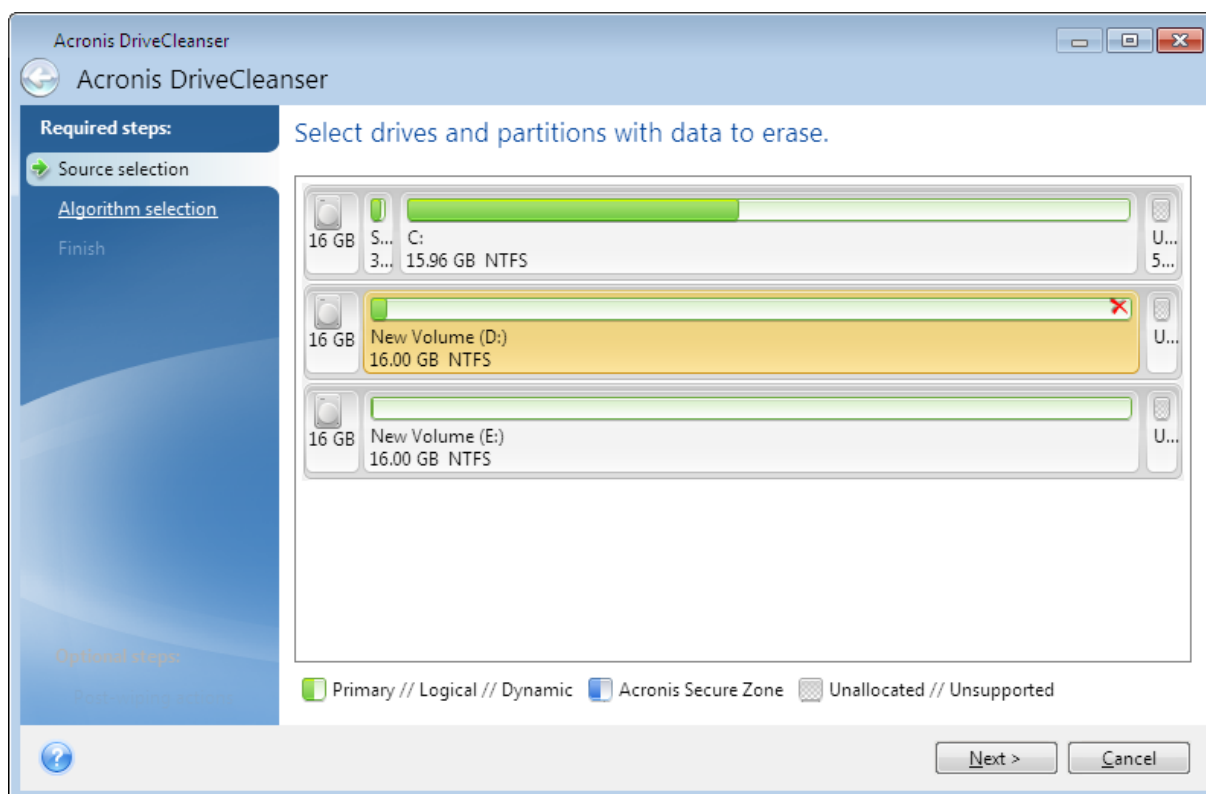
### Upozornění!

Uvědomte si, že v závislosti na celkové velikosti vybraných oddílů a algoritmu k odstranění dat může odstranění dat zabrat mnoho hodin.

## Výběr zdroje

V kroku **Výběr zdroje** vyberte diskové oddíly a disky, na kterých chcete trvale odstranit data:

- Chcete-li diskové oddíly vybrat, klikněte na příslušné obdélníky. Červená značka (✗) znázorňuje, že byl diskový oddíl vybrán.
- Chcete-li vybrat celý pevný disk, klikněte na ikonu disku (📀).



### Poznámka

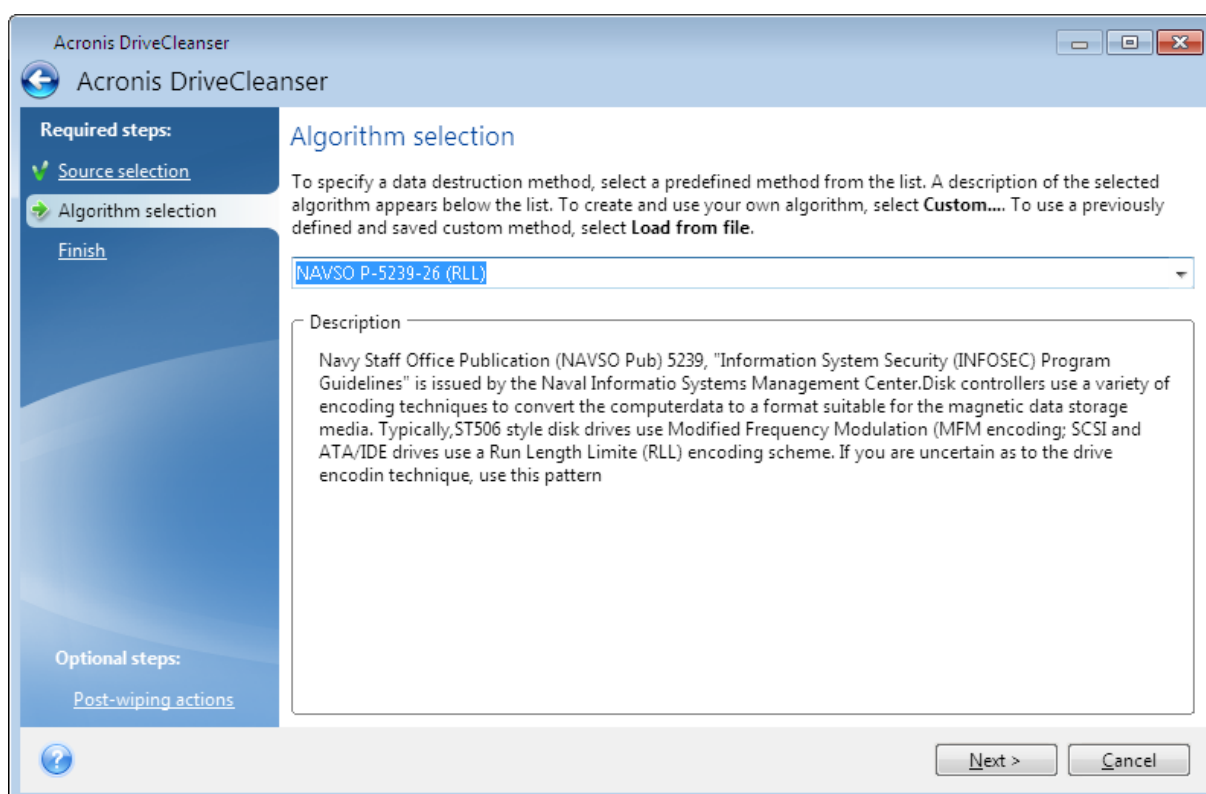
Pomocí nástroje Acronis DriveCleanser nelze vymazat diskový oddíl na dynamických discích nebo discích typu GPT, proto se nezobrazí.



## Výběr algoritmu

V kroku **Výběr algoritmu** proveďte jednu z následujících akcí:

- Chcete-li použít jeden z předdefinovaných algoritmů, vyberte požadovaný algoritmus. Další informace naleznete v části [Metody trvalého odstranění dat z pevného disku](#).
- [Pouze pro zkušené uživatele] Chcete-li vytvořit vlastní algoritmus, vyberte možnost **Vlastní**. V jeho tvorbě dále pokračujte v kroku **Definice algoritmu**. Vytvořený algoritmus poté budete moci uložit do souboru s příponou ALG.
- Chcete-li použít dříve uložený vlastní algoritmus, vyberte možnost **Načíst ze souboru** a poté vyberte soubor, který obsahuje váš algoritmus.



## Tvorba vlastních algoritmů

### Definice algoritmu

Krok **Definice algoritmu** nabízí šablonu pro váš algoritmus.

Tabulka má následující legendu:

- První sloupec obsahuje typ operace (zápis symbolu na disk a ověření zapsaných dat).
- Druhý sloupec obsahuje vzor dat k zápisu na disk.

Každý řádek určuje operaci, která bude provedena během průchodu. Chcete-li vytvořit algoritmus, přidejte do tabulky tolik řádků, kolik podle vás bude dostačovat k bezpečnému trvalému odstranění dat.

### **Jak přidat nový průchod**

1. Klikněte na tlačítko **Add** (Přidat). Otevře se okno Upřesnění průchodů mazání.

**Upřesnění průchodu mazání**

Změňte parametry průchodu vlastního algoritmu.

**Zapisovaný vzorek:**  
Veškerá data budou přepsána zvoleným vzorkem. Vyberte prosím vzorek.

**Zápis náhodného čísla. Délka náhodného čísla:**  
Bude generována náhodná hodnota. Veškerá data budou poté přepsána tímto číslem. Vyberte prosím počet bajtů v náhodném čísle. Délka náhodné hodnoty se může pohybovat od 1 do 512 bajtů.

**Přidat ke vzoru z předchozího průchodu**  
Vyberte tuto operaci, pokud si přejete aby Acronis Cyber Protect Home Office vypočítal komplementární hodnoty k zadanému vzorku. Data budou přepsána nově vytvořeným obrazcem.

**Ověřit**  
Vyberte tuto operaci, pokud si přejete předchozí zapsanou hodnotu ověřit.

2. Vyberte možnost:

- **Zapisovaný vzorek**

Zadejte hexadecimální hodnotu, například hodnotu tohoto typu: 0x00, 0xAA nebo 0xCD atd. Tyto hodnoty mají délku 1 bajt, ale mohou být dlouhé až 512 bajtů. Kromě takových hodnot můžete zadat libovolnou hexadecimální hodnotu libovolné délky (až 512 bajtů).

---

#### **Poznámka**

Pokud je binární hodnota zapsána sekvencí 10001010 (0x8A), doplňková binární hodnota bude zapsána jako sekvence 01110101 (0x75).

---

- **Zapište náhodné číslo.**

Určete délku náhodné hodnoty v bajtech.

- **Přidat ke vzoru z předchozího průchodu**

Aplikace Acronis Cyber Protect Home Office přidá doplňkovou hodnotu k hodnotě zapsané na disk v předchozím průchodu.

- **Ověřit**

Aplikace Acronis Cyber Protect Home Office ověří hodnoty zapsané na disk v předchozím průchodu.

3. Klikněte na tlačítko **OK**.

### ***Jak upravit existující průchod***

1. Vyberte odpovídající řádek a klikněte na tlačítko **Upravit**.

Otevře se okno Upřesnění průchodů mazání.

---

#### **Poznámka**

Vyberete-li několik řádků, bude nové nastavení použito na všechny vybrané průchody.

---

2. Změňte nastavení a klikněte na tlačítko **OK**.

### **Uložení algoritmu souboru**

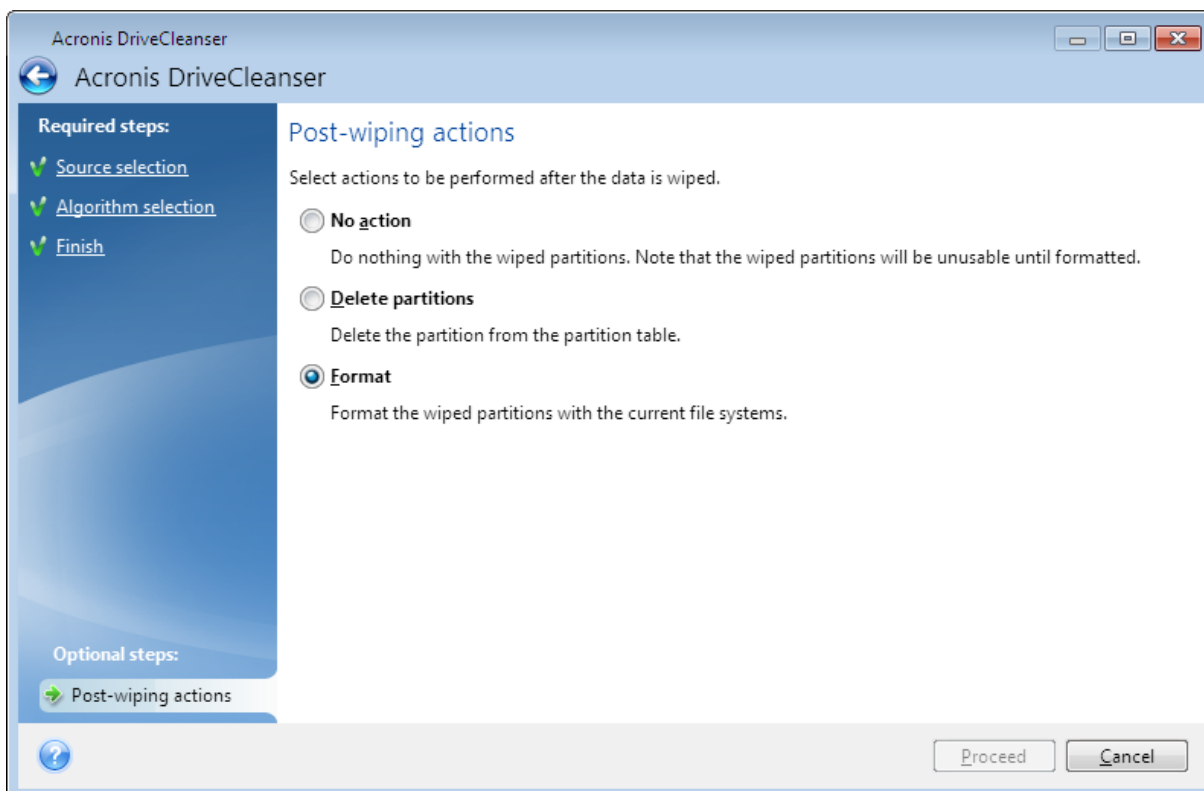
1. V kroku **Uložení vlastního algoritmu** vyberte možnost **Uložit do souboru** a potom klikněte na tlačítko **Další**.

2. V okně, které se otevře, zadejte název a umístění souboru a pak klikněte na tlačítko **OK**.

### **Operace po odstranění dat**

V okně Operace po odstranění dat můžete vybrat akce, které se provedou na diskových oddílech vybraných k trvalému odstranění dat. AcronisDriveCleanser nabízí tři možnosti:

- **Žádná operace**– pouze odstraní data pomocí vybraného algoritmu.
- **Odstranit diskové oddíly**– trvale odstraní data a potom odstraní diskový oddíl.
- **Formátovat**– odstraní data a zformátuje diskový oddíl (výchozí).



## 12.7.2 Vyčištění systému

Průvodce vyčištěním systému umožňuje bezpečně odstranit všechny stopy akcí počítače, což zahrnuje uživatelská jména, hesla a další osobní údaje.

Můžete provádět následující operace:

- bezpečně odstranit data z **koše systému Windows**;
- odebrat **dočasné soubory** z příslušných složek systému Windows;
- vyčistit **volné místo na pevném disku** od všech stop informací, které tam dříve byly uloženy;
- odstranit stopy po **hledání souborů a počítačů** na připojených discích a počítačích v místní síti;
- vymazat seznam **naposledy použitých dokumentů**;
- vymazat seznam **spouštění systému Windows**;
- vymazat historii **otevřených a uložených souborů**;
- vymazat seznam míst v síti, ke kterým se uživatel připojil pomocí **síťových pověření**;
- vymazat **adresář Prefetch systému Windows**, do kterého se ukládají informace o naposledy spuštěných aplikacích.

---

### Poznámka

Operační systémy Windows 7 a novější neukládají informace o vyhledávání souborů a počítačů. Informace o otevřených či uložených souborech se navíc v registru ukládají jinak, a proto je průvodce zobrazuje jiným způsobem.

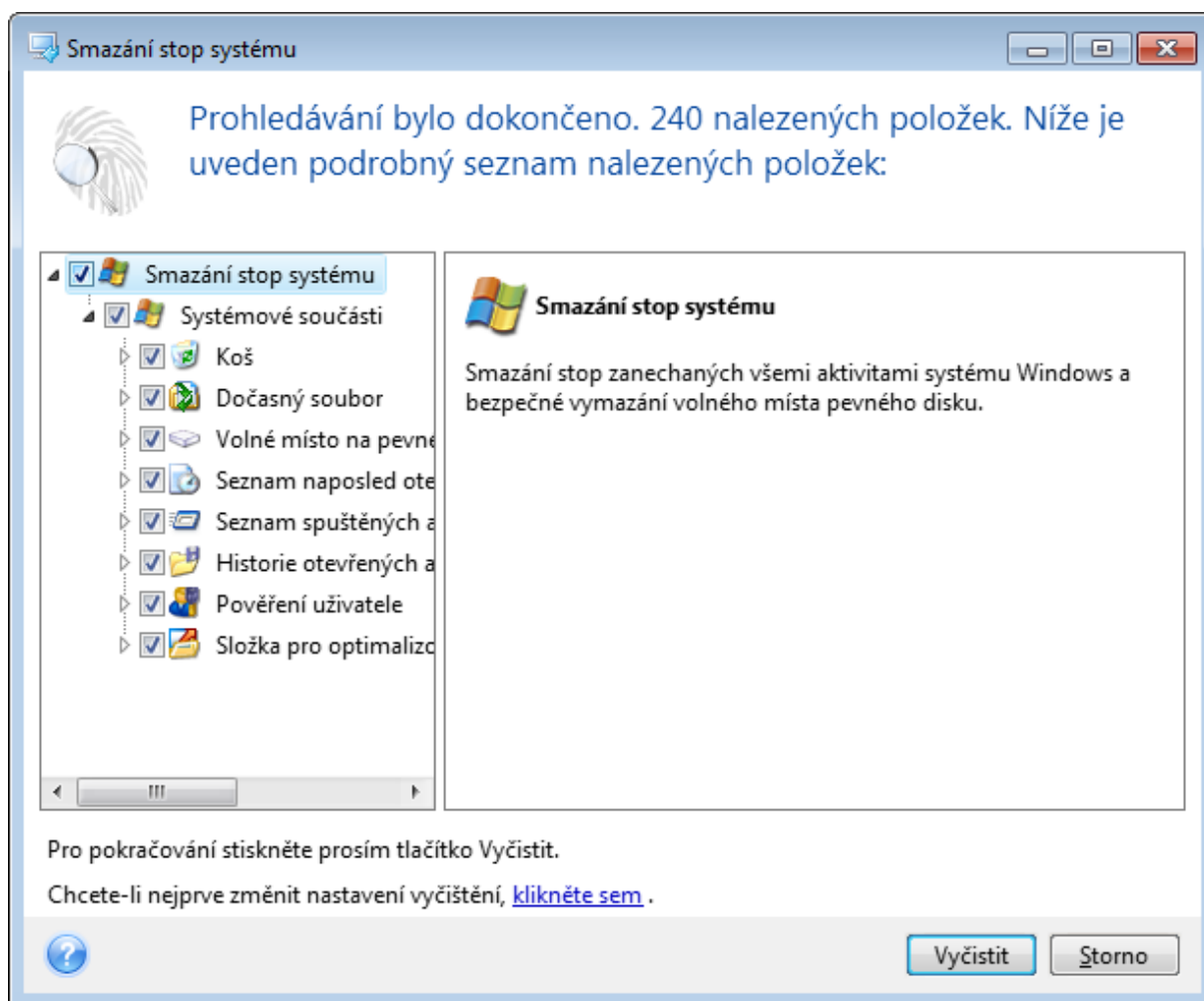
---

## Poznámka

Je nutné si uvědomit, že systém Windows ukládá hesla do konce relace; smazání seznamu pověření uživatelů se tedy neprojeví, dokud aktuální relaci systému Windows neukončíte odhlášením nebo restartováním počítače.

Chcete-li spustit průvodce vyčištěním systému, klikněte na tlačítko **Start** -> **Acronis** (složka produktu) -> **Vyčištění systému**.

Po spuštění průvodce vyhledá všechny stopy uživatelských akcí uložené systémem Windows. Po dokončení vyhledávání se výsledky zobrazí v horní části okna průvodce.



Výsledky si můžete prohlédnout a ručně vybrat položky, které chcete odstranit.

Chcete-li nejprve změnit nastavení vyčištění, klikněte na hypertextový odkaz **Klikněte sem**.

Kliknutím na možnost **Vyčistit** spustíte odstraňování nalezených položek.

## Nastavení vyčištění

V okně možností vyčištění lze změnit nastavení vyčištění pro každou součást systému. Některé parametry se vztahují na všechny součásti.

### **Chcete-li změnit nastavení mazání pro součást:**

- Rozbalte položku **Systémové součásti** ve stromu a vyberte nastavení vyčištění součástí, která chcete změnit. Můžete zapnout nebo vypnout kontrolu součástí průvodcem vyčištěním systému. Provedete to pomocí políčka **Zapnout**.  
Podle potřeby můžete také rozbalit součást a upravit požadovanou metodu smazání dat, vybrat soubory ke vyčištění, vyčistit vyhledávací řetězce v registru, pomocí kterých jste hledali počítače v místní síti atd. Provedete to kliknutím na trojúhelník u součásti, výběrem možnosti v seznamu a určením nastavení.
- Po nastavení požadovaných vlastností součástí klepněte na tlačítko **OK** a nastavení uložte. Toto nastavení se při příštím spuštění průvodce vyčištěním systému použije jako výchozí.

Pokud jste výchozí nastavení vyčištění již měnili, můžete se pomocí tlačítka **Obnovit výchozí** kdykoliv vrátit k výchozím hodnotám aplikace.

### **Systémové součásti:**

- Koš
- Dočasné soubory
- volné místo na disku,
- seznam hledaných počítačů,
- seznam hledaných souborů,
- seznam naposledy otevřených dokumentů,
- Seznam spuštění Windows
- historie otevřených a uložených souborů,
- Přihlašovací údaje uživatele
- Složka pro optimalizované spouštění v systému Windows

## Výchozí možnosti vyčištění

Výchozí možnosti vyčištění jsou dostupné kliknutím na odkaz **Toto nastavení změňte kliknutím** na stránce **Metoda trvalého odstranění dat**.

### **Jak změnit výchozí možnosti vyčištění**

1. Ve stromovém zobrazení vyberte nastavení součásti k vyčištění, které chcete změnit.
2. Potom nastavení uložte kliknutím na tlačítko **OK**.

Pokud jste výchozí nastavení vyčištění již měnili, můžete se pomocí tlačítka **Obnovit výchozí** kdykoliv vrátit k výchozím hodnotám aplikace.

## Obecné

Při výchozím nastavení se dialogové okno souhrnu zobrazí po skončení každého procesu vyčištění (políčko **Zobrazit shrnutí** je zaškrtnuto). Pokud toto okno nechcete zobrazovat, zrušte zaškrtnutí

políčka.

## Možnosti vyčištění

Nástroj Vyčištění systému obsahuje mnoho neznámějších metod k trvalému odstranění dat. Zde můžete vybrat běžnou metodu trvalého odstranění dat, která se bude používat jako výchozí pro všechny součásti.

Metody pro trvalé odstranění dat jsou popsány v této příručce podrobně v tématu [Metody trvalého odstranění dat z pevného disku](#).

## Specifické možnosti smazání stop

Následující možnosti smazání stop lze přizpůsobit:

- Metoda trvalého odstranění dat
- Výchozí možnosti
- Soubory
- Volné místo na disku
- Počítače
- Příkazy
- Filtr míst v síti

## Metoda trvalého odstranění dat

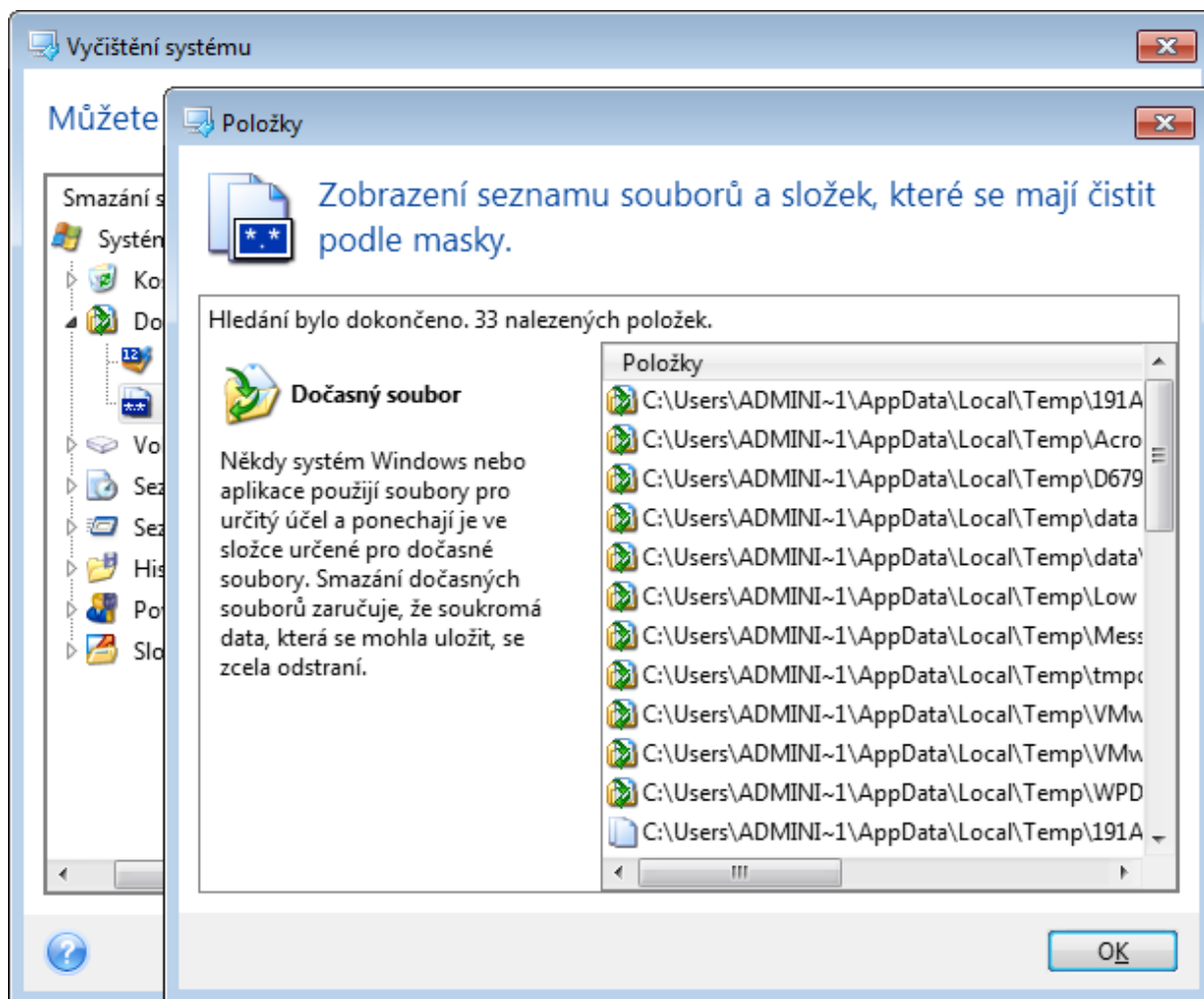
Nástroj Vyčištění systému obsahuje mnoho neznámějších metod k trvalému odstranění dat. Zde je nutné vybrat požadovanou metodu trvalého odstranění dat.

- **Použít běžnou metodu**– pokud necháte toto políčko zaškrtnuté, použije aplikace výchozí metodu (počáteční nastavení je Rychlá metoda).  
Chcete-li jako výchozí nastavit jinou metodu trvalého odstranění dat, klikněte na příslušný odkaz.
- **Použít pro tuto součást vlastní metodu**– po výběru této možnosti můžete vybrat v rozevíracím seznamu jednu z přednastavených metod trvalého odstranění dat.

Metody pro trvalé odstranění dat jsou popsány v této příručce podrobně v tématu [Metody trvalého odstranění dat z pevného disku](#).

## Soubory

Nastavení Soubory určuje názvy souborů, které se mají pomocí průvodce vyčištěním systému smazat, a lze je použít s vyhledávacím řetězcem.



V operačním systému Windows může vyhledávací řetězec znázorňovat úplný nebo částečný název souboru. Vyhledávací řetězec může obsahovat alfanumerické znaky včetně čárky i zástupné znaky systému Windows a může nabývat hodnot podobných následujícím:

- \*.\* – k odstranění všech souborů s libovolným názvem a příponou;
- \*.doc – ke smazání souborů s určitou příponou (v tomto případě dokumenty Microsoft Word);
- read\*.\* – k odstranění všech souborů s libovolnou příponou a názvem souboru, který začíná výrazem „read“;
- read?.\* – k odstranění všech souborů, které mají pět písmenný název a libovolnou příponu, přičemž název začíná písmeny „read“ a páté písmeno je libovolné.

Poslední vyhledávací řetězec například povede k odstranění souborů read1.txt, ready.doc, ale soubor readiness.txt zůstane, kvůli svému dlouhému názvu (bez přípony).

Je možné zadat více různých vyhledávacích řetězců oddělených středníkem, například:

\*.bak;\*.tmp;\*.~~~ (bez mezer mezi řetězci).

Odstraní se všechny soubory, jejichž názvy se shodují alespoň s jedním vyhledávacím řetězcem.



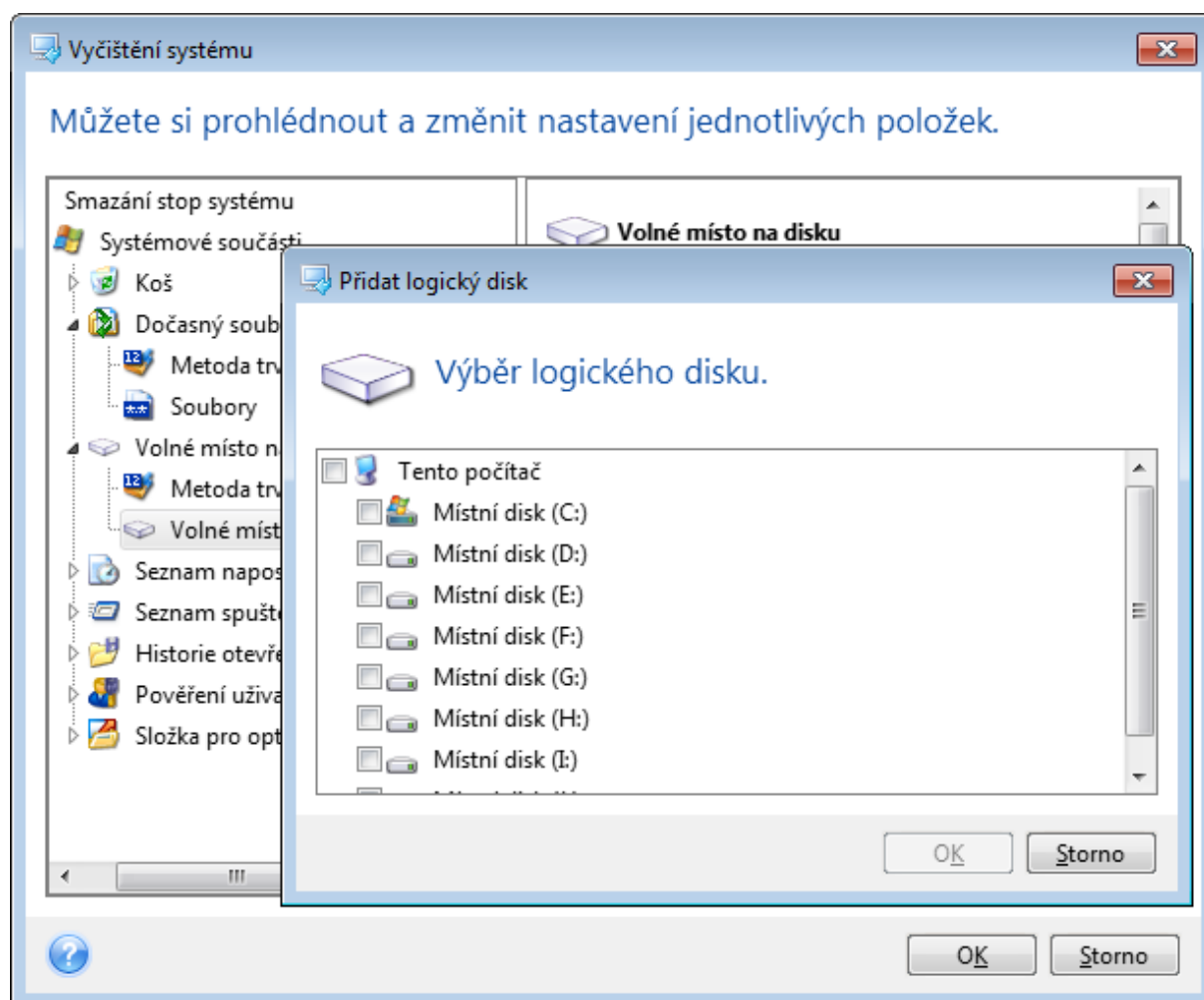
Po nastavení hodnoty Soubory můžete procházet soubory odpovídající vyhledávacím řetězcům. To provedete kliknutím na tlačítko **Zobrazit soubory**. Zobrazí se okno s názvy nalezených souborů. Tyto soubory se smažou.

## Volné místo na disku

Zde můžete ručně zadat fyzické a logické jednotky k vyčištění volného místa. Při výchozím nastavení vyčištění systému se na všech dostupných jednotkách smaže volné místo.

Chcete-li nastavení tohoto parametru změnit, můžete k odstranění jednotek, na kterých nechcete volné místo mazat, použít tlačítko **Odstranit**.

Pokud tyto jednotky chcete znovu přidat, použijte tlačítko **Přidat**.



## Počítače

Nastavení **Počítače** je použito k vymazání vyhledávacích řetězců z registru, které byly použity k vyhledání počítačů v místní síti. Tyto řetězce obsahují informace o tom, co vás zajímalo v síti. Tyto položky je vhodné kvůli zachování bezpečnosti také odstranit.

Nastavení **Počítače** je podobné jako nastavení **Soubory**. Jde o řetězec obsahující libovolný počet úplných nebo částečných názvů počítačů oddělených středníkem. Odstranění vyhledávacích řetězců počítačů je založeno na porovnání s hodnotou nastavení **Počítače** podle pravidel systému Windows.

Pokud potřebujete odstranit všechny vyhledávací řetězce počítačů v místní síti (vhodné ve většině případů), ponechte u tohoto nastavení výchozí hodnotu. Jak obnovit výchozí nastavení:

- Vyberte položku **Seznam hledaných počítačů**.
- Zkontrolujte, zda je políčko **Zapnout** zaškrtnuto.
- Vyberte nastavení **Počítače** a ujistěte se, že je textové pole prázdné.

Ve výsledku se z registru odstraní všechny vyhledávací řetězce počítačů.

Po nastavení hodnoty **Počítače** můžete procházet vyhledávací řetězce nalezené průvodcem vyčištěním systému v registru. To provedete kliknutím na tlačítko **Zobrazit počítače**. Zobrazí se okno s úplnými i částečnými názvy počítačů, které jste hledali v síti. Tyto položky budou odstraněny.

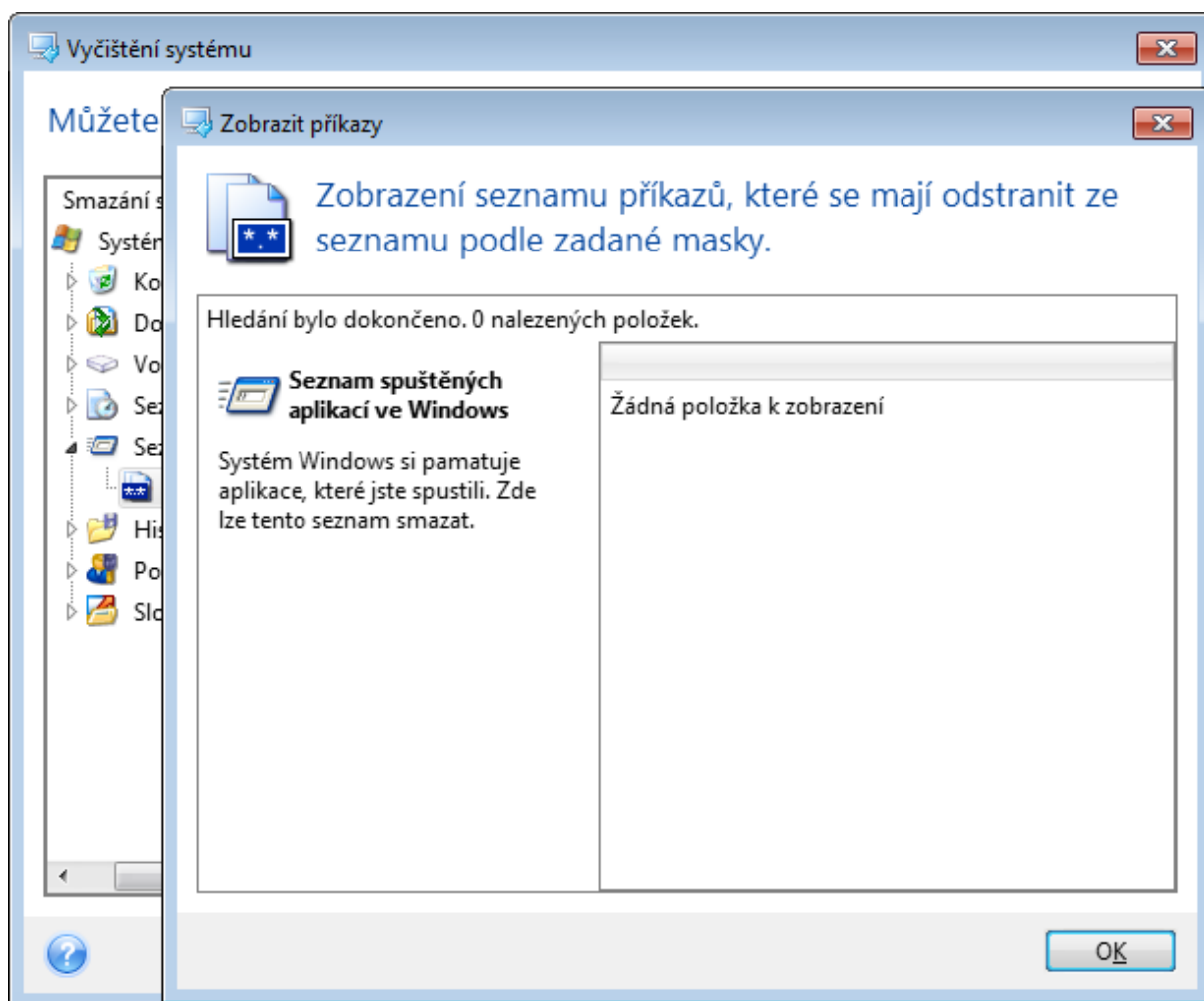
## Nastavení Příkazy

Zde můžete vybrat příkazy, které se mají odstranit během čištění seznamu **spuštěných aplikací ve Windows**.

Tato šablona může obsahovat názvy příkazů nebo jejich části oddělené středníky, například.:

\*help; cmd; reg\*.

Tím odstraníte příkazy, jejichž názvy se shodují nebo obsahují libovolný zadaný název nebo jeho část.



## Filtr míst v síti

Sem můžete zadat názvy hostitelů nebo adresy IP (oddělené středníky) míst v síti, serverů, serverů FTP či sdílených síťových úložišť, ke kterým se připojíte zadáním potřebných informací (uživatelského jména a hesla). Při zadávání hostitelských názvů a adres IP můžete použít zástupné znaky \* a ?.

Klepnutím na možnost **Zobrazit místa v síti** zobrazíte seznam míst v síti navštívených pomocí uživatelských údajů, které chcete odstranit.

## Náhled

Po dokončení kontroly budou všechny výsledky k dispozici v horní části okna průvodce. Při výchozím nastavení jsou všechny systémové součásti kontrolovány pro účely mazání. Pokud chcete nastavit, které součásti se mají kontrolovat a které ne, změňte výchozí nastavení vyčištění.

Výsledky si můžete prohlédnout a ručně vybrat nebo zrušit výběr položek, které chcete odstranit či ponechat. U všech součástí je zobrazen krátký popis, abyste se mohli snáze rozhodnout. Popis se zobrazí v pravé části okna po kliknutí na název součásti.

### Jak vybrat nebo zrušit výběr součástí

- Rozbalte položku **Systémové součásti** ve stromu vyčištění systému a ujistěte se, že součást, kterou chcete smazat je vybrána. Jestliže součást vyčistit nechcete, zrušte její výběr.
- Pokud je to nutné, můžete součásti dále rozbalit a vybrat nebo zrušit výběr jejich obsahu.

Po výběru součástí k vyčištění pokračujte kliknutím na tlačítko **Vyčistit**.

---

### Poznámka

Operační systémy Windows 7 a novější neukládají informace o vyhledávání souborů a počítačů. Informace o otevřených či uložených souborech se navíc v registru ukládají jinak, a proto je průvodce zobrazuje jiným způsobem.

---

## Průběh vyčištění

V okně stavu operace je vypsán stav aktuální operace.

Ukazatel průběhu určuje úroveň dokončení vybrané operace.

Někdy může dokončení operace trvat dlouho. V takovém případě zaškrtněte políčko **Vypnout počítač po dokončení**. Po dokončení operace aplikace Acronis Cyber Protect Home Office počítač vypne.

## 12.7.3 Metody trvalého odstranění dat z pevného disku

### Oč se jedná?

Informace odstraněné z pevného disku nezabezpečeným způsobem (například pouhým smazáním v systému Windows) lze snadno obnovit. Při použití speciálního vybavení je možné obnovit dokonce i opakovaně přepsanou informaci.

### Mechanismus úniku

Data jsou na pevném disku uložena jako posloupnost 1 a 0 (jedniček a nul), zastoupených různě zmagnetizovanými částmi disku.

Obecně řečeno, když se na pevný disk zapíše 1, řadič ji přečte jako 1 a 0 jako 0. Pokud však zapíšete 1 tam, kde byla 0, výsledek bude 0,95 a stejně tak, když zapíšete 1 tam, kde byla 1, výsledek je 1,05. Pro řadič jsou tyto rozdíly nepodstatné. Při použití speciálního vybavení je však možné snadno přecházet «předchozí» posloupnost 1 a 0.

## Metody trvalého odstranění informací používané programem Acronis

Podrobný teoretický základ garantovaného odstranění informací je popsán v článku od Petera Gutmanna. Další informace naleznete v článku „Secure Deletion of Data from Magnetic and Solid-State Memory“ (Bezpečné odstranění dat z magnetických a elektronických pamětí) na adrese [https://www.cs.auckland.ac.nz/~pgut001/pubs/secure\\_del.html](https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html).

Číslo	Algoritmus (metoda zápisu)	Počet průchodů	Záznam
1.	Ministerstvo obrany spojených států 5220.22-M	4	1. průchod – náhodně vybrané symboly na každý bajt sektoru, 2 – doplňky k hodnotám zapsaným v 1. průchodu; 3 – opět náhodné symboly; 4 – ověření zápisu.
2.	Spojené státy: NAVSO P-5239-26 (RLL)	4	1. průchod – 0x01 do všech sektorů, 2 – 0x27FFFFFF, 3 – posloupnost náhodných symbolů, 4 – ověření.
3.	Spojené státy: NAVSO P-5239-26 (MFM)	4	1. průchod – 0x01 do všech sektorů, 2 – 0x7FFFFFFF, 3 – posloupnost náhodných symbolů, 4 – ověření.
4.	Německo: VSITR	7	1.-6. – střídání posloupností: 0x00 a 0xFF; 7. – 0xAA; například. 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
5.	Rusko: GOST P50739-95	1	Logické nuly (čísla 0x00) na každý byte všech sektorů pro systémy s úrovní bezpečnosti 6 až 4.  Náhodně vybrané symboly (čísla) na každý byte všech sektorů pro systémy s úrovní bezpečnosti 3 až 1.
6.	Metoda Petera Gutmanna	35	Metoda Petera Gutmanna je velmi propracovaná. Je založena na jeho teorii o trvalém odstranění informací z pevného disku (viz <a href="#">Secure Deletion of Data from Magnetic and Solid-State Memory</a> – Spolehlivé odstranění dat z magnetických a elektronických pamětí).
7.	Metoda Bruce Schneiera	7	Bruce Schneier ve své knize Applied Cryptography (Aplikovaná kryptografie) popisuje následující sedmiprůchodovou metodu. 1. průchod – 0xFF, 2. průchod – 0x00 a následně pět průchodů s kryptograficky bezpečnou pseudonáhodnou posloupností.
8.	Rychlá	1	Logické nuly (čísla 0x00) do všech sektorů ke smazání.

## 12.8 Připojení diskového obrazu

Připojení diskových obrazů jako virtuálních jednotek umožňuje přistupovat k nim, jako by to byly fyzické jednotky. Můžete připojit místní zálohy obsahující diskové oddíly nebo celé disky a pak vybrat, které diskové oddíly se připojí. Po připojení:

- V systému se zobrazí nový disk pro všechny připojené diskové oddíly.
- Obsah obrazu můžete zobrazit v Průzkumníku souborů a ostatních správčích souborů (v režimu jen pro čtení).

## Poznámka

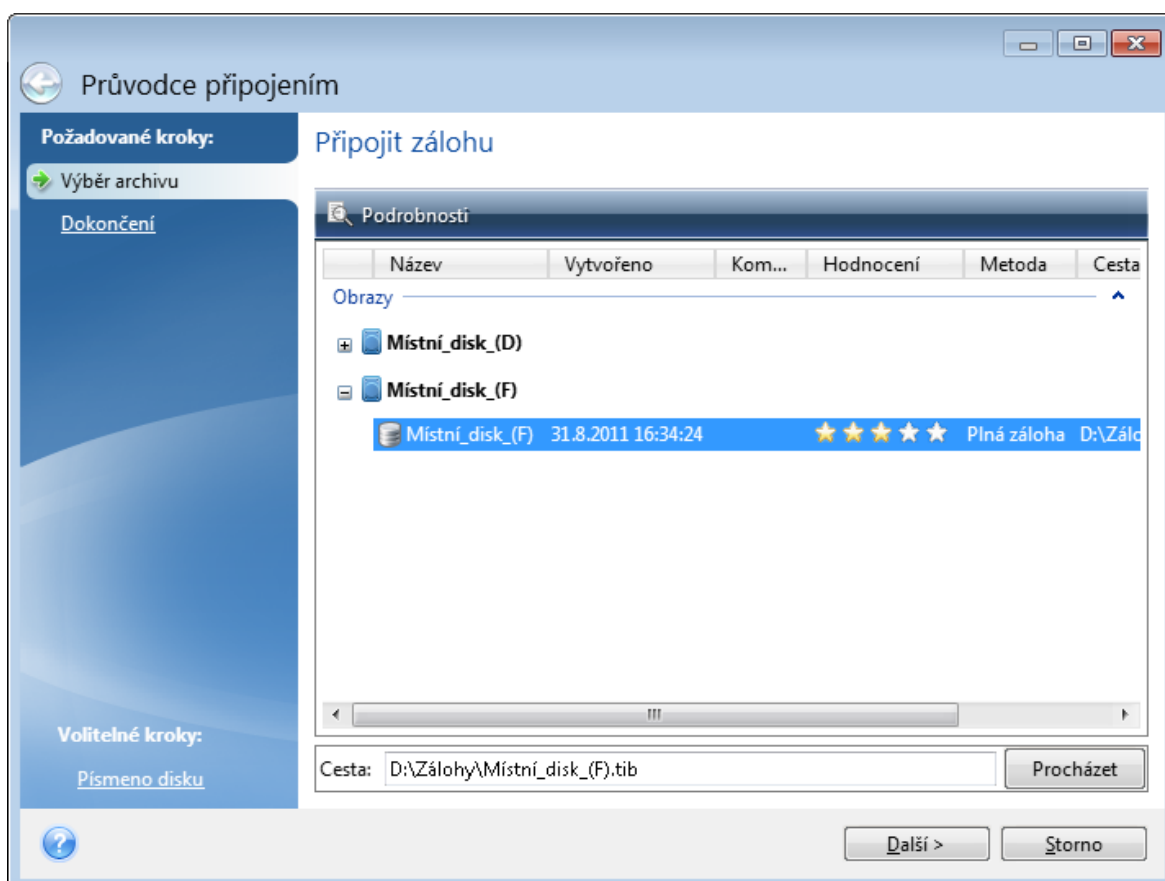
Operace popsané v tomto tématu jsou podporovány pouze v systémech souborů FAT a NTFS.

## Poznámka

Zálohu disku nelze připojit, pokud je uložena na serveru FTP.

## 12.8.1 Jak připojit diskový obraz

1. V Průzkumníku souborů klikněte pravým tlačítkem myši na soubor obrazu disku, který chcete připojit, a pak na tlačítko **Připojit obraz**.  
Otevře se průvodce připojením.
2. Podle data a času vytvoření vyberte zálohu, kterou chcete připojit. Tak je možné prohlížet stav dat až do určitého okamžiku.



3. [volitelný krok] V kroku **Písmeno disku** vyberte v rozevřacím seznamu **Písmeno pro připojení** písmeno, které má být přiřazeno k virtuálnímu disku. V případě, že určitý diskový oddíl nechcete připojit, vyberte v seznamu položku **Nepřipojovat** nebo u tohoto diskového oddílu zrušte zaškrtnutí políčka.
4. Klikněte na tlačítko **Pokračovat**.
5. Po připojení obrazu se spustí Průzkumník souborů a zobrazí jeho obsah.

## 12.9 Odpojení diskového obrazu

Doporučujeme, abyste virtuální disk po dokončení všech nezbytných operací odpojili, protože udržování virtuálních disků spotřebovává mnoho systémových prostředků.

### ***Odpojit obraz lze pomocí jednoho z následujících kroků***

- V Průzkumníku souborů klikněte pravým tlačítkem myši na ikonu disku a poté na tlačítko **Odpojit**.
- Restartujte nebo vypněte počítač.

## 12.10 Práce se soubory VHD(X)

Zálohy (soubory TIB) disků nebo diskových oddílů Acronis lze převést na virtuální pevné disky (soubory VHD(X)).

### 12.10.1 Jak používat soubory VHD(X)

- Počítač můžete spustit z převedeného souboru VHD(X) a otestovat, zda je záloha platná a lze z ní obnovit operační systém.
- Převedený soubor VHD(X) můžete uložit pro případ nouzových situací. Například když se počítač nespouští a potřebujete jej ihned spustit, můžete systém zavést ze souboru VHD(X).
- V systému Windows 7 můžete soubory VHD(X) připojit jako další disk. Soubor VHD(X) může obsahovat jakékoliv diskové oddíly – systémové nebo nesystémové.
- Převedený soubor VHD(X) nelze spustit jako virtuální počítač.

### 12.10.2 Omezení a další informace

- Zálohu souboru nelze převést na soubor VHD(X).
- Aby bylo možné zavést systém z převedeného souboru VHD(X), musí tento soubor obsahovat:
  - Systémový diskový oddíl stejného počítače. Pomocí stejného souboru VHD(X) nelze spustit jiné počítače.
  - Windows 7 nebo novější operační systém.
- Všechny změny provedené v zavedeném nebo připojeném souboru VHD(X) se do něj uloží. Zavedete-li systém ze souboru VHD(X) a provedete změny dat, která nejsou zálohovaná, ovlivní tyto změny váš funkční systém.
- Samostatné verze aplikace Acronis Cyber Protect Home Office, které se spouštějí ze spouštěcího média, nepodporují operace převádění.
- Aplikace Acronis Cyber Protect Home Office neumí převádět soubory TIB obsahující dynamické svazky, které byly původně umístěny na více než jedné diskové jednotce (například prokládané nebo rozložené svazky).

## 12.10.3 Převod zálohy Acronis

Uživatelé verze Enterprise a Ultimate systémů Windows 7 a novějších mohou bitové kopie systémových diskových oddílů ve formátu TIB převést do formátu VHD(X), aby tyto převedené soubory VHD(X) bylo možné použít ke spuštění operačního systému. Tyto bitové kopie lze připojovat i bez použití aplikace Acronis Cyber Protect Home Office.

### ***Jak převést diskový obraz Acronis (soubor TIB) na virtuální disk VHD(X) zálohy systému Windows:***

1. Spustit Acronis Cyber Protect Home Office
2. Přejděte do části **Záloha**.
3. V seznamu záloh klikněte na tlačítko šipky dolů vedle zálohy, kterou chcete převést, pak klikněte na tlačítko **Převést na VHD**.

Pokud je záloha chráněna heslem, aplikace Acronis Cyber Protect Home Office se na něj zeptá. Nezapomeňte, že výsledný soubor VHD(X) nebude chráněný heslem.

4. Vyberte verzi zálohy, kterou chcete převést.

Převod přírůstkové zálohy vyžaduje všechny předchozí přírůstkové zálohy a původní plnou zálohu. Pro převod rozdílové zálohy je třeba původní plná záloha. Výsledkem převodu je vždy plná záloha.

5. Určete cestu k vytvořenému souboru.

Soubor lze uložit do libovolného místního úložiště podporovaného aplikací Acronis Cyber Protect Home Office (kromě Acronis Secure Zone a disku CD/DVD). Navíc lze soubor uložit do sdíleného úložiště SMB.

6. [Volitelný krok] Když je záloha převáděna, můžete zaškrtnout pole **Po dokončení spustit virtuální počítač**. Pokud je tato možnost vybrána, aplikace Acronis Cyber Protect Home Office restartuje počítač a spustí virtuální počítač Hyper-V pomocí vytvořeného souboru VHD(X).

Pokud bitová kopie TIB vybraná pro převod obsahuje diskové oddíly například ze dvou fyzických disků, program vytvoří dva soubory VHD(X) odpovídající jednotlivým fyzickým diskům.

## 12.11 Import a export nastavení zálohování

Aplikace Acronis Cyber Protect Home Office umožňuje import a export nastavení zálohování. To je vhodné například tehdy, pokud potřebujete přenést nastavení do jiného počítače po instalaci aplikace Acronis Cyber Protect Home Office. Uložení nastavení může být také užitečné, když se později rozhodnete upgradovat na novou verzi aplikace Acronis Cyber Protect Home Office.

Takový přenos ulehčí konfiguraci záloh v novém počítači. Stačí pouze exportovat nastavení a importovat je v jiném počítači. Nastavení se exportují ve formě skriptových souborů.

Obsah nastavení se může lišit v závislosti na typu zálohy. V případě klasických záloh disků a souborů se nastavení skládá z následujících položek:



- seznam položek k zálohování,
- možnosti zálohování,
- umístění zálohy,
- plán,
- schéma zálohování,
- pravidla automatického čištění,
- pravidla názvů verzí záloh.

Nastavení nepřetržitého zálohování vypadá následovně:

- seznam položek pro nonstop ochranu,
- umístění datového úložiště nonstop zálohování (případně seznam umístění, pokud jich je více).

---

### **Poznámka**

Import nastavení online zálohování z jednoho počítače do jiného není možný.

---

### ***Export nastavení zálohování***

1. Spustit Acronis Cyber Protect Home Office
2. Na bočním panelu klikněte na tlačítko **Nastavení > Přenos nastavení zálohování**, klikněte na tlačítko **Uložit nastavení do souboru** a pak přejděte do cíle, kam chcete uložit soubory skriptu s nastavením.

### ***Import nastavení zálohování***

1. V dalším počítači spusťte aplikaci Acronis Cyber Protect Home Office.
2. Na bočním panelu klikněte na tlačítko **Nastavení > Přenos nastavení zálohování**, klikněte na tlačítko **Importovat nastavení ze souboru** a pak zobrazte na cestu s uloženými soubory skriptu s nastavením.

Po importu budete možná muset nějaká nastavení změnit tak, aby vyhovovala novému prostředí. Můžete například změnit seznam položek k zálohování, cíl zálohování nebo jiná nastavení.

Pokud budete chtít zkopírovat některé zálohy do jiného počítače, doporučuje se exportovat také nastavení těchto záloh. Díky tomu nepřijdete o žádnou z funkcí záloh.

## 12.12 Acronis Universal Restore

Doplňek Acronis Universal Restore umožňuje vytvořit klon systému spustitelný na jiném hardwaru. Tento nástroj použijte, jestliže systémový disk obnovujete do počítače s jiným procesorem, základní deskou nebo velkokapacitním paměťovým zařízením, než obsahuje původně zálohovaný systém. To může být užitečné například po výměně poškozené základní desky nebo při přesunu systému z jednoho počítače do druhého.

## 12.12.1 Jaký problém se tím vyřeší?

Obraz systémového disku lze snadno obnovit na hardwaru, kde byl vytvořen nebo na identickém hardwaru. Obnovený systém však není možné spustit na jiném hardwaru. Nový hardware totiž není kompatibilní s nejdůležitějšími ovladači obsaženými v obrazu. Tento nástroj najde a nainstaluje ovladače pro zařízení, která jsou důležitá pro spuštění operačního systému, například ovladače pamětí, základní desky nebo čipové sady.

## 12.12.2 Jak jej mám použít?

Před zahájením obnovy na jiném hardwaru zkontrolujte, zda máte k dispozici:

- [Záloha systémového disku](#) nebo [záloha celého počítače](#)
- [Spouštěcí médium Acronis](#)
- [Medium Acronis Universal Boot](#)

---

### **Poznámka**

Pokud máte v počítači nainstalovanou aplikaci Acronis Cyber Protect Home Office a Tvůrce médií Acronis Universal Boot, můžete umístit obě aplikace Acronis Cyber Protect Home Office a Acronis Universal Boot na stejné médium. Další informace naleznete v části [Vytváření média Acronis Universal Boot](#).

---

Chcete-li obnovit systém na jiném hardwaru:

1. Spustíte cílový počítač pomocí spouštěcího média Acronis a pak obnovte systém ze zálohy systému nebo zálohy celého počítače. Další informace naleznete v části [Obnovení systému na nový disk při použití spouštěcího média](#).
2. Spustíte cílový počítač pomocí média Acronis Universal Boot a pak postupujte podle pokynů na obrazovce a nastavte svůj systém jako spustitelný. Další informace naleznete v části [Používání doplňku univerzální obnovy Acronis](#).

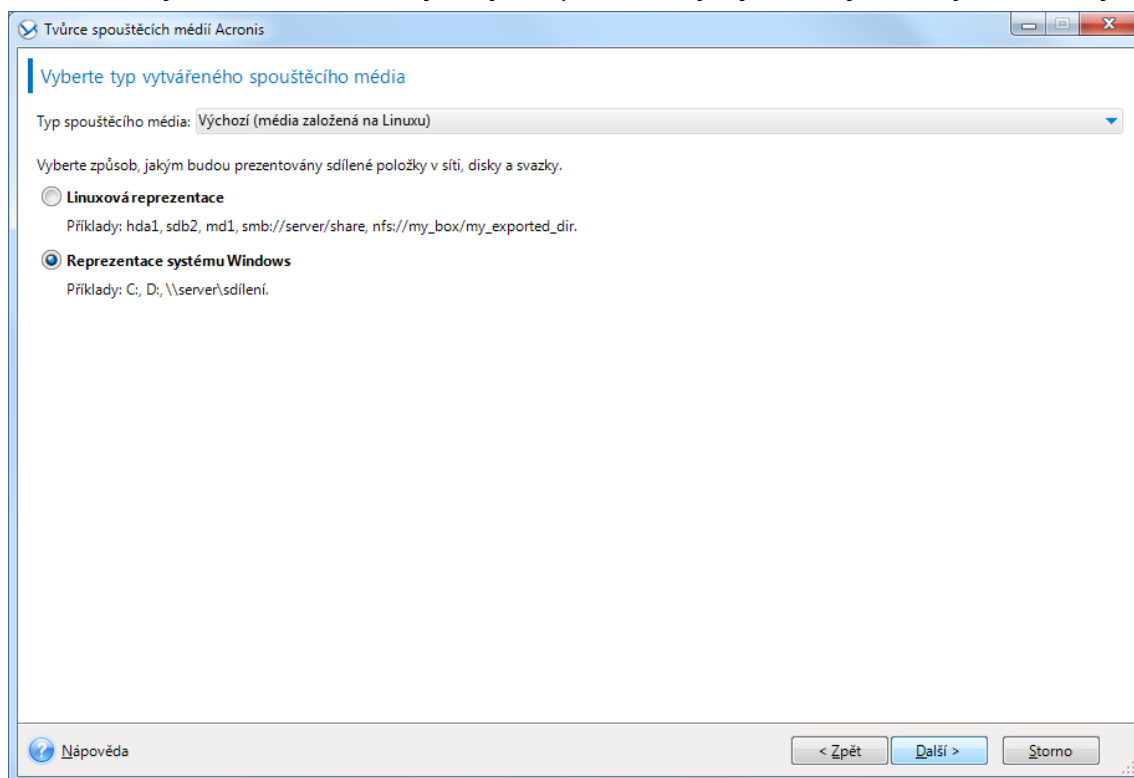
## 12.12.3 Vytváření média Acronis Universal Boot

Médium Acronis Universal Boot se používá k zajištění spustitelnosti počítače po obnovení na odlišném hardwaru. Další informace naleznete v části [Doplňek univerzální obnovy Acronis](#).

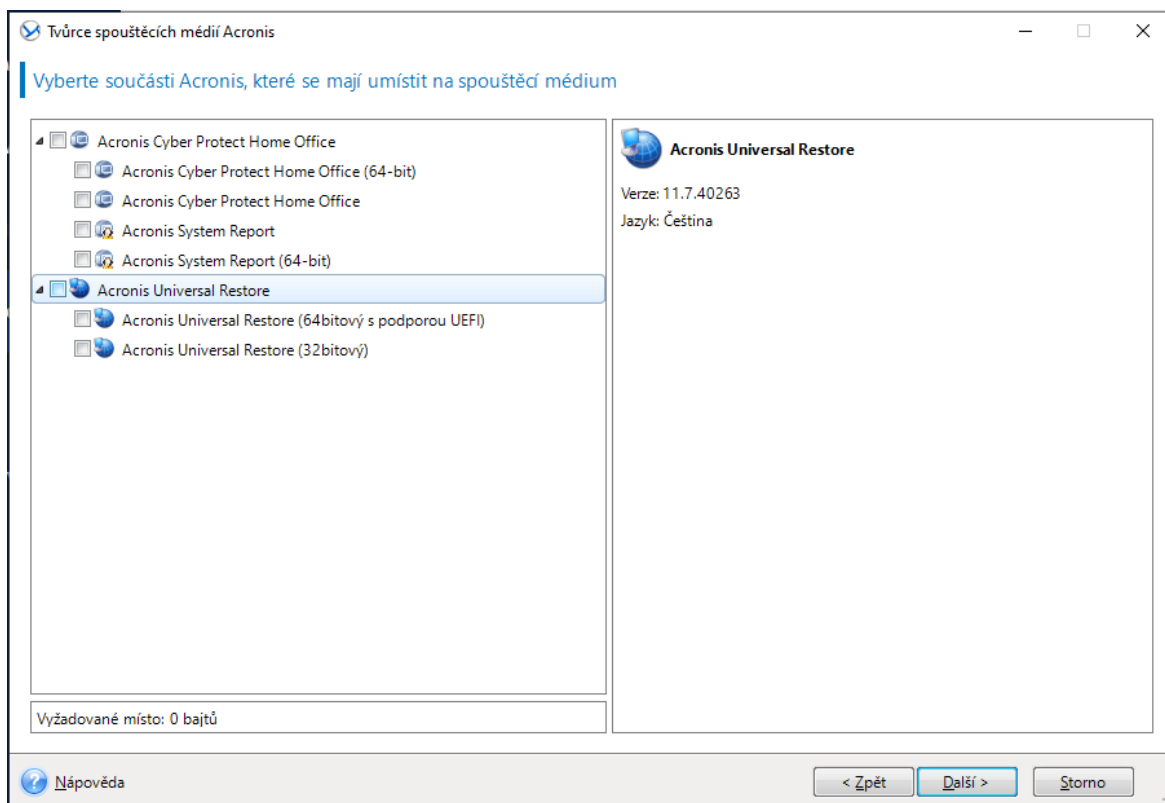
### **Vytvoření média Acronis Universal Boot**

1. Spustit Acronis Cyber Protect Home Office
2. V části **Nástroje** klikněte na položku **univerzální obnovy Acronis**.
3. Klikněte na položku **Stáhnout** a získáte program pro tvorbu médií Acronis Universal Boot.
4. Spustíte stažený soubor a nainstalujete program pro tvorbu médií.
5. Připojte USB flash disk nebo vložte prázdný disk DVD, který chcete učinit spustitelný.

6. Chcete-li spustit program pro tvorbu médií Acronis Universal Boot, proveďte jednu z následujících akcí:
  - V části **Nástroje** klikněte na položku **univerzální obnovení Acronis**.
  - Klikněte na tlačítko **Spustit**, otevřete seznam nainstalovaných programů a pak klikněte na položku **Spustit program pro tvorbu médií Universal Boot**.
7. Zkontrolujte, zda platí, že:
  - Jako typ spouštěcího média je zvoleno linuxové médium.
  - Znázornění systému Windows se vybírá jako způsob, kterým jsou disky a svazky znázorněny.



8. [Volitelné] Určete parametry jádra systému Linux. Další informace naleznete v části [Parametry spuštění spouštěcího média](#).
9. Vyberte součásti aplikace Acronis, které se mají umístit na médium.



Je možné vybrat 32bitové nebo 64bitové součásti. 32bitové součásti mohou pracovat na 64bitovém hardwaru. Ke spuštění 64bitového počítače s rozhraním UEFI (Unified Extensible Firmware Interface) je ovšem nutné použít 64bitové součásti.

Chcete-li médium používat na různých typech hardwaru, vyberte oba typy součástí. Při spuštění počítače z výsledného média bude možné vybrat ve spouštěcí nabídce 32bitové nebo 64bitové součásti.

Pokud je na vašem počítači nainstalována aplikace Acronis Cyber Protect Home Office, můžete ji na médium také umístit. V tomto případě budete mít jedno spouštěcí médium obsahující oba komponenty nezbytné k obnovení na odlišný hardware.

10. Vyberte cílové umístění pro médium:

- **CD**
- **DVD**
- **USB flash disk**
- **Soubor obrazu ISO**

Bude třeba zadat název a cílovou složku souboru ISO.

Po vytvoření obrazu ISO jej můžete vypálit na disk CD nebo DVD. Například v systémech Windows 7 a novějších to lze provést pomocí integrovaného nástroje pro vypalování.

V Průzkumníku souborů dvakrát klikněte na vytvořený soubor obrazu ISO a poté klikněte na možnost **Vypálit**.

11. Určete ovladače velkokapacitního úložiště, které budou použity doplňkem Acronis Universal Boot.

Nyní ovladače přidávat nemusíte. To můžete udělat později, když na počítač použijete doplněk Acronis Universal Boot.

#### 12. Klikněte na tlačítko **Pokračovat**.

Po vytvoření média ho odpojte od počítače. Toto je vaše médium Acronis Universal Boot.

## 12.12.4 Použití technologie univerzální obnovy Acronis

### Příprava

#### Příprava ovladačů

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

#### 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 ve Windows, ale médium založené na Linuxu jej nenalezne, použijte médium založené na prostředí WinPE.

### Nastavení doplňku 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, do pole **Hledat složku** zadejte cestu ke složce.

Doplňěk Universal Restore kromě toho prohledá také výchozí složku úložiště ovladačů systému Windows (obvykle WINDOWS/inf).

#### 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.
- Pokud automatické vyhledání ovladačů nepomůže spustit systém.

Zadejte 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 doplňku Universal Restore

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

Po dokončení procesu budete moci konfigurovat síťové připojení a vybrat ovladače pro grafický adaptér, USB flash disky a další zařízení.

## 13 Odstraňování problémů

### 13.1 Řešení nejčastějších potíží

Zde naleznete seznam nejčastějších potíží, se kterými se uživatelé setkávají v Acronis Cyber Protect Home Office. Příslušná řešení naleznete v Databázi znalostí [Acronis](#).

#### Přihlašování při selhání spuštění programu

**Chyba „Překročili jste maximální počet aktivací pro toto sériové číslo.“**

**Chyba „Toto sériové číslo je již registrováno u jiného účtu.“**

**Soubory a složky se nezobrazí při procházení záloh v Průzkumníku souborů**

**Chyba „Zapojte externí disk“**

**Zálohování do úložiště Acronis Cloud se nezdaří a zobrazí se chyba „Chyba zápisu“ nebo „Při zápisu souboru došlo k chybě“ nebo „Požadavek FES se nezdařil“.**

**Po obnovení na nový hardware se zobrazí modrá obrazovka smrti (BSOD) a chyba „Stop 0x0000007B“ vlivem chybějících ovladačů.**

Úplný seznam oblíbených řešení naleznete na webu <https://kb.acronis.com/true-image-known-solutions>.

Informace o řešení potíží týkající se selhání obnovení naleznete také na webu <https://kb.acronis.com/content/46340>.

### 13.2 Systémová zpráva Acronis

Při kontaktování technické podpory společnosti Acronis jsou mnohdy k vyřešení problému třeba informace o vašem systému. Získávání informací může být složité a může trvat poměrně dlouho.

Nástroj **Generovat systémovou zprávu** vytvoří systémovou zprávu obsahující všechny potřebné technické informace a umožní tyto informace uložit do souboru. V případě potřeby můžete takto vytvořený soubor připojit k popisu problému a odeslat jej do technické podpory. Tím technické podpoře usnadníte hledání řešení.

***Chcete-li generovat systémovou zprávu, proveďte jeden z následujících kroků.***

- Na postranním panelu klikněte na tlačítko **Nápověda** a potom na tlačítko **Generovat systémovou zprávu**.
- stiskněte klávesy **CTRL+F7**. Tuto kombinaci kláves lze používat i v případě, že aplikace Acronis Cyber Protect Home Office provádí jinou operaci.
- Používáte-li systém Windows 11, klikněte na možnost **Všechny aplikace > Acronis > Acronis Systémová zpráva**.
- Používáte-li systém Windows 10, v nabídce **Start** klikněte na možnost **Acronis > Acronis Systémová zpráva**.

- Používáte-li systém Windows 7 či 8, klikněte na možnost **Start > Všechny programy > Acronis > Acronis Systémová zpráva**.

### **Po vygenerování zprávy**

- Chcete-li vygenerovanou systémovou zprávu uložit, klikněte na tlačítko **Uložit** a v zobrazeném okně určete umístění vytvořeného souboru.
- Kliknutím na tlačítko **Storno** můžete hlavní okno aplikace zavřít bez uložení zprávy.

Tento nástroj můžete umístit i na spouštěcí médium jako samostatnou součást a umožnit tak generování systémové zprávy i v případě, že počítač nelze spustit. Po spuštění z média můžete zprávu generovat bez spuštění aplikace Acronis Cyber Protect Home Office. Stačí zapojit USB flash disk a kliknout na ikonu Systémová zpráva **Acronis**. Vygenerovaná zpráva se uloží na USB flash disk.

### **Chcete-li nástroj Systémová zpráva Acronis umístit na spouštěcí médium:**

1. Zaškrtněte políčko Systémová zpráva **Acronis** v okně **Výběr obsahu záchranných médií** v průvodci Tvůrce spouštěcích médií **Acronis**.
2. Pokračujte kliknutím na tlačítko **Další**.

### **Vytvoření systémové zprávy z příkazového řádku**

1. Spusťte program Windows Command Processor (cmd.exe) jako správce.
2. Změňte aktuální adresář na instalační složku produktu Acronis Cyber Protect Home Office. Postupujte následujícím způsobem:

```
cd C:\Program Files (x86)\Acronis\CyberProtectHomeOffice
```

3. Chcete-li vytvořit soubor systémové zprávy, zadejte:

```
SystemReport
```

V aktuální složce se vytvoří soubor SystemReport.zip.

Chcete-li souboru zprávy přiřadit vlastní název, zadejte namísto <file name> název nový:

```
SystemReport.exe /filename:<file name>
```

### **Chcete-li generovat systémovou zprávu pomocí spouštěcího média**

1. Pokud jste tak ještě neučinili, vytvořte spouštěcí médium Acronis. Další informace naleznete v části Program pro tvorbu médií [Acronis](#).
2. Nastavte pořadí spouštění v systému BIOS tak, aby se systém spustil ze spouštěcího média (disku CD, DVD nebo USB flash disku). Podrobnosti naleznete v části [Uspořádání pořadí spouštění v systému BIOS](#).
3. Spusťte systém ze spouštěcího média Acronis a vyberte možnost **Acronis Cyber Protect Home Office**.




---

### Poznámka

Místo kliknutí na možnost **Acronis Cyber Protect Home Office** můžete připojit USB flash disk a kliknout na možnost Systémová zpráva **Acronis**. V tomto případě aplikace vygeneruje zprávu a automaticky ji uloží na flash disk.

---

4. Klikněte na šipku vedle ikony Nápověda () a zvolte možnost **Generovat systémovou zprávu**.
5. Po vygenerování zprávy klikněte na tlačítko **Uložit** a v zobrazeném okně určete umístění vytvořeného souboru.  
Aplikace uloží zprávu do souboru ZIP.

## 13.3 Inteligentní hlášení chyb Acronis

Když při činnosti aplikace dojde k chybě, aplikace Acronis Cyber Protect Home Office zobrazí příslušné chybové hlášení. Chybové hlášení obsahuje kód události a krátký popis chyby.

### 13.3.1 Když jste připojeni k internetu

Chcete-li zobrazit článek znalostní databáze Acronis s navrhovanými řešeními chyby, klikněte na tlačítko **Znalostní databáze**.

Poté se zobrazí potvrzovací okno s informacemi, které se mají přes internet odeslat do znalostní databáze Acronis. Kliknutím na tlačítko **OK** povolíte odeslání informací.

Pokud budete chtít v budoucnu odesílat tyto informace bez potvrzení, zaškrtněte políčko **Vždy odesílat bez potvrzení**.

### 13.3.2 Když nejste připojeni k internetu

1. V okně chybové zprávy klikněte na možnost **Další podrobnosti** a запиšte si kód události. Kód může vypadat například takto:  
0x000101F6 – příklad běžného kódu události,  
0x00970007+0x00970016+0x00970002 – příklad složeného kódu události. Tento druh kódu se může objevit poté, co se vyskytne chyba v nízkoúrovňovém modulu aplikace, poté se přenesou do modulů vyšší úrovně a způsobí tak chyby také v těchto modulech.
2. Až budete moci navázat připojení k internetu nebo budete mít přístup k počítači s připojením k internetu, zadejte kód události na adrese: <https://kb.acronis.com/errorcode/>.

Pokud znalostní databáze kód události nerozpozná, neobsahuje dosud článek popisující řešení tohoto problému. V takových případech otevřete požadavek na podporu pomocí [Zákaznického centra společnosti Acronis](#).

## 13.4 Odeslání zpětné vazby společnosti Acronis

Své produkty a služby často vylepšujeme dalšími funkcemi, větší spolehlivostí a rychlostí. Prostřednictvím formuláře zpětné vazby nás můžete upozornit na potíže a chyby, které je třeba vyřešit, aby byla aplikace Acronis Cyber Protect Home Office ještě lepší. Věnujte prosím několik minut a řekněte nám, co si o našem produktu myslíte, navrhněte nové funkce nebo nahlaste problém. Veškerou zpětnou vazbu čteme a analyzujeme.

---


### **Poznámka**

Neodpovídáme na všechny zprávy se zpětnou vazbou. Pokud potřebujete pomoc s aplikací Acronis Cyber Protect Home Office, obraťte se na technickou podporu.

---

### ***Odeslání zpětné vazby společnosti Acronis***


1. Na postranním panelu klikněte na tlačítko **Nápověda** a potom na položku **Odeslat zpětnou vazbu**. Otevře se formulář zpětné vazby.

 Send Feedback to the Acronis team ✕

Share your thoughts about Acronis Cyber Protect Home Office or report a problem.

Reason ▼

Enter your feedback here

 Attach file...

Attach system report [What is this?](#)

We cannot reply to all messages sent via this form, but we do read and analyze your feedback.

2. Ze seznamu vyberte důvod zpětné vazby.
3. Napište zprávu.
4. Uveďte své jméno a e-mailovou adresu.
5. [Volitelný krok] Můžete přiložit také soubor a systémovou zprávu Acronis. Další informace naleznete v části [Systémová zpráva Acronis](#).  
Systémovou zprávu doporučujeme přiložit v případě, že jste se setkali se závažnou chybou, například když aplikace Acronis Cyber Protect Home Office přestala reagovat.
6. Klikněte na tlačítko **Odeslat**.

## 13.5 Jak získat výpisy stavu systému

Protože havárie aplikace Acronis Cyber Protect Home Office nebo systému Windows může být způsobena různými příčinami, každou havárii je nutné prověřit zvlášť. Zákaznické centrum Acronis uvítá, když poskytnete následující informace:

### ***Při havárii aplikace Acronis Cyber Protect Home Office poskytněte prosím následující informace***

1. Přesný popis kroků, které jste prováděli před vyskytnutím problému.
2. Výpis stavu systému Informace o získání takového výpisu naleznete v článku na adrese <https://kb.acronis.com/content/27931> ve znalostní databázi Acronis.

### ***Pokud aplikace Acronis Cyber Protect Home Office způsobí pád systému Windows***

1. Přesný popis kroků, které jste prováděli před vyskytnutím problému.
2. Soubor s výpisem stavu systému Windows. Informace o získání takového výpisu naleznete v článku na adrese <https://kb.acronis.com/content/17639> ve znalostní databázi Acronis.

### ***Pokud se Acronis Cyber Protect Home Office zavěsí***

1. Přesný popis kroků, které jste prováděli před vyskytnutím problému.
2. Uživatelský výpis stavu procesu. Viz článek znalostní databáze Acronis na adrese <https://kb.acronis.com/content/6265>.
3. Výpis nástroje Procmon. Viz článek znalostní databáze Acronis na adrese <https://kb.acronis.com/content/2295>.

Jestliže k informacím nemáte přístup, kontaktujte zákaznické centrum Acronis, kde vám bude poskytnut odkaz na server FTP k odeslání souborů.

Tyto informace zrychlí proces hledání řešení k potížím.

## 13.6 Program zkušeností uživatelů Acronis

Program zkušeností uživatelů Acronis (CEP) je nový způsob, jak umožnit zákazníkům společnosti Acronis přispívat k funkcím, návrhům a vývoji produktů společnosti Acronis. Tento program umožňuje zákazníkům poskytovat naší společnosti různé informace, včetně informací o konfiguraci hardwaru hostitelských nebo virtuálních počítačů, nejčastěji používaných funkcích a problémech, se kterými se zákazníci setkávají. Pomocí těchto informací budeme moci zlepšovat produkty společnosti Acronis a funkce, které nejčastěji používáte.

### ***Jak se zapojit do programu zkušeností uživatelů Acronis a jak tento program opustit***

1. Na bočním panelu klikněte na možnost **Nastavení**.
2. Chcete-li program opustit, zrušte zaškrtnutí políčka **Zúčastnit se programu zkušeností uživatelů Acronis**.

Pokud se budete chtít tohoto programu zúčastnit, technické informace budou automaticky shromážděny každých 90 dní. Nebudou shromažďována osobní data, například jméno, adresa, telefonní číslo nebo data zadaná prostřednictvím klávesnice. Účast v programu CEP je dobrovolná, jeho výsledky však mají přispívat k vylepšování softwaru a funkcí na základě potřeb našich zákazníků.

# Slovníček

## A

### **Acronis Active Protection**

Technologie, která chrání data před ransomwarem, škodlivým softwarem, který blokuje přístup k některým souborům nebo celému systému a vyžaduje výkupné za odblokování. Na základě heuristického přístupu tato technologie sleduje procesy v počítači v reálném čase a informuje uživatele o pokusech zašifrování dat v počítači. V případě zašifrování souborů je lze obnovit z dočasných kopií nebo záloh.

### **Acronis Secure Zone**

Spolehlivý diskový oddíl určený k zálohování na pevném disku. Výhody: Umožňuje obnovení disku na stejný disk, kde je umístěna záloha disku. Nabízí cenově přístupnou a vhodnou metodu zabezpečení dat před vadným softwarem, útokem viru a chybami obsluhy. Odstraňuje potřebu mít zvláštní médium nebo připojení k síti k zálohování nebo obnovení dat. Omezení: 1) AcronisSecure Zone nelze vytvořit na dynamickém disku. 2) AcronisSecure Zone není dostupná jako umístění záloh v prostředí pro obnovení, když provedete spuštění ze spouštěcího média, prostřednictvím správce Startup Recovery Manager nebo BartPE.

### **Acronis Startup Recovery Manager**

Nástroj na ochranu, který umožňuje spustit samostatnou verzi při spuštění počítače stisknutím klávesy F11. Startup Recovery Manager odstraňuje potřebu spouštěcího média. Startup Recovery Manager je praktický zejména pro mobilní uživatele. Pokud dojde k havárii, uživatel restartuje počítač, na výzvu „Stisknutím klávesy F11 spustíte Startup

Recovery Manager...“ stiskne klávesu F11 a provede obnovení dat stejným způsobem jako u běžného spouštěcího média. Omezení: Nelze umístit na dynamickém disku; vyžaduje ruční konfiguraci zavaděčů, například LILO a GRUB; vyžaduje novou aktivaci zavaděčů třetích stran.

### **AcronisNotary**

Technologie umožňující uživateli zkontrolovat, zda byl ověřený soubor upraven od doby jeho zálohování. Technologie Notary vypočítá kód hodnoty hash na základě kódů hodnoty hash souborů vybraných k ověření a pak odešle kód hodnoty hash do databáze založené na technologii Blockchain. Technologie Blockchain zaručuje, že se kód kontrolního součtu nezmění. Proto lze pravost souboru snadno ověřit porovnáním kontrolního součtu v databázi a kontrolního součtu souboru, který chcete zkontrolovat.

### **Archiv**

Soubor vytvořený jako výsledek archivace. Soubor zahrnuje sadu komprimovaných souborů, které uživatel vybere pro archivaci. Archivy lze uložit do cloudového nebo místního úložiště, například na externí pevný disk nebo do zařízení NAS, a přistupovat k nim v režimu jen pro čtení na virtuálním disku Acronis.

### **Archivace**

Operace, která komprimuje vybrané soubory a přesune je do cloudového nebo místního úložiště, například na externí pevný disk nebo do zařízení NAS. Hlavním účelem tohoto procesu je uvolnit prostor na pevném disku přesunutím starých nebo velkých souborů do jiného úložiště. Po dokončení se soubory

odstraní z původních umístění a jsou dostupné v režimu pouze ke čtení na virtuálním disku Acronis.

## J

### **Jednotka Acronis**

Virtuální disk, který obsahuje jak místní archivy, tak i archivy v cloudu. Disk je dostupný v Průzkumníku souborů pod položkou Oblíbené a poskytuje přístup k archivovaným souborům v režimu jen pro čtení.

## M

### **Mobilní záloha**

Záloha, která obsahuje soubory z mobilního zařízení, například chytrého telefonu nebo tabletu.

## N

### **Nonstop ochrana**

Nonstop ochrana – proces, který provádí funkci Nonstop zálohování, pokud je zapnuta.

### **Nonstop zálohování**

Nonstop zálohování je ve skutečnosti záloha disku, diskového oddílu nebo souborů, která je vytvořena funkcí Nonstop zálohování Acronis. Jedná se o sadu jedné verze plné zálohy a sekvenci verzí přírůstkových záloh, které jsou vytvářeny v krátkých časových intervalech. Data jsou tak souvisle chráněna, neboť je umožněna obnova jejich předchozího stavu v jakémkoliv bodě obnovy, který potřebujete.

## O

### **Obnova**

Obnovení je proces navrácení poškozených dat do předchozího normálního stavu pomocí zálohy.

### **Online zálohování**

Online záloha – záloha vytvořená pomocí nástroje Online zálohování Acronis. Online zálohy jsou uloženy ve zvláštním úložišti pojmenovaném Cloud dostupném prostřednictvím internetu. Hlavní výhodou online zálohování je, že všechny zálohy jsou uloženy ve vzdáleném umístění. To je zárukou, že všechna zálohovaná data budou v bezpečí bez ohledu na místní úložiště uživatele.

### **online zálohy**

Sada pravidel nastavených uživatelem při vytváření nové zálohy. Proces zálohování se těmito pravidly řídí. Později můžete upravit nastavení zálohy a změnit nebo optimalizovat proces zálohování.

### **Operace zálohování**

Jedná se o operaci, která vytváří kopii dat existujících na pevném disku počítače za účelem obnovení nebo vrácení dat do stavu v zadaném datu a čase.

### **Ověřená záloha**

Záloha, která obsahuje soubory ověřené pomocí řešení Acronis Notary.

### **Ověření**

Operace, která kontroluje, zda bude možné obnovit data z určité verze zálohy. V případě plné verze zálohy aplikace ověří pouze plnou

verzi zálohy. V případě rozdílové verze zálohy aplikace ověří původní verzi plné zálohy a vybranou verzi rozdílové zálohy. V případě přírůstkové verze zálohy aplikace ověří původní plnou verzi zálohy, vybranou přírůstkovou verzi zálohy a celý řetězec (pokud existuje) verzí záloh předcházejících vybrané přírůstkové verzi. Jestliže řetězec obsahuje jednu nebo více verzí rozdílových záloh, aplikace ověří (kromě původní plné verze zálohy a vybrané verze přírůstkové zálohy) pouze nejnovější verzi rozdílové zálohy v řetězci všech následných přírůstkových záloh (pokud existují) mezi rozdílovou verzí zálohy a vybranou verzí přírůstkové zálohy.

### **Ověřený soubor**

Soubor ověřený pomocí řešení Acronis Notary. Soubor bude ověřen po jeho přidání do ověřené zálohy a odeslání jeho kódu hodnoty hash do databáze založené na technologii Blockchain.

### **Ověřování**

Proces „zapamatování“ stavu souboru a definování tohoto stavu jako pravého. Řešení Acronis Notary během ověřování vypočítá kód hodnoty hash na základě kódů hodnoty hash souborů vybraných k ověření a poté odešle kód hodnoty hash do databáze založené na technologii Blockchain.

## **P**

### **Plná verze zálohy**

Samostatná verze zálohy obsahující veškerá data vybraná k zálohování. Chcete-li obnovit data z plné verze zálohy, nepotřebujete přístup k žádné jiné verzi zálohy.

### **Plná záloha**

Zálohovací metoda, která uloží veškerá data vybraná k zálohování. Zálohovací proces, který vytvoří plnou verzi zálohy.

### **Podezřelý proces**

Acronis Active Protection využívá behaviorální heuristiku a analyzuje řetězce akcí provedené programem (procesem), které jsou následně porovnány s řetězcem událostí v databázi vzorů škodlivého chování. Pokud je chování programu podobné ransomwaru a pokouší se pozměnit soubory uživatele, je považován za podezřelý.

### **Přírůstková verze zálohy**

Verze zálohy, která ukládá změny dat vůči poslední verzi zálohy. Chcete-li obnovit data z přírůstkové verze zálohy, budete potřebovat přístup k dalším verzím stejné zálohy.

### **Přírůstková záloha**

Metoda zálohování používaná k ukládání změn dat, které se v záloze objevily od poslední verze zálohy (jakéhokoliv typu). Zálohovací proces, který vytvoří přírůstkovou verzi zálohy.

## **R**

### **Rozdílová verze zálohy**

Rozdílová verze zálohy ukládá změny dat, které se objevily od poslední plné verze zálohy. Chcete-li obnovit data z rozdílové verze zálohy, potřebujete přístup k příslušné plné verzi zálohy.

### **Rozdílová záloha**

Metoda zálohování používaná k ukládání změn dat, které se v záloze objevily od poslední plné



verze zálohy. Zálohovací proces, který vytvoří rozdílovou verzi zálohy.

## Ř

### **Řetězec verzí záloh**

Posloupnost alespoň dvou verzí záloh, která se skládá z první plné verze zálohy a následně jedné nebo více přírůstkových nebo rozdílových verzí záloh. Řetězec verzí záloh pokračuje až do další plné verze zálohy (pokud nějaká je).

## S

### **Spouštěcí média**

Fyzické médium (disk CD, DVD, USB disk nebo jiné médium podporované systémem BIOS jako spouštěcí zařízení) obsahující samostatnou verzi aplikace Acronis Cyber Protect Home Office. Spouštěcí médium se nejčastěji používá k obnově operačního systému, který nelze spustit, přístupu a zálohování dat, která zůstala zachována v poškozeném systému, nasazení operačního systému do zcela nového počítače, vytváření základních nebo dynamických svazků ve zcela novém počítači nebo zálohování disků s nepodporovaným systémem souborů sektor po sektoru.

### **Synchronizace**

Stejně jako synchronizace dat. Nastavení synchronizace, které bylo nakonfigurováno v počítači vlastníka synchronizace. Vytvořená synchronizace je spravována pomocí odpovídajícího okna synchronizace. Vytvoření synchronizace neznamena spuštění procesu synchronizace. Další uživatelé se mohou připojit k vytvořené synchronizaci.

### **Synchronizace dat**

Synchronizace dat je proces zachování stejných dat ve dvou nebo více synchronizovaných složkách. Tyto složky mohou být umístěny ve stejném počítači nebo v různých počítačích propojených místní sítí nebo přes internet. Když vytváříte, kopírujete, upravujete nebo odstraňujete soubory nebo podsložky v synchronizované složce, ty samé akce se automaticky provádí v dalších synchronizovaných složkách. To platí i opačně – všechny změny v dalších synchronizovaných složkách se provedou i ve vaší složce.

## V

### **Verze synchronizovaného souboru**

Stav souboru, který je umístěn v synchronizované složce po každé úpravě tohoto souboru. Verze souborů mohou být uloženy v úložišti Acronis Cloud.

### **Verze zálohy**

Výsledek jedné operace zálohování. Ve skutečnosti se jedná o soubor nebo sadu souborů, které obsahují kopii zálohovaných dat z určité doby. Verze záloh souborů vytvořené aplikací Acronis Cyber Protect Home Office mají příponu TIBX. Soubory TIBX vzniklé sloučením verzí záloh se také označují jako verze záloh.

## Z

### **Záloha disku (diskový obraz)**

Záloha obsahující kopii disku nebo diskového oddílu po sektorech v komprimované podobě. Ve většině případů jsou kopírovány pouze sektory, které obsahují data. nabízí možnost vytvořit přesný diskový obraz, tedy zkopírovat všechny sektory disku, a tím umožňuje tvorbu

diskového obrazu nepodporovaných systémů souborů.

### **Zálohování**

Platí to samé jako pro operaci zálohování. Sada verzí záloh vytvořená a spravovaná pomocí nastavení zálohování. Záloha může obsahovat více verzí záloh vytvořených pomocí plné a přírůstkové metody zálohování. Verze zálohy příslušící stejné záloze jsou obvykle ukládány ve stejném umístění.

# Rejstřík

## 1

1. Zálohování celého počítače „Dvě plné verze“ 69

## 2

2. Zálohování souborů „Denně přírůstková verze + týdně plná verze“ 69

## 3

3. Zálohování disku „Plná verze každé 2 měsíce + rozdílová verze dvakrát za měsíc“ 70

32bitové nebo 64bitové komponenty 80

## A

Acronis ASign 97

Acronis Cloud 18

Acronis DriveCleanser 220

Acronis Mobile 58

Acronis Secure Zone 210

Acronis Startup Recovery Manager 203

Acronis Universal Restore 115, 238

Acronis Vyčištění zóny Secure Zone 211

Active protection 160

Aktivace replikace 91

Aktivuje se Acronis Cyber Protect Home Office 16

Antivirové kontroly 164

Archivace dat 149, 151

Archivace v cloudu vs. online zálohování 150

Automatické čištění verzí replik 98

Automatické čištění verzí záloh 98

Automatické vyhledání ovladačů 242

## C

Centrum oznámení 50

Co dělat v případě, že aplikace Acronis Cyber Protect Home Office nerozezná váš disk SSD 187

Co dělat v případě, že předchozí pokyny nepomohly 188

Co je Acronis ASign? 97

Co je Acronis Cyber Protect Home Office? 10

Co je archivace dat? 149

Co je ochrana rodinných dat? 155

Co je rozhraní UEFI? 118

Co je to technologie Blockchain? 94

Co je vyloučeno z archivů? 150

Co je vyloučeno ze záloh disku? 38

Co lze a nelze synchronizovat 170

Co lze vyloučit a jak 73

Co obsahuje záloha disku nebo diskového oddílu? 38

Co se stane, když dojde k přerušení obnovy 135

## Č

Činnost zálohování a statistika 88

Čištění záloh, verzí záloh a replik 97

## D

Další informace 204

Další požadavky 12

- Datové centrum 152
- Datové úložiště Nonstop zálohování Acronis 46
- Definice algoritmu 222
- E**
- E-mailová oznámení 158
- E-mailové oznámení 71, 148
- F**
- Filtr míst v síti 232
- Funkce synchronizace 170
- H**
- Hledání obsahu zálohy 141
- C**
- Chráněné diskové oddíly 208
- I**
- Ikony synchronizace 171
- Import a export nastavení zálohování 237
- Informace ke zkušební verzi 18
- Informace o předplatném 34
- Instalace a odebrání aplikace Acronis Cyber Protect Home Office 15
- Integrace s Windows 50
- Integrovaný obchod 20
- Inteligentní hlášení chyb Acronis 246
- J**
- Jak aplikace Acronis Cyber Protect Home Office využívá technologii Blockchain 95
- Jak jej mám použít? 239
- Jak migrovat původní systém na větší pevný disk? 119
- Jak obnovit smazaný soubor 173
- Jak používat nástroj Acronis DriveCleanser 220
- Jak používat soubory VHD(X) 236
- Jak používat výchozí nastavení výjimek 73
- Jak připojit diskový obraz 235
- Jak režim Try&Decide funguje po restartování počítače 206
- Jak testovat obnovu a zkontrolovat ovladače a síťový adaptér 198
- Jak testovat spouštěcí média 197
- Jak to funguje 45, 134
- Jak vytvořit spouštěcí médium Acronis 23, 192
- Jak zajišťujeme bezpečnost vašich dat 34
- Jak zapnout rozhraní UEFI v systému BIOS? 118
- Jak získat přístup k záloze chráněné heslem 75
- Jak získat výpisy stavu systému 249
- Jaké položky lze obnovit? 142
- Jaký problém se tím vyřeší? 239
- Jazyk uživatelského rozhraní 21
- Jednorázové smazání 102
- Jmenovka diskového oddílu 219
- K**
- Karta Aktivita 88
- Karta Záloha 89
- Kde lze tyto aplikace najít? 58
- Kdy je režim Try&Decide užitečný 205
- Když jste připojeni k internetu 246
- Když nejste připojeni k internetu 246
- Klonování a migrace disku 175

Klonování disku 29

Klonování pevného disku 28

Konfigurace antivirových kontrol 165

Konfigurace služby Active Protection 162

Konfigurace výjimek z ochrany 168

Kontrola přístupu k ovladačům ve spouštěcím prostředí 242

Kontrola, že spouštěcí médium lze v případě potřeby použít 197

Kontrolní panel ochrany 159

Konvence pojmenování pro soubory zálohy vytvořené před aplikací Acronis True Image 2020 49

Konvence pojmenování pro soubory zálohy vytvořené v aplikaci Acronis True Image (2020 či 2021) a Acronis Cyber Protect Home Office 48

Které zálohy zachovávají formát TIB 11

Kterou metodu migrace použít 186

## M

Mechanismus úniku 233

Metoda trvalého odstranění dat 228

Metody trvalého odstranění dat z pevného disku 233

Metody trvalého odstranění informací používané programem Acronis 233

Migrace na disk SSD pomocí metody zálohy a obnovení 188

Migrace systému z pevného disku na disk SSD 186

Minimální systémové požadavky 12

Místní cíl pro mobilní zálohy 59

Možnosti a upozornění režimu Try&Decide 208

Možnosti archivace dat 152

Možnosti obnovy 143

Možnosti obnovy souborů 145

Možnosti ověření zálohy 78

Možnosti ověřování 145

Možnosti přepsání souborů 145

Možnosti vyčištění 228

Možnosti vyměnitelného média 79

Možnosti zálohování 60

## N

Nabídka Operace zálohování 86

Nabídka Start systému Windows 50

Náhled 232

Nastavení antiviru 165

Nastavení diskového oddílu 218

Nastavení doplňku Universal Restore 242

Nastavení napájení notebooku 85

Nastavení ověření 44

Nastavení Příkazy 231

Nastavení vyčištění 226

Nastavení zabezpečení zálohy na úrovni souborů 82

Nastavte ukládání verzí v online úložišti. 173

Nástroj pro klonování disku 175

Nástroje 190

Nástroje zajišťující bezpečnost a soukromí 220

Návrat k předchozí verzi souboru 173

Nejčastější dotazy týkající se zálohování, obnovy a klonování 52

Nonstop zálohování – nejčastěji kladené otázky 47

Nonstop zálohování Acronis 45

## O

Obecná omezení 18

Obecné 227

Obnova dat aplikace Office 365 142-143

Obnova dat pomocí aplikace Online kontrolní panel 157

Obnova disků z úložiště Cloud 134

Obnova dynamických svazků 129

Obnova dynamických/GPT disků a svazků 129

Obnova na úrovni souborů v Průzkumníku souborů 51

Obnova souborů 210

Obnova souborů a složek 139

Obnova systému z úložiště Acronis Cloud 135

Obnova základních svazků a disků 130

Obnovení dat 103

Obnovení disků a diskových oddílů 103, 116

Obnovení počítače 30

Obnovení systému na nový disk při použití spouštěcího média 108

Obnovení systému na stejný disk 104

Obnovení systému po havárii 103

Oč se jedná? 233

Odebrání dat zAcronis Cloud 100

Odeslání zpětné vazby společnosti Acronis 247

Odpojení diskového obrazu 236

Odstranění celé repliky zálohy 98

Odstranění celé zálohy 100

Odstranění celé zálohy a její repliky 98

Odstranění synchronizace 174

Odstranění verzí repliky zálohy v cloudu 101

Odstranění verzí zálohy v cloudu 100

Odstraňování problémů 45, 244

Odstraňuje se Acronis 215

Ochrana 159

Ochrana pomocí online zálohování 76

Ochrana pro aplikace Zoom, Cisco Webex a Microsoft Teams 168

Ochrana proti ransomwaru 160

Ochrana replikovaných dat 91

Ochrana rodinných dat 155

Ochrana systému 21

Ochrana v reálném čase 161

Ochrana zálohy 74

Ochrana zóny Acronis Secure Zone 214

Omezení a další informace 236

Omezení pro operace s dynamickými disky 15

Omezení při používání režimu Try&Decide 206

Omezení služby nonstop zálohování 45

Operace po odstranění dat 224

Operace se zálohami 86

Ověřená záloha 93

Ověřování pravosti souboru 95

Ověřování záloh 91

Oznamovací oblast 171

## P

Parametry denního zálohování 63

Parametry měsíčního zálohování 63

Parametry spuštění při události 63

Parametry spuštění spouštěcího média Acronis 193

Parametry týdenního zálohování 63  
 Písmeno diskového oddílu 219  
 Plánování 61  
 Plná metoda 39  
 Plné, přírůstkové a rozdílové zálohy 39  
 Po dokončení obnovy 115  
 Počítače 230  
 Podepisování souboru 97  
 Podporovaná úložná média 14  
 Podporované operační systémy 12  
 Podporované systémy souborů 13  
 Podporované typy připojení k internetu 14  
 Pojmenování souboru zálohy 11, 48  
 Pokročilá nastavení 62  
 Použití technologie univerzální obnovy  
     Acronis 242  
 Používání funkce Try&Decide 207  
 Používání technologie Blockchain 94  
 Práce se soubory VHD(X) 236  
 Práh volného místa na disku 71, 147  
 Pravidla zachování 46  
 Priorita operace 83, 146  
 Problém Příliš mnoho aktivací 17  
 Proces používání doplňku Universal  
     Restore 243  
 Proč replikovat? 90  
 Proč rozhraní UEFI? 118  
 Proč tuto funkci potřebuji? 28, 220  
 Proč zálohovat data aplikace Office 365? 59  
 Program údržby a podpory 20  
 Program zkušeností uživatelů Acronis 249  
 Prohlášení o autorských právech 9  
 Průběh vyčištění 233  
 Průvodce klonováním disku 175  
 Průvodci 51  
 Průzkumník souborů 171  
 Před spuštěním 29  
 Převod zálohy Acronis 237  
 Přidání existující zálohy do seznamu 92  
 Přidání nového pevného disku 215  
 Přidání nového zařízení do aplikace Online  
     kontrolní panel 155  
 Přidání ovladačů do stávající bitové kopie  
     WIM 195  
 Příkazy místní nabídky 50  
 Příkazy Před/Po pro obnovu 144  
 Příkazy Před/Po pro zálohování 76  
 Příklad obnovy systému UEFI 131  
 Příklad postupu obnovy 131  
 Příklady vlastních schémat 69  
 Připojení diskového obrazu 234  
 Připojení FTP 44  
 Příprava 242  
 Příprava na obnovu 103  
 Příprava nového disku k zálohování 43  
 Příprava ovladačů 242  
 Přírůstková metoda 40  
 Přístup k archivovaným souborům 153

## R

Replikace záloh do úložiště Acronis Cloud 90  
 Restartování počítače 145  
 Rezervní kopie zálohy 78

Režim obnovy disku 144  
Režim tvorby diskového obrazu 74  
Rozdělování záloh 77  
Rozdělování záloh za běhu 92  
Rozdíl mezi zálohami souborů a obrazy disků  
nebo diskových oddílů 37  
Rozdílová metoda 40  
Rozložení diskových oddílů 119  
Ruční čištění místních záloh má následující  
schéma 11  
Ruční ověření pravosti souboru 96  
Ruční rozdělení na diskové oddíly 177  
Ruční správa licencí předplatného 18  
Ruční zálohování a čištění verzí replik 99  
Rychlost průběhu obnovování 146  
Rychlost průběhu zálohování 83  
Rychlost přenosu síťového připojení 84

## Ř

Řešení nejčastějších potíží 244

## S

Sdílení dat 154  
Schéma jedné verze 65  
Schéma řetězce verzí 66  
Schémata zálohování 11, 64  
Síť Wi-Fi pro zálohování do úložiště Acronis  
Cloud 86  
Sledování změněných bloků (CBT) 42  
Snímek zálohy 84  
Soubory 228  
Soukromí v síti 210

Specifické možnosti smazání stop 228  
Správa souborů v karanténě 167  
Správa vlastních schémat zálohování 68  
Správa zjištěných problémů 167  
Stahování aktualizací ochrany 169  
Styl diskového oddílu po obnovení 130  
Synchronizace 18  
Synchronizace dat 170  
Systém souborů 219  
Systém spouštěný ze systému BIOS, GPT, bez  
Windows 126, 183  
Systém spouštěný ze systému BIOS, GPT,  
podpora systému UEFI 126, 182  
Systém spouštěný ze systému BIOS, záznam  
MBR, bez operačního systému  
Windows 125, 181  
Systém spouštěný ze systému BIOS, záznam  
MBR, systém UEFI je podporován 124,  
181  
Systém spouštěný ze systému BIOS, záznam  
MBR, systém UEFI není podporován 124,  
180  
Systém spouštěný ze systému UEFI, GPT, bez  
Windows 129, 186  
Systém spouštěný ze systému UEFI, GPT,  
systém UEFI je podporován 129, 185  
Systém spouštěný ze systému UEFI, záznam  
MBR, bez Windows 128, 184  
Systém spouštěný ze systému UEFI, záznam  
MBR, systém UEFI je podporován 127,  
184  
Systém spouštěný ze systému UEFI, záznam  
MBR, systém UEFI není podporován 127,  
183  
Systémová zpráva Acronis 244



Systémové požadavky a podporovaná média 12

## Š

Šifrování 152

## T

Tabulka 1. Cílový disk je větší než 2 TB 120

Tabulka 2. Cílový disk je menší než 2 TB 122

Technická podpora 20

Technologie patentované společností Acronis 9

Tlačítko Acronis Cyber Protect Home Office na panelu úloh 50

Try&Decide 205

typické případy použití 209

Třídění záloh v seznamu 90

Tvorba diskových oddílů 217

Tvorba vlastních algoritmů 222

Tvůrce médií Acronis 190

Typ oddílu (tato nastavení jsou dostupná pouze pro disky MBR) 219

Typy dat 170

Typy úložišť 170

## U

Účet Acronis 32

Uložení algoritmu souboru 224

Úložiště pro virtuální změny 209

Umístění zóny Acronis Secure Zone 212

Unified Extensible Firmware Interface (UEFI) 118

Upgrade aplikace Acronis Cyber Protect Home Office 19

Upozornění 209

Upozornění na operace obnovení 147

Upozornění na operace zálohování 71

Úprava uživatelských příkazů pro obnovení 144

Úprava uživatelských příkazů pro zálohování 76

Určování příčin havárie 103

Úroveň komprese 83

Uspořádání pořadí spouštění v systému BIOS a UEFI BIOS 133

Úvod 10

Uvolnění místa v Acronis Cloud 99

## V

V každém případě instalovat ovladače velkokapacitních zařízení 242

Velikost 218

Velikost Acronis Secure Zone 213

Velikost SSD 186

Vlastní schémata 67

Vlastnosti diskového oddílu 117

Volné místo na disku 230

Výběr algoritmu 222

Výběr datového centra pro zálohu 85

Výběr grafického režimu při spouštění ze spouštěcího média 201

Výběr metody inicializace 216

Výběr místa k ukládání záloh 42

Výběr pevného disku 215

Výběr zdroje 221

Vyčištění systému 225

Vyčištění záloh formátu TIBX 11  
Vyhodnocení bezpečnostních rizik 166  
Výchozí možnosti vyčištění 227  
Vyloučení položek z klonování 178  
Vyloučení položek ze zálohy 72  
Vypnutí počítače 82  
Vytváření a řízení Acronis Secure Zone 211  
Vytváření média Acronis Universal Boot 239  
Vytvoření sady Acronis Survival Kit 25  
Vytvoření souboru ISO ze souboru WIM 196  
Vytvoření synchronizace 172  
Vyzkoušení softwaru 209  
Vzdálené úložiště 33  
Vzdálené zálohování dat 156

## **W**

Webová aplikace 34  
Webové filtrování 162

## **Z**

Začínáme 21  
Začínáme s úložištěm Acronis Cloud 33  
Základní pojmy 36  
Zakoupení plné verze 19  
Zálohování dat 54  
Zálohování dat aplikace Office 365 59  
Zálohování diskových oddílů a disků 54  
Zálohování do různých umístění 92  
Zálohování mobilních zařízení 57  
Zálohování souborů 27  
Zálohování souborů a složek 55

Zálohování všech dat v počítači 24

Zálohuje se počítač 21

Zálohy vytvořené v aplikaci Acronis True Image (2020 či 2021) a Acronis Cyber Protect Home Office 10

Zpracování chyb 80

Zpracování chyb při zálohování a replikaci do cloudu 81

Způsob migrace 123, 180